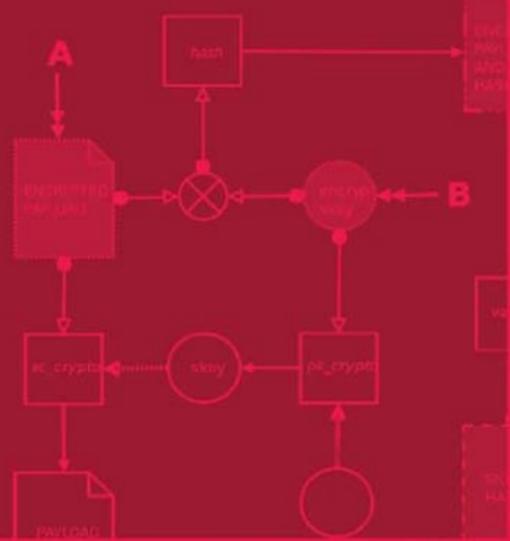


Tarek Sobh
Khaled Elleithy
Ausif Mahmood
Mohamed Karim
Editors



Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications



Springer

Innovative Algorithms and Techniques in Automation,
Industrial Electronics and Telecommunications

Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications

Edited by

Tarek Sobh

*University of Bridgeport
CT, USA*

Khaled Elleithy

*University of Bridgeport
CT, USA*

Ausif Mahmood

*University of Bridgeport
CT, USA*

and

Mohammed Karim

*Old Dominion University
VA, USA*

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN 978-1-4020-6265-0 (HB)
ISBN 978-1-4020-6266-7 (e-book)

Published by Springer,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

www.springer.com

Printed on acid-free paper

All Rights Reserved
© 2007 Springer

No part of this work may be reproduced, stored in a retrieval system, or transmitted
in any form or by any means, electronic, mechanical, photocopying, microfilming, recording
or otherwise, without written permission from the Publisher, with the exception
of any material supplied specifically for the purpose of being entered
and executed on a computer system, for exclusive use by the purchaser of the work.

Table of Contents

Preface	xiii
Acknowledgements	xv
1. A Hybrid Predistorter for Nonlinearly Amplified MQAM Signals <i>Nibaldo Rodríguez A.</i>	1
2. Safe Logon with Free Lightweight Technologies <i>S. Encheva and S. Tumin</i>	5
3. Stochastic Communication in Application Specific Networks-on-Chip <i>Vivek Kumar Sehgal and Nitin</i>	11
4. A Random Approach to Study the Stability of Fuzzy Logic Networks <i>Yingjun Cao, Lingchu Yu, Alade Tokuta and Paul P. Wang</i>	17
5. Extending Ad Hoc Network Range using CSMA(CD) Parameter Optimization <i>Adeel Akram, Shahbaz Pervez, Shoab A. Khan</i>	23
6. Resource Aware Media Framework for Mobile Ad Hoc Networks <i>Adeel Akram, Shahbaz Pervez, Shoab A. Khan</i>	27
7. Cross-Layer Scheduling of QoS-Aware Multiservice Users in OFDM-Based Wireless Networks <i>Amoakoh Gyasi-Agyei</i>	31
8. Development of a Joystick-based Control for a Differential Drive Robot <i>A. N. Chand and G. C. Onwubolu</i>	37
9. Structure and Analysis of a Snake-like Robot <i>Anjali V. Kulkarni and Ravdeep Chawla</i>	43
10. A Novel Online Technique to Characterize and Mitigate DoS Attacks using EPSD and Honeybots <i>Anjali Sardana, Bhavana Gandhi and Ramesh Joshi</i>	49
11. Multi-Scale Modelling of VoIP Traffic by MMPP <i>Arkadiusz Biernacki</i>	55
12. Transparent Multihoming Protocol Extension for MIPv6 with Dynamic Traffic Distribution across Multiple Interfaces <i>Basav Roychoudhury and Dilip K Saikia</i>	61
13. The Wave Variables, A Solution for Stable Haptic Feedback in Molecular Docking Simulations <i>B. Daunay, A. Abbaci, A. Micelli, S. Regnier</i>	67
14. A Model for Resonant Tunneling Bipolar Transistors <i>Buket D. Barkana and Hasan H. Erkaya</i>	75

15.	Developing secure Web-applications – Security Criteria for the Development of e-Democracy Webapplications <i>António Pacheco and Carlos Serrão</i>	79
16.	Data Acquisition and Processing for Determination of Vibration state of Solid Structures – Mechanical press PMCR 63 <i>Cătălin Iancu</i>	85
17.	Quality of Uni- and Multicast Services in a Middleware. LabMap Study Case <i>Cecil Bruce-Boye and Dmitry A. Kazakov</i>	89
18.	Traffic Flow Analysis Over a IPv6 Hybrid Manet <i>Christian Lazo R, Roland Glöckler, Sandra Céspedes U and Manuel Fernández V</i>	95
19.	Designing Aspects of a Special Class of Reconfigurable Parallel Robots <i>Cornel Brisian</i>	101
20.	Performance Analysis of Blocking Banyan Switches <i>D. C. Vasiliadis, G. E. Rizos and C. Vassilakis</i>	107
21.	Demystifying the Dynamics of Linear Array Sensor Imagery <i>Koduri Srinivas</i>	113
22.	On the Robustness of Integral Time Delay Systems with PD Controllers <i>Eduardo Zuñiga, Omar Santos and M.A. Paz Ramos</i>	119
23.	Improvement of the Segmentation in HS Sub-space by means of a Linear Transformation in RGB Space <i>E. Blanco, M. Mazo, L.M. Bergasa, S. Palazuelos and A.B. Awawdeh</i>	125
24.	Obstruction Removal Using Feature Extraction Through Time for Videoconferencing Processing <i>Elliott Coleshill and Deborah Stacey</i>	131
25.	Blade Design and Forming for Fans Using Finite Elements <i>F. D. Foroni, L. A. Moreira Filho and M. A. Menezes</i>	135
26.	On the Application of Cumulant-based Cyclostationary Processing on Bearings Diagnosis <i>F. E. Hernández, Vicente Atxa, E. Palomino and J. Altuna</i>	141
27.	Application of Higher-order Statistics on Rolling Element Bearings Diagnosis <i>F. E. Hernández, O. Caveda, V. Atxa and J. Altuna</i>	145
28.	Extending RSVP-TE to Support Guarantee of Service in MPLS <i>Francisco Javier Rodriguez-Perez and Jose Luis Gonzalez-Sanchez</i>	149
29.	Operators Preserving Products of Hurwitz Polynomials and Passivity <i>Guillermo Fernández-Anaya and José-Job Flores-Godoy</i>	155

30.	A Computer Aided Tool Dedicated to Specification and Verification of the MoC and the MoF <i>N. Hamani, N. Dangoumau and E. Craye</i>	159
31.	Directionality Based Preventive Protocol for Mobile Ad Hoc Networks <i>Hetal Jasani, Yu Cai and Kang Yen</i>	165
32.	The Problem of Accurate Time Measurement in Researching Self-Similar Nature of Network Traffic. <i>I. V. Sychev</i>	171
33.	Wi-Fi as a Last Mile Access Technology and The Tragedy of the Commons <i>Ingrid Brandt, Alfredo Terzoli, Cheryl Hodgkinson-Williams</i>	175
34.	Study of Surfaces Generated by Abrasive Waterjet Technology <i>J. Valíček, S. Hloch, M. Držík, M. Ohlídal, V. Mádr, M. Lupták, S. Fabian, A. Radvanská and K. Páleníková</i>	181
35.	On Length-Preserving Symmetric Cryptography <i>Zheng Jianwu, Liu Hui, and Liu Mingsheng</i>	187
36.	Revocable Proxy Signature Scheme with Efficient Multiple Delegations to the Same Proxy Signer <i>Ji-Seon Lee, Jik Hyun Chang</i>	193
37.	A Robust Method for Registration of Partially-Overlapped Range Images Using Genetic Algorithms <i>J. W. Branch, F. Prieto and P. Boulanger</i>	199
38.	Lips Movement Segmentation and Features Extraction in Real Time <i>Juan Bernardo Gómez, Flavio Prieto and Tanneguy Redarce</i>	205
39.	Droplet Acceleration In The Arc <i>J. Hu and H.L. Tsai</i>	211
40.	A Comparison of Methods for Estimating the Tail Index of Heavy-tailed Internet Traffic <i>Karim Mohammed Rezaul and Vic Grout</i>	219
41.	IEC61499 Execution Model Semantics <i>Kleanthis Thramboulidis, George Doukas</i>	223
42.	Towards a Practical Differential Image Processing Approach of Change Detection <i>KP Lam</i>	229
43.	An ISP level Distributed Approach to Detect DDoS Attacks <i>Krishan Kumar, R C Joshi, and Kuldip Singh</i>	235
44.	Performance Enhancement of Blowfish Algorithm by Modifying its Function <i>Krishnamurthy G.N, Ramaswamy V and Leela G.H</i>	241

45.	A Clustering Algorithm Based on Geographical Sensor Position in Wireless Sensor Networks <i>Kyungjun Kim</i>	245
46.	The Economic Evaluation of the Active DSRC Application for Electronic Toll Collection System in KOREA <i>Gunyoung Kim and Kyungwoo Kang</i>	251
47.	Adaptive Control of Milling Forces under Fractional Order Holds. <i>L. Rubio and M. de la Sen</i>	257
48.	Application of Genetic Algorithms to a Manufacturing Industry Scheduling Multi-Agent System <i>María de los Ángeles Solari and Ernesto Ocampo</i>	263
49.	Pre- and Post- Processing for Enhancement of Image Compression Based on Spectrum Pyramid <i>Mariofanna Milanova, Roumen Kountchev, Vladimir Todorov and Roumiana Kountcheva</i>	269
50.	The Use of Maple in Computation of Generalized Transfer Functions for Nonlinear Systems <i>M. Ondera</i>	275
51.	A Game Theoretic Approach to Regulating Mutual Repairing in a Self-Repairing Network <i>Masakazu Oohashi and Yoshiteru Ishida</i>	281
52.	An Automated Self-Configuring Driver System for IEEE 802.11b/g WLAN Standards <i>Mathieu K. Kourouma and Ebrahim Khosravi</i>	287
53.	Development of a Virtual Force-Reflecting Scara Robot for Teleoperation <i>Mehmet Ismet Can Dede and Sabri Tosunoglu</i>	293
54.	Improving HORSE Again and Authenticating MAODV <i>Mingxi Yang, Layuan Li and Yiwei Fang</i>	299
55.	Curvelet Transform Based Logo Watermarking <i>Thai Duy Hien, Kazuyoshi Miyara, Yasunori Nagata, Zensho Nakao and Yen Wei Chen</i>	305
56.	Fairness Enhancement of IEEE 802.11 Ad Hoc Mode Using Rescue Frames <i>Mohamed Youssef, Eric Thibodeau and Alain C. Houle</i>	311
57.	Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective <i>Mohammad Momani, Subhash Challa and Khalid Aboura</i>	317
58.	Performability Estimation of Network Services in the Presence of Component Failures <i>Mohammad-Mahdi Bidmeshki, Mostafa Shaad Zolpirani and Seyed Ghasssem Miremadi</i>	323
59.	RBAC Model for SCADA <i>Munir Majdalawieh, Francesco Parisi-Presicce and Ravi Sandhu</i>	329

60.	DNPSec Simulation Study <i>Munir Majdalawieh and Duminda Wijesekera</i>	337
61.	A Client-Server Software that Violates Security Rules Defined by Firewalls and Proxies <i>Othon M. N. Batista, Marco A. C. Simões, Helder G. Aragão, Cláudio M. N. G. da Silva and Israel N. Boudoux</i>	343
62.	Mobile Communication in Real Time for the First Time. User Evaluation of Non-voice Terminal Equipment for People with Hearing and Speech Disabilities <i>Patricia Gillard, Gunela Astbrink and Judy Bailey</i>	347
63.	Analyzing the Key Distribution from Security Attacks in Wireless Sensor <i>Piya Techateerawat and Andrew Jennings</i>	353
64.	Hint Key Distribution for Sensor Networks <i>Piya Techateerawat and Andrew Jennings</i>	359
65.	A Model for GSM Mobile Network Design <i>Plácido Rogério Pinheiro and Alexei Barbosa de Aguiar</i>	365
66.	Application of LFSR with NTRU Algorithm <i>P.R. Suri and Priti Puri</i>	369
67.	Adaptive Packet Loss Concealment Mechanism for Wireless Voice Over Ip <i>M. Razvi Doomun</i>	375
68.	Dynamic Location Privacy Mechanism in Location-Aware System <i>M. Razvi Doomun</i>	379
69.	Video Transmission Performance Using Bluetooth Technology <i>M. Razvi Doomun</i>	385
70.	Kelvin Effect, Mean Curvatures and Load Impedance in Surface Induction Hardening: An Analytical Approach including Magnetic Losses <i>Roberto Suárez-Ántola</i>	389
71.	A Simple Speed Feedback System for Low Speed DC Motor Control in Robotic Applications <i>R. V. Sharan, G. C. Onwubolu, R. Singh, H. Reddy, and S. Kumar</i>	397
72.	A Low Power CMOS Circuit for Generating Gaussian Pulse and its Derivatives for High Frequency Applications <i>Sabrieh Choobkar and Abdolreza Nabavi</i>	401
73.	On the Efficiency and Fairness of Congestion Control Algorithms <i>Sachin Kumar, M. K. Gupta, V. S. P. Srivastav and Kadambri Agarwal</i>	405
74.	Hopfield Neural Network as a Channel Allocator <i>Ahmed Emam and Sarhan M. Musa</i>	409

75.	Command Charging Circuit with Energy Recovery for Pulsed Power Supply of Copper Vapor Laser <i>Satish Kumar Singh, Shishir Kumar and S. V. Nakhe</i>	413
76.	Performance Evaluation of MANET Routing Protocols Using Scenario Based Mobility Models <i>Shams-ul-Arfeen, A. W. Kazi, Jan M. Memon and S. Irfan Hyder</i>	419
77.	Analysis of Small World Phenomena and Group Mobility in Ad Hoc Networks <i>Sonja Filiposka, Dimitar Trajanov and Aksenti Grnarov</i>	425
78.	Handoff Management Schemes for HCN/WLAN Interworking <i>Srinivas Manepalli and Alex A. Aravind</i>	431
79.	Cross-Layer Fast and Seamless Handoff Scheme for 3GPP-WLAN Interworking <i>SungMin Yoon, SuJung Yu and JooSeok Song</i>	437
80.	Minimizing the Null Message Exchange in Conservative Distributed Simulation <i>Syed S. Rizvi, K. M. Elleithy and Aasia Riasat</i>	443
81.	An Analog Computer to Solve any Second Order Linear Differential Equation with Arbitrary Coefficients <i>T. ElAli, S. Jones, F. Arammash, C. Eason, A. Sopeju, A. Fapohunda and O. Olorode</i>	449
82.	QoS Provisioning in WCDMA 3G Networks using Mobility Prediction <i>T. Rachidi, M. Benkirane, and H. Bouzekri</i>	453
83.	Patent-Free Authenticated-Encryption as Fast as OCB <i>Ted Krovetz</i>	459
84.	Application of Least Squares Support Vector Machines in Modeling of the Top-oil Temperature <i>T. C. B. N. Assunção, J. L. Silvino and P. Resende</i>	463
85.	Optimal Routing with Qos Guarantees in the Wireless Networks <i>P. Venkata Krishna and N.Ch. S. N. Iyengar</i>	469
86.	RFID in Automotive Supply Chain Processes - There is a Case <i>Viacheslav Moskvich and Vladimir Modrak</i>	475
87.	Reduced – Order Controller Design in Discrete Time Domain <i>Vivek Kumar Sehgal</i>	481
88.	Simple Intrusion Detection in an 802.15.4 Sensor Cluster <i>Vojislav B. Mišić and Jobaida Begum</i>	487
89.	Dim Target Detection in Infrared Image Sequences Using Accumulated Information <i>Wei He and Li Zhang</i>	493

90.	Cooperative Diversity Based on LDPC Code <i>Weijia Lei, Xianzhong Xie and Guangjun Li</i>	497
91.	MEMS Yield Simulation with Monte Carlo Method <i>Xingguo Xiong, Yu-Liang Wu and Wen-Ben Jone</i>	501
92.	A Human Interface Tool for System Modeling and Application Development Based on Multilevel Flow Models <i>Yangping Zhou, Yujie Dong, Yuanle Ma and Hidekazu Yoshikawa</i>	505
93.	Genetic Algorithm Approach in Adaptive Resource Allocation in OFDM Systems <i>Y. B. Reddy</i>	511
94.	Real-time Vehicle Detection with the Same Algorithm both Day and Night Using the Shadows Underneath Vehicles <i>Yoichiro Iwasaki and Hisato Itoyama</i>	517
95.	An Authentication Protocol to Address the Problem of the Trusted 3rd Party Authentication Protocols <i>Y. Kirsal and O. Gemikonakli</i>	523
96.	Autonomous Agents based Dynamic Distributed (A2D2) Intrusion Detection System <i>Yu Cai and Hetal Jasani</i>	527
97.	Modeling and Implementation of Agent-Based Discrete Industrial Automation <i>Yuval Cohen, Ming-En Wang and Bopaya Bidanda</i>	535
98.	Performance of CBR and TCP Traffics in Various MANET Environments <i>Z. M. Yusof, J.A. Flint and S. Datta</i>	541
	Index	547

Preface

This book includes the proceedings of the 2006 International Conference on Telecommunications and Networking (TeNe) and the 2006 International Conference on Industrial Electronics, Technology & Automation (IETA).

TeNe 06 and IETA 06 are part of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 06). The proceedings are a set of rigorously reviewed world-class manuscripts presenting the state of international practice in Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications.

TeNe 06 and IETA 06 are high-caliber research conferences that were conducted online. CISSE 06 received 690 paper submissions and the final program included 370 accepted papers from more than 70 countries, representing the six continents. Each paper received at least two reviews, and authors were required to address review comments prior to presentation and publication.

Conducting TeNe 06 and IETA 06 online presented a number of unique advantages, as follows:

- All communications between the authors, reviewers, and conference organizing committee were done on line, which permitted a short six week period from the paper submission deadline to the beginning of the conference.
- PowerPoint presentations, final paper manuscripts were available to registrants for three weeks prior to the start of the conference
- The conference platform allowed live presentations by several presenters from different locations, with the audio and PowerPoint transmitted to attendees throughout the internet, even on dial up connections. Attendees were able to ask both audio and written questions in a chat room format, and presenters could mark up their slides as they deem fit
- The live audio presentations were also recorded and distributed to participants along with the power points presentations and paper manuscripts within the conference DVD.

The conference organizers are confident that you will find the papers included in this volume interesting and useful.

Tarek M. Sobh, Ph.D., PE

Khaled Elleithy, Ph.D.

Ausif Mahmood, Ph.D.

Mohammed Karim, Ph.D.

Bridgeport, Connecticut

June 2007

Acknowledgements

The 2006 International Conferences on Telecommunications and Networking (TeNe) and Industrial Electronics, Technology & Automation (IETA) and the resulting proceedings could not have been organized without the assistance of a large number of individuals. TeNe and IETA are part of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE). CISSE was founded by Professors Tarek Sobh and Khaled Elleithy in 2005, and they set up mechanisms that put it into action. Andrew Rosca wrote the software that allowed conference management, and interaction between the authors and reviewers online. Mr. Tudor Rosca managed the online conference presentation system and was instrumental in ensuring that the event met the highest professional standards. We also want to acknowledge the roles played by Sarosh Patel and Ms. Susan Kristie, our technical and administrative support team.

The technical co-sponsorship provided by the Institute of Electrical and Electronics Engineers (IEEE) and the University of Bridgeport is gratefully appreciated. We would like to express our thanks to Prof. Toshio Fukuda, Chair of the International Advisory Committee and the members of the TeNe and IETA Technical Program Committees including: Abdelshakour Abuzneid, Nirwan Ansari, Hesham El-Sayed, Hakan Ferhatosmanoglu, Ahmed Hambaba, Abdelsalam Helal, Gonhsin Liu, Torleiv Maseng, Anatoly Sachenko, Paul P. Wang, Habib Youssef, Amr El Abbadi, Giua Alessandro, Essam Badreddin, John Billingsley, Angela Di Febbraro, Aydan Erkmen, Navarun Gupta, Junling (Joyce) Hu, Mohamed Kamel, Heba A. Hassan, Heikki N. Koivo, Lawrence Hmurgcik, Luu Pham, Saeid Nahavandi, ElSayed Orady, Angel Pobil, Anatoly Sachenko, Sadiq M. Sait, Nariman Sepehri, Bruno Siciliano and Keya Sadeghipour.

The excellent contributions of the authors made this world-class document possible. Each paper received two to four reviews. The reviewers worked tirelessly under a tight schedule and their important work is gratefully appreciated. In particular, we want to acknowledge the contributions of the following individuals: Farid Ahmed, ElSayed Orady, Mariofanna Milanova, Taan Elali, Tarek Taha, Yoichiro Iwasaki, Vijayan Asari, Bruno Siciliano, Navarun Gupta, Mohamed Kamel, Giua Alessandro, Hairong Qi, Abdul Awwal, Seddik Djouadi, Ram Reddy, Anatoly Sachenko, Leon Tolbert, Shuqun Zhang, Mohammad Kaykobad, Vojislav Misic, Sudhir Veerannagari, Osman Tokhi, Mahmoud Mahmoud, Min Song, Mohammad Yeasin, John Billingsley, Alamgir Hossain, Ferdous Alam, Elissa Seidman, Tyler Ross, Fangxing Li, Selim Akl, Anish Anthony, Syed Sajjad Rizvi, Sarhan Musa, Srinivas Manepalli, Hossam Diab, Abdelshakour Abuzneid, Hikmat Farhat, Tingting Meng, Torleiv Maseng, Yenumula Reddy, Zulkefli Yusof, Vojislav

Misic, Hetal Jasani, Hesham El-Sayed, Yu Cai, Casimer DeCusatis, Tyler Ross, Abdelsalam Helal, Muhammad Azizur Rahman, Patricia Gillard, Paul Wang, Mohamed Youssef, Sanjiv Rai, Nirwan Ansari, Munir Majdalawieh, Gonhsin Liu, Ahmed Hambaba, AmirAbdessemed, Kaitung Au, Navarun Gupta, Ram Reddy and Sudhir Veerannagari.

Tarek Sobh, Ph.D., P.E.
Khaled Elleithy, Ph.D.
Ausif Mahmood, Ph.D.
Mohammed Karim, Ph.D.
Bridgeport, Connecticut
June 2007

A Hybrid Predistorter for Nonlinearly Amplified MQAM Signals

Nibaldo Rodríguez A.

University Catholic of Valparaíso of Chile,
Av. Brasil, 2241 nibaldo.rodriguez@ucv.cl

Abstract – This paper proposes an adaptive baseband Predistortion scheme in order to reduce both nonlinear amplitude and phase distortion introduced by a travelling wave tube amplifier (TWTA) over transmitted 16QAM and 256QAM signals. This compensator is based on a radial basis function neural network (RBF NN) and its coefficients are estimated by using a hybrid algorithm, namely generalised inverse and gradient descent. Computer simulation results confirm that once the 16QAM and 256QAM signals are predistorted and amplified at an input back off level of 0 dB, there is a reduction of 25 dB and 29 dB spectrum regrowth; respectively. In addition proposed adaptive Predistortion scheme has a low complexity and fast convergence.

Index Terms – Predistortion, neural network and multilevel quadratura amplitude modulation.

I. INTRODUCTION

Due to their high spectral and power efficiency, multilevel quadrature amplitude modulation (MQAM) is a technique widely used in commercial communications systems, such as digital video broadcasting satellite and terrestrial standards [1,2]. However, MQAM shows a great sensibility to the non-linear distortion introduced by the travelling wave tube amplifier (TWTA), due to fluctuations of its non-constant envelope. Typically, a TWTA is modulated by non-lineal amplitude modulation to amplitude modulation (AM-AM) and phase to modulation (AM-PM) functions in either polar or quadrature form [3]. To reduce both AM-AM and AM-PM distortions, it is necessary to operate the TWTA with a large power back off level, but these operations reduce the TWTA's output power. During the last year, other solutions have been proposed to reduce both AM-AM and AM-PM distortion by using Predistortion (PD) based on polynomial model [4-7], Volterra serie [8-10] and neural network [11-16]. This paper only deals with the neural network model, due to its capacity of approximating to different non-lineal functions. The predistorters have been reported in references [11-16] to use two neural networks for compensating both nonlinear amplitude and phase distortion. The disadvantage of these neural network predistortion techniques is their slow convergence speed, due to the classical back-propagation algorithm, and also to the ignorance of the early data. However, our predistortion scheme only uses one radial basis function neural network for compensating both nonlinear AM-AM and AM-PM distortions introduced by TWTA, which permits to reduce computer storage requirements, and to increase the predistorer coefficients adaptation speed.

The aim of the proposed radial basis function neural network predistorter is to reduce both nonlinear amplitude and phase distortion introduced by TWTA over transmitted 16QAM and 256QAM signals. The predistorter structure is based on a radial basis function neural network and its coefficients are found by using a hybrid algorithm, which combined gradient-descent method with Moore-Penrose

generalized inverse [17].

The remainder of this paper is organized as follows: In section II, it is presented a systems description of the proposed scheme. The linearisation technique of the TWTA, and hybrid learning algorithm for adjusting the neuronal predistorter coefficients are presented in Section III. The performance curves of the spectrum regrowth and signal constellation warping effect of the 16QAM and 256QAM signals are discussed in Section IV. Finally, the conclusions are presented in the last section.

II. SYSTEM DESCRIPTION

The input data bits are encoded by using the M-QAM mapper device, which maps a k -tuple of bits over MQAM ($M=2^k$) symbols by using Gray coding. The transmitter filter is implemented as a square root raised cosine (SRRC) pulse shaping distributed at the transmitter and receiver with L -taps, roll-off parameter β and over-sample factor of 8 samples per symbol. The modulated baseband signal $x(t)$ is first pre-distorted and nonlinearly amplified, then propagated over an additive white Gaussian noise (AWGN) channel. The signal amplified is represented by:

$$z(t) = A(|y(t)|) \exp[j \cdot \angle y(t) + \Phi(|y(t)|)] \quad (1)$$

where $|y(t)|$ and $\angle y(t)$ are the amplitude and phase of the predistorted complex signal $y(t)$. The function $A(\cdot)$ and $\Phi(\cdot)$ denote AM-AM conversion (nonlinear amplitude) and AM-PM conversion (nonlinear phase); respectively. For a TWTA, the expressions for $A(\cdot)$ and $\Phi(\cdot)$ are given by [3] as:

$$A(|y(t)|) = \frac{\alpha_A |y(t)|}{1 + \beta_A |y(t)|^2} \quad (2)$$

$$\Phi(|y(t)|) = \frac{\alpha_\phi |y(t)|^2}{1 + \beta_\phi |y(t)|^2} \quad (3)$$

with $\alpha_A = 2$, $\beta_A = 1$, $\alpha_\phi = \pi/3$ and $\beta_\phi = 1$.

The nonlinear distortion of a high power amplifier depends on the back off. The input back off (IBO) power is defined as the ratio of the saturation input power, where the output power begins to saturate, to the average input power:

$$IBO = 10 \log_{10} \left(\frac{P_{i,sat}}{P_{i,avg}} \right) \quad (4)$$

where $P_{i,sat}$ is the saturation input power and $P_{i,avg}$ is the average power at the input of the TWTA.

At time t , the received signal $r(t)$ is defined by

$$r(t) = z(t) + n(t) \quad (5)$$

where $n(t)$ represent the complex AWGN with two-sided spectral density $N_0/2$.

The received signal $r(t)$ is passed through the matched filter (SRRC), and then sampled at the symbol rate $1/T$. The sequence at the output of the sampler p_k is fed to the MQAM Demapper. The Demapper splits the complex symbols into quadrature and in-phase components, and puts them into a decision device, where they are demodulated independently against their respective decision boundaries. Finally, output bits stream \hat{d}_k are estimated.

III. HYBRID PREDISTORTION ALGORITHM

Consider the input signal $x(t)$ with polar representation given by:

$$x(t) = r_x(t) \exp[j\theta_x(t)] \quad (6)$$

where r_x and θ_x represent the modulated envelope and the phase; respectively.

The output of the PD is then given by:

$$y(t) = M[r_x(t)] \exp[j\{\theta_x(t) + N(r_x(t))\}] \quad (7)$$

Now, using equation (1) and equation (7) we obtain complex signal envelope at the TWTA output as:

$$z(t) = A[M(r_x(t))] \exp[j\{\theta_x(t) + N(r_x(t)) + \Phi[M(r_x(t))]\}] \quad (8)$$

In order to achieve the ideal predistortion function, the signal $z(t)$ will be equivalent to the input signal $x(t)$. That is:

$$M[r_x(t)] = A^{-1}[r_x(t)] \quad (9)$$

where $A(\cdot)^{-1}$ represents inverse amplitude function of the TWTA and:

$$N[r_x(t)] = -\Phi[A^{-1}(r_x(t))] \quad (10)$$

where $N(\cdot)$ represents inverse phase function of the TWTA.

Therefore, ideal predistorted output $y(t)$ is obtained as:

$$y(t) = A^{-1}[r_x(t)] \exp[j\{\theta_x(t) - \Phi(A^{-1}[r_x(t)])\}] \quad (11)$$

Finally, in order to achieve the ideal predistortion function $f_{PD}(\cdot) = y(t)$, it is only necessary to find the real-valued function $A^{-1}(\cdot)$. To approximate the function $A^{-1}(\cdot)$, a radial basis function neural network is used and the weights are determined from a finite number of samples of the function $A(\cdot)$.

During the training process, the signal $x(t)$ is equal to the signal $y(t)$, but during decision-direct mode the signal $y(t)$ will be the desired predistorted signal. The training process was done by using the trial and error method. In order to implement the training process, it is necessary to obtain a database Γ containing the output amplitude $r_z(n)$ of the TWTA, and the corresponding desired output

$r_x(n)$, $\Gamma = \{r_z(n), r_x(n); n = 1, \dots, N_s\}$, where the N_s value represents the sample number of the function $A(\cdot)$, and the desired output r_x is obtained as:

$$r_x(n) = \frac{|x(n)|}{\max\{|x(n)|\}} \cdot IBO \quad (12)$$

The output of the PD is obtained as:

$$\begin{aligned} \hat{y}_k &= \sum_{j=0}^{N_c} w_j H_{jk}, \quad k = 1, 2, \dots, N_s \\ H_{jk} &= \Psi(u), \quad H_{0k} = 1 \\ u &= \| |z_k| - c_j \|^2 \\ \Psi(u) &= u + 1 \end{aligned} \quad (13)$$

where the N_c value represents the number of centre in the hidden layer. The weights $\{w_j, c_j\}$ represent the interconnections of the hidden and output layer, respectively, and $\Psi(\cdot)$ denoted the non-linear activation function of the hidden centres.

The goal of the learning algorithm is to find the weights vector that minimizes the cost function defined by:

$$\begin{aligned} E[r_z(n), c, w] &= \frac{1}{N_s} \sum_{n=1}^{N_s} e^2(n) \\ &= \frac{1}{N_s} \sum_{n=1}^{N_s} [Gr_x(n) - \hat{y}(r_z(n), c, w)]^2 \end{aligned} \quad (14)$$

where $Gr_x(n)$ represents desired linear model, and G depends on Peak Back off (PBO) of the TWTA, which denotes the difference between saturation power P_s and the maximum desired output power of the linearised TWTA, SP_s . The PBO is obtained as:

$$\begin{aligned} PBO &= -10 \log_{10}(S) \\ S &= \frac{G}{P_s}, \quad 0 < S \leq 1 \end{aligned} \quad (15)$$

The PD parameters are estimates by using a hybrid algorithm based on both the Moore-Penrose generalised inverse and gradient descent method.

Assuming the c_j weights in the previous iterations are known, we can derive the generalised inverse solution as:

$$\hat{w} = (H^T H)^{-1} H^T |Gx| \quad (16)$$

Once w_j are obtained, gradient descent method can be used to update the c_j weights. Then the new c_j weights are found as:

$$c = c - \mu \frac{\partial E}{\partial c} \quad (17)$$

Where μ represent learning rate and $\partial E / \partial c$ is gradient vector of E with the j th element of the vector c and the gradient vector of E is given by:

$$\frac{\partial E}{\partial c_j} = \sum_{k=1}^{N_s} 2\Psi' \left[\left(|z_k| - c_j \right)^2 \right] \left(|z_k| - c_j \right) \left(Gx_k - \hat{y}_k \right) \hat{w}_j \quad (18)$$

IV. SIMULATION RESULTS

In this section, it is presented the performance evaluation of the nonlinear distortion compensation scheme. The signals are filtered with 81-tap SRRC pulse shaping for the power spectral density (PSD) calculation and with 47-tap SRRC pulse shaping for the constellation. In addition, in all calculations the pulse shaping filter was implemented with a roll-off factor of $\beta = 0.35$ and 8 samples per symbol.

The parameters of the neural predistorter were estimated during the training process using $N_s = 100$ samples of the amplitude $A(.)$ for 16QAM signals, and the TWTA was operated with IBO of -0.5 dB and a power PBO of -0.22 dB. The neural predistorter was configured with one input node, one linear output node, four nonlinear hidden centres and one bias unit for hidden layer; respectively. In the training process the initial weights, $c(0)$, were initialised by a Gaussian random process with a normal distribution $N(0,1)$. The training process was run with 3 trials and the normalised mean square error (NMSE) after convergence was approximately equal to -50 dB.

In decision-direct mode, the neural predistorter is simply a copy of the neural network obtained in training process.

Figure 1, show the power spectral density (PSD) curves of multilevel quadrature amplitude modulation schemes for both linearly and nonlinearly amplified 16QAM and 256QAM signals. In one hand, for the nonlinear amplification case only with TWTA, the PSD curves are denoted as 16QAM TWTA and 256QAM TWTA; respectively. By the other hand, for the nonlinear amplification case with predistortion and TWTA, the curves are denoted as 16QAM PD TWTA and 256QAM PD TWTA. It can be seen that 16QAM TWTA and 256QAM TWTA have a degradation of PSD about 25 dB and 29dB; respectively. Moreover, from the figure can be seen that the curves of spectral re-growth of the nonlinear case with predistortion are very close to the linear case due to the incorporation of the proposed neural predistorter. Therefore, the proposed predistortion schemes allow to reduce significantly the degradation of the spectral re-growth for 16QAM and 256QAM signals at an IBO level of 0 dB.

The effects of nonlinearity on the received 256QAM constellations in the absence of the channel AWGN are shown in Figure 2 and 3, which correspond to the TWTA without and with predistortion scheme operated at an input back off level of 0 dB. According to Figures 2, it is observed that square 256QAM constellation is severely distorted by the nonlinear AM-AM and AM-PM characteristics of the TWTA without predistortion. This distortion is interpreted as noise in-band, and it is called constellation warping effect. According to Figures 3, the proposed predistorter reduces significantly the constellation warping effect on received 256QAM signals. Therefore, comparing Figures 2 and 3, it can be seen that constellation warping effect is reduced significantly by using proposed predistorter. Moreover, it permits to reduce

both computer storage requirements and coefficients adaptation time of the predistorter, which is achieved due to the proposed hybrid algorithm; it only uses one radial basis function neural network for compensating both nonlinear AM-AM and AM-PM characteristics of the TWTA.

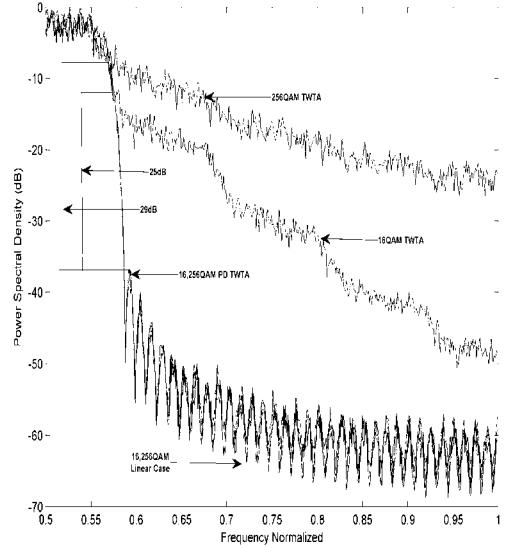


Figure 1 Power spectral densities of 16QAM and 256QAM signals with and without predistortion at IBO= 0 dB.

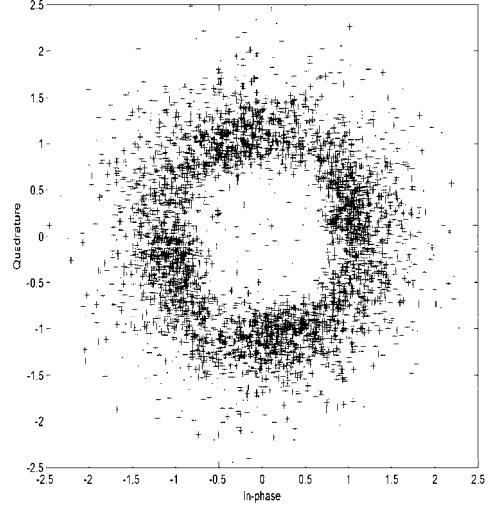


Figure 2 Constellation warping effect over received 256QAM signal due to TWTA with IBO= 0 dB

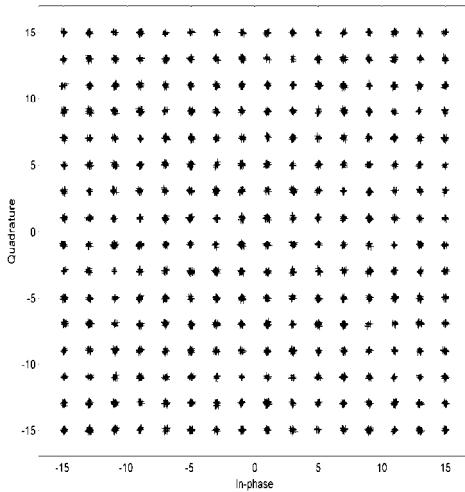


Figure 3 Constellation warping effect over received 256QAM signal compensate with predistortion at IBO= 0 dB

V. CONCLUSIONS

An adaptive baseband predistortion scheme based on a radial basis function neural network for linearising a TWTA has been presented in this paper. The proposed predistorter uses only a neural network with nine coefficients to compensate non-lineal amplitude and phase distortion introduced by the TWTA over transmitted 16QAM and 256QAM signals. The predistorter coefficients adaptation was found by using 3 iterations of a hybrid algorithm based on both generalised inverse and gradient descent method. Simulation results have shown that the proposed predistortion scheme can prevent the RF transmitter from spectrum re-growth and constellation warping effect due to TWTA's nonlinearity with a low complexity and fast convergence.

REFERENCES

- [1] ETSI, *Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for 11/12 GHz Satellite Services*, EN 300 421 v.1.1.2, August 1997.
- [2] ETSI, *Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television*, EN 300 744, August 1997.
- [3] A. M. Saleh, *Frequency-Independent and Frequency-Dependent nonlinear models TWT amplifiers*, IEEE Trans. Comm., Vol. COM-29, pp. 1715-1719, November 1981.
- [4] R. Raich, H. Qian, and G. T. Zhou, *Orthogonal polynomials for power amplifier modeling and predistorter design*, IEEE Trans. on Vehicular Technology, Vol. 53, N°. 5, pp. 1468-1479, September 2004.
- [5] L. Ding and G. T. Zhou, *Effects of even-order nonlinear terms on power amplifier modeling and predistortion linearization*, IEEE Trans. on Vehicular Technology, Vol. 53, N°. 1, pp. 156-162, January 2004.
- [6] R. Marsalek, P. Jardin and G. Baudoin, *From post-distortion to pre-distortion for power amplifier linearization*, IEEE Comm. Letters, Vol. 7, N°7, pp.308-310, July, 2003.
- [7] M. Ghaderi, S. Kumar and D.E. Dodds, *Fast adaptive polynomial I and Q predistorter with global optimisation*, IEE Proc-Comm., Vol. 143, N°. 2, pp. 78-86, April 1996.
- [8] L. Ding, R. Raich, and G.T. Zhou, *A Hammerstein predistortion linearization design based on the indirect learning architecture*, Proc. Int. Conference on Acoustics, Speech, and Signal Processing (ICASSP'2002), Vol. 3, pp. 2689-2692, Orlando, FL, May 2002.
- [9] M. Ibnkahla, *Natural gradient learning neural networks for adaptive inversion of Hammerstein systems*, IEEE Signal Processing Letters, pp. 315-317, October 2002
- [10] C. Eun and E. J. Power, *A new Volterra predistorter based on the indirect learning architecture*, IEEE Trans. Signal Processing, Vol. 45, pp. 223-227, January 1997
- [11] D. Hong-min., H. Song-bai and Y. Jue-bang, *An adaptive predistorter using modified neural networks combined with a fuzzy controller for nonlinear power amplifiers*, Int. Journal of RF and Microwave Computer-Aided Engineering, Vol. 14, N° 1, pp. 15-20, December, 2003
- [12] N. Rodriguez, I. Soto and R. A. Carrasco, *Adaptive predistortion of COFDM signals for a mobile satellite channel*, Int. Journal of Comm. Systems, vol. 16, N° 2, pp. 137-150, February, 2003.
- [13] F. Abdulkader, Langket, D. Roviras and F. Castanie, *Natural gradient algorithm for neural networks applied to non-linear high power amplifiers*, Int. Journal of Adaptive Control and Signal Processing, Vol. 16, pp. 557-576, 2002
- [14] M. Ibnkahla, *Neural network modelling predistortion technique for digital satellite communications*, in Proc. IEEE ICASSP, Vol. 6, pp. 3506-3509, 2000.
- [15] M. Ibnkahla, J. Sombrin J., F. Castanié and N.J. Bershad, *Neural network for modeling non-linear memoryless communications channels*, IEEE Trans. Comm. N° 45 (7), pp. 768-771, July 1997.
- [16] B.E. Watkins and R. North, *Predistortion of nonlinear amplifier using neural networks*, in Proc. IEEE Military communications Conf., Vol.1, pp. 316-320, 1996
- [17] D. Serre, *Matrices: Theory and applications*. New York: Springer-Verlag, 2002

Safe Logon with Free Lightweight Technologies

S. Encheva

Stord/Haugesund University College
Department Haugesund
Bjørnsonsg. 45, 5528 Haugesund
Norway

S. Tumin

University of Bergen
IT Department
P.O.Box 7800, 5020 Bergen
Norway

Abstract—In this paper we address some security problems and issues about implementing Web applications and Web services. In order to do this, we first identify trust relationships among users and systems. In particular, we look into the problems of a secure communication between two parties over insecure channels using a signed digital envelope. We propose a simple and secure way of sign-on into Web applications without using enterprise user-identification and password pair. We try to adhere to simplicity principle in our modeling of the system. By using simple model and free lightweight technologies, we show that it is possible to implement secure Web applications and services.

I. INTRODUCTION

Security within information systems context is based on a complicated trust relations and questions on communication prospective. Trust relations are established between two communicating parties in a relation such as sender/receiver and client/server. When such relations cannot establish trust directly, trusted third parties are used as mediators, which can complicate matters even farther. Security is taken differently by different persons with different prospective of the communicating systems. To a user, security might mean protection on privacy, identity theft and against framing. To an administrator, responsible for the correct working of the applications, security might mean protection on data and process integrity, information flow and recourses protection. The (user, application) pair leads to the necessary establishment of four trust relations among them; application-application, user-application, application-user and user-user. In practice these trust relations are made mutual by, 'I trust you if you trust me' principle. For example, an application trusts a user if the user provides a valid credential at sign-on, the user in turn trusts the application to protect its data and process such that, his/her identity has not being compromised. Whose fault is it when an identity is caught doing an illegal act? Is it a dishonest user, who is the owner of the identity, or an application with weak security policies and implementation, which allow identities theft to occur? It might well be the fault of a weak communication link protocol which leak users' identity under the establishment of trust relations mention above.

In this paper we propose some security tools based on open-source software for Web applications/services for

teams of developers and implementers of limited size. Web applications/services have been developed and deployed due to necessity and not based on commercial goals.

Members of development teams (developers and engineers), normally have different levels of technical knowledge, experience and know-how. Usually, such a project concentrates on workability of a system in a complex environment rather than producing commercial grade software for an assumed environment. To meet the workability goal, security concerns are not taken into consideration due to lack of experience and/or work knowledge. We believe that by using simple and open-ended software tools, developers, and implementers can achieve both workability and a higher level of security due to the fact that a system being developed is under a full control of the developers.

The paper is organized as follows. Related work is presented in Section 2. Trust relations are discussed in Section 3. In Section 4 we proposed the use of signed message of digital envelope package to be used in XML-RPC communication that ensures security, privacy and non-repudiation. A method of using password card called PASS-card for Web sign-on that does not disclose users' system credentials is presented in Section 5. The paper ends with a conclusion.

II. RELATED WORK

Network security problems are discussed in [1]. A set of hints for designing a secure client authentication scheme is described in [4]. A taxonomy of single sign-on systems is presented in [9].

XML-RPC [8] is a Remote Procedure Calling protocol that works over the Internet. An XML-RPC message is an HTTP-POST request. The body of the request is in XML. A procedure executes on the server and the value it returns is also formatted in XML. Procedure parameters can be scalars, numbers, strings, dates, etc., and can also be complex record and list structures.

PGPi is the international variant of Pretty Good Privacy (PGP) [7], which provides an email encryption system. PGP is normally used to apply digital signatures to emails and can also encrypt emails, and thus provides privacy.

A public key encryption program was originally written in 1991. Later PGP versions have been developed and distributed by MIT, ViaCrypt, PGP Inc., and Network Associates Inc. (NAI). PGP is used as a standard for email encryption today, with millions of users worldwide.

PGP does not depend on the traditional hierarchical trust architecture but rather adopts the 'web of trust' approach [10]. Trust issues related to network are discussed by [5].

Limitations to existing e-commerce technologies: data resides in traditional databases, and security is difficult to guarantee across network [2]. Practical sides of Public Key Infrastructure (PKI) are presented in [3].

III. TRUST RELATIONS

Application-Application

Here the sender and the receiver are communicating programs across an insecure channel. A message can be a data synchronization job using push or pull mechanism, a remote procedure request and response, or an even reported by a software agent. The message can be stored and copied. The message needs to be protected against disclosure and tempering on route.

User-Application

Users' credentials and authorization data are protected by a secure sign-on service. When a user gives his/her credentials or other sensitive information to an application, he/she needs to be sure that these data really go to the intended server and are not copied and forwarded to another programs.

Application-User

The user-management system must provide users with strong password policies and a framework where applications will not be compromised by weak users' passwords and weak authentication and authorization mechanism.

User-User

The sender and the receiver agree on a non-refutable mutual contract on the originality and validity of the messages passed between them.

IV. DIGITAL ENVELOPE

In our framework, the sender (Fig. 1), encrypts a message (*payload*) by a symmetric cryptographic function (*sc_crypto*) using a secret-key (*skey*) to produce encrypted payload (*A*).

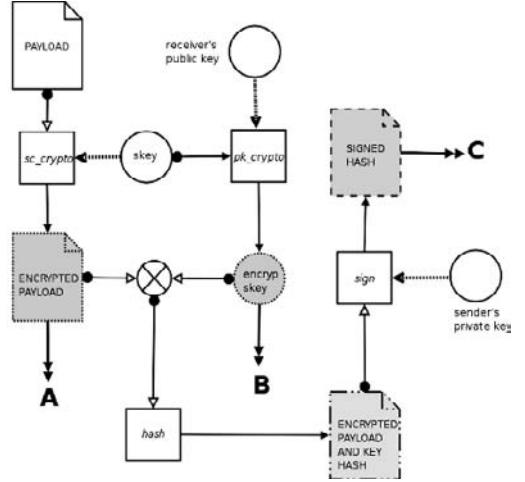


Fig. 1. Sender

A public-key cryptography function (*pk_crypto*) is used to encrypt the secret-key (*B*) using the public-key of the receiving party. Symmetric cryptographic (for example Blowfish) functions for encryption and decryption using a secret key are faster and less resources (CPU, memory) intensive than the public-key cryptography. Together, they (*A* and *B*) make a message in a digital envelope.

The sender takes the digital envelope and runs it through a hash function (*hash*) to produce a hash value. A one-way hash function generates a unique text string to the given input. The hash value is then encrypted by public-key cryptography function (*sign*) using the sender's private key to create a digital signature (*signed hash*) and this authenticates the sender, since only the owner of that private key could encrypt the message.

The *A*, *B* and *C* components are then packed together into a request package. On message arrival, the receiver unpacks the request package back into *A*, *B* and *C* and does the reverse process of decryption and verification (Fig. 2).

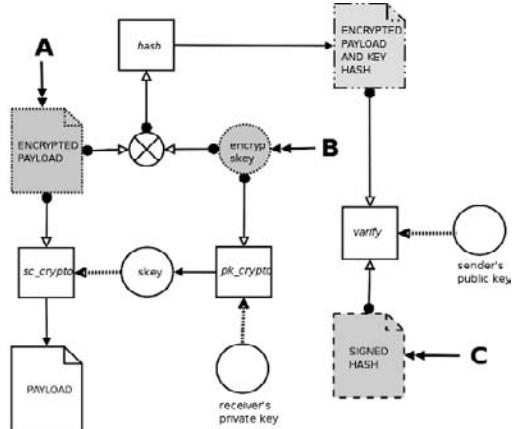


Fig. 2. Receiver

For *Application-Application* communication based on an XML-RPC (XML based remote procedure call over HTTP) request, the receiver unpacks the *payload* to get the procedure name and its parameters. On XML-RPC response, the receiver unpacks the *payload* to get return values. Actually, the payload data is a data structure made into XML by using a Python's `xmlrpclib` module.

For XML-RPC messages, the *skeys* used are made different for different messages. The requester signs its request message and the responder signs its response message.

Most User-User communications are based on email. Users exchange messages using SMTP (Simple Mail Transfer Protocol). Sadly, it is easy to spoof email (forge email sender) because SMTP (Simple Mail Transfer Protocol) lacks authentication. With a wrong configuration of a mail server which allows unrestrictive connections to the SMTP port will let anyone from anywhere to connect to the SMTP port of the site and send email with a forged email sender.

By email spoofing, a user receives email that appears to have originated from one sender when it actually was sent from another sender. Email spoofing is often an attempt to frame another user of making a damaging statement. By claiming to be from a system administrator, a user is tricked into releasing sensitive information (such as passwords).

Users can exchange authenticated email messages by using cryptographic signatures, for example PGP. Authenticated email provides a mechanism for ensuring that messages are from whom they appear to be, as well as ensuring that the message has not been altered in transit. However, PGP does not provide privacy since the messages are not encrypted in any way.

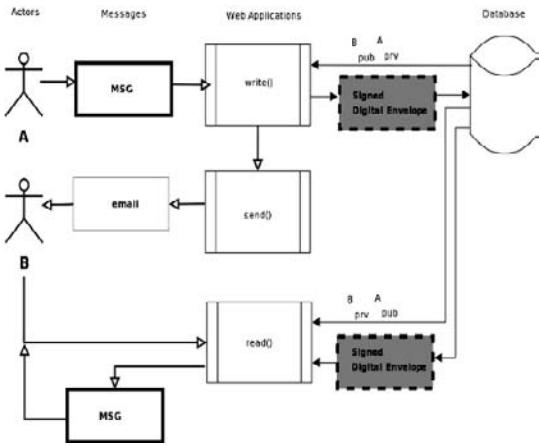


Fig. 3. User-User

Signed digital envelope mechanism can be used in a Web application for User-User communication that ensures secure and non-refutable exchange of messages. In a simple implementation, both the private and public keys of the user are stored in a secure database by the application. The private keys are protected by users' passwords. After a valid sign-on, the writer uploads

his/her message. The application will then ask a list of recipients of this message. Each message to each recipient will then be made into a digital envelope using public key of the recipient. Each of these digital envelopes is then signed using the writer's private key.

These messages packed in signed digital envelopes are then saved in the database ready to be read by the recipients. The application will then send an email to each recipient about the message and on how to read it. A recipient can follow the hyper-link provided in the email to read the message. The recipient is sure that the message is written by the writer if the verify process using the writer's public key is successful. By using the recipient's private key, the recipient can extract the secret-key used to encrypt message. Using this secret-key the recipient can then decrypt the encrypted message in order to read it.

V. THE PASS CARD

Consider the environment in which a user is connected to a Web application. A user can run a Web browser on any PC, some of which are situated in public rooms. The user can not be sure that the PC is secure and free from spy-wares.

A single credential policy increases the risk of the system wide security breach, should that credential got stolen. A keyboard grabber program can easily steal users' credentials without user's knowledge. One solution is not to use a {user-identification, password}-pair credentials for Web applications' sign-on. Some of the technologies supporting such a solution are the use of Smart-cards, biometric devices, and a {client certificate, pin}-pair method.

fh	7a	hW
c8	a4	ed
mi	9q	bL
Gt	br	AR
1163245494-74		

Fig. 4. PASS-Card

We propose a method of using a password card called PASS-card for Web sign-on that does not disclose users' system credentials. A user can produce a PASS-card (a randomly generated image, similar to Fig. 4) via a Web application from a PC within a trusted network, like for example organization's internal network, at anytime. A user has to choose a nick-name and a PIN-code while producing a PASS-card. A PASS-card contains twelve couples and a serial number (Fig. 4). Each couple consists of two randomly generated characters.

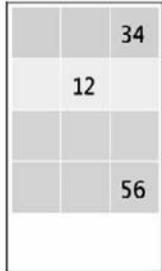


Fig. 5. KEY-map

During any process of sign-on, the system will present to the users with KEY-map diagrams similar to the one on Fig. 5 as a part of the sign-on process. The sign-on application randomly picks and places three couples on the KEY-map locations.

These three couples are randomly positioned in the KEY-map diagram to form a PASS key for this particular sign-on session, Fig. 6.

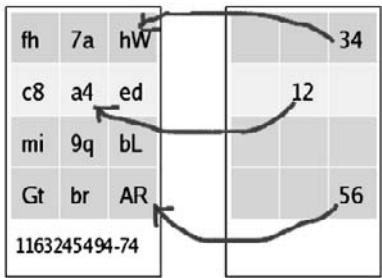


Fig. 6. PASS Keys

To sign-on the user must provide the correct PASS-key correspond to the given KEY-map (the right-hand side figure in Fig. 6). For this particular example (Fig. 6), the PASS key contains three pairs: the first pair (12) which corresponds to the couple *a4*, the second pair (34) which corresponds to the couple *hW* and the third pair (56) which corresponds to the couple *AR*. The resulting sequence *a4hWAR* is the user's PASS-key for this particular sign-on process.

The KEY-map diagram is an image file randomly generated by the Web application using the Python's GD module for each sign-on. PASS-card and KEY-map provide system's users with changing six characters password for each new sign-on.

The user proves his/her authenticity to the application by giving a correct PASS-key from the PASS-card mapped by the KEY-map, the correct nick-name connected to his/her PASS-card and the correct PIN-code. The system then proves its validity by presenting the user with the PASS-card serial number. The valid triplet {PASS-key, nick-name, PIN-code} is then mapped to the real system user.

A user can revoke his/her PASS-card from anywhere and obtain a new one within a trusted network at anytime.

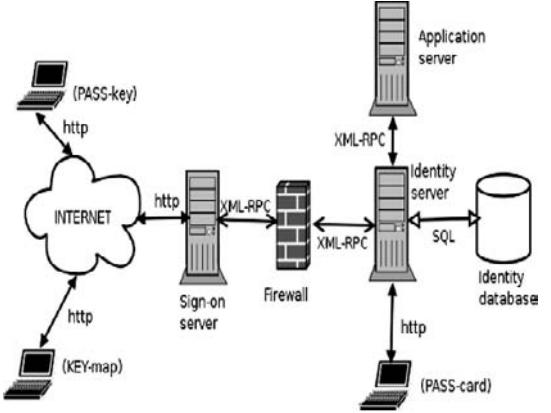


Fig. 7. PASS-Card sign-on

The system architecture that supports PASS-card is shown in Fig. 7. The XML-RPC traffics are made secure by sending messages in signed digital envelopes.

VI. CONCLUSION

In this paper we have identified trust relationships among users and applications. These trust relationships can be broken by undesirable events made possible due to insecure communication environment between two communicating parties. We propose several security tools that can be used to increase the security on the communication channels, thus also increase the trust level.

We adhere to simplicity principle in our modeling of the system. By using simple model and free lightweight technologies, we show that it is possible to implement secure Web application/services. All the applications mentioned in this paper are written in Python scripting language and are making use of Python modules.

XML-RPC with signed digital envelope makes it possible to transmit request/response messages trustworthy, securely and privately over an insecure public network. Users can write private and non-refutable messages to each other using signed digital envelope. A secure User-User messaging system based on signed digital envelope, in which messages between application's users are made private and trustworthy, was proposed.

The use of public-key cryptography introduces the problem of public-key management. The management of users' identities and public-keys is not a trivial matter. The security of private-keys is the essential part of the public-key cryptography.

User authentication based on user-identification and password for sign-on to Web based applications can break the security of the entire enterprise. We proposed a sign-on mechanism using PASS-cards. We use Apache Web server with mod_python to implement the system shown in Fig. 7. PASS-cards allow the user to sign-on from virtually anywhere (by using only http) without

fear of disclosing his/her real system credential. The users themselves administer the usage and validity the PASS-cards they owned.

REFERENCES

- [1] J. Albanese, J., and W. Sonnenreich, 2003, "Network Security Illustrated," *McGraw-Hill Professional*, 2003.
- [2] S. Garfinkel, "Web Security, Privacy and Commerce," *O'Reilly*, 2002.
- [3] E. Geschwind, and H.-J. Schonig, "PostgreSQL, Developer's Hadbook," *Sams Publishing*, USA, 2001.
- [4] K. Fu, E. Sit, K. Smith, and N. Feamster, "Dos and Don'ts of Client Authentication on the Web," *10th USENIX Security Symposium*, Washington, D.C, 2001.
- [5] Y. Lu, W. Wang, D. Xu, and B. Bhargava, "Trust-based Privacy Preservation for Peer-to-peer Data Sharing," *Proceedings of the 1st NSF/NSA/AFRL workshop on Secure Knowledge Management (SKM)*, 2004.
- [6] <http://www.pubcookie.org>
- [7] <http://www.pgpi.org>
- [8] <http://www.xmlrpc.com/>
- [9] A. Pashalidis, and C. J. Mitchell, "A taxonomy of single sign-on Systems," *Lecture Notes in Computer Science*, vol. 2727, pp.249-264, 2003.
- [10] P. Zimmermann, "Pretty Good Privacy User's Guide," *Distributed with the PGP software*, 1993.

Stochastic Communication in Application Specific Networks-on-Chip

Vivek Kumar Sehgal¹ and Nitin²

¹Department of ECE and ²Department of CSE & IT

Jaypee University of Information Technology
Waknaghat, Solan-173215, HP, INDIA
[{vivekseh, er.nitin}](mailto:{vivekseh, er.nitin}@gmail.com)@gmail.com

Abstract- Networks-on-chip (NoC) is a new approach to System-on-chip (SoC) design. NoC consists of different Intellectual Property (IP) cores. The NoC solution brings a networking method to on-chip communication and claims roughly a threefold increase in performance over conventional bus systems. In this paper we proposed a new method for stochastic communication between the different IP cores. These IP cores are connected with different routers or switches and are treated as different compartments on the single chip. The spread of information among these IP cores can be represent using a closed donor control based compartmental model, which can be converted into a stochastic model. The stochastic model is more realistic and enables us to compute the transition probability from one IP to other IP core as well as latency.

I. INTRODUCTION

System-on-chip (SoC) designs provide integrated solutions to challenging design problems in the telecommunications, multimedia, and consumer electronic domains. With deep sub-micron technology, chip designers are expected to create SoC solutions by connecting different Intellectual Property (IP) cores using efficient and reliable interconnection schemes known as Networks-on-Chip (NoC). This methodology makes a clear distinction between computation (the tasks performed by the IP cores) and communication (the interconnecting architecture between the IP cores). NoC are formed by connecting either homogeneous or heterogeneous IP cores on a single chip. Since modern NoC are becoming extremely complex, so there are many challenges in this new area of research. On-chip wire delays have become more critical than gate delays and recently synchronization problems between Intellectual Properties (IPs) are more apparent. This trend only worsens as the clock frequencies increase and the feature sizes decrease [1]. However, low latency which is an important factor in real time applications [2].The interconnects on chip are subject to new types of malfunctions and failures that are harder to predict and avoid with the current SoC design methodologies.

These new types of failures are impossible to characterize using deterministic measurements so, in the near future, probabilistic metrics, such as average values and variance, will be needed to quantify the critical design objectives, such as performance and power [3]. The IPs communicates using probabilistic broadcast scheme called on-chip stochastic communication. This algorithm achieves many of the desire features of the future NoC [3] and provides:

- 1) Separation between computation and communication.

2) Fault-tolerance.

Despite of these features, low latency is major challenge in modern NoC. Latency in NoC can be measure by calculating the latency in switch and propagation delay in chip interconnects [4] but it depends on the type of NoC i.e. single chip NoC or multiple chip NoC (also known as Networks-in-Package). The different NoC topologies are already used in [5] and these topologies give different communication structure in NoC [6].

We proposed a method for stochastic communication, which is suitable for homogeneous as well as heterogeneous NoC. We used compartmental based stochastic communication method for Application-Specific Networks-on-Chip in, which different IPs is used. These IPs are treated as compartmental IPs moreover the flow of data from source IP to Destination IP can be represented by a compartmental network or model. From this model we can derive the compartmental matrix, which retains the properties of Metzler matrix. The derived compartmental matrix gives us the inter compartmental flow of IP cores, which help us to calculate the transition probability matrix and hence we can convert the resultant matrix into Markov Chain [7]. In IPs based compartmental models, some models are having feedback and some are not. Those models with feedback can be converted into stochastic models using Regular Markov Chains and the others using Absorbing Markov Chains. If the compartmental model is linear than we can easily generate the stochastic model, otherwise it has to be linearized using Jacobian matrix about the equilibrium points.

II. DATA FLOW NETWORK IN NOC FOR STOCHASTIC COMMUNICATION

In this section we have suggest the compartmental based probabilistic data broadcasting among the IP cores in a NoC. This process of communication is a random process. When a data in the form of packets is transmitted from source to destination IP core in the grid based square network as shown in Fig.1 then IP core communicates the data using a probabilistic broadcast scheme, similar to the randomized gossip protocols [3]. The source IP core sends the data packets to the destination IP core through its neighbors. We know that in homogeneous and heterogeneous NoC, any IP can be used as the source IP or intermediate IP or destination IP. There are many possible ways in which data can flow, depending upon the requirement.

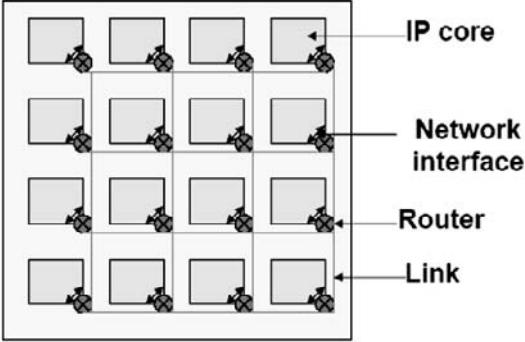


Fig. 1. Topological illustration of a 4-by-4 grid structured homogeneous NoC.

In this paper we used one of the data flow network in Application-Specific heterogeneous NoC. This NoC consist of few IPs and routers as shown in the Fig. 2.

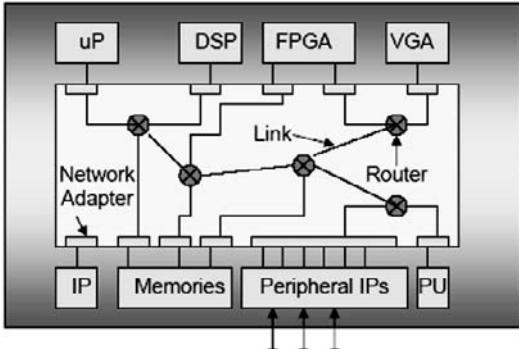


Fig. 2. Application-Specific heterogeneous NoC.

If the data has to be sent from DSP to FPGA and PU core then we can extract one of the data flow network from NoC. There are five compartments in data flow network as shown Fig. 3. These compartments are: source IP (X_1), intermediate IPs (X_2 and X_3), and destination IPs (X_4 and X_5).

This model of data flow network is also known as stochastic network and can be used for stochastic modeling by following certain assumptions:

- 1) The total number of data packets is constant.
- 2) The model is donor control based model.
- 3) The model is mass conservative.

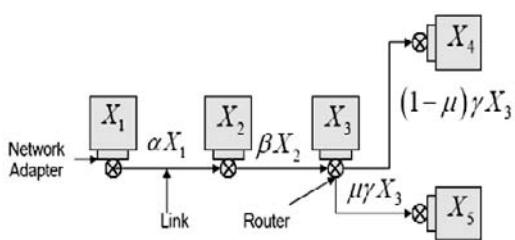


Fig. 3. Data flow network for stochastic communication.

The behavior of data flow model is shown in Fig. 3 can be described by the following set of differential equations:

$$\frac{dX_1}{dt} = -\alpha X_1 \quad (1)$$

$$\frac{dX_2}{dt} = \alpha X_1 - \beta X_2 \quad (2)$$

$$\frac{dX_3}{dt} = \beta X_2 - \gamma X_3 \quad (3)$$

$$\frac{dX_4}{dt} = (1 - \mu)\gamma X_3 \quad (4)$$

$$\frac{dX_5}{dt} = \mu\gamma X_3 \quad (5)$$

$$N = X_1 + X_2 + X_3 + X_4 + X_5 \quad (6)$$

Where α , β and γ are the different data flow rates from respective compartment.

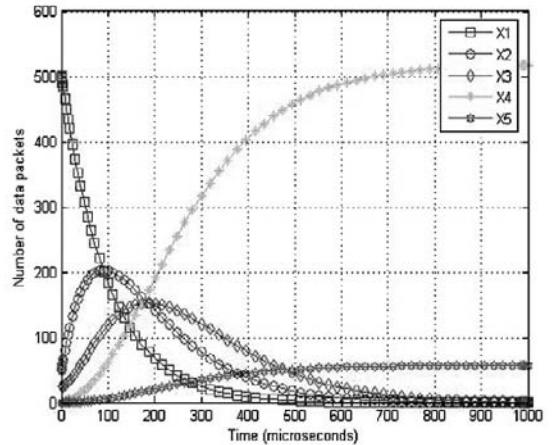


Fig. 4. Dynamic behavior of data flow network in NoC.

The dynamic behavior (number of packets transferred per unit of time) of basic data flow network in NoC is shown using Fig.4. So from here we deduce that for $N = 575$, $x_1(0) = 500$, $x_2(0) = 50$, $x_3(0) = 25$ and $x_4(0) = x_5(0) = 0$

Where N is total no. of data packets to be transmitted. For on chip synchronization all the flow rates are taken equal. $\alpha = \beta = \gamma = 0.01$. The separation constant μ is 0.1. Since the equations (1-6) describing the behavior of stochastic network and these are linear differential equations in addition to this the five compartments (X_1 - X_5) can be treated as physical state space variables. Since the given set of equation is linear in nature, we can find the homogeneous solution for these equations

III. COMPARTMENTAL MODELING OF DATA FLOW NETWORK IN NOC

In this section we derived the compartmental matrix from the state space equations (1-6), defining the dynamic behavior of data flow networks (refer Fig. 4). These state space equations can be expressed in the form of matrix given below.

$$\dot{X}(t) = AX(t) \quad (7)$$

$$\begin{pmatrix} \dot{X}_1 \\ \dot{X}_2 \\ \dot{X}_3 \\ \dot{X}_4 \\ \dot{X}_5 \end{pmatrix} = \begin{pmatrix} -\alpha & 0 & 0 & 0 & 0 \\ \alpha & -\beta & 0 & 0 & 0 \\ 0 & \beta & -\gamma & 0 & 0 \\ 0 & 0 & (1-\mu)\gamma & 0 & 0 \\ 0 & 0 & \mu\gamma & 0 & 0 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \\ X_4 \\ X_5 \end{pmatrix} \quad (8)$$

$$A = \begin{pmatrix} -\alpha & 0 & 0 & 0 & 0 \\ \alpha & -\beta & 0 & 0 & 0 \\ 0 & \beta & -\gamma & 0 & 0 \\ 0 & 0 & (1-\mu)\gamma & 0 & 0 \\ 0 & 0 & \mu\gamma & 0 & 0 \end{pmatrix} \quad (9)$$

Where A is called compartmental matrix. The solution of this homogeneous state equation is:

$$x(t) = e^{At} x(0) \quad (10)$$

$$x(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \\ x_3(t) \\ x_4(t) \\ x_5(t) \end{pmatrix} \quad (11)$$

$$e^{At} = L^{-1} [(sI - A)^{-1}] \quad (12)$$

$$\text{or } e^{At} = I + At + \frac{1}{2!} A^2 t^2 + \dots + \frac{1}{i!} A^i t^i \quad (13)$$

Where e^{At} called state transition matrix of data flow network and $x(0)$ is the column matrix which shows the initial conditions of model.

A. Properties of Compartmental Matrix

The certain important properties of compartmental matrix are retained by the matrix A, are given below:

- 1) The diagonal elements of compartmental matrix are zero or negative elements.
- 2) The non-diagonal elements of compartmental matrix are zero or positive.
- 3) The first eigenvalue of compartmental matrix is zero.
- 4) The sum of elements in each column of compartmental matrix is equal to zero.
- 5) Compartmental matrix is Metzler matrix.
- 6) It obeys the law of mass conservation

IV. STOCHASTIC MODELING OF DATA FLOW NETWORK IN NOC

In this section we converted the compartmental matrix A into the probability transition matrix P and obtained observing Markov Chain for stochastic modeling. Stochastic modeling is very useful to calculate the latency in NoC and also the transition probability and expected time of data flow from one IP to other IP. The transition probability matrix can be derived from compartmental matrix using following relation [8].

$$P = (I + hA)^T \quad (14)$$

The probability $p_i(n)$ that the random variable is in state i at any time n may be found from the level of numbers or quantity of random variables $x_i(n)$ in that state (now called compartment) at time n . Indeed $p_i(n) = x_i(n) / \sum_{j=1}^k x_j(n)$,

where k is the number of states. The levels at time $n+1$ are given in terms of those at time n by the same equation,

$$X_{n+1}^T = X_n^T P, \quad n = 0, 1, 2, \dots \quad (15)$$

as the probabilities. Here, X_n is a column vector of material levels. Then, we have

$$X_{n+1}^T \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} x_{n+1,1}, x_{n+1,2}, \dots, x_{n+1,k} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = X_n^T P \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = X_n^T \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \quad (16)$$

Since $[1, 1, \dots, 1]^T$ is always a right eigenvector corresponding to the steady state eigenvalue of 1 of P. If we started with a quantity $q = \sum_{j=1}^n x_j(0)$ of materials in the system, then the total quantity in the system remains at q for all time by (16). Thus, we have $p_i(0) = \frac{x_i(0)}{q}$.

Thus, (15) is one form of equation of a compartmental system, but a more common format is as a difference equation

$$X_{n+1}^T - X_n^T = X_n^T (P - I)$$

or by taking transpose it becomes

$$\Delta X_n = (P^T - I) X_n \quad (17)$$

If the time step, i.e., the time between trials, is h rather than 1, then $X_n = X(nh)$ and the left side of (17) is replaced by the difference quotient

$$\frac{X(nh+h) - X(nh)}{h} = \frac{1}{h} (P^T - I) X(nh) = A X(nh)$$

Let $t = nh$

$$\Rightarrow \frac{X(t+h) - X(t)}{h} = A X(t)$$

This left side is approximately the derivative, so we have $X' = AX$. This is the differential equation for the

compartmental matrix and Hence $A = \frac{1}{h} (P^T - I)$, Where P the transition probability matrix and h is the time between events or trials or more specifically $P = (I + hA)^T$.

$$P = \begin{pmatrix} 1-h\alpha & 0 & 0 & 0 & 0 \\ h\alpha & 1-h\beta & 0 & 0 & 0 \\ 0 & h\beta & 1-h\gamma & 0 & 0 \\ 0 & 0 & h(1-\mu)\gamma & 1 & 0 \\ 0 & 0 & h\mu\gamma & 0 & 1 \end{pmatrix}^T$$

$$= \begin{pmatrix} p_{x_1 x_1} & p_{x_1 x_2} & p_{x_1 x_3} & p_{x_1 x_4} & p_{x_1 x_5} \\ p_{x_2 x_1} & p_{x_2 x_2} & p_{x_2 x_3} & p_{x_2 x_4} & p_{x_2 x_5} \\ p_{x_3 x_1} & p_{x_3 x_2} & p_{x_3 x_3} & p_{x_3 x_4} & p_{x_3 x_5} \\ p_{x_4 x_1} & p_{x_4 x_2} & p_{x_4 x_3} & p_{x_4 x_4} & p_{x_4 x_5} \\ p_{x_5 x_1} & p_{x_5 x_2} & p_{x_5 x_3} & p_{x_5 x_4} & p_{x_5 x_5} \end{pmatrix}$$

$$P = \begin{pmatrix} 1-h\alpha & h\alpha & 0 & 0 & 0 \\ 0 & 1-h\beta & h\beta & 0 & 0 \\ 0 & 0 & 1-h\gamma & h(1-\mu)\gamma & h\mu\gamma \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (18)$$

From (18) we can see that the sum of all elements in each row of transition probability matrix P is equal to 1. Hence

$$\sum_{j=0}^{j=4} p_{ij} = 1 \text{ Where } i, j = 0 \dots 5 \quad (19)$$

A. Properties of Transition Probability Matrix

The certain important properties of transition probability matrix P are given below:

- 1) The first eigenvalue of transition probability matrix is equal to 1.
- 2) The sum of all elements in each row of transition probability matrix is equal to 1.
- 3) This matrix is also known as Markov Matrix.

B. Markov Chain from Transition Probability Matrix

The Fig. 5 shows the stochastic diagram of transition probability matrix P .

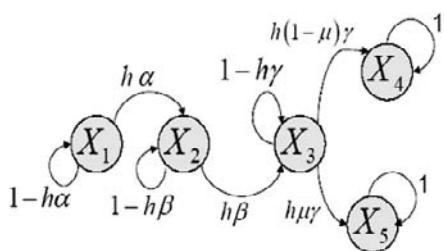


Fig. 5. Stochastic diagram (Absorbing Markov Chain) of data flow network in NoC.

In an Absorbing Markov Chain with states ordered such that the transition probability matrix P has the form:

$$P = \begin{bmatrix} Q & R \\ 0 & I \end{bmatrix} \quad (20)$$

And the following hold:

- 1) $Q^t \rightarrow 0$ as $t \rightarrow \infty$.
- 2) $R_\infty = (I - Q)^{-1} R$.
- 3) The expected number of times a chain is in the non absorbing state k_j given that it started in k_i is given by the corresponding element of $(I - Q)^{-1}$.

The matrix $(I - Q)^{-1}$ is often referred to as *Markov chain's fundamental matrix* for each non absorbing state, there is an absorbing state with a path of minimum length. Let r be the maximum length of all such paths. Therefore, in r steps, there is a positive probability p of entering one of the absorbing states regardless of where you started. The probability of not reaching an absorbing state in r steps is $(I - p)$. After the next r steps, it is $(I - p)^2$ and after kr steps, $(I - p)^k$. Since this approaches 0 as $k \rightarrow \infty$, the probability of being in any non absorbing state approaches 0 as $t \rightarrow \infty$. But the elements of Q^t are just these probabilities. In this paper $(I - Q)^{-1}$ will give us the expected time of data flow from one IP core to other IP core. And $R_\infty = (I - Q)^{-1} R$ will give us the probability of data transmission to the destination IP core.

V. STOCHASTIC ANALYSIS OF ON CHIP COMMUNICATION

In this section we verified the compartmental based stochastic communication scheme. From (18) and (20), we get

$$P = \begin{bmatrix} Q & R \\ 0 & I \end{bmatrix} = \begin{bmatrix} 1-h\alpha & h\alpha & 0 \\ 0 & 1-h\beta & h\beta \\ 0 & 0 & 1-h\gamma \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ h(1-\mu)\gamma & h\mu\gamma \end{bmatrix}$$

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The last state of this Markov Chain I is the absorbing state which consists of destination IPs in NoC. For $\alpha = \beta = \gamma = 0.01$ and μ is 0.1. The time for each event or transition h is 0.1. This implies

$$P = \begin{bmatrix} 0.999 & 0.001 & 0 & 0 & 0 \\ 0 & 0.999 & 0.001 & 0 & 0 \\ 0 & 0 & 0.999 & 0.0009 & 0.0001 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$Q = \begin{bmatrix} 0.999 & 0.001 & 0 \\ 0 & 0.999 & 0.001 \\ 0 & 0 & 0.999 \end{bmatrix}, R = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0.0009 & 0.0001 \end{bmatrix},$$

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

For transient response

$$(I - Q)^{-1} = \begin{bmatrix} 1000 & 1000 & 1000 \\ 0 & 1000 & 1000 \\ 0 & 0 & 1000 \end{bmatrix}$$

From $(I - Q)^{-1}$ matrix we can calculate:

- 1) Expected time during which the data available with source IP core (X_1) = 1000 microseconds.
- 2) Expected delay to reach the intermediate IP (X_3) = $1000 + 1000 = 2000$ microseconds.
- 3) Expected time during which the data live on intermediate IP core (X_3) = 1000 microseconds.
- 4) Expected delay to reach from intermediate IP (X_2) to the destination IP (X_4) = $1000 + 1000 = 2000$ microseconds.
- 5) Expected delay to reach from source IP (X_1) to the destination IP (X_4) = $1000 + 1000 + 1000 = 3000$ microsecond.

For steady state response

$$R_\infty = (1 - Q)^{-1} R = \begin{bmatrix} 0.9 & 0.1 \\ 0.9 & 0.1 \\ 0.9 & 0.1 \end{bmatrix}$$

From $R_\infty = (1 - Q)^{-1} R$ matrix we can calculate:

- 1) Probability of data reception by IP X_4 = 0.9.
- 2) Probability of data reception by IP X_5 = 0.1.

For the steady state, complete transition probability matrix is

$$P_\infty = \begin{bmatrix} Q_\infty & R_\infty \\ 0 & I \end{bmatrix}$$

$$P_\infty = \begin{bmatrix} 0 & 0 & 0 & 0.9 & 0.1 \\ 0 & 0 & 0 & 0.9 & 0.1 \\ 0 & 0 & 0 & 0.9 & 0.1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

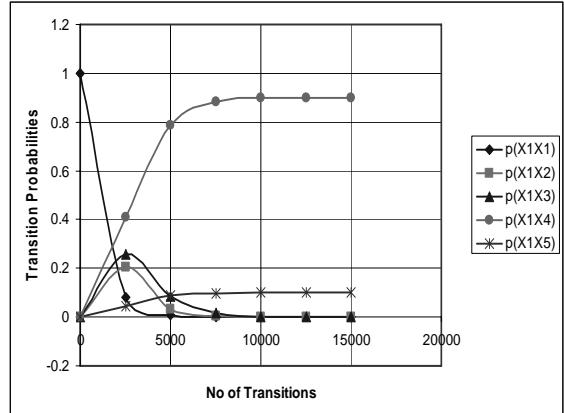


Fig. 6. Transition probabilities of data flow for IP(X_1)

TABLE I
TRANSITION PROBABILITIES OF DATA FLOW FOR IP(X_1)

No. of Transitions	Transition probabilities				
	$p(X_1X_1)$	$p(X_1X_2)$	$p(X_1X_3)$	$p(X_1X_4)$	$p(X_1X_5)$
1	0.999	0.001	0	0	0
2500	0.082	0.2052	0.2566	0.4106	0.0456
5000	0.0067	0.0336	0.0842	0.7879	0.0875
7500	0.0006	0.0041	0.0155	0.8818	0.098
10000	0	0.0005	0.0023	0.8975	0.0997
12500	0	0	0.0003	0.8997	0.1
15000	0	0	0	0.9	0.1

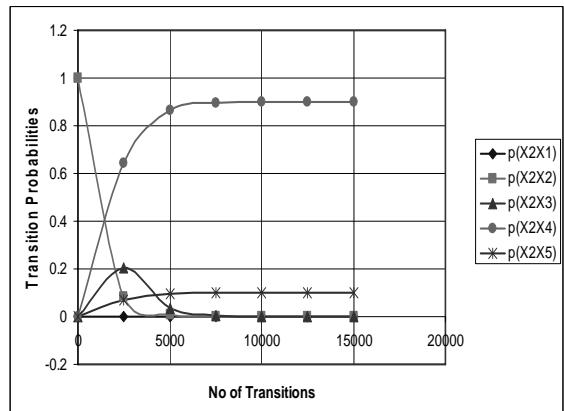


Fig. 7. Transition probabilities of data flow for IP(X_2)

TABLE II
TRANSITION PROBABILITIES OF DATA FLOW FOR IP(X_2)

No. of Transitions	Transition probabilities				
	$p(X_2X_1)$	$p(X_2X_2)$	$p(X_2X_3)$	$p(X_2X_4)$	$p(X_2X_5)$
1	0	0.999	0.001	0	0
2500	0	0.082	0.2052	0.6416	0.0713
5000	0	0.0067	0.0336	0.8637	0.096
7500	0	0.0006	0.0041	0.8958	0.0995
10000	0	0	0.0005	0.8996	0.1
12500	0	0	0	0.9	0.1
15000	0	0	0	0.9	0.1

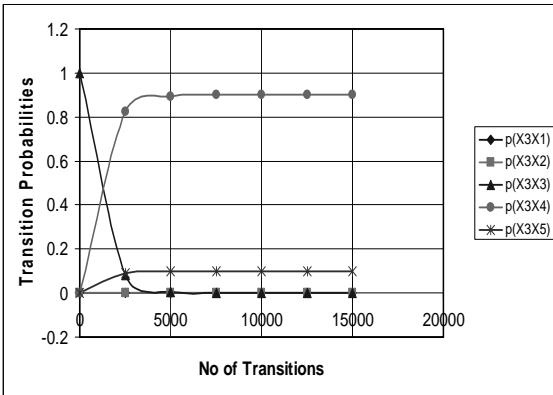
Fig. 8. Transition probabilities of data flow for IP (X_3)

TABLE III
TRANSITION PROBABILITIES OF DATA FLOW FOR IP (X_3)

No. of Transitions	Transition probabilities				
	p(X3X1)	p(X3X2)	p(X3X3)	p(X3X4)	p(X3X5)
1	0	0	0.999	0.0009	0.0001
2500	0	0	0.082	0.8262	0.0918
5000	0	0	0.0067	0.894	0.0993
7500	0	0	0.0006	0.8995	0.0999
10000	0	0	0	0.9	0.1
12500	0	0	0	0.9	0.1
15000	0	0	0	0.9	0.1

In Fig. (6-8) and Table (I-III), P_{ij} shows the transition probabilities of data flow from one X_i IP core to X_j IP core where $i = 1..3$ and $j=1..5$. From this stochastic model we can calculate the total transition probabilities between any two IP cores, which is very useful to calculate the latency. In addition to this the proposed method makes separation between communication and computation.

VI. CONCLUSION AND FUTURE WORK

In this paper we have proposed a new method for stochastic communication between the different IP (Intellectual Property) cores. In addition to this our method helps in building the compartmental model of IPs on the NoC and moreover calculating the latency as well as the transition probabilities of data flow between any two IPs. From the Fig. 6-8 and Tables (I-III) it is depicted that the transient and steady state response of transition probabilities gives us the state of data flow latencies among the different IPs in NoC.

In future the work presented here can be applied on any kind of on-chip interconnects topology. In addition to this we can find out the controllability and absorbability for each NoC and can design a condensed compartmental network for stochastic communication in NiP. The method for stochastic modeling is very useful to calculate the latency only if; we use the inflow and outflow in a NoC in NiP architecture. We can use this work to merge the two kind of communications one is inter NoC and another is inter NiP.

ACKNOWLEDGEMENT

The authors would like to thank the editor and the anonymous reviewers for their constructive comments and suggestions that significantly improved the quality of the paper. Finally we would like to thank Professor Ashok Subramanian PhD (CS – Stanford University USA) for his moral support and technical inputs.

REFERENCES

- [1] L. Kangmin, L. Se-Joong, K. Donghyun, K. Kwanho, K. Gawan, K. Joung, and Y. Hoi-Jun, "Networks-on-chip and Networks-in-Package for High-Performance SoC Platforms," *IEEE* pp. 485-488, 2005.
- [2] L. Kangmin, L. Se-Joong and Y. Hoi-Jun, "Low-Power Network-on-Chip for High-Performance SoC Design," *IEEE Transactions On Very Large Scale Integration (VLSI) Systems*, Vol. 14, No. 2, pp. 148-160, February 2006.
- [3] D. Tudor and M. Radu, "On-Chip Stochastic Communication," *Proceedings of the Design, Automation and Test in Europe Conference and Exhibition*, 2006.
- [4] K. Kwanho, L. Se-Joong, L. Kangmin and Y. Hoi-Jun, "An Arbitration Look-Ahead Scheme for Reducing End-to-End Latency in Networks on chip," *IEEE*, pp. 2357-2360, 2005.
- [5] S. Murali, and G. Micheli, "SUNMAP: A Tool for Automatic Topology Selection and Generation for NoCs," *IEEE DAC*, San Diego, California, USA, pp. 914-919, June 7-11, 2004.
- [6] T. Bjerregaard and S. Mahadevan, "A Survey of Research and Practices of Network-on-Chip," *ACM Computing Surveys*, Vol. 38, Article 1, pp. 1-51, March 2006.
- [7] V. K. Sehgal, "Stochastic Modeling of Worm Propagation in Trusted Networks," *SAM*, Las Vegas, USA, pp. 482-488, June 26-29, 2006.
- [8] G. Gilbert, Walter and Martha Contreras, "Compartmental Modeling with Networks". *Morgan-Kauffman*, 2000.

A Random Approach to Study the Stability of Fuzzy Logic Networks

Yingjun Cao, Lingchu Yu, Alade Tokuta

Department of Mathematics & Computer Science
North Carolina Central University
Durham, NC 27707
ycao@nccu.edu, lyu@mail.nccu.edu, atokuta@nccu.edu

Paul P. Wang

Department of Electrical & Computer Engineering
Duke University
Durham, NC 27708
ppw@ee.duke.edu

Abstract-In this paper, we propose a general network model, fuzzy logic network (FLN), and study its stability and convergence properties. The convergence property was first deduced theoretically. Then a random approach was adopted to simulate the convergence speed and steady-state properties for a variety of fuzzy logical functions. The simulation results show that MV logical function causes the system to be on the edge of chaos when the number of nodes increases. Thus this logical function is more useful to infer real complex networks, such as gene regulatory networks.

I. INTRODUCTION

One of the most challenging problems in bioinformatics is to determine how genes inter-regulate in a systematic manner which results in various translated protein products and phenotypes. To find the causal pathways that control the complex biological functions, researchers have been modeling gene regulatory mechanisms as a network topologically in order to gain more detailed insight [1]. It, in return, arouses the need of novel network models. The importance of the networking model is that normal regulatory pathways are composed of regulations resulting from many genes, RNAs, and transcription factors (TFs). The complicated inter-connections among these controlling chemical complexes are the driving force in maintaining normal organism functions. The simplest yet commonly used model for gene regulatory networks is the so called *NK* Boolean network [2]. It is a directed graph to model the situation where gene *A* and gene *B* interact during some time intervals and their interactions will determine or regulate the status of another gene *C* through a Boolean logical function at the next step. If numerous genetic regulations occur simultaneously, the participating genes with their unique logical functions form the components of a gene regulatory network. This network will be self-evolutionary and eventually reach certain final states. In the *NK* network nomenclature, *N* is the total number of genes in the network, and *K* denotes the maximum number or the average number of regulating genes. The *NK* Boolean network theory has been carried out in a variety of ways both in deduced mathematical approximation and computer simulations [2-4]. Due to the binary limitation inherent in Boolean values, however, the exact properties of gene regulation cannot be expressed in detail based on this model. Thus other approaches were adapted to model the gene regulation mechanism, such as differential equations [5], Bayesian net-

works [6], and genetic circuits [7]. These models, however, have stressed different aspects of the regulatory behavior, and each model has contributed good inference results in certain aspect of the issue. The ongoing research on those models has focused on non-linear data processing, noise tolerance, and model over fitting [8].

In this paper, we propose and study a general network model, the fuzzy logic network (FLN) which is believed to possess the capacity of modeling complex networks and self-organizable systems, such as biological or economical systems. In a sense, the FLN is the generalization of Boolean network, but is capable of overcoming the unrealistic constraint of Boolean value (ON/OFF symbolically). Fuzzy logic has evolved as a powerful tool over 40 years, and its applications are widely available in scientific research and engineering literature. The proposed FLN is able to inherit all the good properties of Boolean networks, especially the causal property in the dynamic network behavior. Additionally, it is also expected to be a more effective model with the nuance of membership function adjustment and inference rules. The FLN also has numerous known advantages such as modeling the highly non-linear relationships and periodicity. With distinctive properties in processing real-life incomplete data and uncertainties, the gene regulation analysis based on fuzzy logic theory did emerge after 2000 [9] and some good developments have been documented since then [10-16].

The general study of FLN's convergence and stability presented in this paper is organized as follows. In section II, the FLN's definitions and their appropriate meanings are given. Two important theorems concerning the evolutionary property of the FLN are proved. In section III, the simulation algorithm is illustrated. In the following section, the simulation results are presented and discussed in detail. Conclusions and future research are discussed in section V.

II. FUZZY LOGIC NETWORK

A. Definitions

1) Fuzzy logic network

Given a set of *N* fuzzy variables (genes),

$\bar{X}_t = \{x_t^1, x_t^2, \dots, x_t^N\}, x_t^i \in \{0,1\}, i \in \underline{N}$, index *t* represents time; the variables are updated by means of dynamic equa-

tions, $x_{t+1}^i = f_i(x_t^{i_1}, x_t^{i_2}, \dots, x_t^{i_K})$ where f_i is a randomly chosen fuzzy logical function.

In the FLN, the fuzzy logical functions can be constructed using the combination of AND, OR, \leftarrow and COMPLEMENT. The total number of choices for fuzzy logical functions is decided only by the number of inputs. If a node has K ($1 \leq K \leq N$) inputs, then there are 2^K different fuzzy logical functions. In the definition of FLN, each node x_t^i has K inputs on average.

2) Fuzzy logical functions

Fuzzy logical function is a binary operation that satisfies the identity, commutative, associative and increasing properties. A fuzzy logical function usually has to satisfy the so called **t-norm/t-co-norm**. Table I is a list of commonly used fuzzy logical functions with the AND, OR and COMPLEMENT [17].

TABLE I
COMMONLY USED FUZZY LOGICAL FUNCTIONS

Fuzzy Logical Function	$a \wedge b$	$a \vee b$	\bar{a}
Max-Min	$\min(a, b)$	$\max(a, b)$	$1 - a$
GC	$a \times b$	$\min(1, a + b)$	$1 - a$
MV	$\max(0, a + b - 1)$	$\min(1, a + b)$	$1 - a$
Probabilistic	$a \times b$	$a + b - a \times b$	$1 - a$

3) Quenched update

If all the fuzzy logical functions, f_i ($i \in \underline{N}$), and their related variable set, $\{x_t^{i_1}, x_t^{i_2}, \dots, x_t^{i_K}\}$, chosen at the initial state of the system remain the same throughout the whole dynamic process, then the system is termed as quenched updated.

4) Synchronous update

If all the fuzzy variables, x_t^i , are updated at the same time, then the system is called synchronously updated; otherwise, it is asynchronously updated. In this paper, the FLN is assumed to be synchronously updated.

5) Basin of attraction

It is the set of points in the system state space, such that initial conditions chosen in this set dynamically evolve toward a particular steady state.

6) Attractor

It is a set of states invariant under the dynamic progress, toward which the neighboring states in a given basin of attraction asymptotically approach in the course of dynamic evolutions. It can also be defined as the smallest unit which cannot be decomposed into two or more attractors with distinct basins of attraction.

7) Limit cycle

It is an attracting set of state vectors to which orbits or trajectories converge, and upon which their trajectories are periodic.

B. Theorems

Theorems in this section have focused on the dynamical convergence process of the FLN. The reason is not all FLNs

have limit cycles or attractors as strictly as in the case of Boolean. Excellent work has been done in Boolean Network on the characteristics of the cycles [18-19], but it has been shown that power law appears when the system has exponentially short cycles locally. The length of cycles and the number of cycles are heavily affected by the chaotic property. This property arouses the motivation to simulate the convergence of randomly FLNs.

Theorem 1: Quenched FLN using the Max-Min logical function must reach limit cycles or attractors

Proof:

If the initial conditions of the network are $\vec{x}_1 = [x_1^1, x_1^2, \dots, x_1^N]$, and the Max-Min logical function is used, it is obvious that the possible values of any variable, x_t^i , at any time t can be only selected from

$$\{x_1^1, 1 - x_1^1, x_1^2, 1 - x_1^2, \dots, x_1^N, 1 - x_1^N\}$$

So the state space initially includes maximally $2N$ possible values (some values out of $2N$ may be the same so $2N$ is the upper limit). Since the FLN is quenched, the initial configurations will remain the same throughout the whole dynamic process. So the state space remains the same, which are all the possible iterations of $2N$ values on a $N \times 1$ vector space. Thus the state space includes maximally $(2N)^N$ different vectors.

After $(2N)^N$ updates at most, the network must have reached a state where it has already visited. So the network must have limit cycles or attractors.

This property is only valid for the quenched network using the Max-Min logical function. If other types of logical functions (GC, MV or Probabilistic shown in Table I) are used, then the network cannot be guaranteed to reach exact limit cycles or attractors. Take GC logical function as an example. A simple two variable network, $\{x_t^1, x_t^2\}$, has the following update rules.

$$\begin{aligned} x_{t+1}^1 &= x_t^1 \wedge x_t^2 \\ x_{t+1}^2 &= x_t^2 \end{aligned}$$

Suppose the initial value is $\{x_1^1 = 0.2, x_1^2 = 0.5\}$, then the network will evolve through the following states:

$$(0.2, 0.5) \rightarrow (0.2 \times 0.5, 0.5) \rightarrow \dots (0.2 \times 0.5^i, 0.5) \dots$$

As can be seen, it will never reach a previously visited state because the value of the first variable at the current time is always different from any of its ancestors. However, one trend can be seen is that although some FLNs will not reach the exact steady state, the network can be thought as reaching a pseudo-steady state asymptotically. In this example, the pseudo steady state is $(0, 0.5)$. However, the convergence properties of FLNs based on different logical functions are unknown. We have found that given a precision, all FLNs we simulated converged. Fig.1 shows examples of convergence based on the four logical functions shown in Table I.

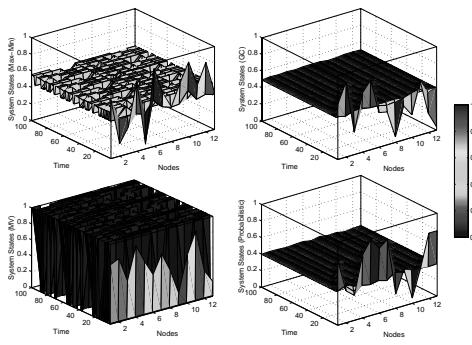


Figure 1. The selected convergence phenomena of FLNs based on the four logical functions: Max-Min, GC, MV, and Probabilistic. The x-axis represents the numerically-numbered nodes in the system. There are 13 nodes in all four sub-figures. The systems were simulated for 100 updates (y-axis). The z-axis represents the states of the system after each update. The initial values were randomly selected.

As can be seen, the convergence speed and the steady-states of the four logical functions are different. The phenomena are further illustrated in section IV.

Theorem 2: For a quenched FLN using the Max-Min logical function, the values of all variables at the end of the process has a lower bound of $\min\{x_1^1, 1-x_1^1, x_1^2, 1-x_1^2 \dots, x_1^N, 1-x_1^N\}$ and an upper bound of $\max\{x_1^1, 1-x_1^1, x_1^2, 1-x_1^2 \dots, x_1^N, 1-x_1^N\}$

Proof:

Suppose at time t , the system reaches steady state. Then for $\forall x_t^i$, we can trace it back to the initial configurations due to the quenched property,

$$x_t^i = f_i(x_{t-1}^{i_1}, x_{t-1}^{i_2}, \dots, x_{t-1}^{i_K})$$

$$x_{t-1}^{i_j} = f_{i_j}(x_{t-2}^{p_1}, x_{t-2}^{p_2}, \dots, x_{t-2}^{p_K}), \text{ where } 1 \leq j \leq K$$

⋮

After t steps of tracing back, we trace the value of x_t^i as the composite of K^t membership functions applied on the initial conditions. For any Max-Min logical function, it can be decomposed as the conjunction of disjunctions (the same as minterm presentations in Boolean logic). Since the Max-Min logical function preserves its initial values, so each disjunction preserves its input values. From the definition of composite functions, the composite of those disjunctions will also preserve input values. Thus we have proved that the initial values will be channeled to the steady state.

So the values of all variables at the end of the process have a lower bound of $\min\{x_1^1, 1-x_1^1, x_1^2, 1-x_1^2 \dots, x_1^N, 1-x_1^N\}$ and an upper bound of $\max\{x_1^1, 1-x_1^1, x_1^2, 1-x_1^2 \dots, x_1^N, 1-x_1^N\}$.

III. SIMULATIONS

To study how the FLN evolves according to different number of nodes and different functions, the convergence property of the FLN was simulated. We have focused on two parameters

that govern the stability and convergence speed of the FLN: the length of limit cycles and the number of updates before reaching a limit cycle. The number of updates is a measurement of how the system converges and with what speed. The length of limit cycles shows the steady-state behavior of the system as well as its stability. If the number of limit cycles appears to follow the power law, then the system is believed to be on the edge of chaos [19]. The simulation algorithm is illustrated as follows.

Input: N (number of variables), $MaxUpdates$ (Maximum number of iterations allowed), δ (Precision of the Hamming distance)

Output: $Length$ (limit cycle length), $NumUpdates$ (the number of updates before reaching the steady state)

Algorithm 1

Randomly generate initial values for $\bar{X}_1 = [x_1^1, x_1^2, \dots, x_1^N]$

Apply algorithm 1.1 to randomly generate $\bar{F} = [f_1, f_2, \dots, f_N]$

$L=0$

FOR $i = 1 \rightarrow MaxUpdates$

COMPUTE $\bar{X}_{i+1} = [x_{i+1}^1, x_{i+1}^2, \dots, x_{i+1}^N]$

$$x_{i+1}^j = f_j(x_i^1, x_i^2, \dots, x_i^{j-1}, x_i^{j+1}, x_i^N)$$

$$\text{where } = OR_{w=1 \rightarrow L_j} (AND_{q=1 \rightarrow (N-1)} (f_j(w, q) \times x_d + (1 - f_j(w, q)) \times (1 - x_d)))$$

$j=1 \rightarrow N$ and $d=1, 2, \dots, j-1, j+1, \dots, N$

FOR $p = 1 \rightarrow i$

COMPUTE

$$Difference(i+1, p) = \| \bar{X}_{i+1} - \bar{X}_p \| = \sum_{k=1}^N H(x_{i+1}^k, x_p^k)$$

$$H(x_{i+1}^k, x_p^k) = \begin{cases} 1, & \text{if } |x_{i+1}^k - x_p^k| \geq \delta \\ 0, & \text{if } |x_{i+1}^k - x_p^k| < \delta \end{cases}$$

IF $Difference(i+1, p) == 0$,

THEN $L = i + 2 - p$, BREAK

END FOR

END FOR

$Length = \max(L, 0)$

$NumUpdates = \min(p, MaxUpdates)$

Algorithm 1.1

Input: N (number of variables)

Output: $\bar{F} = [f_1, f_2, \dots, f_N]$ (function vector, where f_j is $(N-1) \times L_j$)

FOR $m = 1 \rightarrow N$

```

 $l = 1$ 
Random generate  $\vec{S} = \{s_i\}_{1 \times 2^{N-1}}$ ,  $s_i = \{0,1\}$ 
FOR  $i = 1 \rightarrow 2^{N-1}$ 
  IF  $s_i == 1$ 
    THEN  $B = \text{binary}(i)_{1 \times N-1}$ ,  $f_j(t, l) = B(t)$ 
     $t = 1 \rightarrow N-1$ ,  $l = l + 1$ 
  END FOR
   $L_j = l$ 
END FOR

```

In the simulations presented in section IV, uniform random number generator was used. The number of nodes in a FLN was limited to be no more than 13. The precision used to compute the Hamming distance was 0.0001. The maximum number of iterations was 100.

IV. RESULTS AND DISCUSSIONS

The algorithm was implemented with the number of nodes in the FLNs ranging from 2 to 13. All four logical functions in Table I were tested. Firstly, the number of updates a FLN needs to reach limit cycles is shown in Fig. 2.

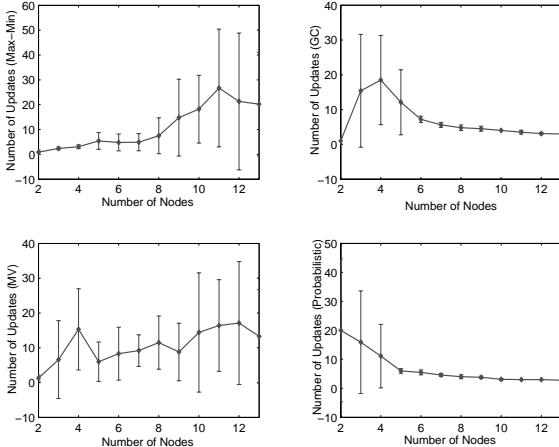


Figure 2. The average number of updates before randomly generated FLNs reach limit cycles or attractors. The logical functions tested were Max-Min, GC, MV, and Probabilistic. The x-axis shows the number of nodes in the randomly generated FLN, and the y-axis shows the average number of updates before the FLN reaches limit cycles. The average number of updates was computed as the mean of 10 simulations. The variations among the 10 simulations were also presented as error bars in the figures.

As can be seen, the number of updates required for GC and Probabilistic logic functions declines rapidly after the number of nodes reaches 6. However, Max-Min and MV logical functions' convergence speed slows down if there are more nodes in the network. The trend of variations on the number of updates in Max-Min and MV logical functions also confirms that systems using these two logical functions are becoming more unstable for a large number of variables.

Another important measurement on FLN's stability is the length of limit cycles. If the length of limit cycles has greater variations as the number of nodes increases, then the system's

stability is weakening because the possible outcomes of system behaviors are more diverse. As expected, the Max-Min and MV logical functions have a greater variety of cycle lengths as the system possess more nodes while GC and Probabilistic do not (Fig. 3).

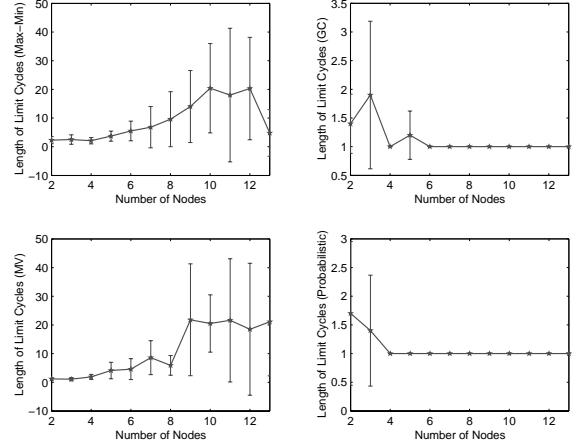


Figure 3. The average length of limit cycles for randomly generated FLNs. The logical functions tested were Max-Min, GC, MV, and Probabilistic. The x-axis shows the number of nodes in the randomly generated FLN, and the y-axis shows the average length of limit cycles. The average number was computed as the mean of 10 simulations. The variations of the 10 simulations were also presented as error bars in the figures.

As shown in Fig. 3, when the number of variables is greater than 6, GC and Probabilistic logical functions always reach the steady states in the form of attractors. The Max-Min and MV logical functions have limit cycles with a wide range of lengths.

It is believed that a fit network should be on the edge of chaos when it is applied to infer gene regulatory network. It has been found that inference results using the MV logical function did not introduce as many false positives as that from using other commonly used fuzzy logical functions. Furthermore, MV logical function causes the algorithm to be less sensitive to small variations of δ . These properties help to reduce the effects of noise from the microarray data [14]. The simulation results in this paper confirm that MV logical function indeed can generate a general chaotic phenomenon.

V. CONCLUSIONS AND DISCUSSIONS

In this work, the focus was on the convergence and stability of a randomly generated FLN. The simulation results not only show the properties of different logical functions, but also confirm the assumption that the MV logical function is fit for inferring gene regulatory networks.

Regarding future research on the theoretical aspects of the FLN, we think that the dynamics and the steady-state properties of the FLN should be mathematically deduced. Furthermore, the time invariant constraint on the selection of fuzzy logical functions should be extended to be time variant in order to infer more accurate and more realistic complex networks.

REFERENCES

- [1] S. Strogatz, "Exploring complex networks," *Nature*, vol. 410, pp. 268–276, 2001.
- [2] S.A.Kauffman, Origins of order: Self-Organization and selection in evolution, New York, NY: Oxford University Press, 1993.
- [3] C.H. Yuh, H. Bolouri and E.H. Davidson, "Genomic cis-regulatory logic: experimental and computational analysis of a sea urchin gene," *Science*, vol. 279, pp. 1896-1902, 1998.
- [4] T. Akutsu, S. Miyano and S. Kuhara, "Inferring qualitative relations in genetic networks and metabolic pathways," *Bioinformatics*, vol. 16, pp. 727-734, 2000.
- [5] T. Chen, H.L. He, G.M. Church, "Modeling gene expression with differential equations," *Pacific Symposium on Biocomputing*, pp. 29-40, 1999.
- [6] N. Friedman, M. Linial, I. Nachman and D. Pe'er, "Using Bayesian network to analyze expression data," *Journal of Computational Biology*, vol. 7, pp. 601-620, 2000.
- [7] D. Sprinzak and M.B. Elowitz, "Reconstruction of genetic circuits," *Nature*, vol. 438, no. 24, 2005.
- [8] Z.B. Joseph, "Analyzing time series gene expression data," *Bioinformatics*, vol. 20, pp. 2493-2503, 2004.
- [9] P.J. Woolf and Y. Wang, "A fuzzy logic approach to analyzing gene expression data," *Physiological Genomics*, vol.3, pp. 9- 15, 2000.
- [10] B.A. Sokhansanj, J.P. Fitch, J.N. Quong and A.A. Quong, "Linear fuzzy gene network models obtained from microarray data by exhaustive search," *BMC Bioinformatics*, vol. 5, no. 108, 2004.
- [11] Y. Cao, P.P. Wang and A. Tokuta, Gene Regulating Network Discovery Studies in Computational Intelligence, Verlag: Springer, vol. 5, pp. 49-78, Jul 2005.
- [12] Y. Cao, P.P. Wang and A. Tokuta, "A study of two gene network - the simplest special case of SORE (Self Organizable & Regulating Engine)," Proc. of 7th JCIS joint conference, pp. 1716-1720, 2003.
- [13] P.P. Wang, Y. Cao and A. Tokuta, "SORE - an example of a possible building block for a 'Biologizing' control system," in *Proc. 4th International Symposium on Intelligent Manufacturing Systems*, Sajarya, Turkey, May 2006, pp. 42-48.
- [14] Y. Cao, P. Wang, and A. Tokuta, "*S. pombe* regulatory network construction using the fuzzy logic network," Poster, LSS Computational Systems Bioinformatics Conference, Stanford University, August 2006.
- [15] G. Resconi, Y. Cao, and P. Wang, "Fuzzy biology," in *Proc. 5th International Symposium on Intelligent Manufacturing Systems*, Sajarya, Turkey, May 2006, pp. 29-31.
- [16] Y. Cao, P. Wang, and A. Tokuta, *Gene regulatory network modeling: a data driven approach*, ser. Fuzzy Logic - A Spectrum of Theoretical & Practical Issues. Springer-Verlag GmbH, accepted, to appear in 2007.
- [17] C.A. Reiter, "Fuzzy Automata and Life," *Complexity*, vol. 7, no. 3, pp. 19-29, 2002.
- [18] Z. Somogyvari and S. Payrits, "Length of state cycles in random Boolean networks: an analytical study," *Journal of Physics*, vol. 33, pp. 6699-6706, 2000.
- [19] R. Sole and B. Luque, "Phase transitions and anti-chaos in generalized Kauffman networks," *Physical letters A*, vol. 196, pp. 331-334, 1996.

Extending Ad hoc Network range using CSMA(CD) parameter optimization

Adeel Akram, Shahbaz Pervez, Shoab A. Khan

University of Engineering and Technology, Taxila, Pakistan.

Email: {adeel, shahbaz, shoab}@uettaxila.edu.pk

Abstract—In this paper we present an optimal combination of various key factors in CSMA(CD) that affect the performance of 802.11 ad hoc networks for outdoor long range communication. These factor not only improve performance but also help in extending the possible range of connection.

Keywords; 802.11, Outdoor Communication, CSMA(CD), Multimedia over Ad hoc

I. INTRODUCTION

The 802.11 standard was originally designed to provide indoor communication. Its main focus was to provide low cost solution to small office SOHO LAN deployment with allowance of mobility for client nodes.

With the passage of time, the technology has matured and much work has been done on improvement in standard and removal of shortcomings of 802.11 Protocol.

Today's work requirements especially in educational campus like setups emphasize on deployment of 802.11 based networks for Outdoor use. Students and faculty members can roam around the various buildings but still want to get connectivity with their Office/LAN network.

Outdoor deployment of 802.11 was limited by inherent problems in the design of the standard. In outdoor deployment, timeouts and retries were encountered frequently, which caused instability and poor reliability. Specifically, extending the range of 802.11 devices with antennas and amplifiers has its limitations at the communications level.

As 802.11 medium access control is carried out by CSMA-CD, A device does not transmit when it senses any other devices transmitting on the channel. Occasionally, two or more devices may try to send packets at the same time. In order to prevent collision between simultaneous uses of the medium, "CTS" (Clear-To-Send) is used to signal to one of the sender that the receiver is ready to receive.

In long range communication, when distances are extended between two points, the packets have to travel a longer distance. The longer distance leads to an increase in transit time and therefore the packets may not reach the other end within the timeout window.

For long-range applications using the 802.11 standard, CTS has to be increased to prevent timeouts.

During normal communication over 802.11 networks, "ACK" (Acknowledgement) packets are sent from sender to receiver, and a time limit is set for obtaining a reply, failing which the sender assumes packet loss and resends. An ACK timeout of

20 μ sec is defined for 802.11b and 9 μ sec is defined for 802.11a/g standards by IEEE.

Under the 802.11 standards, packets are retransmitted if ACK is not received within the allowed timeout duration.

Continuous loss of ACK packets leads to network instability and poor reliability.

Furthermore collisions in the medium will cause the sender to wait a certain amount of time before retransmitting. This is known as the "slot-time". The sender is informed of collision by other device on the network, and the time taken to do so is added to calculate the slot-time. In long-range applications, the slot time has to be increased in order to prevent further collisions due to timeouts.

Following are the key factors that inhibit the performance of 802.11 devices:

- ACK timeout was too small to work correctly over long distance links.
- The contention window slot-time needed to be increased to adapt to the longer distances.
- CTS timeout values must be increased to allow longer distance communication

II. EXPERIMENTAL SCENARIO:

We deployed an 802.11b outdoor access point with 16db directional antenna at one end, while on the other end we used a Laptop with Atheros chipset and 802.11b compliant (HP IPAQ 6365) PDAs (Figure 1) with internal antennas to make an ad hoc network.

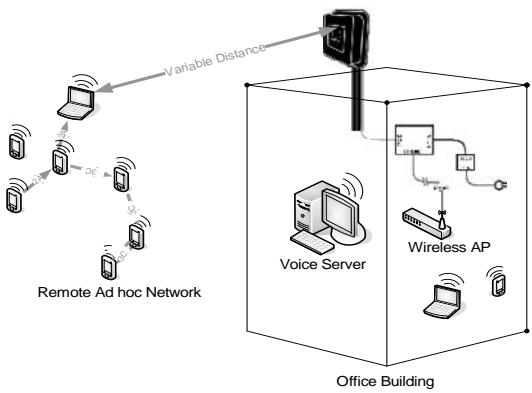


Figure 1. A roof top outdoor access point with directional Antenna was setup at the office building to communicate with a variable distance ad hoc network. The setup equipment used Atheros Chipset that allows modification of key CSMA(CD) performance parameters to enhance the distance between the two communicating peers.

We ensured that the Laptop and the roof top access point have clear line of sight connectivity.

We increased the distance between the two communicating devices and varied the slot time, ACK time and CTS timeout values for best performance. We started with the values specified by the IEEE 802.11 standard. According to the standard, the default values of Slot time, ACK Time and CTS Timeout are 9, 18 and 18 μ sec respectively. We increased the distance between the transmitter AP and the receiving laptop in increments of 20 meters. The values provided by the standard worked perfectly till the 90 meter mark after which the connectivity deteriorates significantly. We then started to increase the values of Slot Time, ACK Time and CTS Timeout gradually to find suitable combination for these values.

The following table shows these values according to distance variation (Table 1).

802.11 CSMA(CD) Parameters variation with Distance			
Distance (meters)	SlotTime (μ sec)	ACKTime (μ sec)	CTSTimeOut (μ sec)
10	9	18	18
30	9	18	18
50	9	18	18
70	9	18	18
90	9	18	18
100	10	23	23
300	11	25	25
600	12	27	27
900	13	29	29
1200	14	31	31
1500	15	33	33
1800	16	35	35
2100	17	37	37
2400	18	39	39

Table 1: Distance vs. 802.11 Parameter values

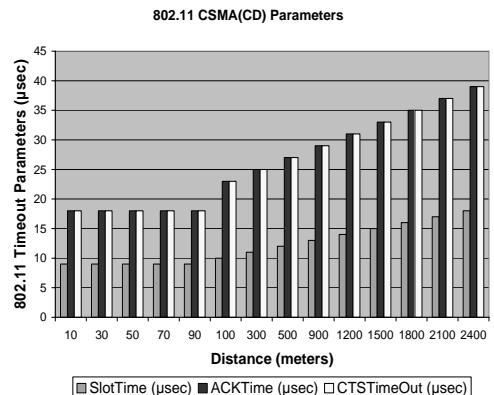
We tested the connectivity as well as voice communication using “Teamtalk” software SDK. The software incorporates a configurable audio encoder that allows reduction of codec complexity for use on less resourceful devices and low bandwidth networks.

The following equations represent the relation of 802.11b Parameter values with the variation of distance.

$$\text{SlotTime} = 8.6802x^6 + 0.0092x^5 - 0.00003x^4$$

$$\text{ACKTime} = 16.6438x^6 + 0.0433x^5 - 0.0001x^4$$

$$\text{CTSTimeOut} = 16.6438x^6 + 0.0433x^5 - 0.0001x^4$$



These values can be further fine tuned to further improve performance according to the environmental conditions. In our case, the values are appropriate for clear line of site communication without any foliage.

To confirm our calculations, we setup a peer to peer ad hoc network at the remote side using the laptop and PDAs. In the office, we connected the outdoor access point to a Wireless router that connects other indoor wireless clients to it using the IEEE 802.11b standard. Using the table parameter values on the laptop, we used the PDAs on remote side to perform voice communication with the Voice Server, Laptop and the PDA in the office building.

III. CONCLUSION

This setup was done as a proof of concept; it would be very useful in connecting different ad hoc networks when the distance between them is too large for small devices to remain in range.

Multiple such setups providing cell like coverage in a particular area can also be used during relief work and military scenarios.

The same parameter values can be used to extend the range of peer to peer ad hoc networks provided the devices have high gain antennas installed on them.

IV. FUTURE WORK

The current setup didn't utilize any QoS support from the network. We are planning to perform the same setup for video communication using QoS.

REFERENCES

- [1] C. Toh, "Ad Hoc Mobile Wireless Networks: Protocols and Systems", PTR Prentice Hall, 2002.
- [2] Lohier et al, "QoS Routing in ad hoc networks", 2002
- [3] Clausen & Jacquet, OLSR; rfc3626, October 2003
- [4] Atheros Chipset and <http://www.atheros.org>
- [5] TeamTalk software SDK provided by <http://www.bearware.dk>
- [6] M. Zorzi, R.R. Rao, L.B. Milstein, "ARQ error control for fading mobile radio channels," IEEE Transactions on Vehicular Technology, Vol. 46, No. 2, pp. 445-455.
- [7] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing protocol," International Multi Topic Conference, Pakistan, 2001.
- [8] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," ACM Computer Communication Review, vol. 24, no. 2, pp.234-244
- [9] C. M. Calafate and M. P. Malumbres, "Testing The H.264 Error Resilience On Wireless Ad-Hoc Networks"
- [10] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva, "The dynamic source routing protocol for mobile ad hoc networks," Internet Draft, MANET Working Group,draft-ietf-manet-dsr-07.txt, February 2002, Work in progress
- [11] Meguerdichian, Farinaz, "Coverage Problems in Wireless Ad-hoc Sensor Networks", Infocom '01

- [12] Mischa Schwartz, "Network Management and Control Issues in Multimedia Wireless Networks," IEEE Personal Communications, Vol. 2, No. 3, June 1995, pp. 8-16

Resource Aware Media Framework for Mobile Ad hoc Networks

Adeel Akram, Shahbaz Pervez, Shoab A. Khan

University of Engineering and Technology, Taxila, Pakistan.

Email: {adeel, shahbaz, shoab}@uettaxila.edu.pk

Abstract—In this paper we present a framework that acts as a distributed media encoder/decoder for real-time multimedia streams. The paper proposes an implementation of a Multimedia encoder/decoder that works by partitioning and distributing various tasks allocated to different stages of the encoder/decoder to different computers having the minimum required capabilities for that task. At the end the combined work by these different nodes creates the actual encoded/decoded multimedia stream. As encoding is a resource hungry process, we divide it into separable stages and perform their tasks on multiple nodes, while decoding is performed on the single intended target device if it is capable to do so. In case of less capable target device, the Middleware can convert the encoded video into a format suitable for the client node.

Keywords: Computation Offloading, Task Partitioning, Time- constrained task scheduling, Multimedia over Ad hoc Networks, OMAP Architecture

I. INTRODUCTION:

With the phenomenal improvements in capability of devices that can become part of Ad hoc networks, the demand for higher level time constrained services such as multimedia and voice communication over ad hoc networks is increasing.

Multimedia transmission over ad hoc network is an application that requires computational resources as well as high throughput network links to provide information rich contents to the receiving nodes in real-time.

Digital Multimedia transmission over Ad hoc network requires encoding of source media in a format that become more resilient to errors and delays due to the intermittent jitters in transmission due to route changes or link failures. Moreover as the intermediate nodes in an Ad hoc network act as repeaters to forward multimedia packets towards the destination nodes, the probability of failure increases with the increase in the number of intermediate nodes.

II. PROBLEM DEFINITION:

As multimedia scheduling is a multi-objective and constrained problem with all its known difficulties, the our objective is to minimize the complexity of the scenario ensuring delivery of contents to the desired target node in a bounded time frame as imposed by the multimedia traffic constraints.

The understanding of actual scenario is the first step towards the solution of this complex real world problem.

A. System Scenario

Consider a wireless ad hoc network composed of mobile nodes that utilize the OMAP (Open Multimedia Applications Platform) architecture.

For the sake of simplicity we assume that all mobile nodes have same capabilities and characteristics. Each mobile node is equipped with a camera, a low-power microprocessor, and 802.11b WiFi Network Interface Cards that allows these nodes to communicate over the wireless channel.

As OMAP is software and hardware architecture that enables multimedia applications in third-generation (3G) wireless appliances, it is targeted for superior performance in Video and Speech Processing Applications.

In our experiments, we have used iPAQ6365 PDAs that are equipped with TI OMAP 1510 Rev 2. It utilized a Dual-core processor architecture optimized for efficient operating system and multimedia code execution.

The TMS320C55x DSP core performs the multimedia and other signal processing related tasks while utilizing lowest system-level power consumption.

The TI-enhanced ARM™ 925 core with an added LCD frame buffer runs command and control functions and user interface applications.

Performance of the Multimedia algorithms is usually measured in Mcycles/s, defined as the frequency at which

the core must run to sustain real-time speech coding and decoding. The DSP Core of OMAP 1510 can achieve upto 200 Mcycles/s.

Task Type	ARM 9E	S.ARM 1100	TMS320 C5510	Units
MPEG4/H.263 Decoding (QCIF @ 15 fps)	33	34	17	Mcycles/s
MPEG4/H.263 Encoding QCIF @ 15 fps	179	153	41	Mcycles/s
JPEG Decoding (QCIF)	2.1	2.06	1.2	Mcycles/s
MP3 Decoding	19	20	17	Mcycles/s
Echo Cancellation 16 bits (32 ms - 8 kHz)	24	39	4	Mcycles/s
Echo Cancellation 32 bits (32 ms - 8 kHz)	37	41	15	Mcycles/s
Avg. Cycle Ratio with TMS320C5510	3.09	3.04	1	

Table 1: Shows the performance comparison of OMAP architecture's TMS320C5510 DSP Core with currently available RISC processors designed for PDAs.

Various video encoding algorithms have been devised according to different hardware resources. e.g. H.261 is an audio/video codec for low quality online video conferencing and/or online chatting with voice and/or video. H.263 / i263 is an audio/video codec for medium quality online video conferencing and/or online chatting with voice and/or video.

H.264 is an MPEG4 Advanced Video codec, also known as MPEG4 part 10, H.26L, or AVC. This codec has excellent compression with an excellent picture quality and is supposed to be a universal video codec. H.323 is an ITU-T standard for transferring multimedia videoconferencing data over packet-switched networks, such as TCP/IP.

The complexity and hardware resource requirements increase with the enhancement in quality of video/audio in these Codecs.

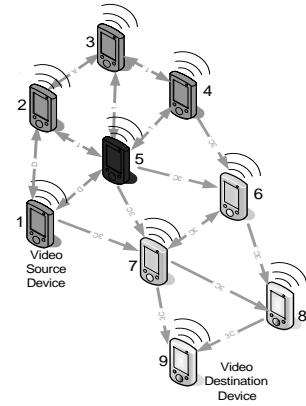


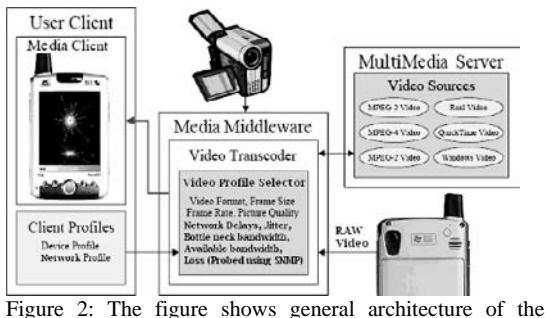
Figure1: Resource Aware Media Framework dedicates various Ad hoc nodes for specific tasks. Node 1 is the video source node. The devices 1 to 4 are acting as computation sharing nodes while node 5 is acting as consolidator node. Nodes 6 and 7 act as relay nodes

B. Communication Procedure

- When node 1 wants to initiate a multimedia transfer, it sends a RREQ packet to all the neighboring nodes with destination as node 9.
- Each neighboring node provides its relative distance (hops) from node 1 and node 9 in their RREP packets.
- Source Node (1) sends a special broadcast packet AROL to all nodes. AROL packet contains list of all nodes that will participate in the communication with their Assigned ROles during this process i.e 1=Compute, 2=Consolidator, 3=MDRelay, 4=Source, 5=Destination
- In case of failure or removal of a node from the network at any time, the Source node (1) sends an AROL broadcast packet to all the nodes to inform them about the Change of ROLE of node(s).
- In case of low battery or overload, any node can send a RROL packet to the source node to Request a Role change.
- The option of assignment of “AROL 1” depends on the availability and available computational resources of the nodes closest to the source node.
- In the presence of any High Performance Computers in this ad hoc network, the Assign Role “AROL 2” packet is preferred to be sent to such node. Moreover the source node can also assign “Consolidation” role to more than one node, if no node is capable of performing that task individually.

- The “AROL 3” is preferred to be assigned to nodes that are closer to the consolidator(s) and to the Destination node.
- Each node on receiving the AROL packet with its address in it sends a Role acknowledgement packet RACK to the source node to announce that it has assumed its Role.
- The Source node (1) sends a JDES packet which provides Description of the Job to be handled by all participating nodes.
- JDES packet provides parameters such as Video Codec Type, Frame Format, Bit Rate etc. specific to that transmission
- Source node sends RAW frames to the “Compute” nodes (1 to 4 in example scenario). These nodes compress / encode the source frame in the format described in the JDES packet and send them to the “Consolidator” node(s).
- The “Consolidator” node (5 in example) assembles the encoded frames according the the video format and forwards them to the “MDRelay” nodes. MDRelay nodes can also share their loads in case of network congestion or overload.
- The Destination node provides feedback on the Quality of stream being received at its end through the reverse path to the source node. This Feedback packet FBCK provides essential information to be used by the Framework for improvement of quality of the ongoing stream at realtime. FBCK packet also provides the source with the information of how much information has been received by the destination node.
- When the source receives acknowledgements of all intended information from the destination, it sends a Transmission End TEND broadcast packet to the participating nodes.
- The participating nodes clear their roles and go into idle mode until the next transmission.

C. Media Framework



Media Framework for complete end to end video transmission and reception over ad hoc network.

The framework is divided into three distinct blocks:

- Media Source Components
- Video Middleware (Transcoder)
- Media Destination Components

The Media Source Components can be a PDA transmitting RAW video frames from camera or a video streaming source that has high bit rate or a video source that uses a video format that is not decodable by the receiver node or requires too much computation by an ordinary ad hoc receiver node. In figure 1, node 1 is the Media source.

The Video Middleware is a modular transcoder that is capable of conversion of video formats in real time. The important thing in the design of this transcoder is that it can work in distributed fashion over different groups of ad hoc nodes to maximize its performance. Middleware Transcoder is capable of selecting appropriate video profile to suit the resource constraints of the target node.

All nodes have Middleware and Client Components installed on them. But the selection of a node to act as a Middleware node depends on its Device and Network Profiles. If a device is has sufficient resources and network bandwidth, it is considered to be capable of becoming a middleware node. In figure 1 the nodes 1 to 4 are sharing the Video Middleware load.

The Media Destination Components are the clients that are part of the ad hoc network which are capable of communicating with the Media framework through the User Client component of the Framework. The Client component creates the Device’s Resource Profile and Network Profile that helps in selection of any device as Middleware node as well. Node 9 in figure 1 is the Destination node running the Multimedia client software.

The Framework identifies all the nodes that are part of the ad hoc network, and try to map different stages of the Framework on different sets of nodes called groups. The number of nodes in a group depends upon the abilities (availability of resources) of nodes. Each group performs a specific task collaboratively.

In case of Reactive Ad hoc routing protocols, Whenever a Multimedia Transaction is going to start, the communication

procedure is run to assign their respective roles to all devices part of the Multimedia Framework.

In Proactive Ad hoc routing protocol based Ad hoc Networks, the Communication Procedure described above is executed from time to time during the transmission of Routing table update packets. Therefore the Media Framework is always ready for Media Transmission.

III. CONCLUSION:

The Media Framework allows less capability mobile devices to perform computation intensive tasks by following a novel task partitioning algorithm as proposed in this paper. The Algorithm assigns different roles to all nodes participating in the communication.

The result of implementation of Media Framework on Ad hoc nodes is that resource constrained nodes are able to perform complex tasks such as video encoding in real-time by distributing different stages of the process on different nodes. The Media Middleware acts as a distributed collaborative video transcoder to assigned tasks to different nodes.

REFERENCES

- [1] Shunan Lin, Shiwen Mao, Yao Wang, Shivendra Panwar. "A reference picture selection scheme for video transmission over ad-hoc networks using multiple paths"
- [2] Shunan Lin, Shiwen Mao, Yao Wang, Shivendra Panwar. "Video transmission over ad-hoc networks using multiple paths"
- [3] C. M. Calafate and M. P. Malumbres. "Testing The H.264 Error-Resilience On Wireless Ad-Hoc Networks"
- [4] Shiwen Mao, Shunan Lin, Shivendra S. Panwar, Yao Wang, and Emre Celebi. "Video Transport Over Ad Hoc Networks: Multistream Coding With Multipath Transport"
- [5] Shiwen Mao, Dennis Bushmitch, Sathya Narayanan, and Shivendra S. Panwar. "MRTP: A Multi-Flow Realtime Transport Protocol for Ad Hoc Networks"
- [6] Shiwen Mao, Shunan Lin, Shivendra S. Panwar, Yao Wang. "Reliable Transmission of Video over Ad-hoc Networks Using Automatic Repeat-Request and Multi-path Transport"
- [7] "Cross-layer design for video streaming over wireless ad hoc networks."
- [8] Charles E. Perkins and Elizabeth M. Royer, "Ad hoc On-Demand Distance Vector Routing," in Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, February 1999, pp. 9CL100.
- [9] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva, "The dynamic source routing protocol for mobile ad hoc networks," Internet Draft, MANET Working Group,draft-ietf-manet-dsr-07.txt, February 2002, Work in progress.
- [10] V. Park and S. Corson, "Temporally-ordered routing algorithm (TOM) version 1 – functional specification," Internet Draft, MANET Working Group, draft-ietf-manet-tora-spec-03.txt, November 2000, Work in progress.
- [11] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," ACM Computer Communication Review, vol. 24, no. 2, pp.234-244, October 1994.
- [12] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing protocol," International Multi Topic Conference, Pakistan, 2001.
- [13] Burd, T. and Brodersen, R. "Energy Efficient CMOS Microprocessor Design," Proceedings of the Twenty-Eighth Annual Hawaii International Conference on System Sciences; Vol.1; Wailea, HI, Jan. 1995.

Cross-Layer Scheduling of QoS-Aware Multiservice Users in OFDM-Based Wireless Networks

Amoakoh Gyasi-Agyei

Faculty of Sciences, Engineering & Health
Central Queensland University
QLD 4702, Australia, gyasi-agyei@ieee.org

Abstract—Constraint scheduling is a dynamic process of arbitrating between competing users sharing a finite resource. Cross-layer scheduling allows vertical interactions between some protocol layers to optimize system performance. This article proposes a cross-layer scheduling for orthogonal frequency-division multiplexing (OFDM) based wireless networks. The scheduler combines opportunistic communications and link adaptation to serve users with multiple concurrent flows (applications) of different quality of service (QoS) requirements. For each time slot and on each OFDM subcarrier, the scheduler computes a cost function for each flow that depends on a flow's instantaneous link quality and service history. The flow with the least cost on an OFDM subcarrier is assigned the subcarrier, provided no other flow's delay constraint is in violation. The scheme is scalable, optimizes wireless throughput, traffic delay-aware, guarantees minimum service to all active flows, and has low implementation complexity.

Index Terms—Adaptive modulation and coding, constrained optimization, cross-layer RRM, dc-BLOT, wireless scheduling.

I. INTRODUCTION

Quality of service (QoS) provisioning is a versatile feature in multiservice wireless networks, as the multiple applications (services) they support have varying characteristics. Some traffic types (e.g. Email) are more sensitive to transmission errors and data loss than delay, while other traffic types (e.g. packet voice) are more sensitive to delay than errors and data loss. This dictates that the network be designed to provide different types of services to support individual services. Scheduling is one of the mainstream mechanisms for QoS provisioning in multi-user networks. It is a dynamic process of efficiently allocating a finite resource to multiple competing resource users to meet certain network constraints. Relevant network constraints here include maximizing wireless throughput, providing fair service to avoid service starvation to certain users or flows, and guaranteeing that traffic delay constraints are not violated. Cross-layer scheduling is a new paradigm in scheduling whereby vertical interactions between protocol layers are permitted to achieve an optimized system design.

Wireless networks rely on transmission media whose behavior depends on operating radio frequency, spatial position of a wireless user, and the instantaneous time of communications, i.e. spectro-spatio-temporally varying connectivity. This dynamic channel behavior is attributed to multipath signal propagation, user mobility, non-stationary clutter and the length of the wireless communications link.

Multipath signal propagation causes short-term fading (aka fast fading), while non-stationary environmental clutter causes long-term fading (aka slow fading, shadowing or local mean). The length of the communications link, i.e. distance between a transmitter and a receiver, causes path loss (aka large-scale fading or path attenuation). Path loss increases with frequency, distance and environmental clutter. Furthermore, as user population and traffic patterns are randomly varying, so is the network topology, and more so for infrastructureless networks. Owing to the above factors, multiple users sharing a wireless resource experience asynchronous and independently varying channel qualities: some users experience poor channels while others experience good channels at a given time. This is referred to as multi-user diversity [1], [2], the basis of opportunistic communications. The origin of opportunistic communications is attributed to the works in [1], [3]. Opportunistic scheduling is a channel-aware scheduling which exploits multi-user diversity to maximize the total system throughput (sum network capacity) [4], [2], [6], [7].

Orthogonal Frequency-Division Multiplexing (OFDM) [8] is a multicarrier transmission technique which divides a wideband channel into several equally spaced orthogonal narrowband subchannels in order to support a high data rate on otherwise a frequency-selective fading channel. An OFDM based network lends itself readily to OS as the frequency-selectivity and spatial-selectivity of its multiple channels increase the degrees of freedom in multi-user diversity compared to single-carrier networks. As its name suggests, a composite OFDM symbol is composed of several subsymbols multiplexed together, each of which is modulated onto an independent radio frequency carrier (precisely, an OFDM subcarrier). Each OFDM subsymbol (or set of subsymbols) can contain independent information and hence be used by different users or flows.

This article proposes a scheduling algorithm for OFDM based wireless networks. The algorithm considers the interplay between wireless channel dynamics due to multipath signal propagation (or fading) and user mobility and queuing dynamics arising from heterogeneous traffic of different QoS demands. The scheme is scalable, optimizes wireless throughput, respects traffic delay constraints, guarantees minimum service to all active flows, and has low implementation complexity. According to the classification of radio resource management (RRM) algorithms in [6],

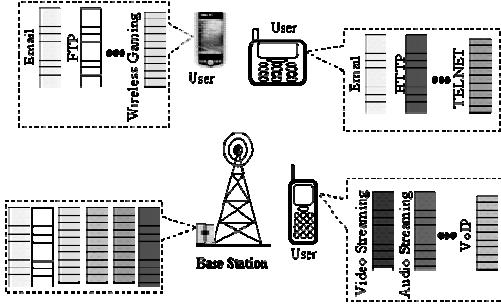


Fig. 1. Multi-user system serving users with multiple concurrent services of varying QoS requirements.

this article engages on Type IV resource allocation scheme. The proposed scheme is a direct consequence of OCASD [2] and BLOT [6]. While OCASD and BLOT serves single-carrier systems, this work considers multicarrier systems. Also BLOT serves only non-real-time traffic, and its performance was not studied analytically, but by simulations.

II. NETWORK MODEL

We consider a time-slotted wireless networks using an orthogonal frequency-division multiplexing/multiple access (OFDM/OFDMA) air interface with a base station (BS) serving multiple mobile users concurrently (Fig. 1). We refer to the discrete-time interval $[t, t+1]$, $t=0,1,2,\dots$ as time slot t . The star network topology adopted in this work can represent a cell of a cellular wireless network, or the interface between multiple stations and a relay station in infrastructureless wireless networks [9]. Each user can maintain multiple queues of different applications simultaneously. Packets in each queue have the same delay requirements and hence are managed by the first-in first-out (FIFO) principle. However, in times of buffer overflow, packets are discarded from a queue according to the random early discard [10] principle to prevent the occurrence of global synchronization [10], [11]. Each of the multiple queues active at a user has different QoS or delay requirements. Table I defines key parameters used in the algorithm described herein.

In each time slot the scheduler serves a user/queue pair (referred to as *flow* and denoted by $F_{i,m}$ which minimizes a cost function $f(R_m(t), B_{im}(t))$ subject to traffic QoS constraints. Hence, each OFDM subcarrier is assigned to only a single flow in a given time slot. A fundamental challenge in such a system is how the BS can serve the system to achieve both flow-level and user-level fairness on a time-varying and random wireless channel, while meeting an individual flow's quality-of-service requirements and still use the radio resource optimally. The architecture in Fig. 1 explores all these issues to serve multiple real-time flows with delay constraints and non-real-time flows without delay constraints. For example, each user can maintain concurrently one or more sessions comprising of a streaming video, streaming audio, wireless

TABLE I NOTATION

Parameter	Meaning
t	Time slot or instantaneous time
t_c	Scheduling time frame for short-term fairness
m	User index, $m = 1, 2, \dots, M$
i	Traffic class or queue index, $I = 1, 2, \dots, I$
F_{im}	Flow index, i.e. traffic class i at user m
W	Wideband wireless channel bandwidth
K	Number of OFDM subcarriers in the system
$K_{im}(t)$	Number of OFDM tones assigned to flow F_{im}
$L_{im}(t)$	Size of the head-of-line (HOL) packet in queue F_{im}
K_{im}^{max}	Number of tones needed by HOL packet of flow F_{im}
$R_{mk}(t)$	Maximum data rate on user m 's k th OFDM subchannel
$B_{im}(t)$	Average amount of traffic scheduled from queue F_{im}
$D_{im}(t)$	Queuing delay of HOL packet in flow F_{im} 's queue
$D_{max,i}$	Maximum queuing delay of packets of traffic class i

Internet gaming, packet voice (VoIP), Email, file transfer, Web browsing and telnetting, and still expects a guaranteed minimum service for each of these active flows.

A. Link Layer Model

We consider a wideband wireless channel disturbed by an additive white Gaussian noise (AWGN) and a frequency-selective Rayleigh fading. However, in accordance with the OFDM philosophy, we assume that the wideband channel is so partitioned into subchannels that each OFDM subchannel is approximately liable to flat fading. Let B_c be the coherence bandwidth of the wideband channel of width W Hz and K be the number of OFDM subcarriers in the system. If K is chosen such that $\Delta f = W/K < B_c$ then each of the OFDM subchannels experiences approximately a flat fading. This is one of the key motivations behind OFDM transmission. If K_x^t is the set of OFDM subcarriers allocated to flow x at time t then

$$K_l^t \cap K_j^t = \emptyset, \forall l \neq j \text{ and } \sum_n K_n^t \leq K \quad (1)$$

Assume that both flows l and j are active at a given user, say m , at the same time t , and $K_l^t, K_j^t \notin \{\emptyset\}$. This requires user m to serve two independent flows between itself and two different receivers at the same time. Can a single antenna at user m be used to accomplish this? Or, multiple antennas are required? This is where MIMO technology becomes necessary. Precisely, a MIMO system which uses different elements of an antenna array to transmit different signals. However, this article does not explore MIMO issues further.

Assume that the physical layer uses multi-level quadrature amplitude modulation (M-QAM) and two-dimensional Gray encoding with perfect carrier and clock recovery circuits. Under such an environment the average BER, the average signal-to-interference plus noise ratio ($\bar{\gamma}_{m,k}$) of user m 's k th OFDM subchannel and the M-QAM constellation size M relate approximately as $\bar{\gamma}_{m,k} \approx 2(M-1) \cdot (0.2/\overline{BER}_{m,k}-1)/3$

[12]. In the following we slightly abuse terminology and replace average values by their corresponding instantaneous values, and approximation by equality, i.e.

$$\gamma_{m,k}(t) = 2(M-1) \cdot (0.2/BER_{m,k}(t) - 1)/3 \quad (2)$$

Hence, the maximum feasible transmission rate on the k th OFDM subchannel at user m at time t is given by the Shannon-Hartley channel capacity theorem as

$$R_{m,k}(t) = W \log_2 (\gamma_{m,k}(t) + 1) \\ = \frac{W}{K} \log_2 \left[1 + \frac{2(M-1)}{3} \left(\frac{0.2}{BER_{m,k}(t)} - 1 \right) \right] \quad (3)$$

For a packet of length L_{im} with independent bit errors the bit-error rate $BER_{m,k}(t)$ relates to the corresponding instantaneous packet error rate as $BER_{m,k}(t) = 1 - [1 - PER_{m,k}(t)]^{L_{im}(t)}$.

Wireless channel estimation is an essential mechanism in all channel-aware protocols. Various methods have been proposed to estimate the instantaneous quality of channels of wireless users in the form of signal-to-interference plus noise ratios (SINR) or bit-error rates. The SINR or BER aids in the estimation of the feasible data transmission rate on the channel at a given time. Interested readers may find more information on this topic in e.g. [13], [14], [15], [16].

B. Cross-Layer Scheduling at Layer 2

We want to design a simple resource allocator that guarantees a minimum service to each active flow over a given length of time, maximizes wireless throughput and meets individual flow's delay bounds. Designing such a scheduler is difficult, except by heuristic methods. We define a time-varying cost function which depends on active flows' service history and instantaneous data transmission rate of their corresponding users. This cost function provides only fairness and throughput maximization. To guarantee delay bounds to timing-sensitive traffic we subject the cost function to traffic delay constraints. Fig. 2 shows the protocol layers that communicate vertically in the proposed cross-layer scheduling. The instantaneous wireless channel quality in form of the instantaneous bit-error-rate on each OFDM subcarrier is estimated at the physical layer and fed to the Medium Access Control (MAC) sublayer at Layer 2 (L2) which hosts the scheduler. A traffic delay constraint, $D_{\max,i}(t)$, is precisely known only by the corresponding application that generates it. Hence, these delay bounds are fed to the MAC sublayer from the Application Layer. Just as the delay, the amount of service, $B_{im}(t)$, that each active flow has received so far is communicated from the Application Layer to the MAC layer. Using these three instantaneous parameters, the MAC layer computes a cost function $C_{im}^k(t) = f(B_{im}(t), PER_{m,k}(t))$ for each active flow at the beginning of each time slot. The flow that minimizes the cost function on the given OFDM subcarrier is allocated the corresponding carrier to meet its delay bound of $D_{\max,i}(t)$.

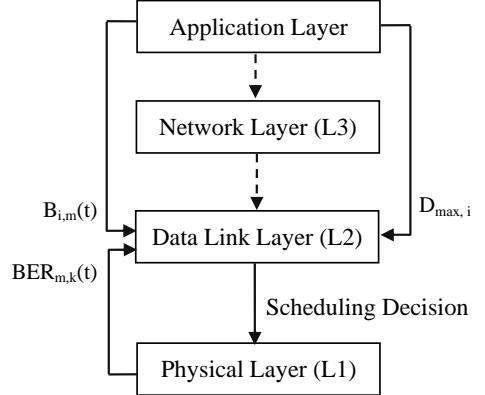


Fig. 2. Protocol interactions in the delay-aware cross-layer scheduling.

For $m=1,2, \dots, M$; $i=1,2,\dots, I$; $k=1,2, \dots, K$ we define the cost function [6]

$$C_{im}^k(t) = \frac{B_{im}^2(t)}{R_{m,k}(t)} = \frac{KB_{im}^2(t)}{W} \log_2 \left[1 + \frac{2(M-1)}{3} \left(\frac{0.2}{BER_{m,k}(t)} - 1 \right) \right] \quad (4)$$

with progression $B_{im}(t+1) = (1 - 1/t_c)B_{im}(t) + 1/t_c J_{im}^k(t)L_{im}(t)$, where $J_{im}^k(t)=1$ if flow F_{im} is scheduled on the k th OFDM subchannel in time slot t , otherwise $J_{im}^k(t)=0$. The resource allocation problem in each time slot t is then

$$\text{Minimize} \quad C_{im}^k(t) \quad (5)$$

$$\text{Subject to} \quad D_{im}(t) \leq D_{\max,i} \quad (6)$$

Thus the scheduler allocates the k th OFDM subchannel to flow F_{im} that fulfils (5) and (6). We note from the delay constraint (6) that the more a flow is delay insensitive the higher its delay bound. Hence, for non-real-time traffic class i we have $D_{\max,i} \rightarrow \infty$. In the following we define the optimization vector $x = [x_1, x_2, x_3]^T \stackrel{\Delta}{=} [B_{im}(t), BER_{m,k}(t), D_{im}(t)]^T$ where T denotes the transposition operator. Hence, $c(x)$ replaces $C_{im}^k(t)$. Also, define $g(x) = D_{im}(t) - D_{\max,i} \leq 0$. The scheduling algorithm is compiled in Table II. We refer to the scheduling algorithm described above as delay-constrained BLOT (dc-BLOT), as it originated from [6] and [2].

III. OPTIMIZATION USING NEURAL NETWORKS

Optimization neural networks are gradient type networks whose behavior can be modeled by analog electrical circuits [17]. The temporal evolution of these neural networks is a motion in the state space whose trajectory follows the direction of the negative gradient of the system's energy function, which can be made equivalent to the cost function to be minimized. The solution of the optimization problem is equivalent to the point of minimum system energy.

Table II Pseudocode for the cross-layer scheduling algorithm

For (int $t=1$; $t \leq t_c$; $t++$)
If $D_{im}(t) \leq D_{i,\max}$
Allocate the best K_{im}^{\max} subcarriers at user m to flow F_{im}
Else
For (int $k=1$; $k \leq K$; $k++$)
For (int $m=1$; $m \leq M$; $m++$)
Estimate BER _{mk} (t)
Compute PER _{mk} (t) = f(BER _{mk} (t))
Evaluate $R_{mk}(t) = f(W, K, \text{PER}_{mk}(t))$
For (int $i=1$; $i \leq I$; $i++$)
Evaluate $U_{im}^k(t)$
End
End
End
Compute $C_{im}^k(t)$ as in (4)
Find flow $(i^*, m^*) = \arg \min_{i,m} C_{im}^k(t)$
Any ties?
No → Allocate OFDM subcarrier k to flow (i^*, m^*)
Yes → Pick a flow among the ties by earliest delay bound violations and allocate OFDM subcarrier k to it until $K_{im}(t) = K_{im}^{\max}$
For all $i=1, 2, \dots, I$ and $m=1, 2, \dots, M$ update $B_{im}(t)$
End
End
End

We use neural networks' techniques to compute the vector $x^* = [B_{im}^*(t), \text{BER}_{mk}^*(t), D_{im}^*(t)]^T$ in each time slot that exploits the limited radio resource in an optimal way. To do this we first need to convert the constrained optimization problem into equivalent system of differential equations. These differential equations constitute the basic neural network algorithms that must be solved to solve the optimization problem in real-time.

The Lagrange function $L : \Re^{n+k} \rightarrow \Re$ for the problem (5)-(6) is

$$L(x, v, \lambda) = c(x) + \lambda(g(x) + v^2) \quad (7)$$

where $\lambda \in \Re^k$, $k=1$ is the Langrangian multiplier. In accordance with their roles in searching for the optimum solution of (5)-(6), v and x are referred to as variable neurons or primal variables while λ is the Langrangian neuron. As the neural network dynamically searches for the optimum solution the variable neurons decrease $L(x, v, \lambda)$ while the Langrange neuron leads the search trajectory into the feasible region $S = \{x | g(x) \leq 0\}$. The Kuhn-Tucker optimality conditions are

$$\begin{aligned} \nabla_x L(x^*, v^*, \lambda^*) &= 0 \\ \nabla_v L(x^*, v^*, \lambda^*) &= 2\lambda^* v^* = 0 \\ \nabla_\lambda L(x^*, v^*, \lambda^*) &= g(x^*) + v^{*2} = 0 \\ \lambda^* &\geq 0 \end{aligned} \quad (8)$$

We want to design an artificial neural network (ANN) with an equilibrium point that fulfills the K-T conditions in (8). By noting that

$$dx_k/dt = -\partial L(x, v, \lambda)/\partial x_k, k = 1, 2, 3 \quad (9)$$

we can formulate the state equations governing the transient behavior of this ANN by the system of equations [18]

$$dx_1/dt = -2bx_1/\log_e[1+a(0.2/x_2-1)]^A = f_1(\tilde{x}) \quad (10)$$

$$dx_2/dt = -abx_1^2/[5x_2(0.2a+x_2-ax_2)]^A = f_2(\tilde{x}) \quad (11)$$

$$\cdot \log_e^2(1-a+0.2a/x_2)]^A = f_3(\tilde{x}) \quad (12)$$

$$dx_3/dt = -\lambda^A = f_4(\tilde{x}) \quad (13)$$

$$d\lambda/dt = \nabla_\lambda L(x, v, \lambda) = g(x) + v^2 = f_5(\tilde{x}) \quad (14)$$

where $\tilde{x} = (x^T, v, \lambda)^T$, $b = K \log_e 2/W$, $a = 2(M-1)/3$. A physically stable neural network has the equilibrium point x^* satisfying $d\tilde{x}_k/dt|_{\tilde{x}=\tilde{x}^*} = 0$ which are equivalent to the Kuhn-Tucker sufficient conditions for optimality, (8). Hence, the state equations of the neural network, (10)–(14), are referred to as Lagrange Programming Neural Network [18].

A. Convexity of the Objective Function $c(x)$

In order to apply artificial neural network to solve the optimization problem we need to ensure that $c(x)$ is twice continuous differentiable in x . If $c(x)$ is convex then it is twice continuous differentiable in x . A sufficient condition for $c(x)$ to be convex is that its Hessian matrix is positive semidefinite. From (4) we obtain the Hessian matrix of $c(x)$ as

$$H_x(x) = \nabla_{xx}^2 c(x) = \begin{pmatrix} D_{11} & D_{12} & D_{13} \\ D_{12} & D_{22} & D_{23} \\ D_{13} & D_{23} & D_{33} \end{pmatrix} \quad (15)$$

where

$$D_{31} = D_{13} = D_{23} = D_{32} = D_{33} = 0 \quad (16)$$

$$D_{11} = 2b/\log_e[1+a(0.2/x_2-1)] \quad (17)$$

$$D_{12} = 2abx_1/[5x_2(x_2+0.2a-ax_2)\log_e^2(1-a+0.2a/x_2)] \quad (18)$$

and

$$\begin{aligned} D_{22} &= \frac{abx_1^2}{5x_2^3[1+a(0.2/x_2-1)]\log_e^2(1-a+0.2a/x_2)} \\ &\cdot \left(\frac{2a}{5x_2[1+a(0.2/x_2-1)]\log_e(1-a+0.2a/x_2)} \right. \\ &\left. + \frac{a}{5x_2[1+a(0.2/x_2-1)]} - 2 \right) \end{aligned} \quad (19)$$

Theorem 1: We establish conditions under which $H_c(x)$ is a positive semidefinite matrix. *Proof.* A sufficient condition for $H_c(x)$ to be a positive semidefinite matrix is that the determinants of all its upper-left submatrices are positive. Denote by $\det H_c(k)$ the determinant of the square upper-left submatrix of $H_c(x)$ of size k . Noting that $H_c(x)$ is a symmetric matrix we require that

$$\det H_c(1) = D_{11} \geq 0 \quad (20)$$

$$\det H_c(2) = D_{11}D_{22} - D_{12}^2 \geq 0 \quad (21)$$

$$\det H_c(3) = D_{11}D_{22}D_{33} - D_{11}D_{23}^2 - D_{12}^2D_{33} + 2D_{12}D_{13}D_{23} - D_{13}^2D_{22} \geq 0 \quad (22)$$

The validity of (20) is obvious from (17). Equation (16) obviously yields $\det H_c(3)=0$. Condition (21) is fulfilled if

$$D_{22} = \frac{a}{5x_2[1+a(0.2/x_2-1)]} \left[1 + \frac{2}{\log_e(1-a+0.2a/x_2)} - 2\log_e(1-a+0.2a/x_2) \right] \geq 2 \quad (23)$$

Figure 3 shows that this condition is fulfilled if $x_2(t) > 10^{-7}$. The required BER range is realistic for practical wireless systems. Fig. 3 also shows a plot of $\det H_c(1)$. We observe that $\det H_c(1) > 0$ for all practical BER values. Hence, we have proved that $H_c(x)$ is a positive definite matrix.

Theorem 2: Positive semidefiniteness of $\nabla_{xx}^2 L(x, v, \lambda)$

From (7) we obtain $\nabla_x L(x, v, \lambda) = \nabla c(x) + \lambda^T \nabla g(x)$. By noting that $\nabla g(x) = (0, 0, 1)^T$ we obtain $\nabla_{xx}^2 g(x) = (0, 0, 0)^T$, yielding the Hessian matrix $\nabla_{xx}^2 L(x, v, \lambda) = \nabla_{xx}^2 c(x) = H_c(x)$. Hence, $\nabla_{xx}^2 L(x, v, \lambda) > 0$ if $\rho_m(t) > 3$ dB, as ascertained above.

B. The Lyapunov Function & Stability Test

This section establishes the convergence and hence the stability of the set of differential equations (10)-(14) that represent our optimization problem via Lyapunov's method. Lyapunov stability theory is based on the idea that if some measure of the energy associated with a dynamic system is decreasing, then the system converges to its equilibrium state. To do this we first need to compute a *Lyapunov function*, $V(x) = E(x) - E(x^*) \in C^1$, of the given system, where $E(x)$ is the energy function of the system and x^* is the optimum point in the feasible set being searched for. The system's energy function is a function defined on the state space $S = \{x | g(x) \leq 0\} \subset \mathbb{R}^3$ which is non-increasing along the trajectories and it is bounded from below. Let us define the energy function

$$E(x, v, \lambda) = \frac{1}{2} \|\nabla_x L(x, v, \lambda)\|_2^2 + \frac{1}{2} \|g(x) + v^2\|_2^2 = \frac{1}{2} \|\nabla c(x) + \lambda \nabla g(x)\|_2^2 + \frac{1}{2} \|g(x) + v^2\|_2^2 \quad (24)$$

whereby $\|y\|_2^2 = (\sum_k y_k^2)^{1/2}$ is the L_2 -norm of y . It follows that

$$\frac{dE(x, v, \lambda)}{dt} = \frac{\partial E}{\partial x} \frac{dx}{dt} + \frac{\partial E}{\partial v} \frac{dv}{dt} + \frac{\partial E}{\partial \lambda} \frac{d\lambda}{dt} \quad (25)$$

The system is globally stable in the Lyapunov sense, i.e., the trajectories $x_k(t)$, $k=1,2,3$, $\lambda(t)$ and $v(t)$ converge to stationary points as $t \rightarrow \infty$, if and only if

$$dE/dt = 0 \Rightarrow dx/dt = dv/dt = d\lambda/dt = 0$$

At the stationary point we have $dE/dt|_{x=x^*}=0$. Proving the stability of the system requires us to establish that

$$E(x, v, \lambda) \geq 0 \text{ and } dE(x, v, \lambda)/dt \leq 0 \quad (26)$$

The subsections below prove (26).

Theorem 3: Positive semidefiniteness of $E(x, v, \lambda)$.

Proof. Proving that $E(x, v, \lambda) \geq 0$ is an obvious consequence of its definition. Hence, the Lyapunov function

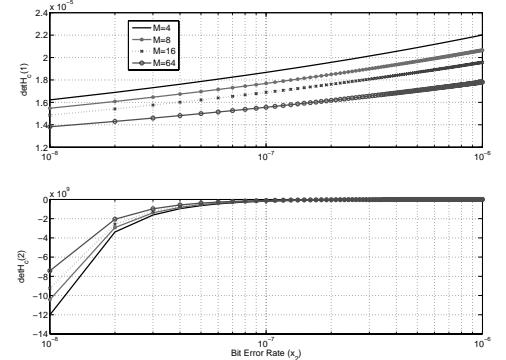


Fig. 3. Plot of $\det H_c(k)$ for $K=1024$, $W=5$ MHz and $x_1=50$ bytes

$V(x, v, \lambda) = E(x, v, \lambda) - E(x^*, v^*, \lambda^*)$ is positive definite.

Theorem 4: We prove that $dE(x, v, \lambda)/dt \leq 0$

Proof. We prove that $E(x, v, \lambda)$ is a bounded monotonically decreasing function of time. Using the state conditions (10)-(14) in (25) yields

$$\begin{aligned} \frac{dE(x, v, \lambda)}{dt} &= [\nabla_x L(x, v, \lambda)^T \nabla_{xx}^2 L(x, v, \lambda) \\ &\quad + v(g(x) + v^2) \frac{d\nu}{dt} + (g(x) + v^2)^T \nabla g(x)] \frac{dx}{dt} \\ &\quad + \nabla_x L(x, v, \lambda)^T \nabla g(x) \frac{d\lambda}{dt} \\ &= -\nabla_x L(x, v, \lambda)^T \nabla_{xx}^2 L(x, v, \lambda) \nabla_x L(x, v, \lambda) \\ &\quad - 2\lambda v^2 (g(x) + v^2) \end{aligned} \quad (27)$$

As $\lambda \geq 0$ and $d^T A d \geq 0$ if $A \geq 0$ for any nonzero vector d , $dE(x, v, \lambda)/dt < 0$ as $\nabla_{xx}^2 L(x, v, \lambda) \geq 0$ has been proved in Theorem 2.

IV. SIMULATION & NUMERICAL RESULTS

We analyze the performance of dc-BLOT with respect to delay violations, stability, system throughput and minimum service guarantees to individual flows active at multiflow users over flat Rayleigh fading channels in this section. We assume that each user can have up to a mixture of three real-time and non-real-time flows active at the same time. Each flow generates a single packet in each time slot and, for the simplicity of comparison all packets have the same size. We apply multivariate fourth-order Runge-Kutta numerical integration method to evaluate the transient behaviors of the state variables describing the neural network for the dynamic system as given in (10)-(14). The fourth-order Runge-Kutta method is reputed for its good accuracy and simplicity. The fourth-order Runge-Kutta method for our multivariate system of differential equations (10)-(14) can be adapted from ([19], p. 326) as

$$\begin{aligned}
a_{k,t} &= h f_k(\tilde{x}_{1,t}, \tilde{x}_{2,t}, \dots, \tilde{x}_{5,t}), k = 1, 2, \dots, 5 \\
b_{k,t} &= h f_k(\tilde{x}_{1,t} + a_{1,t}h/2, \tilde{x}_{2,t} + a_{2,t}h/2, \dots, \tilde{x}_{5,t} + a_{5,t}h/2) \\
c_{k,t} &= h f_k(\tilde{x}_{1,t} + b_{1,t}h/2, \tilde{x}_{2,t} + b_{2,t}h/2, \dots, \tilde{x}_{5,t} + b_{5,t}h/2) \quad (28) \\
d_{k,t} &= h f_k(\tilde{x}_{1,t} + c_{1,t}h, \tilde{x}_{2,t} + c_{2,t}h, \dots, \tilde{x}_{5,t} + c_{5,t}h) \\
\tilde{x}_{k,t+1} &= \tilde{x}_{k,t} + (a_{k,t} + 2b_{k,t} + 2c_{k,t} + d_{k,t})/6
\end{aligned}$$

where $f_k(\tilde{x})$, $k = 1, 2, \dots$ are as given in (10)-(14), respectively.

Fig. 4 shows the effects of inappropriate initial conditions on the transient behaviors of the state variables.

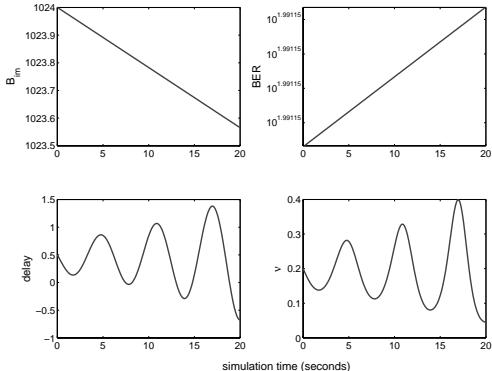


Fig. 4. Transient behaviors of x_1, x_2, x_3 , and x_4 using the initial conditions $x_1(0)=1024$ bits $x_2(0)=10^{-3}$, $x_3(0)=0.5$, $x_4(0)=0.2$, $x_5(0)=0.3$

V. CONCLUSION

This article discusses the problem of delay-constrained cross-layer scheduling in multicarrier multiuser wireless networks to guarantee a minimum service in both flow level and user level. The proposed algorithm is Lyapunov stable for bit error rates higher than 10^{-7} . Hence, it is attractive for multi-service wireless networks. Our future work will extend the proposed scheme to serve both real-time and non-real-time flows in a multiple-input, multiple-output wireless networks.

REFERENCES

- [1] R. Knopp and P. A. Humblet, "Information capacity and power control in single-cell multiuser communications," in Proc. IEEE Int. Conf. on Commun., vol. 1, Seattle, 18-22 June 1995, pp. 331–335.
- [2] A. Gyasi-Agyei, "Multiuser diversity based opportunistic scheduling for wireless data networks," IEEE Commun. Lett., vol. 9, no. 7, July 2005.
- [3] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," IEEE Trans. Inform. Theory, vol. 48, o. 6, pp. 1277–1294, Jun 2002.
- [4] A. Gyasi-Agyei, "BL2xF-channel state-dependent scheduling algorithms for wireless IP networks," in Proc. IEEE Int. Conf. on Networks (ICON'03), Sydney, September 2003, pp. 623–628.
- [5] ——, "OCASD-channel-aware scheduling for multi-service wireless IP networks," in Proc. Australian Telecommunications and Networks Applications Conference (ATNAC), Sydney, December 2004, pp. 582–589. [Online]. Available: <http://www.titr.uow.edu.au/atnac/Proceedings/abstract.pdf>
- [6] A. Gyasi-Agyei and S.-L. Kim, "Cross-layer multiservice opportunistic scheduling for wireless networks," IEEE Commun. Mag., vol. 44, no. 6, June 2006.
- [7] ——, "Comparison of opportunistic scheduling policies in time-slotted AMC wireless networks," in IEEE Int. Symp. on Wir. Pervasive Computing, Phuket, Thailand, Jan. 2006.
- [8] L. Hanzo, M. Munster, B. J. Choi, and T. Keller, OFDM and MC-CDMA for broadband multi-user communications, WLANs and broadcasting. John Wiley & Sons, 2003.
- [9] Q. Liu, X. Wang, and G. B. Giannakis, "A cross-layer scheduling algorithm with QoS support in wireless networks," IEEE Trans. Veh. Techn., vol. 55, no. 3, pp. 839–847, May 2006.
- [10] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," IEEE/ACM Trans. Networking, vol. 1, no. 4, pp. 397–413, August 1993.
- [11] G. R. Arce, K. E. Barner, and L. Ma, "Red gateway congestion control using median queue size estimates," IEEE Trans. on Signal Processing, vol. 51, no. 8, pp. 2149–2164, Aug 2003.
- [12] X. Qiu and K. Chawla, "On the performance of adaptive modulation in cellular systems," IEEE Trans. Commun., vol. 47, no. 6, June 1999.
- [13] C.-S. Yeh and Y. Lin, "Channel estimation using pilot tones in ofdm systems," IEEE Trans. on Broadcasting, vol. 45, no. 4, pp. 400–409, Dec. 1999.
- [14] C. Pandana, Y. Sun, and K. Liu, "Channel-aware priority transmission scheme using joint channel estimation and data loading for ofdm systems," IEEE Trans. on Sig. Proc., vol. 53, no. 8, pp. 3297–3310, August 2005.
- [15] X. Wang and K. Liu, "Model-based channel estimation framework for mimo multicarrier communication systems," IEEE Trans. on Wir. Commun., vol. 4, no. 3, pp. 1050–1063, May 2005.
- [16] X. Wang, P. Ho, and Y. Wu, "Robust channel estimation and isi cancellation for ofdm systems with suppressed features," IEEE JSAC, vol. 23, no. 5, pp. 963–972, May 2005.
- [17] V. Sharma, R. Jha, and R. Naresh, "An augmented lagrange programming optimization neural network for short-term hydroelectric generation scheduling," Engineering Optimization, vol. 37, no. 5, pp. 479–497, July 2005. [Online]. Available: <http://www.tandf.co.uk/journals>
- [18] S. Zhang and A. G. Constantinides, "Lagrange programming neural networks," IEEE Trans. Circuit Syst. II, vol. 39, pp. 441–452, July 1992.
- [19] C.-E. Fröberg, Numerical mathematics: theory and computer applications. Menlo Park, CA: Benjamin/Cummings Publishing Company, Inc., 1985.

Development of a Joystick-based Control for a Differential Drive Robot

A. N. Chand and G. C. Onwubolu

Mechatronics Laboratory, School of Engineering and Physics

University of the South Pacific, Suva, Fiji Islands

chand_an@fit.ac.fj, onwubolu_g@usp.ac.fj

Abstract-The design paradigm of a joystick based control mechanism intended to provide real time control for a differential drive robot built in-house is presented and described in this paper. The novelty of the work reported in this article is the attainment of a full 360-degree of freedom movement of the robot utilizing a low cost joystick while also allowing for a secondary or keyboard mode of control to be implemented.

I. INTRODUCTION

The use of computers and computer-based peripherals in control systems is steadfastly growing and they now form an integral part of most control systems [1]. As such, there are many scientific and engineering applications such as engineering computation and analysis, data acquisition and measurement and most importantly control systems, which are best suited to computers and their associated peripherals. The reason for this is mainly twofold [2]: first, because the Personal Computer (PC) offers un-paralleled processing abilities at remarkable speeds. And secondly, it forms the ideal front-end human machine interface through the use of Graphical User Interfaces (GUIs). Globally, research and usage of control systems using embedded computer systems/peripherals is immense. A common computer peripheral used in robotics is a joystick.

Originally intended for use as a games console, the joystick has now surpassed its customary use and has evolved as a popular choice of control mechanism in many robotic applications. It is now commonly found as the controlling mechanism of wheelchairs, robotic arms and custom-made vehicles and a number of robotic literature make references to joysticks being used in robotic applications [3]. A wireless computer-based vehicle has been developed, which is controlled using a joystick [4]. Elsewhere, a stepper motor and DC motor hybrid controlled robot has been developed and a PC is used for it's controlling purposes while a joystick provides a secondary mode control of the robot [5]. High precision teleoperation control of a robot crane has been achieved through the use of a joystick [6]. The *OmniMate* mobile robot has been developed achieving full omni-directional mobility through the sole use of a joystick [7]. The amount of literature on the use of joysticks in robotic applications is vast: using joystick for controlling a four-legged robot [8], with a similar project discussed by [9] for example. Such is the usefulness and versatility of joysticks that one has even been used to control a humanoid robot [10].

The primary goal of the work reported in this article is to use a low budget-end conventional joystick in providing real time control of an existing differential drive robot [11]. The attainment of such an implementation has the implication of accelerated development of future robots requiring a real time controlling mechanism.

II. DESIGN AND IMPLEMENTATION

A. Design Overview

The conceptual model showing the framework development of the work reported in this paper is presented in Fig. 1. A typical inexpensive, commercial off-the-shelf joystick is used as the input controlling mechanism to translate analogue signals (the operator's actions), into a digital representation through the PC's game port. A computer is a digital machine; therefore those numbers are the language of computers. The joystick gives its digital output as a byte written at the PC's game port. Customized software written in a high level language constantly accesses this port and the current data on it and reads the joy-stick position. The software constantly retrieves the data from the PC's game port, compares it with a reference set of values obtained during calibration phase and makes out meaningful sense of those numbers in deciding what the instantaneous position of the joystick is and then relays appropriate four (4) bit codes to a micro controller resident on the robot via the PC's standard parallel port. The pre-programmed micro controller then carries out the appropriate physical task – the maneuvering direction associated with those instructions. Meanwhile the joystick button is used as the emergency stop or halt command for the robot so that for as long as the button is pressed, the robot will remain stationary. Releasing the button lets the robot resume its path. With this preamble, formal treatment is next discussed.

B. Joystick Driver Software

The joystick driver software used to read in the button states and position of the control joystick was written in C++ language in Disk Operating System (DOS) environment. C++ allows easy access to a PC's ports using the `outportb()` and `inportb()` functions.

The internal construction, architecture and electronics of a joystick varies from manufacturer to manufacturer so for the

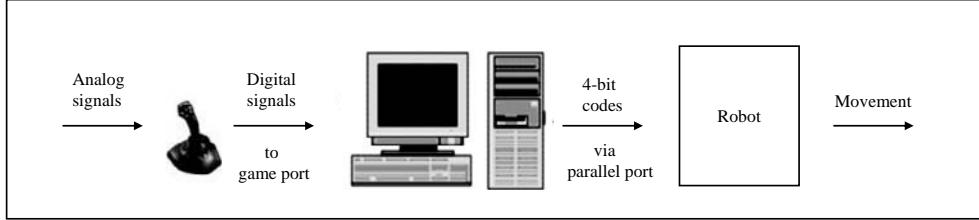


Fig. 1. Conceptual Framework

purpose of this paper it will suffice not to endeavor with the implementation details of the joystick but to just present the generalized layout, which will be common to all joysticks, and to understand the operation of a joystick. In principle, a joystick consists of two potentiometers which are used to give a numerical indication of the joystick's movement. Because the joystick moves in a two (2) dimensional plane, the two potentiometers give the output reading in terms of x and y co-ordinates on an imaginary x and y axis planes.

The corresponding joystick port is a very simple eight (8) bit Input/Output (I/O) card which resides in the Industry Standard Architecture (ISA) bus I/O address 201_h . The Central Processing Unit (CPU) can read and write to the joystick port I/O address 201_h . Reading from this address starts joystick position measurement and when a byte is read from the I/O address 201_h , the status information of the joystick interface is returned.

A joystick writes its instantaneous status (information about its position and button states) as a byte written at ISA bus address 201_h . The orientation or position of the joystick is represented as a two dimensional coordinate of the form (x, y) and the button states have logic representation of either a high (1) or a low (0). Having prior knowledge of what bit of the byte at ISA address 201_h carries which particular information, a joystick's position and button states may be read by the software and this is illustrated in the exhibit of Fig. 2.

The four most significant bits contain the state of the joystick buttons while the four least significant bits contain the values of the x and y coordinate values, which are used for measuring the resistance values of the joystick position potentiometers. This is how the button states (0 if pressed and 1 if not pressed) and position of the joystick have been read by the software in the work reported in this paper.

The joystick's range of permissible movement was then divided into four regions, namely Forward, Right, Left and Back. This was done during the calibration phase of the joystick, by noting the position values it writes at the game port at the Points A, B, C and D (see Fig. 3). These values are then used as a reference set during the writing of the software to determine in what region the joystick is positioned at a particular point in time by the use of case decision structures.

There has to be a way of letting the robot realize its desired direction of movement. A four (4) bit code representing each region of movement is then written at the parallel port which

Game port 210_h byte:

8 Button4	7 Button3	6 Button2	5 Button1	4 y_2	3 x_2	2 y_1	1 x_1
--------------	--------------	--------------	--------------	------------	------------	------------	------------

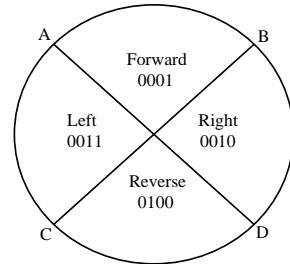
Fig. 2. Individual bits of port 210_h with corresponding joystick information

Fig. 3. Joystick movement region and corresponding codes

is used as a gateway to the robot. The codes used are depicted in Fig. 3.

In summary, the joystick software continuously reads the instantaneous position and button states of the joystick via the game port. When the joystick is positioned in any of the abovementioned regions, the software writes the corresponding four (4) bit code to the parallel port. Likewise if the joystick button is pressed, the joystick writes the halt code 0000 to the parallel port. The halt command is given precedence over other directional commands so that even if the joystick is in Forward mode but its button is pressed and held, it will remain stationary until the button is released.

A. Parallel Port Interfacing Circuit

When the four bit codes have been written to the parallel port, they next have to be interfaced to the microcontroller. A custom-made, unidirectional, Enhanced Parallel Port (EPP) based, software controlled output interfacing card was designed to provide the parallel port-microcontroller interfacing medium. A simple circuit consisting of a 74LS373 octal D-type tri state latch and a 74LS244 octal driver tri state buffer was used to buffer the four bit code arriving through the parallel port. The 74LS373 IC is used to latch the data and the 74LS244 IC boosts up the output current. In addition, resistors of values 150Ω and $1k\Omega$ have been used to ground

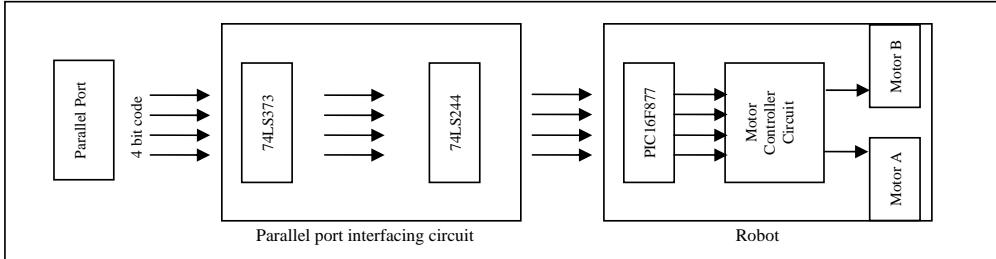


Fig. 4. Block diagram showing interfacing between parallel port, parallel port interfacing circuit and PIC16F877

the data lines of the interfacing card to ensure correct logic levels. This circuit serves the prime and sole purpose of providing an interface medium between the PC and the microcontroller housed on the robot as direct interfacing of the data lines of the parallel port to the microcontroller is not considered good design practice as it may damage the computer's motherboard. Hence, the four bit codes arriving at the parallel port are latched in this circuit; this circuit is then interfaced to one of the input ports of the microcontroller. The exhibit of Fig. 4 illustrates the design of the unidirectional parallel port interfacing card.

A. Microcontroller

The hub of operations and intelligence of the differential drive robot is a PICmicro® microcontroller, specifically the Microchip Technology PIC16F877 eight bit CMOS microcontroller with built in EPROM. The microcontroller is available as a 40-pin DIP package containing a central processor, EPROM, RAM, timer(s), and TTL/CMOS compatible input/output lines. It will coordinate the four (4) bit code it receives from the buffering circuit and according to those codec instructions it will maneuver the robot accordingly. Other microcontrollers may be used; giving the microcontroller its intelligence is just elementary programming, described next. Port B of the PIC16F877 has been assigned as the input port. (Choice of using Port B as the input port was arbitrary and any port may be used). Being the input port, it has been interfaced to the buffering circuit so that it may receive the four bit codes and make the decision.

The micro controller software, programmed in the C programming language continuously reads port B for any arriving four-bit codes sent via the parallel port and the buffering circuit. Once a four-bit code is registered as port B, the micro controller makes a decision as to which motors (of the robot) it should control to attain the specified movement associated with that four bit code. This is done through the use of simple decision structures. The way in which the robot direction is controlled, based on the input signals provided to the motor controller circuits sent via the microcontroller is illustrated in the logic table of Table 1.

Thus, a low budget-end joystick and microcontroller has been used to provide real time control of a robot.

TABLE 1
MOVEMENT CODES AND CORRESPONDING MOTOR ACTIONS

Code	Movement	Motor Action
0000	Halt	Motor A= off Motor B=off
0001	Forward	Motor A= on Motor B=on
0010	Right	Motor A= on Motor B=off
0011	Left	Motor A=off Motor B=on
0100	Back	Motor A=on (Anti C/W) Motor B=on (Anti C/W)

B. Robot

The subject robot is in principle a relatively simple and existing differentially-driven mobile platform with each wheel of the robot coupled to an independently driven dc motor [11]. Attendant freely rotating passive wheels, castors, are fixed at the front and rear sides of the mobile base for easy movement and stability. The control electronics of the robot encompasses a motor controller circuit, microcontroller board, infra red sensors for obstacle detection and a simple regulator circuit.

The motor controller circuit consists of one monolithic, high voltage, high current Darlington pair current driver (ULN2003A) and four (4) Single Pole Double Throw (SPDT) relays which are used to control the rotational direction of the dc motors by controlling the direction of the flow of current through the motors. The microcontroller board is adapted on the circuit schematics provided by Microchip Technology [12].

III. KEYBOARD MODE OF CONTROL

The modular design of the hardware and microcontroller software settings has made it possible to implement a second mode of control with ease: the keyboard keys have been used to provide control of the robot as well, with the arrow keys being used to provide the four (4) directions and the space bar key used as the halt command. This is done by retrieving the ASCII codes of these keys using the `bioskey()` function on the `bios.h` header. The ASCII codes (American Standard Code for Information Interchange) are a set of distinct eight (8) bit codes assigned to each key on the keyboard such that examining the ACSII code of a key

reveals what key it is. This concept is used for establishing the identity of what arrow keys has been registered. Once an arrow key or the space bar has been registered, the corresponding four-bit code of that command is then again written to the parallel port just as in the case of using the joystick.

IV. SYSTEM REQUIREMENTS

A. Control Software

The joystick driver software for this research project was written with Borland® C++ 5.02 Compiler for Microsoft's Windows® Operating System. The software can only be executed on machines running Windows® 98 and will not execute on Windows® 2000 / NT / XP platforms, as direct hardware access is not possible in these newer versions of Windows® operating systems without the use of invoking device drivers. The recommended minimum systems requirements are 64 MB RAM and 2 GB hard drive with one unused game port, one serial port and one parallel port.

B. Microcontroller Software

The software for the PIC16F877 micro controller was written with PIC C Compiler® which was used to convert the high level language into machine language compatible for the microcontroller. Tera Term Pro software was then used to send the machine language file to the micro controller through a serial port.

In summary, a Personal Computer with Windows 98 Operating System, Borland C++ compiler, PIC C Compiler, and Tera Term software together with one unused game port, serial port and parallel port were required.

V. TESTING AND EXPERIMENTATION

The validation and verification of any newly proposed or developed system is imperative. Therefore experimentation of the developed prototype was carried out to measure the performance of the joystick based control mechanism with several tests designed and executed to measure the efficacy of the system. Although this research attained results already accomplished elsewhere utilizing other controlling mechanisms, it demonstrates that reasonable functionality can be accomplished with low budget-end components. It is noteworthy to realize that the concept of *real time* control is directly related to how fast the robot responds to an input signal, provided by a user. Therefore, the important metric of measurement was the time lapse (t) between an input command provided by a user and the triggering of the robots motion in response to the input command. The first test consisted of a straight-line path investigation using the joystick control system developed. For the test results shown in Fig. 5 and Table 2, A = initial starting point, B = expected destination, B' = actual destination, α = deviation of robot, β = braking distance of robot and t = time lapse between input signal and movement of robot.

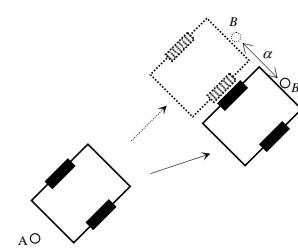


Fig. 5. Test Case 1: Straight line investigation of joystick control

TABLE 2
TEST CASE 1 RESULTS

Trial	α (meters)	β (meters)	t (seconds)
1	0.20	0.05	0.00
2	0.19	0.04	0.00
3	0.21	0.05	0.00
4	0.21	0.03	0.00
5	0.20	0.05	0.00
6	0.17	0.04	0.00
7	0.19	0.03	0.00
8	0.21	0.03	0.00
9	0.20	0.04	0.00
10	0.19	0.05	0.00
mean $\bar{\mu}$	0.18	0.04	0.00
std dev. σ	0.01257	0.008756	0.00

The second test consisted of a multi path investigation of the joystick control system developed. For the test results shown in Fig. 6 and Table 3, A = initial starting point; B, C, D = expected destinations; B', C', D' = actual destinations; $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ = deviations of robot and $\beta_1, \beta_2, \beta_3, \beta_4$ = the braking distances of robot.

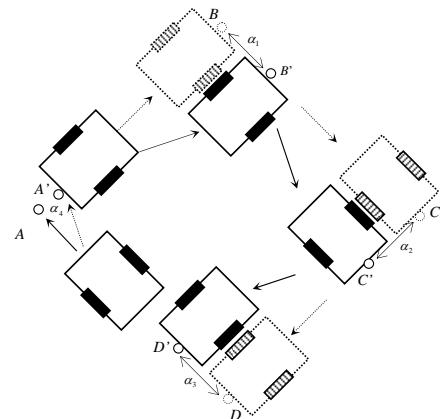


Fig. 6. Test Case 2: Multi path investigation of joystick control

TABLE 3
TEST CASE 2 RESULTS

Trial	α_1 (m)	β_1 (m)	α_2 (m)	β_2 (m)	α_3 (m)	β_3 (m)	α_4 (m)	β_4 (m)
1	0.20	0.05	0.21	0.04	0.19	0.03	0.17	0.04
2	0.19	0.04	0.21	0.04	0.19	0.05	0.18	0.03
3	0.21	0.05	0.19	0.03	0.17	0.04	0.18	0.03
4	0.21	0.03	0.18	0.02	0.18	0.04	0.18	0.04
5	0.20	0.05	0.19	0.05	0.19	0.03	0.19	0.03
6	0.17	0.04	0.20	0.05	0.21	0.02	0.18	0.03
7	0.19	0.03	0.21	0.04	0.20	0.03	0.19	0.03
8	0.21	0.03	0.20	0.03	0.21	0.03	0.22	0.03
9	0.20	0.04	0.18	0.02	0.19	0.04	0.19	0.04
10	0.19	0.05	0.20	0.03	0.19	0.04	0.17	0.04
$\bar{\mu}$	0.18	0.04	0.197	0.036	0.192	0.0372	0.185	0.037
σ	0.012	0.008	0.011	0.010	0.012	0.008	0.014	0.005

From the experimentations, it is important to indicate that it was noted in the testing phase that (1) there is *no* measurable time lapse (using a stopwatch) between an input command provided by the joystick and the triggering off of the robot's motion implying the achievement of an excellent real time control, (2) any directional movement may be attained by the joystick, resulting in a full 360 degrees of freedom. In addition, the braking distances (β) and deviations (α) of the robot in reaching the desired destination points are negligible and therefore may be trivialized.

VI. CONCLUSION

The design and implementation of a joystick based control mechanism has been presented and successfully implemented in giving real time control of a differential drive robot. The hardware and micro controller software settings make it possible to utilize the computer keyboard arrow keys for controlling the direction and the space bar key as the stop button command as a secondary mode of control of the robot. A Graphical User Interface (GUI) forms the front-end human interface and allows the end user to choose between the two modes of control. The control mechanism has been tested and found to give very reasonable control. There is no measurable time lapse between the joysticks movement and the robot's triggered motion implying the achievement of a very reasonable real time control. That the proposed mechanism should be a low cost and economical one was achieved as the whole control mechanism was implemented at a mere cost of a value of less than US\$150. Accomplishing real time control using a low budget end computer joystick was the novelty of this research project. Current ongoing work includes incorporating wireless transmission to ease the inherent restrictions in having a hardwired system.

ACKNOWLEDGEMENT

The authors would like to thank Mr. Shivendra Kumar and Mr. Hamendra Reddy of the School of Engineering and Physics at the University of the South Pacific.

REFERENCES

- [1] Hordeski, M. F. (1992) Control System Interfaces. Design and Implementation Using Personal Computers, *Prentice Hall*.
- [2] Toolley, M. (1995) PC Based Instrumentation and Control, *Butterworth-Heinemann Ltd.*
- [3] Chiri, M. (2002) Joystick Control for TinyOS Robot. *Department of Electrical Engineering and Computer Science. University of California, Berkeley*.
- [4] Lobato, E. P. (2000) A wireless computer-controlled vehicle. *Departamento de Ingenieria de Sistemas -Universidad de Antofagasta, Chile*.
- [5] Li, Y.(2000) Design of Stepper Motor and DC Motor Hybrid Controlled Robot. *Proceedings of International Conference on Advanced Manufacturing Systems and Manufacturing*.
- [6] Dagalaki, H.G., Albus, J. S., Bostelman, R.V. and Fiala, F. (2000) Development of the NIST Robot Crane Teleoperation Controller. *National Institute of Standards and Technology*.
- [7] Borenstein, J. and Evans, J. (1997) The OmniMate Mobile Robot. *Proceedings of the IEEE International Conference on Robotics and Automation, Albuquerque, NM, Apr. 21-27, 1997, pp. 3505-3510*.
- [8] Germann, D., Bruckmann, T. and Hiller, M. (2001) Joystick Force Feedback based on Proximity to the Linearised Workspace of the Four-legged Robot ALDUBRO. *4th International Conference on Climbing and Walking Robots CLAWAR, Karlsruhe, Germany, September 24-26*.
- [9] Moore, K. L., and Flann, N. S. (1999) A Six-wheeled Omnidirectional Autonomous Mobile Robot. *Proceedings of 1999 IEEE International Symposium on Intelligent Control / Intelligent Systems and Semiotics, Cambridge, MA, September 1999*.
- [10] Sian, N. E., Yokoi, K., Kajita, S., Kanehiro, F. and Tanie, K. (2002) Whole Body Teleoperation of a Humanoid Robot. Development of a Simple Master Device using Joysticks. *Proceedings of the 2002 IEEE/RSJ Intl. Conference on Intelligent Robots and Systems, EPFL, Lausanne, Switzerland*.
- [11] Reddy, H. M., Maharaj, A. R. C., Prasad, S. D and Onwubolu, G. C. (2003) Development of Obstacle Avoiding Mobile Robotic Platform using low-end Budget Microcontroller-PIC. *Proceedings of the Tenth Electronics New Zealand Conference*.
- [12] AN732 Implementing a Bootloader for the PIC16F87X, Microchip Technologies Inc, 2000, USA.

Structure and Analysis of a Snake-like Robot

Anjali V. Kulkarni
anjalik@itk.ac.in
Indian Institute of Technology
Kanpur-208016, INDIA

Ravdeep Chawla
raydeepchawla@gmail.com
Punjab Engg. College,
Chandigarh-160012, INDIA

Abstract- A snake is an extremely capable organism that can conquer harsh terrains like rock and sand with apparent ease. The present work highlights the design, development and testing of a snake-like robot prototype. So called ‘SnakeBOT’, is a modular, wheeled snake-like robot. It simulates the sinusoid motion of a snake and is controlled by human voice such that it could actively respond to its milieu. The motion commands to SnakeBOT are delivered via an Infra red (IR) link. The speech recognition software converts the chosen set of commands (forward, left, right and stop) into motion commands. These are transmitted via the IR transmitter interfaced to parallel port of the control PC. On-Off keying technique is used for transmission. IR receiver residing on the tail module of the robot receives these commands and the snakeBOT motion is performed accordingly. The details of the structure of the SnakeBOT and its analysis of motion while on level terrain are presented. The applications of these kinds of robots are mainly in space exploration, disaster management, bomb disarmament, etc.

Keywords: SnakeBOT, slithering motion, navigation, motion control, uneven terrain

I. INTRODUCTION

In an effort to relieve the burden of time-consuming activities, a versatile robot is required to follow in man's footsteps. The pioneering work in developing biologically inspired robots was carried out by S. Hirose [1]. He developed cord mechanism [2] [3], oblique swivel mechanism [4] [5], and heavy articulated mobile robot [6] [7] [8]. Chirikjian and Burdick developed ‘Sneaky’ [9] [10] [11] [12], and snake robot locomotion theory. Most robotic vehicles use a wheel and axle based propulsion system [13] [14] simply because it gives lots of flexibility and high speeds even on rugged terrain. Moreover, if the diameter of the wheel is appropriate, it can easily climb small steps. A wheeled system provides greater traction while navigating variable terrain. Use of passive wheels has been experimented in [15] for achieving the smooth motion. Autonomous gating has been implemented in [16] [17] [18]. Use of specially designed joints has been discussed in [19] [20] [21] to achieve variety of motions. Another novel coupled-drive-based joint mechanism has been designed [22] and studied

the dynamics of snake robots and their motion [23]. A highly flexible robot prototype named the GMD-Snake [24] describes the design and implementation of dynamic distributed real-time control applications. Saito and colleagues have established a mathematical framework for the modeling, analysis, and synthesis of serpentine locomotion with a multilink robotic snake [25]. The research will continue in all the directions to explore the maximal use of snake-like robots.

In this paper the design and development of a free moving wheeled snake-like robot prototype named as ‘SnakeBOT’ is discussed. It is a modular robot comprising four body modules and one tail module. At a time it uses four of eight actuated wheels for propulsion, creating a larger surface area of contact giving greater traction. The low center of gravity creates stability, and the small size helps in passing through small crevices.

SnakeBOT is nimble on its wheels with its extremely flexible joints accounting for the ease with which it can climb up obstacles and move around them with one or more of the modules standing almost vertical and the others pushing the snake along the obstacle. During practical tests, SnakeBOT easily climbed over the keyboard of the computer and a small step of 2 cm height with ease. Such a serpent is very cost effective, compact in size and dexterous enough to replace expensive rovers used in space exploration and can be useful in disaster management.

The present paper is organized as follows, part I give the introduction; in part II the structure of the SnakeBOT is described. Section III gives the details of the voice and IR control. Section IV describes the slithering motion of the snake with mathematical analysis including the simulation of the actual snake. Finally section V presents the important conclusions and discusses the future work that can be carried out.

II. STRUCTURE OF THE SNAKEBOT

The structure of the SnakeBOT is modular. It is mainly divided in three parts: Body, Tail, and Skin. Body and tail modules run in a chain. Body comprises of 4 similar body modules. Total length of the snakeBOT is around 41 cm. It is 7.3 cm wide. The skin is the top cover, which covers the robot in a specially designed way so as to provide the flexibility and ease while moving. This design of the snakeBOT provides following important features:

- The combined torque provided by the modules is responsible for navigation on an uneven elevation.
- Even if one of the modules is twisted and rises above the ground at an angle around 70° to the horizontal, the other modules are not affected and continue to follow their path.
- The S-shaped curve formed by the snake during motion aids moving around obstacles.

A. Body

Coupling similar body modules forms the body. In the present design, four body modules are connected to form the main body. A body module consists of three major parts:

1. Motor holding assembly
2. Two Motors
3. Two Wheels

Motor holding assembly has three sub parts as shown in Fig. 1. The bottom and top covering lids and the inner box, which holds the motors. It is the basic building block of the body module. The slots inside the inner box hold the motors. The slots are placed side by side to minimize the dimensions of a single module. The system is both dynamically and statically stable as the weight is uniformly distributed. Placement of motors side by side as shown gives the effective sinusoidal motion. DC motors running at 80 rpm with a gear reduction of 175:1 are used. These give the necessary torque to sustain motion in the adverse conditions. The bottom and top covering lids cap the two motors. This ensures the proper positioning of the motors. Wheels made up of nylon 66 material are directly connected to the motor shafts. The wheel design is shown in Fig. 2. The large diameter (43 mm) helps in scaling obstacles that are comparable in size to the modules. The tire inserts on the wheels are designed to give maximum traction and reduce the chances of toppling. Tires are made up of molded rubber. Fig. 3 shows the front and rear view of the assembled single body module. Specially designed joints as discussed connect body modules to each other later.

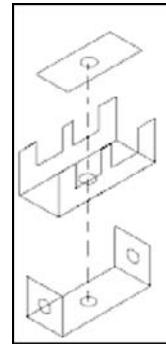


Fig. 1. Motor holding assembly

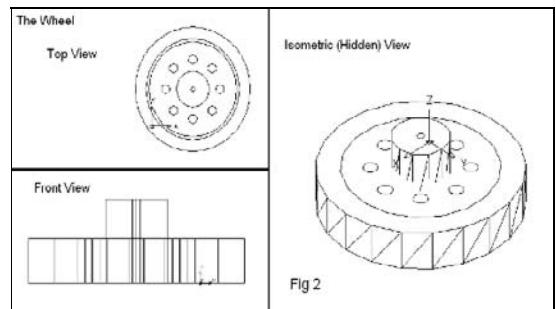


Fig. 2. Wheels

B. Tail

The tail is the inactive part of the SnakeBOT. It houses the battery pack; IR control and motors drive circuitry. Four idle wheels (castors) are attached to the bottom of this structure to make it mobile. Tail module is connected to the last body module by means of signal and power wires. These wires run all along the length of the snakeBOT

C. Skin

The skin is the outer cover provided on the snakeBOT. The skin consists of two parts: the joints and the covering of the modules. The joints in the skin are made of tire tube used in trucks. Cuts are provided at appropriate places (Fig. 4) to make turning easier. The joint made of tire tube provide rotational degrees of freedom. The elasticity of tire tube is advantageous as it enables smooth motion and helps in returning back to the same orientation. Fig. 5 shows the actual joint while the snake tries to turn. The covering of the module is made up of hosepipe. Figure 6 shows the completed snakeBOT with 4 body modules and the tail module.

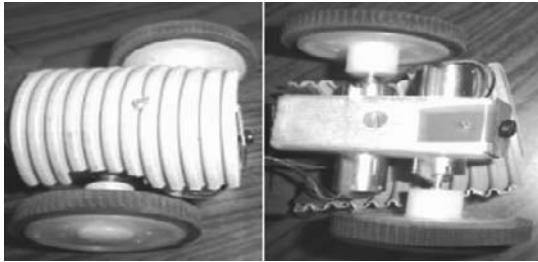


Fig. 3. Front and rear view of the body module

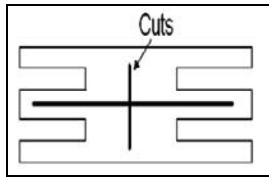


Fig. 4. Cuts in the tire tube for Turning

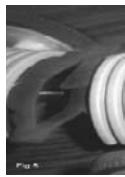


Fig. 5. Joint



Fig. 6. The snakeBOT

The control of the snakeBOT is described in the following section.

III. VOICE AND IR CONTROL

The snakeBOT simulates the sinusoid motion of a snake by design of its structure. Moreover actuation of only one wheel in one module and the alternate wheels in the body structure are also responsible for achieving the sinusoidal motion. It is controlled by human voice such that it could actively respond to its milieu. It is trained to respond to the voice commands from the user. A trained Microsoft's speech recognition engine recognizes these voice commands. The speech

recognition software converts the chosen set of commands (forward, left, right and stop) into text. Corresponding to this text, a bit stream is sent to one of the signal lines of the parallel port. The bit stream is then transmitted over an IR

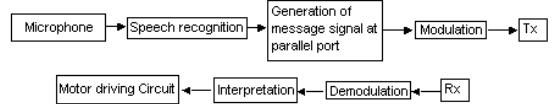


Fig. 7. Block diagram of the control strategy

transmitter (working at 38 KHz) using On-Off Keying (OOK) technique. The IR receiver residing on the tail module of the robot receives these commands and the snakeBOT motion is performed accordingly.

Fig. 7 gives the block diagram of the control strategy.

The bit stream decides the On-Off timing of the motors to determine the direction of motion of the robot. Thus, for moving in the forward direction, the left motor is made 'On' for 200 ms and right motor is made 'Off' for the same time. During the next 200ms time interval the right motor is made 'On' and left motor is 'Off'. This results in forward sinusoidal motion. For turning sideways, the 'On' and "Off" times are unequal and it is 200ms-400ms or 400ms-200ms accordingly. Thus for turning left, the right motor is 'On' for 400ms while left motor is 'Off' and during the next time period the left motor is 'On' for 200ms and right motor is 'Off' for that time interval. The resulting wavy turn is as shown in the following section describing the simulation.

L298 IC is used as the amplifier to driver the motors. The control and drive electronics resides on the tail module.

IV. MOTION ANALYSIS AND SIMULATION

SnakeBOT has 8 actuated wheels i.e. two in each of the four modules as described in section II. Periodic switching on alternate wheel in the consecutive body module of the serpent such that only four of the eight wheels are moving at a specific moment generates the slithering motion. We have generated a simulation for analyzing the motion of this serpent on ground level by neglecting the inertia of the motors, noise due to the IR transmitter and receiver circuit. The analysis is carried out for one of the body modules. The rest of the modules follow the first one with a specific delay. Hence the analysis of one module is an apt description of motion of the whole serpent. The motion of the center of the mass of the first body module is analyzed in the simulation.

Fig. 8 gives all the dimensions of an individual body module. The radius of curvature of the arc is the distance between the contact points of wheels and is around 73 mm.

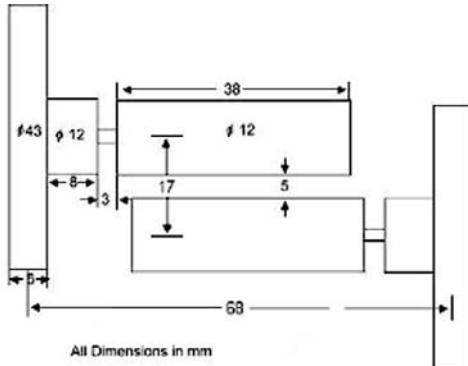


Fig. 8. Dimensional details of a body module

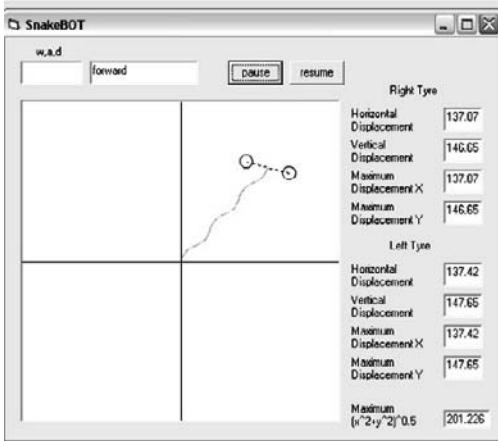


Fig. 9 Simulated 'forward' motion

The DC motors rotate at 80 rpm at 12 V and thus, the linear velocity of the tires with diameter 43 mm is around 360 mm/s and the angular velocity comes out to be around 5.14 rad/s. With this data the motion of the snakeBOT is simulated using Visual Basic software.

The simulated 'forward' motion is as shown in Fig. 9. It gives the trace of the centre of mass.

In Fig. 10 complete 'left' turn is described with the center point of the module tracing a wavy circle. The turning radius is calculated as half of the maximum displacement of the center point. This distance is shown in the bottom right corner of Fig 9 comes out to be 92 mm.

Fig. 11 gives the simulation result for turning 'right' condition. While turning right the turning radius comes out to be 94 mm. The simulation results are the true replica of the

nature of motion of snakeBOT. The turning radius are observed more than in the practical motion due to the inertia of the motors which is neglected in the simulation results.

V. CONCLUSION

In this paper, the structure of a free moving wheeled serpentine robot has been presented. Its wavy motion on level terrain is analyzed and simulated and tested with the real robot. It gives the feasibility of such kind of robots and their practical implementation. These kinds of robots can negotiate the clumsy workspace due to their wavy motion.

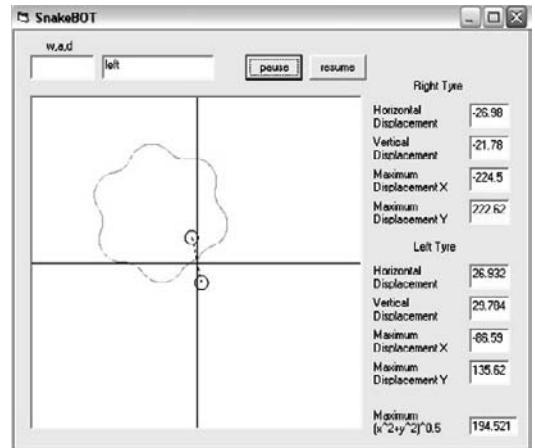


Fig. 10 Simulated 'left' turn

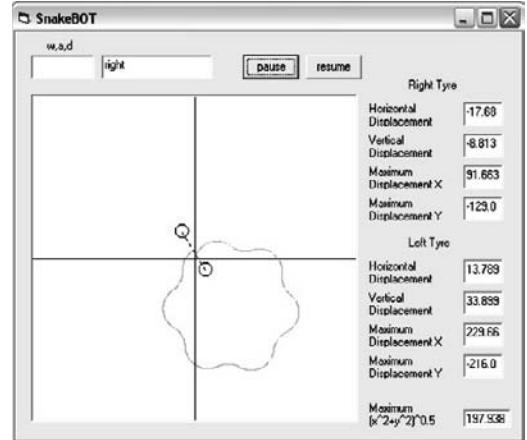


Fig. 11 Simulated 'right' turn

ACKNOWLEDGMENT

Thanks are due to Dr. Bhaskar Dasgupta of ME Department for giving the idea of developing snake-like robot. Mr. Rajendra, Mr. Sanjay helped in fabricating the modules. Their help is gratefully acknowledged.

REFERENCES

- [1] Shigeo Hirose, “*Biologically Inspired Robots*”, Oxford University Press, 1993, ISBN 0-19-856261-6.
- [2] Yoji Umetani and Shigeo Hirose, “Biomechanical study of active cord-mechanism with tactile sensors”, In *Proc. 6th Int. Symp. On Industrial Robots*, pages c1–1–c1–10, Nottingham, 1976.
- [3] Mori M. and Hirose, S., “Development of active cord mechanism ACM-R3 with agile 3D mobility”, In Proceeding of the IEEE/RSJ International Conference on Intelligent Robots and Systems, Maui, Hawaii, pp. 1552–1557, 2001.
- [4] Shigeo Hirose and Yoji Umetani, “An active cord mechanism with oblique swivel joints and its control”, In *Proc. 4th RoManSy Symp.*, pages 327–340, Zaborow, Poland, 1981.
- [5] Shigeo Hirose, “Connected differential mechanism and its applications”, In *Proc. 2nd Int. Conf. On Advanced Research*, pages 319–326, 1985.
- [6] Shigeo Hirose and Akio Morishima, “Articulated body mobile robot”, In *Proc. 7th RoManSy Symp.*, pages 1–8, Hermes, 1988.
- [7] Shigeo Hirose and Akio Morishima, “Basic motion regulation of articulated body mobile robot”, In *Proc. 5th Int. Symp. On Robotics Research*, pages 433–440, Tokyo, 1989.
- [8] Shigeo Hirose and Akio Morishima, “Design and control of a mobile robot with an articulated body”, *Int. J. Robotics Research*, 9(2):99, 1990.
- [9] G. S. Chirikjian and J. W. Burdick, “Design, implementation, and experiments with a thirty-degree-of-freedom ‘hyper-redundant’ robot”, In *ISRAM 1992*, November 1992.
- [10] G. S. Chirikjian and J. W. Burdick, “The kinematics of hyper-redundant robotic locomotion”, *IEEE Trans. on Robotics and Automation*, 11(6):781–793, December 1995.
- [11] J. W. Burdick, J. Radford, and G. S. Chirikjian, “A ‘sidewinding’ locomotion gait for hyper-redundant robots”, *Advanced Robotics*, 9(3):195–216, 1995.
- [12] J. P. Ostrowski and J. W. Burdick, “Gait kinematics for a serpentine robot”, In *Int. Conf. On Robotics and Automation*, 1996.
- [13] Rainer Worst, “Robotic Snakes”, Third German Workshop on Artificial Life, pp. 113–126 Verlag Harri Deutsch, 1998, ISBN: 3-8171-1591-1.
- [14] L. Jammes, Yasumasa Kyodo, Masahiko Hiraki and Shigeo Ozono, “Design Concept and Ondulatory Motion Mode of a Modular Snake-Like Robot”, Proc. IROS 97, IEEE.
- [15] Hisashi Date, Yoshihatsu Hoshi, Mitsuji Sampei, Shigeki Nakaura, “Locomotion Control of a Snake Robot with Constraint Force Attenuation”, Proceedings of the American Control Conference, Arlington, VA, 2001
- [16] P. Prautsch and T. Mita, Control and analysis of the gait of snake robots. In IEEE International Conference on Control Applications, pages 502–507, 1999.
- [17] J. Ostrowski and J. Burdick, “The geometric mechanics of undulatory robotic locomotion”, The Int. J of Robotics Research, 17(7):683–701, 1998.
- [18] K. Mogi and F. Matsuno, Control of a snake robot with redundancy based on kinematic model. In Proc. The 5th Int. Symp. on Artificial Life and Robotics, pages 507–510, 2000.
- [19] Martin Nilsson, “Why Snake Robots Need Torsion-free Joints and How to Design them”, Proceedings of the 1998 IEEE International Conference on Robotics & Automation, Leuven, Belgium, May 1998.
- [20] Nilsson, M., “Ripple and Roll: Slip-free Snake Robot Locomotion”, Proc. Mechatronic Computing for Perception and Action (MCPA ’97) Italy, pp. 75–81.
- [21] Martin Nilsson, “Snake Robot Free Climbing”, IEEE Control Systems, pp 21–26, 1998.
- [22] Changlong Ye, Shugen Ma, Yuechao Wang, Bin Li, “Coupled-Drive-Based Joint Design of a Snake Robot and its Body-Lifting Method”, Proc. of IEEE Int. Conf. on Robotics Intelligent Systems and Signal Processing, China, October 2003
- [23] Shugen Ma, “Analysis of creeping locomotion of a snake-like robot,” Advanced Robotics, vol. 15, no.2, pp.205–224, 2001.
- [24] K. Paap, M. Dehlwisch and B. Klaassen, “GMD-Snake: A Semi-Autonomous Snake-like Robot”, *Distributed Autonomous Robotic Systems 2*, Springer-Verlag, pp71–77, Tokyo, 1996.
- [25] M. Saito, M. Fukaya, and T. Iwasaki, Serpentine locomotion with robotic snakes. IEEE Control Systems Magazine, 22:64–81, 2002.

A Novel Online Technique to Characterize and Mitigate DoS Attacks using EPSD and Honeypots

Anjali Sardana, Bhavana Gandhi and Ramesh Joshi

Indian Institute of Technology Roorkee

anjali_zakky@yahoo.com, bhavana.s.gandhi@gmail.com, joshifcc@iitr.ernet.in

Abstract-Denial of Service Denial of Service (DoS) attacks pose a severe security threat to the steady functioning of any network. These attacks aim at depleting the resources of a server or an administrative network by overwhelming it with enormous and useless traffic. The outcome of this is the fact that legitimate users are denied service. Though an array of schemes has been proposed for the detection of the presence of these attacks, characterizing of the flows as a normal flow or a malicious one, identifying the sources of the attacks and mitigating the effects of the attacks once they have been detected, there is still a dearth of complete frameworks that encompass multiple stages of the process of defense against DoS attacks. In this paper, we propose a novel framework which deals with the characterization of the TCP and UDP flows, identification of the source of the flow once it has been characterized as an attack flow and mitigating the influence of the attack. The characterization of the flows has been achieved by an innovative Exactly Periodic Subspace Decomposition (EPSD) based approach, whereas a proactive roaming honeypot scheme has been deployed for the identification of the source of the attack flow and mitigation of the effects of the same. We validate the effectiveness of the approach with simulation in ns-2 on a Linux platform.

I. INTRODUCTION

DoS attacks, which aim at overwhelming a target server with an immense volume of useless traffic from distributed and coordinated attack sources, are a major threat to the stability of any network. The number and assortment of both the attacks as well as the defense mechanisms is monstrous. It is essential that we be able to detect DoS attacks fast, accurately and further ascertain the attacks with high confidence and trace back the attackers in real time.

In this paper, we present a novel framework for defense against DoS attacks. The framework consists of two stages: stage 1 deals with the characterization of the flows as legitimate or attack, whereas stage 2 copes with the attack source identification and the mitigation of the influence of the attack.

The characterization of the flows, i.e. determining whether a flow is a legitimate flow or an attack one, is done by an EPSD-based approach. Once the characterization is done, the proactive roaming honeypot scheme is used to lessen the effects of the attack. A honeypot [1] is an information system resource whose value lies in unauthorized or illicit use of that resource.

The remainder of the paper is organized as follows. Section II discusses the background and related work. We highlight

the overall structure of our proposed framework in Section III. Section IV gives a brief overview of the EPSD technique and defines the packet process that will be used and explain the reason behind its periodicity. Section V describes the roaming mechanism for the honeypots and connection migration techniques that comprise stage 2 of the framework. Section VI defines the topology used as simulation testbed. Section VII describes various simulation scenarios and evaluates the performance of proposed solution. Section VII concludes our work and suggestions for future work have been provided in Section IX.

II. BACKGROUND AND RELATED WORK

Several schemes have been suggested to detect and characterize attack flows. It was proposed in [2] a spectral analysis method to distinguish attack flows from the normal ones by determining the periodicity in the packet process as defined in this paper. But the method does so by using the Welch's modified periodogram, which has several disadvantages as compared to the EPSD technique used in stage 1 of this paper. The Welch's modified periodogram is calculated by applying a window function to the time-domain data, computing the Discrete Fourier Transform (DFT), using Fast Fourier Transform (FFT).

FFT itself has many restrictions [3] like picket-fence effect and the leakage effect. The EPSD-based technique does away with the disadvantages [4] of the Welch's modified periodogram. Also, in [2], no simulation was used to test generic flows. Instead, available traces of a sample network were subjected to determination of the periodicity.

After their characterization, several proposals have been made to cope with DoS attacks. Broadly the approaches can be categorized into two parts:

i. Mitigation of the impact

ii. Identification of the sources of attack

In the proposed mechanism, roaming honeypots have been used. They identify the sources of the attacks and further mitigate the impact of the attacks. This is in contrast to a hybrid architecture [5] for defense against DoS attacks, where a passive honeypot is used for protection against relatively static attacks.

III. PROPOSED FRAMEWORK

Fig. 1 shows the overall structure of the framework. A normal TCP flow is purported to reveal periodicity in the

number of packet arrivals associated with RTTs. Any flow not exhibiting this behavior can reliably be classified as an attack flow. We consider a random process, which we shall refer to as the *packet process*, which represents the number of packet arrivals for a TCP flow at various instants monitored on the deployment router, preferably the bottleneck router. The use of the EPSD technique to detect the presence or absence of periodicity in the packet process is much more efficient than the techniques currently in use. In case of UDP flows, honeypot-based characterization is used as a UDP flow will not exhibit periodicity and may give false positives with EPSD.

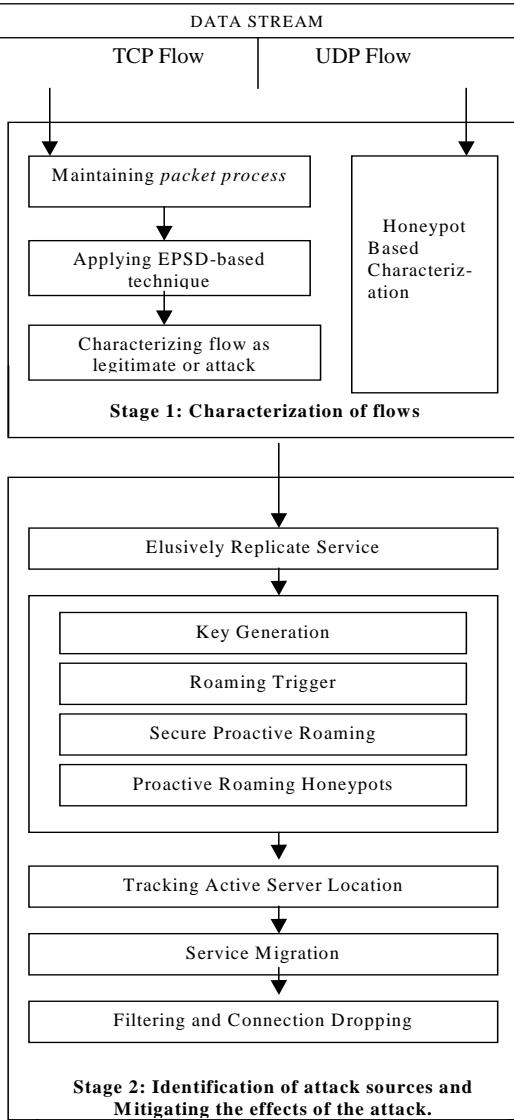


Fig. 1. Overall Structure of the Framework

After the characterization of flows, honeypots and active servers change their location among a pool of servers to defend against unpredictable and likely undetectable attacks. Only legitimate clients will be able to follow the server as it roams. Requests on flows characterized as attack in stage 1 is sent directly to a randomly selected honeypot.

IV. EXACTLY PERIODIC SUBSPACE DECOMPOSITION FOR CHARACTERIZATION

Muresan et al. [6] proposed the EPSD technique to identify different frequency components in noise prone data. In this paper, we use EPSD based technique to demonstrate the two methodologies of online and offline detection of DoS attacks.

Definition: A signal S is of exactly period P if S is in $R(\psi^P)$, and the projection of S onto $R(\psi^{P'})$ is zero for all $P' < P$ (where $R(\psi^{P'})$ is the subspace of signal of period P') [6].

With the above definition, a signal of exactly period P is not exactly period of $2P$, $3P$, etc. In addition, not every periodic signal is exactly periodic, but every exactly periodic signal is periodic. For example, an exactly periodic 4 signal is

$$R = [1, 1, -1, -1, 1, 1, -1, -1, 1, 1, -1, -1]$$

The EPSD technique finds the subspace corresponding to the signal of exactly periodic P and shows that these subspaces are orthogonal to each other.

In [7], the advantages of the EPSD technique over the Welch's periodogram method are described in detail. In this paper, we have shown how EPSD can be applied in detection of anomalous flows. Every data packet arriving at the receiver can permit the receiver to transmit an ACK packet to the sender [2]. Similarly, every ACK packet arriving at the sender allows it to place a new data packet on the network. Thus, if we monitor the network at any point between the sender and the receiver and if we observe a certain number of packets belonging to a particular flow, then it is very likely that the same number of packets belonging to that flow will be visible after one Round Trip Time (RTT) between the sender and the receiver. This gives rise to periodicity in a normal TCP flow. In an attack flow, the attackers do not wait for ACK packets before the outstanding data packets can be sent. Thus, such attack flows would be aperiodic in nature. EPSD technique can be used to determine the presence of or lack of periodicity in the flows incident on a server.

V. PROACTIVE ROAMING HONEYHOT SCHEME

The following steps are involved in identification of the sources of the flows characterized as attack in stage 1 and mitigation of the effects of the same.

Step 1: Replicated Elusive Service

Replicated elusive service [8] causes the service to physically migrate from one physical location to another to mitigate DoS attacks.

Step 2: Server Roaming

In server roaming [9], the active server changes its location within a pool of servers. Server roaming serves as a

mechanism not only for DoS defense by itself but also as a building block in a larger integrated DoS defense system.

a) Secure Proactive Roaming

The active server [9] changes its location within a pool of N homogenous servers to defend against unpredictable and undetectable attacks. Only legitimate clients can follow the active server as it roams. The flows characterized as attack flows in stage 1 will not be aware of the location and time for which servers are active in this stage.

b) Roaming Trigger

It uses the algorithm in [9] utilizes backward hash chains, where members of the chain are generated using one-way hash functions like MD5 [10] and used in reverse direction of their generation. Service time is divided into *epochs*; at the end of each epoch, the service migrates from one server to another in the server pool.

A long hash chain is generated using a one-way hash function $H(\cdot)$, and used in a backward fashion. The last key in the chain, K_n , is randomly generated and each key, K_i ($0 < i < n$), in the chain is computed as $H(K_{i+1})$ and used to calculate both the length, R_i , of service epoch E_i and the location, S_i , of the active server during E_i as follows:

$$R_i = \text{MSB}_m(H'(K_i)) \quad (1)$$

$$S_i = \text{servers}[\text{MSB}_{\log N}(H''(K_i))] \quad (2)$$

where $\text{MSB}_j(x)$ are the j most significant bits of x , 2^m represents an upper bound on epoch length, N is the number of servers, and the array *servers* contains an <IP address, TCP port> pair for each server in the server pool. H' and H'' are public one-way hash functions, such as MD5 [10].

c) Proactive Roaming Honeyhops

Proactive roaming honeypots are achieved as follows: A subset of servers is active and providing service, while the rest are acting as honeypots. The locations of current active servers and honeypots are changed so as to be unpredictable to the attackers identified in stage 1.

Step 3: Tracking the Active Server Location

This information can be simply obtained by using a series of communication. In a high threat period this upper bound m is set to be small, while it is set to a larger value in normal conditions. All connections are migrated to next active server as the active server moves.

Step 4: Service Migration

TCP Migrate and Migratory TCP [11,12] have been modified to suit the roaming requirements. The clients perform state recovery as it filters out attackers of stage 1 because *only* subscribed legitimate clients know the address of the next roaming server and the roaming time and only these clients will be able to create state entries for their connections at the new server.

Step 5: Filtering and Connection Dropping

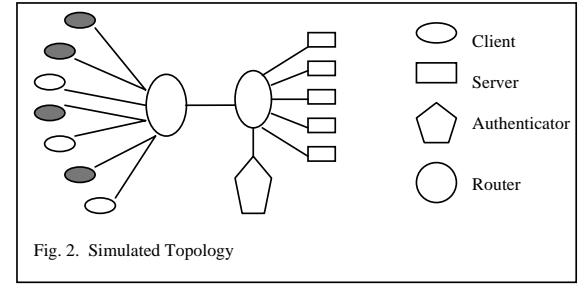
Firstly, idle servers (honeypots) detect attacker addresses so that all their subsequent requests are filtered out. Secondly,

each time a server switches from idle to active; it drops all its current (attack) connections, opening a window of opportunity for legitimate requests before the attack re-builds up. These two benefits the filtering effect and the connection-dropping effect [9], respectively.

VI. EXPERIMENTAL DESIGN

A. Simulation Topology

Fig. 2 depicts the simulated network topology. The shaded clients are the attackers; the others are legitimate. They request files of size 1 Mbps each with request inter-arrival times drawn from a Poisson distribution.



Let T_{sample} be the time interval after which the flow statistics (packet arrivals) are monitored continuously per flow. Let N_{current} be the number of packets arrived till the sample instant from the time the flow was active minus the number of packets arrived till the last sample instant. Let *small_stats* be an array of length N_{stats} which stores the value of N_{current} for the last N_{stats} instants. Once the flow is past its slow start phase, for every T_{EPSD} seconds, the EPSD functionality is invoked online for the *small_stats* array, i.e. for the latest N_{stats} samples. This is done as even a legitimate flow lacks periodicity in its slow start phase. We should delay the decision of tagging the flow as attack or legitimate till EPSD has been called for *cnt_thresh* times. For each time that the periodicity is found to be missing from the array *small_stats*, another counter *bad_flow* is incremented. If *bad_flow* is greater than a pre-defined threshold *bad_thresh*, then the flow is tagged as an attack flow and further packets from the flow are discarded. The detailed steps are shown in the form of a flowchart in Fig. 3.

The value of N_{stats} should be chosen such that it should neither be too large to cause a great overhead in terms of storage and processing requirements, and at the same time it should be large enough to indicate at least two complete cycles with respect to the RTT from the source node to the server in order to safely judge the periodicity, i.e.

$$N_{\text{stats}} > 2 * \text{RTT} / \text{Sample Period} \quad (3)$$

VII. RESULTS

A. Stage 1 Simulation Results

In this subsection, we present the simulation results of stage 1

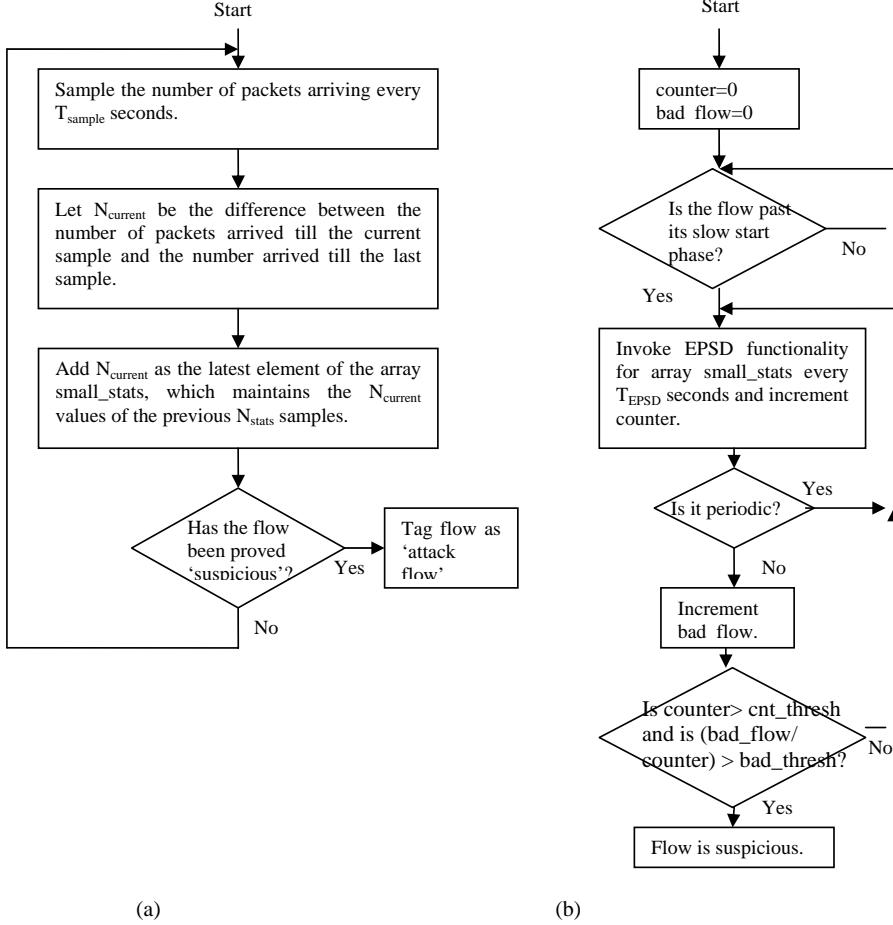


Fig. 3. (a) Flowchart for sampling the number of packets per flow. (b) Flowchart for invoking the EPSD functionality for the online methodology.

TCP flow. The domain of analysis includes the observation of the Exactly Periodic Subspace (EPS) energy vs. the period at which it occurs. The period, other than 1 (as period of 1 denotes the dc component of the energy), at which the significant positive EPS energy is observed denotes the exact period of the packet process. Honeypot-based characterization is used for UDP flows. Any flow directed towards honeypot is illegitimate and hence a UDP flow destined for a honeypot is characterized as an attack flow.

1) Legitimate Flow

Let T_{sample} be 10ms, T_{EPSD} be 1 sec and N_{stat} be 11. An enlarged view of the packet process passed on to one run of the EPSD procedure is shown in Fig. 4. As can be observed, the packet process is visibly periodic in nature. The resulting EPSD graph is shown in Fig. 5. The energy at period 1 is the dc component of the signal. The period where the next highest

energy is observed is the actual period of the signal, which is 5 here, i.e. the signal due to the packet process is periodic with a period of 50 ms (as the samples are taken at 10ms intervals), which is the RTT.

2) Attack Flow

The result of applying the EPSD technique on the packet process of an attack flow is shown in Fig. 6.

Our doubts of the lack of periodicity in the packet process for an attack flow are confirmed by the resultant EPSD graph. There is no significant energy at any non-dc component to qualify it as a periodic signal. To qualify this flow as a normal flow, there should have been significant energy at period 5, but there appears to be none according to the generated EPSD graph, thus characterizing the flow as an attack flow.

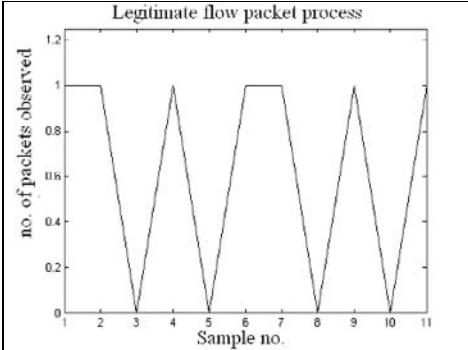


Fig. 4. A few sample observations from the legitimate flow packet process.

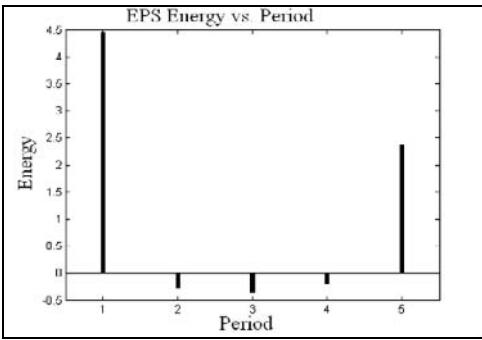


Fig. 5. EPS Energy vs. Period for legitimate TCP Flow

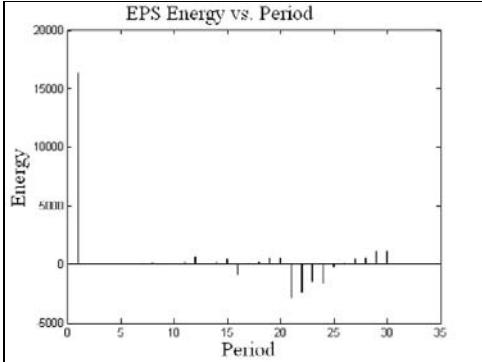


Fig. 6. EPS Energy vs. Period for an attack flow

B. Stage 2 Simulation Results

Once a flow has been characterized and directed to a honeypot and an active server respectively, average response time and number of packets dropped are used as metrics for comparing the performance of the scheme.

1) Cost of honeypots

Fig. 7 shows cost incurred by roaming honeypot scheme under no attack condition.

As the number of honeypots increase, even under low or no attack conditions, the average response time increases because the number of active servers which could have otherwise furnished client requests take up the role of honeypots even when there are no attacks.

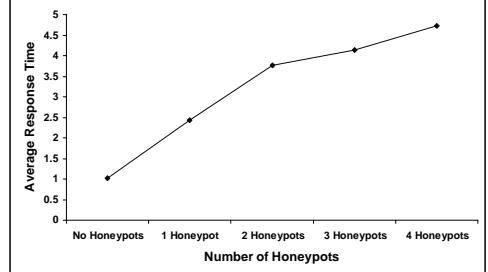


Fig. 7. Cost of honeypots incurred under absence of attacks (Attack Load = 0 Mbps; Client Load = 5 Mbps; Migration Interval = 2s)

2) Benefit of Honeypots in case of UDP Flows

In case of UDP attack flow, in the absence of honey pots, the number of packets dropped increase with increase in client load, as expected. However in the presence of honey pots, the attack flow is filtered as soon as an attack is detected by a honeypot. Thus the attack traffic in the network decreases substantially, giving chance to more and more legitimate traffic reaching their destination. This gives a stable behavior even with increase in client load upto a limit in presence of honeypots, as shown in Fig. 8.

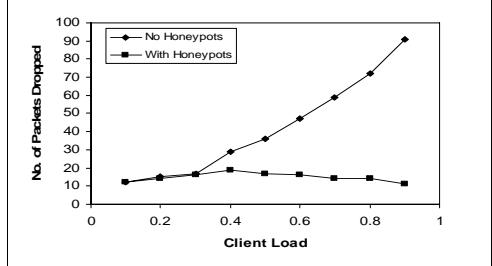


Fig. 8. Benefit of Honeypot under the presence of UDP based DoS attack (Attack load = .5 Mbps ; Migration Interval =2s)

3) Benefit of Honeypots in case of TCP Flows

Fig. 9 shows the expected behavior in the graph as average response time increases with increasing attack load in case of none, 1 and 4 honeypots. 3 Honeypots and 2 servers provide the most optimum combination for this set of <client load, migration interval parameters> because the average response time increases marginally with increase in attack load and then decreases. The unexpected decrease in average response time is due to the fact that as soon as the attacks are detected, they are filtered out and after some time no attacks persist, thus decreasing the average response time for a given client load.

The challenge is the determination of optimum values for a set of parameters for a scenario.

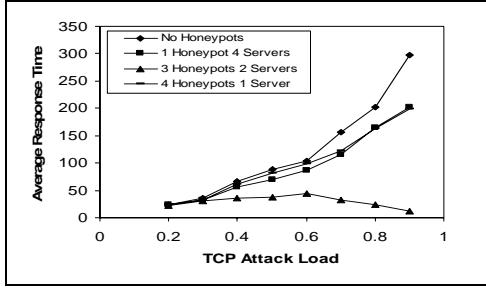


Fig. 9. Behavior of Honeypots under the presence of TCP attacks.

4) Optimum Migration Interval

As shown in Fig. 10, optimum migration interval is the function of parameters specific to the scenario. For a given attack load, for each value of migration interval, increasing client load increases the number of clients done, up to a maximum value and then resulting in a decrease. For the given attack load and a particular value of client load, the curve that contains the maximum value of number of clients done gives the optimum value of migration interval for the given combination of parameters.

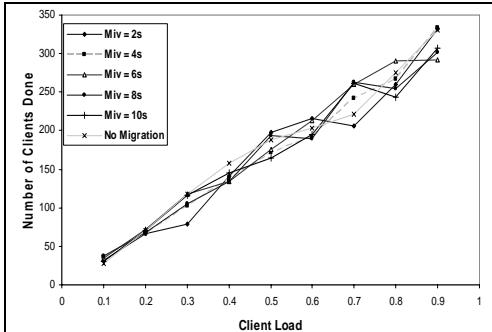


Fig. 10. Optimum Migration Interval

VIII. CONCLUSIONS

In the proposed framework, we are using the EPSD technique to distinguish legitimate TCP flows from the attack ones. We illustrate the effectiveness of this approach by applying the technique on both kinds of flows.

Proactive roaming honeypot has been presented to mitigate DoS attacks. The scheme takes advantage of both filtering and connection dropping effect.

Results show that the framework has potential to improve the DoS defensive strategy in both TCP and UDP flows. However, because of sacrificing some servers to act as honeypots, distributing the load on all the servers outperforms the roaming honeypots scheme in the case of a high legitimate client load combined with a low attack load.

IX. FUTURE WORK

The RTT of a TCP flow may vary slightly from trip to trip, due to queuing delay variations. For characterization to be successful in stage 1, the sampling period has to be large enough to tolerate RTT fluctuation, while small enough to make the periodicity to be observed distinguishable. Thus, it would be challenging to identify TCP flows with very small RTTs. These flows generally do not pose severe security threats because they are mostly local traffic, or traffic between two administratively close networks. Nevertheless, one possible remedy of this is to set up a list of neighboring sites and treat the traffic related to these sites separately. Another possibility is to add artificial delay at the router where we take measurements, so that the range within which RTTs vary is relatively small.

Although stage 2 of the framework focuses on physically roaming honeypots, the potential of logically roaming honeypots is notable. Further, the number of honeypots varied adaptively depending on attack load would solve the shortcomings and is left for future work.

REFERENCES

- [1] Honeypot Project, URL <http://project.honeynet.org>
- [2] Chen-Mou Cheng, H. T. Kung, and Koan-Sin Tan, "Use of Spectral Analysis in Defense Against DoS Attacks," *In the Proceedings of Global Telecommunications Conference, 2002, GLOBECOM '02. IEEE*, Vol. 3, pp: 2143 – 2148, Nov. 2002.
- [3] Rong-Ching Wu, and Ta-Peng Tsao, "Theorem and Application of Adjustable Spectrum," *IEEE Trans. on Power Delivery*, Vol. 18, No. 2, pp: 372-376, April 2003.,
- [4] P.L. Feibig, D.M. Eter, and S.D. Stearns, "A Software Tool for comparing Spectral Estimation Techniques," *Twenty-Third Asilomar Conference on Signals, Systems and Computers, 1989*. Vol. 1, pp: 371 – 375, 1989.
- [5] K. Anagnostakis, S. Sidiropoulos, P. Akritidis, K. Ximidis, E. Markatos, and A. Keromytis, "Detecting targeted attacks using shadow honeypots", *In Proceedings of the 14th USENIX Security Symposium*, Aug. 2005.
- [6] D. Darian Muresan, and Thomas W. Parks, "Orthogonal, Exactly Periodic Subspace Decomposition," *IEEE Trans. on Signal Processing*, Vol. 51, No. 9, pp. 2270-2279, Sep. 2003.
- [7] B. Gandhi, K. Kumar, R.C. Joshi, "A Novel EPSD Based Approach for Characterization of DDoS Attacks," *International Conference of Next Generation Communications ICONGENCOM-06*, in press.
- [8] C. Sangpachatanaruk, S. M. Khattab, T. Znati, R. Melhem, D. Moss, "Design and analysis of a replicated elusive server scheme for mitigating denial of service attacks," *In The Journal of Systems and Software*, Vol. 73 , pp: 15–29 , 2004.
- [9] C. Sangpachatanaruk, S. M. Khattab, T. Znati, R. Melhem, and D. Moss, "Server Roaming for Mitigating Denial of Service Attacks". *In Proceedings of ANSS'03*, 2003.
- [10] R. Rivest. The md5 message-digest algorithm. *In RFC 1321*, 1992.
- [11] A. C. Snoeren, H. Balakrishnan, and M. F. Kaashoek, "The migrate approach to Internet mobility," *In Proceedings of the Oxygen Student Workshop*, July 2001.
- [12] F. Sultan, K. Srinivasan, D. Iyer, and L. Iftode, "Migratory TCP: Connection migration for service continuity in the Internet," *In Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS)*, 2002.

Multi-Scale Modelling of VoIP Traffic by MMPP

Arkadiusz Biernacki

Abstract—The concept of multiplexing voice traffic sent over IP protocol (VoIP) on a common channel for efficient utilisation of the transmission link capacity is a great concern to network engineers. A VoIP gateway allocates a channel capacity that lies between the average and peak rates of traffic intensity and buffers the traffic during periods when demand exceeds channel capacity. In order to evaluate performance of the gateway a traffic model is needed. In this work we propose Markov Modulated Poisson Process (MMPP) for modelling of multiplexed VoIP traffic, generated by a number of independent sources, which flows into a VoIP gateway. We apply this model to analytical analysis of the gateway performance using fluid flow modelling techniques. We give a cumulative distribution function of the number of packets in the gateway buffer and evaluate it against the simulation.

Index Terms—Computer network performance, Integrated voice-data communication, Markov processes, Modelling.

I. INTRODUCTION

The growth of communication based on Voice over IP protocol (VoIP) has been exceptional during recent years and is expected to continue in the future. Consequently, voice packets produced during telephone conversations are to have considerable share in all voice packets sent through computer networks. When certain amount of voice calls is performed simultaneously on a single link, the link needs to be shared between them, and a statistical multiplexing of voice packets is necessary. The multiplexing process is usually performed by a voice gateway which resides in a border between the traditional telecommunication network and a computer network transporting VoIP packets, Fig 1.

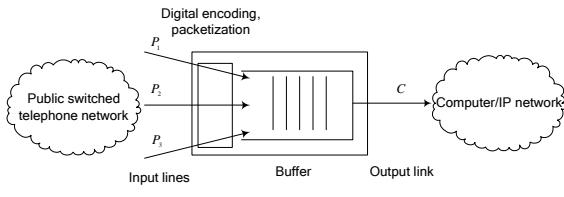


Fig. 1 A VoIP gateway

The gateway performs time division multiplexing, where periodically one user at time gains control of a full capacity of a

Arkadiusz Biernacki is with the Institute of Computer Science, Silesian University of Technology, Akademicka 16, 44-100 Gliwice, Poland (e-mail: arkadiusz.biernacki@polsl.pl).

link for a short instance of time. VoIP gateway can be considered as a kind of statistical multiplexer thus it is usually modelled as queuing systems with buffer space, to which are connected variable bitrate (VBR) sources, served by a transmission link of fixed capacity. If the sum of VBR sources peak rates P_i is not allowed to exceed an output link rate C_l of a multiplexer, i.e. $\sum_i P_i \leq C_l$, then a multiplexer is working under a peak rate allocation. The advantages of peak rate allocation multiplexing are no packet loss due to a buffer overflow at a burst level as well as a minimal packet delay. The disadvantage is that bandwidth is wasted when input links are sending at a lower rate than their peak rate. This motivates the argument for statistical multiplexing where the sum of the connection peak rates is allowed to exceed the link capacity, i.e. $\sum_i P_i > C_l$.

The ratio of the number of VBR sources that can be multiplexed on a fixed capacity link under a specified delay or loss constraint to the number of sources that can be supported on the basis of a peak rate allocation is called a statistical multiplexing gain (SMG). To determine and maximise the SMG, admission control rules are formulated that relate to traffic characteristics, which flows into the buffer of a VoIP gateway, the gateway performance constraints and parameters. In order to formulate these rules a multiplexed traffic model as well as a performance analysis of VoIP gateway are needed.

In this work we created MMPP model of multiplexed VoIP traffic and using this model we computed cumulative distribution of packet of the number of packets in the VoIP gateway. We based our model on Markov processes, because they provide flexible and efficient means for the description and analysis of computer system properties. Performance and dependability measures can be easily derived.

VoIP traffic exhibits properties of self-similarity and long-range dependence (LRD) [1, 2]. These characteristics have significant impact on a network performance. However, as pointed out in [3], matching the LRD is only required within finite time-scales of interest to the system under study. One of the consequences of this result is that more traditional traffic models such as Markov Modulated Poisson Process (MMPP) can still be used to model a traffic exhibiting long-range dependence

The rest of this paper is organised as follows: in section II

we gave theoretical background of our work. In section III we described the previous researches in the area of packet voice modelling. In section IV we presented our models of multiplexed VoIP and validated it. The performance analysis of the VoIP gateway was presented in V. Section VI is a conclusion of our work.

II. THEORETICAL BACKGROUND

Definition 1 A stochastic process $\{X(t) : t \in T\}$ constitutes a Markov Process (MP) if for all $0 = t_0 < t_1 < \dots < t_n < t_{n+1}$ the conditional cumulative distribution function of $X(t)$ depends only on the last previous value $X(t_n)$ and not on the earlier values $X(t_{n-1}), \dots, X(t_0)$, i.e.:

$$\begin{aligned} P[X(t) \leq x | X(t_n) = x_n, X(t_{n-1}) = x_{n-1}, \dots, X(t_0) = x_0] &= \\ &= P[X(t) \leq x | X(t_n) = x_n]. \end{aligned} \quad (1)$$

Definition 2 MP is time-homogeneous when $P[X(t) \leq x | X(t_n) = x_n]$ depends only on $(t - t_n)$ and is not function of t and t_n .

When a state space of MP is discrete the MP is called a Markov chain. When the time parameter t it is continuous a Markov chain is called continuous-time Markov chain (CTMC). The CTMC is described by matrix \mathbf{Q} which is called the infinitesimal generator of CTMC and is defined as:

$$\mathbf{Q} = [q_{ij}], \quad (2)$$

where q_{ij} is transition rate (intensity) coefficient and there is

$$\text{a dependency } q_{ii} = \sum_{\substack{j=1 \\ i \neq j}}^M q_{ij}, i = 1, 2, \dots, M \quad [4].$$

When time parameter t is discrete, i.e. $t \in \mathbb{N}$, than a Markov chain is called a discrete-time Markov chain (DTMC). DTMC is described by the matrix \mathbf{P} which is called one-step transition probabilities matrix and is defined as:

$$\mathbf{P} = [p_{ij}], \quad (3)$$

where p_{ij} is a probability of transition between a state i and state j , i.e. $p_{ij} = P(X_{n+1} = j | X_n = i)$.

A Markov-modulated Poisson Process (MMPP) is a doubly stochastic process where the intensity of a Poisson process is defined by the state of a Markov chain. The Markov chain can therefore be said to modulate the Poisson process, hence the name. MMPP is characterized by matrices \mathbf{Q} (2) and \mathbf{R} , the latter is the matrix of Poisson arrival rates. When the modulating process is in the state $X(t_n) = i, i = 1, 2, \dots, M$ than events are generated and their interarrival times are described by the exponential distribution

$$\alpha_i(t) = r_i \exp(-r_i t), i = 1, 2, \dots, M. \quad (4)$$

This distribution is valid during all the time the Markov process remains in state $X(t_n) = i, i = 1, 2, \dots, M$. The state sojourn times of CTMC are exponentially distributed.

Discrete time MMPP (dMMPP) evolves over time in constant time intervals and the number of events in each interval have a Poisson distribution whose parameter is a function of the state of the modulator Markov chain.

Formally, a two-dimensional Markov chain $(X, J) = \{(X_n, J_n), n = 0, 1, \dots\}$ with state space $\mathbb{N} \times S$ is considered dMMPP if for $n = 0, 1, \dots$

$$P(X_{n+1} = l, J_{n+1} = j | X_n = k, J_n = i) = \begin{cases} 0, & l < k \\ p_{ij} e^{-r_i} \frac{r_i^{l-k}}{(l-k)!}, & l \geq k \end{cases} \quad (5)$$

for all $m, n \in \mathbb{N}$ and $i, j \in S$. r_i and i are non-negative real constants $r_i, i \in S$ and \mathbf{P} is matrix defined in (3). Whenever (5) holds, we say that (X, J) is a dMMPP with set of modulating states S and parameters \mathbf{P} and \mathbf{R} , and write $(X, J) \sim \text{dMMPP}_S(\mathbf{P}, \mathbf{R})$, (6)

where \mathbf{R} is a matrix of Poisson arrival rates. A graphical interpretation of dMMPP was presented on Fig. 2.

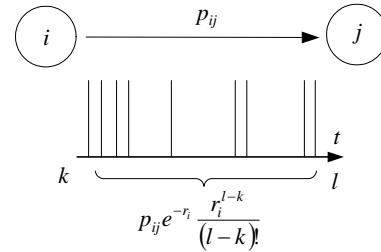


Fig. 2 Graphical interpretation of dMMPP

For time-homogeneous CTMC, for a very small interval $t = \Delta\tau$, there is a linear dependency:

$$p_{ij} = q_{ij} \Delta\tau, \quad (7)$$

where p_{ij} is probability of transition between the states i and j (3), and q_{ij} is transition rate (intensity) coefficient (2) [4].

III. PREVIOUS WORKS

The performance analysis of packet voice traffic usually includes the analysis of an appropriate queuing model. The works related to the analysis can be divided into two groups.

In the first group, authors concentrated on a microscopic view of network traffic and tried to model dependency between subsequent packets (micro scale). Eckberg treated multiplexed voice as the $\sum D_i / D/1$ queuing system and derived the exact delay distribution for it in [5]. In [6] it was stated that the multiplexed voice streams may be approximated with quite good results by a Poisson process. In [7] renewal processes were used and voice multiplexer was modelled as $G_i / D/1$ queuing system.

The second group consist of works in which authors tried to match the behaviour of the VoIP traffic over a relatively long time interval (macro scale) neglecting the dependency between subsequent packets. Usually, statistical properties of a voice source are taken into account. Stern [8] presented a queuing model based on the exponential ON/OFF model and an imbedded CTMC whose states represent the number of currently active speakers. Daigle et. al in [9] investigated three different approximations for aggregated arrival process based on a semi-Markov process model, a CTMC model, and a uniform arrival and service model. In [10] a multiplexer with infinite buffer was studied with a stochastic fluid flow model but it is shown in [11] that this model only works for a multiplexer under heavy load. A multiplexer with finite buffer is studied in [12] using the fluid flow model but it does not work well for small buffers. Some authors proposed approximate methods, mainly based on a Markov Modulated Poisson process (MMPP). A two-state MMPP was used quite successfully in [13] to estimate the delay in a multiplexer with infinite buffer. In [14] a different method for finding the parameters of the MMPP was developed. Besides authors proposed two other concepts based on renewal processes and fluid models to estimate multiplexer efficiency. In [15] the arrival process is approximated with a two-state MMPP and a method called asymptotic matching is suggested for the calculation of the parameters of the MMPP. However, in all cases above, the number of MMPP states was insufficient to capture a correlation of traffic over a longer period.

The common conclusion of macro scale models is that they lack stochastic properties of a process but they are better for a correlation modelling in comparison to the micro scale models. None of the models took into consideration connection scale, i.e. statistics of connections durations and interarrival times between them.

We proposed the model that took into account both burst and connection scales, neglecting inter-packets dependencies. Also, our modelling methodology was different in comparison to the above-mentioned works. We did not create aggregated model from single sources models but we approximated synthetic traffic obtained from trace driven simulation. The advantage of our methodology is simplicity and a good level of accuracy; the disadvantage is a lack of flexibility. When changing traffic parameters, one must generate again the synthetic trace and repeat the fitting procedure to update the model.

IV. TRAFFIC MODELLING

A. Traffic generation process

The synthetic trace was generated from real data recorded on both connection and burst level.

The connection level data were captured at the main telephone exchange of the Silesian University of Technology in Poland. It contained the record of about eighty thousand connections recorded in December 2005 using traditional telephone lines. The record included the beginning time of a con-

nexion and its duration time with one-second accuracy. Having excluded the data from holidays and weekends, we analyzed the set generating between 10-14 o'clock, which was a homogenous arrival Poisson process not influenced by time dependencies. In order to get busier multiplexed VoIP traffic, we increased the arrival rate. However, Poisson property of the arrival process was maintained.

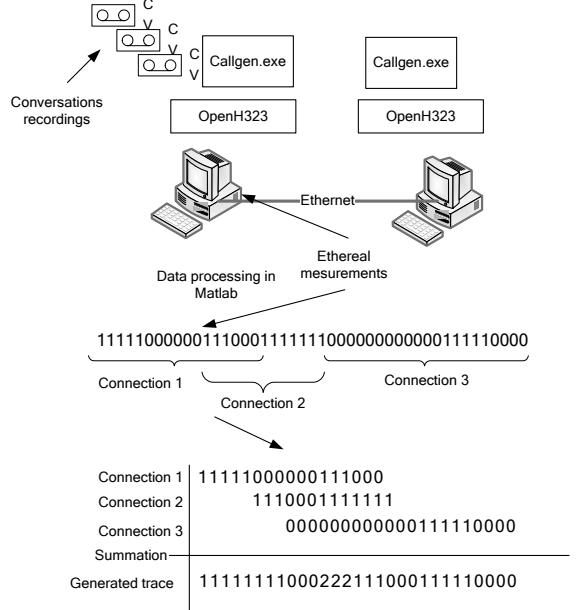


Fig. 3 The generation process of simulated VoIP traces

Than, with the use of Windows Sound Recorder we recorded one side of several real phone conversations held using popular VoIP software. We connected two computers equipped with OpenH323 library [16] with Ethernet cable. Previously recorded conversations were played and encoded by G.711 voice coder. Next, they were sent through the network to the second computer where we recorded the timestamps of the voice packets using Ethereal software [17]. We obtained single binary time series, where 0-values corresponded to OFF periods and 1-values corresponded to ON periods. Then, we concatenated the binary time series into one single series.

From these series, for each starting connection, a subset was randomly chosen. Its length equalled the connection duration time. For the all active connections we were totalling up the values of the subsets in discrete periods obtaining the time series which represented the traffic intensity, Fig. 3.

We generated several traces, each containing about one hundred thousands elements. The traces were divided into two categories; the model was trained on the traces from the first category (training set) and validated against the traces from the second category (test set). The sets represented the traffic which flows into VoIP gateway, which was capable of servicing up to 45 or 90 users, i.e. the VoIP gateway was assumed to

be equipped with 45 or 90 connection lines.

B. Parameters estimation

The inference procedure for model parameter estimation matched both the autocovariance and marginal distribution of the counting process which represented the number of packets in a time unit. The MMPP was constructed as a superposition of L 2-MMPP and one M -MMPP, where L is the number of two-states Markov chains and M is the number of states in Markov chain. The 2-MMPPs were designed to match the autocovariance and the M -MMPP to match the marginal distribution of a traffic trace. Each 2-MMPP modelled a specific time-scale of the data. The procedure started by approximating the autocovariance by a weighted sum of exponential functions that model the autocovariance of the 2-MMPPs. We adjusted the autocovariance tail to capture the long-range dependence characteristics of the traffic, up to the time-scales of interest to the system under study. The procedure then fitted the M-MMPP parameters in order to match the marginal distribution, within the constraints imposed by the autocovariance matching. The final MMPP with $M 2^L$ states was obtained by superposing the L 2-MMPPs and the M -MMPP. An important feature of the procedure was that both L and M were not defined a priori, since they were determined as part of the procedure. Detail of the procedure are given in [18]. In the end we obtained two matrices \mathbf{P} and \mathbf{R} representing dMMPP as in equation (6).

C. Model evaluation

We evaluated our model against trace-driven simulation. In Table 1 we presented comparison of mean and variance between the model, test and training traffic sets for traces produced by up to 48 and 96 users. Values after “ \pm ” symbol correspond to 95% confidence interval for simulated measurements.

TABLE I
COMPARISON OF THE SIMULATION AND MODEL STATISTICS

	Number of lines	P matrix size	Model	Simulation
Mean	48	9	515	532 \pm 3
Variance			2.3e+4	1.53e+4 \pm 300
Mean	96	56	1025	1028 \pm 12
Variance			3.4e+4	3.7e+4 \pm 720

At Fig. 4 we presented the comparison of packet arrivals density function between the simulated traffic and model. At Fig. 5 we presented similar comparison for an autocorrelation function.

V. VOIP GATEWAY PERFORMANCE

In this section we analyse queuing behaviour of VoIP gate-

way buffer using the fluids models theory. In these models, fluid flows into a fluid reservoir according to a stochastic process. In our case, fluid buffer was either filled or depleted, or both, at rates which are determined by a state of a background Markov process.

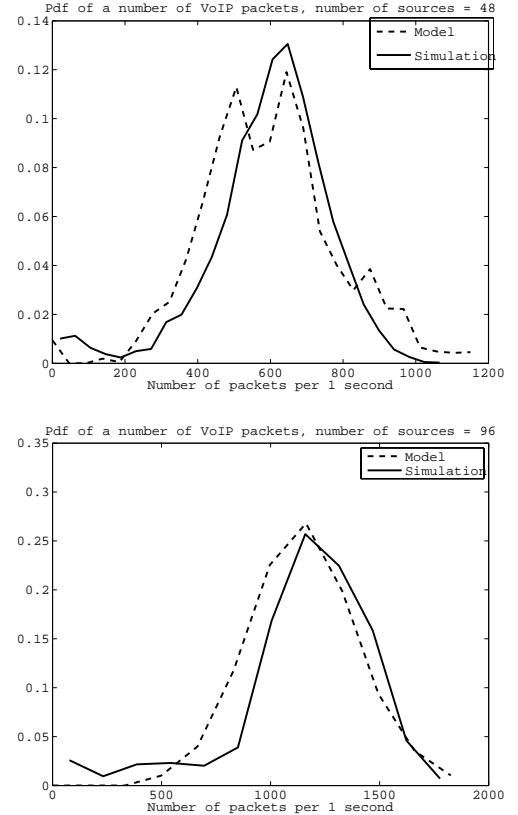


Fig. 4 Probability density function of a number of VoIP packets in a time unit

Let $C(t)$ denote the amount of fluid at time t in this reservoir. Furthermore, let $X(t)$ be a continuous time Markov process. $X(t)$ is said to evolve "in the background". The content of the reservoir $C(t)$ is regulated in such a way that the net input rate into the reservoir (i.e. the rate of change of its content) is $\tilde{r}_i = r_i - C_i$ at times when $X(t)$ is in state $i \in N$. Hence we have:

$$\frac{dC(t)}{dt} = \begin{cases} 0 & \text{if } C(t) = 0 \text{ and } r_x < 0 \\ \tilde{r}_{X(t)} & \end{cases} \quad (8)$$

A graphical interpretation of Markov fluid model was presented on Fig. 6.

The stability condition is given, $\sum_{i \in N} p_i \tilde{r}_i < 0$, where p_i is a stationary probability that $X(t)$ is in state $i \in N$. When the stability condition is satisfied $[X(t), C(t)]$ converges in distri-

bution as $t \rightarrow \infty$. Hence, the stationary joint distribution of $X(t)$ and $C(t)$ exists and is given by

$$F_i(y) = P[X = i, C \leq y] \quad i \in N, y \geq 0 \quad (9)$$

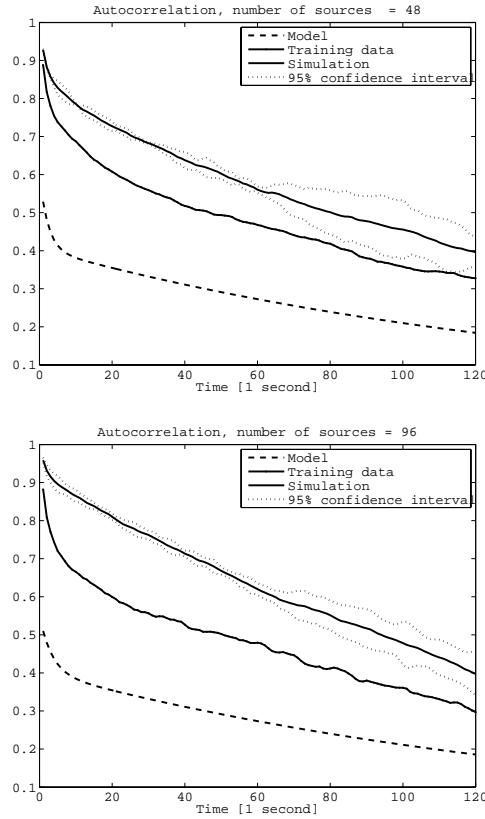


Fig. 5 Comparison of autocorrelation functions obtained from the model and trace-driven simulations

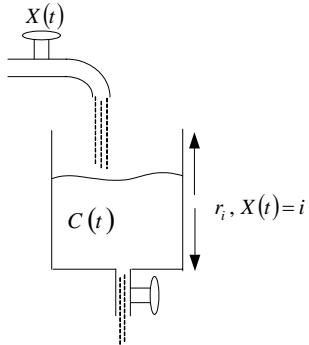


Fig. 6 Graphical interpretation of Markov fluid model

It can be shown that the vector $\mathbf{F}(\mathbf{y}) = [F_1(y), F_2(y), \dots, F_n(y)]^T$ satisfies the differential equation

$$\mathbf{R}\mathbf{F}'(\mathbf{y}) = \mathbf{Q}^T\mathbf{F}(\mathbf{y}), \quad (10)$$

where prime denotes differentiation and superscript T denotes transpose. \mathbf{R} is a diagonal matrix $\mathbf{R} = \text{diag}(\tilde{\gamma}_1, \dots, \tilde{\gamma}_N)$, \mathbf{Q} is the generator of the Markov process $X(t)$ of size $n \times n$. By assuming that \mathbf{R} is non-singular, i.e. $\tilde{\gamma}_i \neq 0$ for $i \in N$, the solution of (10) is given by

$$\mathbf{F}'(\mathbf{y}) = \mathbf{R}^{-1}\mathbf{Q}^T\mathbf{F}(\mathbf{y}) \quad (11)$$

In case the eigenvalues are simple, it follows that

$$\mathbf{F}(\mathbf{y}) = \sum_{i=1}^N a_i e^{\xi_i y} v_i \quad (12)$$

where the (ξ_i, v_i) are the eigenvalue-eigenvector pairs of the matrix $\mathbf{R}^{-1}\mathbf{Q}^T$ and a_i are constants that can be determined by boundary conditions. Further details of the above method can be found in [19]

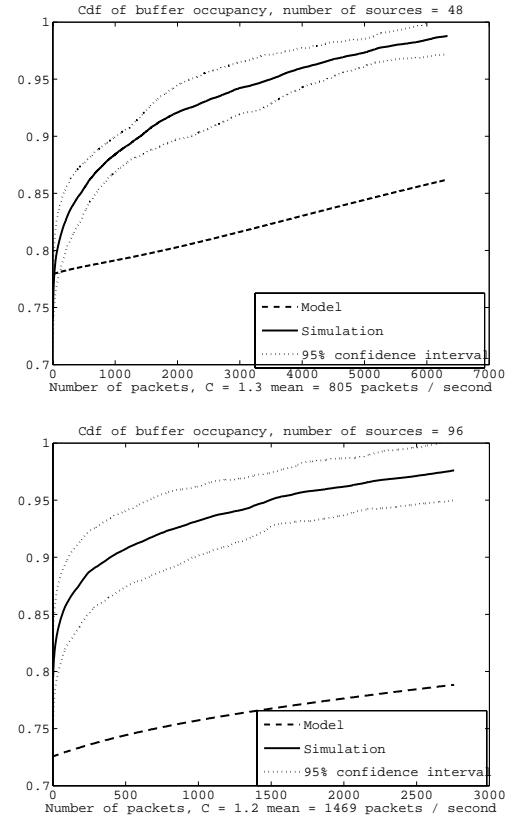


Fig. 7 Cumulative distribution of packets number in a VoIP gateway buffer

Through a few simple computations we transformed the matrix \mathbf{P} (3) of dMMPP into matrix \mathbf{Q} (2) representing CMTC, which was the argument of (10). Solving the mentioned equation we obtained the solutions as in (12), which were compared with results obtained during simulation. The comparison was presented at Fig. 7 for the traffic generated up to 48 and

96 sources. The output line capacity was set at 130% and 120% of mean traffic intensity respectively.

VI. CONCLUSION

In this paper, we examined the suitability of MMPP for modelling of multiplexed VoIP traffic, which flows into a VoIP gateway. We stated that MMPP might approximate the second order statistics of the traffic with good level of accuracy, although it made errors in variance estimation. We applied the model to evaluate a VoIP gateway performance by computing cumulative distribution of packets number in the VoIP gateway buffer. The results were in good agreement with the simulation.

REFERENCES

- [1] T. D. Dang, B. Sonkoly, and S. Molnár, "Fractal Analysis and Modelling of VoIP Traffic," presented at NETWORKS 2004, Vienna, Austria, 2004.
- [2] A. Biernacki, "Analysis of VoIP Traffic Produced by Coders with VAD," presented at 4th Polish-German Teletraffic Symposium, Wroclaw, Poland, 2006.
- [3] M. Grossglauser and J. C. Bolot, "On the relevance of long-range dependence in network traffic," *Networking, IEEE/ACM Transactions on*, vol. 7, pp. 629-640, 1999.
- [4] T. Czachórski, *Modele kolejkowe w ocenie efektywności pracy sieci i systemów komputerowych (in Polish only)*. Gliwice: Wydawnictwo Politechniki Śląskiej, 1999.
- [5] A. Eckberg, Jr., "The Single Server Queue with Periodic Arrival Process and Deterministic Service Times," *Communications, IEEE Transactions on [legacy, pre - 1988]*, vol. 27, pp. 556-562, 1979.
- [6] K. Byung, "Characterization of Arrival Statistics of Multiplexed Voice Packets," *Selected Areas in Communications, IEEE Journal on*, vol. 1, pp. 1133-1139, 1983.
- [7] Y. C. Jenq, "Approximations For Packetized Voice Traffic in Statistical Multiplexer," presented at IEEE INFOCOM, 1984.
- [8] T. E. Stern, "A Queueing Analysis of Packet Voice," presented at IEEE Global Telecomm. Conf., San Diego, USA, 1983.
- [9] J. Daigle and J. Langford, "Models for Analysis of Packet Voice Communications Systems," *Selected Areas in Communications, IEEE Journal on*, vol. 4, pp. 847-855, 1986.
- [10] D. Anick, D. Mitra, and M. M. Sondhi, "Stochastic theory of a datahandling system with multiple sources," *Bell System Technical Journal*, vol. 61, pp. 1871-1894, 1982.
- [11] S. Zheng, "Capacity Study of Statistical Multiplexing for IP Telephony," Department of Mathematics, Linkoping University, Sweden. LiTH-MAT-EX-98-12 1998.
- [12] R. C. F. Tucker, "Accurate method for analysis of a packet-speech multiplexer with limited delay," *Communications, IEEE Transactions on*, vol. 36, pp. 479-483, 1988.
- [13] H. Heffes and D. Lucantoni, "A Markov Modulated Characterization of Packetized Voice and Data Traffic and Related Statistical Multiplexer Performance," *Selected Areas in Communications, IEEE Journal on*, vol. 4, pp. 856-868, 1986.
- [14] R. Nagarajan, J. F. Kurose, and D. Towsley, "Approximation techniques for computing packet loss in finite-buffered voice multiplexers," *Selected Areas in Communications, IEEE Journal on*, vol. 9, pp. 368-377, 1991.
- [15] A. Baiocchi, N. B. Melazzi, M. Listanti, A. Roveri, and R. Winkler, "Loss performance analysis of an ATM multiplexer loaded with high-speed on-off sources," *Selected Areas in Communications, IEEE Journal on*, vol. 9, pp. 388-393, 1991.
- [16] Vox-Gratia, "OpenH323," 2005.
- [17] E. S. Inc., "Ethereal, A Network Protocol Analyzer," 2005.
- [18] A. D. Nogueira, P. S. Ferreira, R. Valadas, and A. Pacheco, "Modeling Self-Similar Traffic through Markov Modulated Poisson Processes over Multiple Time Scales," presented at IEEE International Conf. on High-Speed Networks and Multimedia Communications - HSNMC, Estoril, Portugal, 2003.
- [19] W. Scheinhardt, "Markov-modulated and feedback fluid queues," vol. Ph.D. thesis: University of Twente, the Netherlands, 1998.

Transparent Multihoming Protocol Extension for MIPv6 with Dynamic Traffic Distribution across Multiple Interfaces

Basav Roychoudhury

Department of Computer Science
St. Anthony's College
Shillong 793001 INDIA
rcbasav@dataone.in

Dilip K Saikia

Department of Computer Science and Engineering
Tezpur University
Tezpur 784028 INDIA
dks@tezu.ernet.in

Abstract— Mobile devices are now equipped with multiple interfaces for diverse access technologies that make up the wireless communication infrastructure. In this arena, the initial research was focused on tackling vertical handover – whereby the nodes move from one type of network to another (in terms of access technology) – while of late, works have been more oriented towards the use of these multiple interfaces to improve performance over the wireless network. In this paper, we propose modifications to Mobile IP to allow simultaneous use of multiple interfaces for performance enhancement, while keeping this multiplicity transparent to the upper layers. In addition, we suggest mechanisms to dynamically distribute the traffic over the available interfaces, depending on the network characteristic at these interfaces. We also present results of simulated experiments illustrating the gain in performance due to simultaneous use of multiple interfaces towards achieving seamless mobility and higher overall throughput.

Index Terms—MIPv6, mobile communication, mobility management, multihoming

I. INTRODUCTION

Current trends indicate that in near future, most mobile devices will come equipped with more than one network interface providing connectivity through multiple access technologies such as Wi Fi, GPRS, Bluetooth, etc. The provision of multiple network interfaces with multiple network addresses is referred to as Multi-homing [1][2]. The benefits of multi-homing includes seamless connectivity, multi-streaming, load balancing, fault tolerance and preferential routing [1][3].

The *Mobile IP* (MIP) [4][5] protocol provides a solution to take care of host mobility. As the *mobile node* (MN) changes its point of attachment, so does its IP address. The TCP connections are identified by the tuple – source IP address, source port, destination IP address, and destination port. This tuple changes when MN's IP address changes, resulting in TCP connection disruption. To keep the TCP connection alive, this tuple should remain invariant. MIP achieves this by allowing the MN to have two IP addresses – the *Home*

Address (HoA) which does not change with MN's movement, and a topologically valid *Care-of Address* (CoA) which depends on the network to which the MN connects from time to time. The CoA is transparent to the transport layer, and only the invariant HoA is used for the TCP connection.

The MIP in its present form, however, does not support multiple network interfaces. Considering the possible benefits of multi-homing, IETF has initiated work to provide support for multi-homing in MIPv6 [6], and has set up a new IETF working group – the Mobile Nodes And Multiple Interfaces in IPv6 (monami6) Working Group[7].

In IETF terminology, a host is called multi-homed if it has multiple network layer addresses – in case of IP networks this means that the host has multiple IP addresses. This does not necessarily mean that the host has multiple link layer interfaces – a single interface can also be connected to various *access routers* (ARs) resulting in multiple IP addresses. However, given the trend of mobile nodes equipped with multiple interfaces, we focus on multi-homed hosts having multiple link layer interfaces.

Montavont et al [8] proposed MMI (*Mobile IPv6 for Multiple Interfaces*) which focused on the MN's ability to use a backup interface for communications and to spread flows across its own interfaces. MMI distinguished the ways in which multiple interfaces can be used – *Per-correspondent node mobility*, *Per-flow mobility*, and *Per-flow load balancing*. Their work suggested extensions to MIP to support multiple interfaces at the MN. It introduced the *Load Balancing Mobility Option* to inform the *Correspondent Node* (CN), when MN is the sender, about the IP addresses of the MN interfaces. Conversely, if CN is the sender, the Load Balancing Mobility Option is used to inform the CN about the addresses of the MN interfaces and the proportion of the packets to be sent to each of these. However, the proportion is decided by MN and cannot be dynamically adjusted by CN, when CN is the sender.

Wakikawa et al in [6] addressed the fact that under the current form of MIPv6, it is impossible for a MN to register multiple CoAs in the CN's binding cache. They proposed the

use of a new identification number called *Binding Unique Identification Number* (BID) for each binding cache entry to accommodate multiple binding registrations for the MN's interfaces having the same HoA.

In this paper, we propose a scheme that allows the sender of the flow (MN or CN, as the case may be) to dynamically adjust the proportion of packets transferred using the multiple interfaces, without adding appreciable overhead to the existing protocol. The scheme allows the use of multiple HoAs and CoAs without coupling the two, thereby making the protocol robust to HA failures. We introduce a *Convergence Module* (CM) in the network layer to take care of the multiple interfaces while hiding such multiplicity from the transport layer so that the widely deployed TCP can function unaltered. The proposed modification is required only at the end hosts without needing any change within the subnet.

The paper is organized as follows. In Section II, we present an analysis in support of multiple interfaces. Section III introduces our scheme. Simulated experimental results are presented in Section IV. Section V summarizes the paper.

II. SIMULTANEOUS USE OF MULTIPLE INTERFACES-ADVANTAGES

In order to justify the use of multiple interfaces of a MN, we present an analysis for the available bandwidth in case of multi-homed MNs due to aggregation vis-à-vis that in case of single-interfaced node.

Let us assume that the total packets sent to the only interface of single-interfaced MN in time t be m , the fraction of the packets lost on the average due to transmission and other errors be p , the average packet size (considering only the payload) be x , and the average time the MN remains under the same access router be t sec. Let Δt be the time needed to complete a handover (handover latency).

The effective bandwidth at the MN interface, considering only the user data reaching the single interfaced mobile node, will be

$$W_{\text{eff}-s} = \frac{xm(1-p)}{t^2}(t - \Delta t) \text{ bytes/sec} \quad (1)$$

In case of multiple interfaced node too, let us assume that every t secs there will be a handover. Let m_i be the number of packets sent to interface i in time t . Let p_i be the fraction of packets lost in transit, and Δt_i be the handover latency at interface i . As before, let x be the average packet size.

The effective bandwidth at MN, considering the user data reaching across its n interfaces, will be

$$W_{\text{eff}-m} = \frac{1}{t} \left[\sum_{k=1}^n xm_k (1-p_k) - \frac{xm_i(1-p_i)\Delta t_i}{t} \right] \text{ bytes/sec} \quad (2)$$

where k runs over all available interfaces, and i is the interface which performs the handover in the interval t .

For simplification, if we assume $\sum_{k=1}^n m_k = nm$, and $m_i = m$, then (2) gets the form

$$W_{\text{eff}-m} = \frac{xm}{t^2} \left[nt \sum_{k \neq i} (1-p_k) + (nt - \Delta t)(1-p_i) \right] \text{ bytes/sec} \quad (3)$$

The second term in (3) is greater than the value in (1) (assuming $p = p_i$). Thus the total bandwidth given by (3) will be greater. To visualize the benefits achieved by using the multiple interfaces simultaneously, we plot $W_{\text{eff}-m} / W_{\text{eff}-s}$ versus t in Fig. 1, considering $\Delta t=4$ sec, $p=0.1$, $r=50$ where r is the number of packets sent per unit time, $x=1500$, $n=2$, and $m=t \times r$.

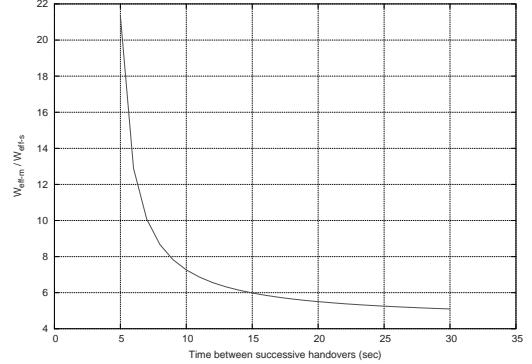


Fig. 1. Plot of $W_{\text{eff}-m} / W_{\text{eff}-s}$ versus t , time between successive handovers

With limited range of frequencies available, the cells will grow smaller, resulting in a reduced value for t . However due to the signaling involved, there will be no corresponding reduction in the handover latency Δt , making Δt comparable to t and resulting in the drop in W_{eff} . Thus, we must consider the use of multiple interfaces not only for enhanced reliability and seamless connectivity, but for increase in the effective bandwidth through aggregation. This is borne out by the exponential increase in $W_{\text{eff}-m} / W_{\text{eff}-s}$ with decreasing t , especially at lower values of t (Fig 1).

III. PROPOSED SCHEME

We propose a scheme which incorporates minor modifications to MIPv6 to support node multi-homing. This *Transparent Multihomed MIPv6 (TMMIPv6)* scheme envisages to

1. provide seamless mobility through horizontal and/or vertical handover, leading to ubiquitous Internet access
2. improve performance through bandwidth aggregation in scenarios where simultaneous usage of multiple interfaces is possible,

3. dynamically distribute traffic across the available interfaces in proportions commensurate with current network conditions,
4. allow usage of multiple HoAs and CoAs without coupling the two, thereby making the protocol robust to HA failures.

Our TMMIPv6 scheme proposes to achieve the above goals transparently, without any change to the existing infrastructure, except at the communication endpoints. Towards this end, we propose the introduction of a *Convergence Module* (CM) at layer 3 of the protocol stack.

A. Support for Multiple HoAs

The multi-interfaced MN may have more than one HoA, registered at the same or separate networks. It is possible that a single network interface is associated with multiple HoAs, or conversely, several network interfaces share the same HoA. However, assigning a single HoA to a given network interface is more advantageous because the applications do not need to be aware of the multiplicity of HoAs [6].

To reap the full benefit of simultaneous use of multiple interfaces, the MN should have more than one HoA. This is because:

1. If all the interfaces are registered with the same HoA, it will not be possible to utilize the other interfaces once one interface gets attached to the home link. This is because if the proxy neighbour advertisements for the sole HoA are stopped, packets will always be routed to the interface attached to the home link.
2. If the proxy neighbour advertisements are not stopped, packets will never be routed to the interface attached to the home link.

Conversely, if the interfaces are registered with separate HoAs, while the proxy neighbour advertisements for one HoA is stopped (because the interface under question has returned to its home network), the same for other HoAs can continue (as the interfaces registered with these HoAs continue to be in foreign networks) as usual. However, multiple HoAs can create problems for the base protocol [4,5]:

1. The MN registers the CoA with its HA when it moves to a new network. With more than one HoA, there would be an increase in control overhead if the MN now has to register all its CoAs with all its HAs.
2. For route optimized operation, the CoA is registered at the CN's binding cache. The HoA identifies the MN at CN's binding cache. With multiple HoAs, the MN can no longer be identified by its HoA.
3. As for DNS, if all the HoAs of every single MN are to be included, it might become unmanageable in the presence of numerous such MNs with their multiple HoAs.

We, therefore, introduce the concept of a *Primary HoA* (PHoA). The MN will always register one of its CoAs with the HA corresponding to the PHoA. This PHoA can be included in the DNS, so that an interested CN can communicate with the MN using this IP address. The PHoA for every MN can be

assigned initially, and should be invariant over node mobility.

The single PHoA can identify the MN at CN's binding cache. Being an IP address, the PHoA will be unique over the Internet. In the face of multiple HoAs, the TCP connection will be maintained with the help of this single static PHoA.

Apart from the MN, its multiple interfaces will also have to be uniquely identified. This can be achieved through the BID [6]. The binding update (BU) sent to the CN will therefore contain the PHoA, the BID for that interface, the HoA to which the CoA under question is registered, and of course, the CoA. Before updating the binding cache corresponding to the node/interface identified by the PHoA/BID, the CN needs to authenticate the BU coming from the MN. This is done through the return routability procedure, which requires the corresponding HoA [5].

In TMMIPv6 scheme, no interface needs to be permanently attached to a given HoA. An interface can use any of the available HoAs, and register its CoA at the corresponding HA. With multiple HAs available corresponding to multiple HoAs, the protocol will be more stable to HA failures. Once the communication starts, the PHoA is used mainly for node identification. Thus a physical failure of even the HA corresponding to the PHoA will not effect the ongoing communication.

B. The Convergence Module

To manage multiple IP interfaces and to perform dynamic adjustment of traffic flow from CN to the various interfaces of MN, as also the flow from MN interfaces to CN, we introduce a *Convergence Module* (CM) at layer 3 of the protocol stack. The function of the CM is to split a single flow across different interfaces at the sender, and accumulate the packets from the various interfaces and converge them into a singular flow at the receiver. The TCP connections are maintained based on the HoA (or by PHoA in case of multiple HoAs) of the MN, which does not change with latter's movement.

In a foreign network, MN would connect to an AR and would be assigned a CoA. The multiple interfaces may connect to different ARs and have distinct CoAs. At the network layer the packets will be sent or received at these topologically valid addresses, but will be replaced by an invariant HoA (or PHoA) for transport layer's consumption, leaving the mobility transparent to the latter. The functions of the convergence module are-

1. to distribute the traffic across multiple interfaces,
2. to dynamically decide on the proportion of traffic at each interface, depending on network conditions,
3. estimate the link characteristics to dynamically decide on the traffic distribution,
4. replace the topologically valid, but varying CoAs with the fixed HoA (or PHoA) for the TCP connection,
5. manage the handover at interfaces by redistributing the traffic across the remaining interfaces till the handover at the given interface concludes.

To decide on the proportions of the packets it shall also be

necessary to evaluate the suitability of the interfaces based on certain criteria. The possible criteria can be static ones such as cost, security, etc. and dynamic ones such as delay, available bandwidth, etc. While the static parameters are known a priori, it is crucial to make necessary provisions for estimating the dynamic ones.

The CM will therefore be required at both communication end points. The CM at the sender's end will estimate the link characteristics at the available interfaces with due assistance from the CM at the other end. When MN is the sender, the CM at this end will decide on the proportion of the packets to be sent through its available interfaces. On the other hand, with MN as the receiver, the CM at MN will inform its counterpart at CN about the available interfaces to which the packets pertaining to the flow can be distributed. Consequently, the CM at CN will decide on the proportion of packets to each of the MN interfaces.

In general, the CM at the sender's will initiate the process of link quality estimation and distribute the flow accordingly, while that at the receiver's will collect the packets pertaining to a given flow and pass them on to the transport layer after replacing the CoAs with the HoA (or PHoA), apart from assisting in link quality evaluation.

C. Estimation of Link Characteristics

The estimation process will always be initiated by the CM at the sender. For this, the CM at the sender will insert a timestamp (TS_s) into the outgoing packet (possibly at regular intervals to reduce overhead). This timestamp, meant only for the CM at the other end, can be placed onto the *destination option* of IPv6 header. The CM at the receiver's end will proceed with link characteristics estimation as follows:

1. set up buffers, one for each MN interface, at the receiver,
2. record the timestamp TS_s in the respective buffer,
3. record the current time (TD_D) in the buffer along with the packet size (PS),
4. replace the CoA with MN's HoA (or PHoA), and forward the payload to higher layer

Later on, when a packet is sent from the receiver to the sender (possibly a TCP ACK message) using the particular interface, the CM at the receiver will

4. calculate the delay (ΔT_D) between the time the last packet was received at this interface and the time when the current packet has been queued, i.e., $\Delta T_D = TS_{Df} - TS_{Di}$, TS_{Df} being the time when the outgoing packet is queued
5. include TS_s , PS and ΔT_D in the destination option of the IP packet to be sent through/to the particular interface

Once the CM at the original sender receives this packet, it will estimate the round trip time as $\Delta T = TS_r - (TS_s + \Delta T_D)$, where TS_r is the timestamp when the current (ACK) packet is received back at the original sender. If $\Delta T_1, \Delta T_2, \dots, \Delta T_n$ are the round trip times estimated at the n interfaces, then the CM at the sender can estimate the packets Δm_i of the total m packets to be sent using this particular interface i ($1 \leq i \leq n$) as

$$\Delta m_i = \frac{m \times \left(1 - \frac{\Delta T_i}{\sum_{j=1}^n \Delta T_j} \right)}{(n-1)} \quad (4)$$

As per (4), if ΔT_i is large, i.e., the estimated Round Trip Time is large, the fraction of total packets sent though that interface would be small, and vice-versa. The calculation for ΔT is done by the same module that had originally set the value for TS_s thereby avoiding the need for clock synchronization between CN-MN pairs.

The proposed interactions between the CMs at MN and CN for link quality estimation are shown in figure 2. If the CN initiates the flow, instead of the MN as in figure 2, the communication scenario will be very similar.

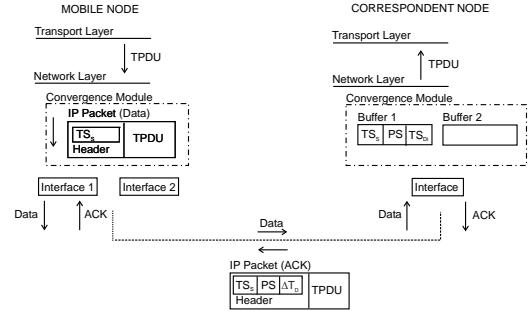


Fig. 2. Communication from the Convergence Module of the sender to the receiver, where sender is the Mobile Node

D. The Modified Protocol

With the introduction of CM at the communication endpoints, the flow of the protocol has to be appropriately amended. The protocol will now progress as follows:

1. **MN not communicating with any CN:** As the MN moves out of its home network, its CM will send BUs to its HA as envisaged in [5], except that it will now be sent to the HA corresponding to PHoA. In the absence of any communication, the MN will only use a single interface, and that too preferably the one with least communication cost (unless other considerations like security, etc. are involved). As MN moves to yet another foreign network, it will attempt to configure a new CoA at the previous interface, failing which it will try to configure some other interface in increasing order of cost.
2. **MN initiates communication with CN:** To benefit from bandwidth aggregation, the MN will get CoAs assigned and registered for its other available interfaces. To achieve route optimization, the CM at MN will then inform the CN of these CoAs, which will be registered after authentication. The CM at MN will also distribute the outgoing traffic to CN across these CoAs. Initially this distribution will be uniform, but these will be readjusted

once the link characteristics at each interface get estimated (as in Section III.C). When a handover takes place at an interface, the CM will set the proportion of packets handled by that interface to zero. On completion of handover, the CM at MN will once again start sending packets through this interface at the previous rate. If the new link has different characteristics, this rate will get readjusted on link characteristics estimation.

On the other end, the CM at CN will collect the packets of the same flow originating from different MN interfaces, and forward them to higher layer after replacing the source IP address with the HA (or PHoA), in addition to assisting assist in link quality estimation.

3. **CN initiates communication:** The CN will send packets to the MN's HA corresponding to its PHoA. These will be redirected to the CoA corresponding to interface configured with this HA. The MN will then activate its other interfaces, register the CoAs, and send BU to CN. After authentication, the CM at CN will send traffic distributed over these CoAs. As before, it will be a uniform distribution to begin with, followed by readjustments commensurate to link capacities. For a MN interface handover, the CM at MN will inform the same to its corresponding CM at CN if the former can preempt the same (by an L2 trigger, say). Alternatively, the CM at CN will infer the same by the absence of (ACK) packets from the other direction, or by detecting ICMP error messages such as ICMP_UNREACHABLE. In such a case, the CM at CN will stop sending packets to that interface, till it receives a BU for that interface. The proportion of packets sent to the new CoA will be guided the same principle as before.

The flow of the proposed protocol, when MN initiates the communication, is shown in figure 3. Similar will be the case when CN is the flow initiator.

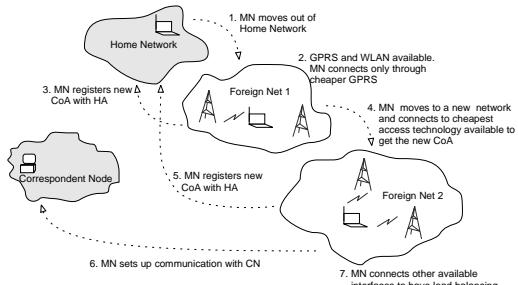


Fig. 3. Protocol - when MN initiates the flow

The route optimization may not always be desired, e.g. for location privacy. The CM at MN will then inform CN of other HoAs corresponding to MN interfaces. This information will be sent through HA corresponding to PHoA. If MN is the sender, this allows the CN to expect packets from these HoAs.

Conversely, if CN is the sender, its CM will distribute the traffic over these addresses.

IV. SIMULATION AND RESULTS

We conducted simulation experiments using NS2 to compare the performance of multi-interfaced MNs vis-à-vis those with only one interface. We used the NS2 version 2.28 [9] for the simulation. The multi-interfaced MN was equipped with two interfaces. We used TCP as the transport layer protocol, which was running over IP at the network layer, and the node mobility was managed by MIP. We considered the MN to be the recipient of an ftp flow from a CN. The general outline of our topology is shown in figure 4.

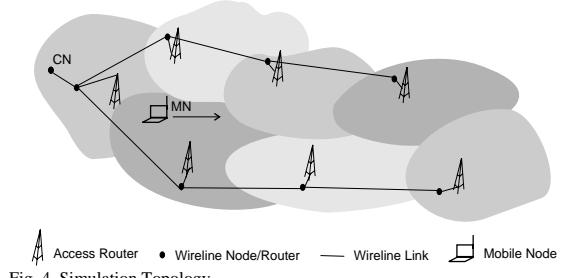


Fig. 4. Simulation Topology

We considered a topology where the ARs were placed with a lateral separation of 250 metres. That is, the horizontal component of the distance between two nearest ARs (horizontally) is 250 metre, but these two ARs are on different links. The distance between two successive ARs on the same link was therefore 500 metre. The MN was made to move away from its HA at a uniform speed of 10m/s, keeping equal distance from the two links. The two links were separated by a distance of 400 m.

We kept the same characteristics for all the nodes. The wireline link delay was set to 2 ms. In order to compare our scheme with base MIP, we ran these simulations alternately with mobile nodes equipped with single and double interfaces. We carried out simulation individually for a base station range of 400m and 500m respectively.

In the simulations, all the packets from the CN pass through the HA, and not directly to the MN as envisaged in route optimization. This is because the route optimization has not been implemented in the simulator. Thus if all the parameters are kept same, the CN-HA link might result in a bottleneck, constricting the traffic at the two interfaces. In order to avoid this bottleneck, we set the CN-HA link bandwidth to double of that between the HA and the base stations. The bandwidth of the wireline link was, therefore, set to 256 kbps, except that between the CN and the HA, which was set to 512 kbps. For each base station range, we ran two groups of simulations:

In the first case, the two interfaces were allowed to connect to any base station once they move out of the home network,

except that the both could not simultaneously connect to the same base station. This would be the situation, if the interfaces of MN support same access technology in real life.

In the other case, we introduced a restriction on the base stations a MN interface could connect to. Only one set of base stations was now made accessible to one interface, while the second interface of the multihomed MN was allowed access to the other set. As for the single interfaced node, it was allowed to connect only to one of these two sets, while the base stations in the other set were made transparent to the node. This would be the situation, if the two interfaces of the MN support distinct technologies.

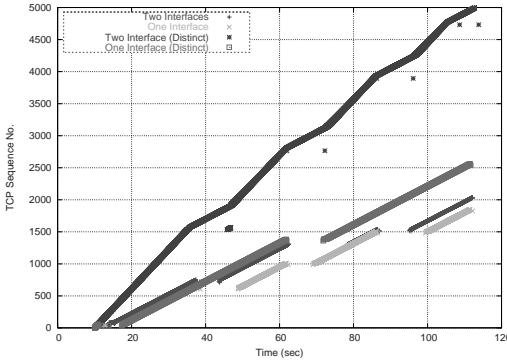


Fig. 5. Simulation result with base station range set to 400m

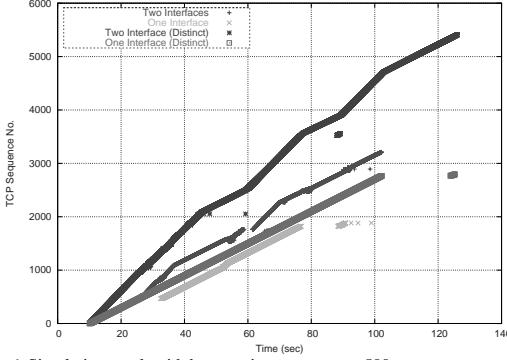


Fig. 6. Simulation result with base station range set to 500m

The results with the base station range set to 400m is shown in figure 5, while that with the base station range of 500m is shown in figure 6.

In all the plots of figures 5 and 6, we see that the performance, in terms of throughput, is mostly better (and never worse) in case of multi-interfaced MN as compared to one with a single interface. There is also a marked decrease in the handover delay in the two interfaced case. The result is surely better in cases where each interface was allowed to connect to a distinct set of base stations (marked *Distinct* in the plot legends), compared to the other cases. This is because

the router advertisements from one link is received by only one interface and is ignored by the other, resulting in fewer handovers. For the *Distinct* cases, the improvement is more remarkable for the smaller range of 400m compared to the 500m range. The reduced base station range minimizes number of distinct router advertisements that the MN received, which results in better performance.

Our experiments indicate that the benefit due to multi-interfaces can be appreciable if the interfaces under consideration support distinct, rather than the same wireless access technologies. In addition, the simulation results discourages the use of very high range for the base stations which, in turn satisfies the condition that the base station ranges be kept small for frequency re-utilization and reduced interference.

V. CONCLUSION

In this paper, we have described TMMIPv6, an extension to MIPv6 that would allow dynamic sharing of flow among available interfaces and thereby experience an enhanced bandwidth. This scheme will allow seamless mobility across overlaid networks with heterogeneous access technologies. We have introduced the concept of PHoA, which would allow a MN to be registered with more than one HoA. The available HoAs may no longer be coupled with particular interfaces, but can be used by any interface depending on availability. We have also presented the results of simulated experiments carried out to evaluate the basic premise of our scheme – sharing of load among multiple interfaces to enhance performance – and have shown that under various conditions, a multi-interfaced MN will experience a better throughput with seamless mobility as compared to its single-interfaced counterpart.

REFERENCES

- [1] N. Montavont, R. Wakikawa, T. Ernst, C. Ng and K. Kuladiniti, "Analysis of Multihoming in Mobile IPv6", IETF MIP6 Working Group Int. Draft (Wk. in Progress) (June 2006)
- [2] M. Riegel and M. Tuexen, "Mobile SCTP", IETF Network Working Group Internet Draft (Work in Progress) (Oct. 2006)
- [3] T. Ernst, N. Montavont, R. Wakikawa, E. Paik, C. Ng, K. Kuladiniti and T. Noel, "Goals and Benefits of Multihoming", Internet Draft (Expired) (October 2005)
- [4] C. Perkins, "Mobility Support for IPv4", RFC 3344 (August 2002)
- [5] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775 (June 2004)
- [6] R. Wakikawa, T. Enrst and K. Nagami, "Multiple Care-of Address Registration", MIPv6 Working Group (Work in Progress) (Oct. 2006)
- [7] Mobile Nodes and Multiple Interfaces in IPv6 (monami6) Working Group Official Charter, <http://www.ietf.org/html.charters/monami6-charter.html>
- [8] N. Montavont, T. Noel and K. Kassi, "Mobile IPv6 for Multiple Interfaces", IETF Mobile IP Working Group Internet Draft (Expired) (July 2005)
- [9] URL: <http://www.isi.edu/nsnam/ns/>

The wave variables, a solution for stable haptic feedback in molecular docking simulations

B. Daunay, A. Abbaci, A. Micaelli, S. Regnier

Abstract— This paper presents a new method for a six degrees of freedom haptic feedback in molecular docking simulations in virtual reality. The proposed method allows haptic interaction even in the case of classical molecular simulation which implies notoriously long computation time. These simulations are based on the Newtonian mechanics theory and imply an energetic interaction description between atoms. To use wave variables with delayed simulations appears as a solution to provide stable and robust teleoperation. This method can then be used with any energetic force field using a minimization process, thus avoiding the fastidious optimization of molecular simulation programs.

I. INTRODUCTION

Drugs are made of small molecules (ligands) which interact with proteins in order to inactivate them through a specific pocket (binding sit). The computational process of searching for a ligand that is able to fit the binding site of a protein is called molecular docking. The docking configuration should satisfy some constraints based on geometry, electrostatic, and chemical reactions between the ligand and the protein's atoms. The conformation (atoms' positions) of the ligand in the binding site has the lower potential energy. Therefore the energy surface generated by the atoms' force field has to be explored. All of these simulations are fully automated and can take, in the worst case, up to one month [1]. The only informations provided by the used softwares during the simulation, are a visual return of the conformation of the molecules and the value of the involved energy. Because of the relatively low success rates of the docking for fully automated algorithms, including a human operator in the loop appears as a novel solution.

Interactive haptic feedback for molecular docking can give additional information on the behaviour of the forces present inside the receptor. The operator would then be able to feel the repulsive or the attractive areas and define the best geometry of the ligand.

There are three primary methods for predicting protein behaviour: the ab-initio methods based on the Schrödinger equation, the semi-empirical methods (same as previous but some parameters are obtained from empirical data) and the

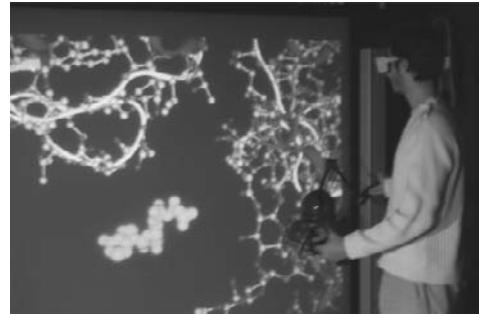


Fig. 1. Manipulation scene. The ligand has to be moved through the protein to the binding site.

empirical methods based only on the Newtonian theory.

The method we use, is the empirical one. All the molecular interactions are approximated by the Newtonian theory, therefore this method allows to simulate big proteins in an acceptable computational time. In order to simulate the proteins' behaviour, several methods are used and differ according to their applications.

The one we use is based on the minimization of the force field during the ligand manipulation. The goal is to reach the potential minimum but independently of time.

The aim of our work is not to optimize the molecular simulators (as proposed in some other works [2], [3]) but to conceive a method that takes into consideration their specificities. Indeed, the pharmaceutical engineers use softwares which are not real-time but which describe the interatomic interactions very precisely. Moreover, during their research, they use several force fields, each one being specific to a molecular property. Knowing that several force fields need to be minimized, that energetic interactions need to be described, and that the computing time for conformational changes is important, we developed a method allowing to feel the forces during a molecular docking using any molecular simulator based on a force field minimization process.

This article is structured as follows: the first paragraph describes the force field and the simulation we use in order to evaluate both the interaction energy between the ligand and the protein and the conformational change of these two molecules. The second paragraph describes a simple force/position bilateral coupling in order to specify the different problems to overcome. Then we propose a stable method for the control scheme of such a simulation and show

B. Daunay and A. Micaelli are with the Commissariat à l'Energie Atomique, 18 route du panorama 92256 Fontenay Aux Roses, France. (bruno.daunay@cea.fr; alain.micaelli@cea.fr)

A. Abbaci and S. Regnier are with the Laboratoire de Robotique de Paris CNRS – UPMC BP 61, 92265 Fontenay Aux Roses, France. (abbaci@robot.jussieu.fr; regnier@robot.jussieu.fr)

how the forces can conveniently be felt in order to make the operator “feel” the binding site’s force field.

II. FORCE FIELD MODEL AND SIMULATION METHOD

A. Force field

Many different force field models can be used to simulate proteins as AMBER [4], [5], CHARMM [6], MM3 [7], MM4 [8] and MMFF94 [9]. The multiple existing force fields differ more by their parameter set and their realism to model particular chemical species (proteins for example) than by the analytical form of the energies contributions. The one we use and which is described below is called MMFF94 (without solvation energy). It is more suitable for small molecules, as ligands, but it is also applicable for big proteins.

The model described above is typically expressed as summations of several potential energy components. A general equation of total energy, such as (1), includes terms for bond stretching (E_{Bond}), angle bending (E_{Angle}), torsion ($E_{Torsion}$), and non-bonded interactions such as electrostatic (E_{Elec}) and Van der Waals energies (E_{vdW}).

$$E_{Total} = E_{Bond} + E_{Angle} + E_{Torsion} + E_{Elec} + E_{VdW} \quad (1)$$

Bond stretching and angle bending energies are included in this force field and allow a flexible geometry. The simplest approach, based on the fact that most bonds are near the minimum of their energy, employs a quadratic term to model bond stretching and angle bending energies, as in (2) and (3).

$$E_{Bond} = \sum k_{Bond} / 2(l - l_0)^2 \quad (2)$$

$$E_{Angle} = \sum k_{Angle} / 2(\theta - \theta_0)^2 \quad (3)$$

Where k_{Bond} and k_{Angle} (stiffness of the bond and the angle) are experimentally obtained. l , l_0 and θ , θ_0 are respectively actual and ideal bond lengths and actual and ideal bond angles. In fact, these energy terms are more complicated. For bond energies, cubic terms are introduced as angle energies [10].

The torsion energy expression is represented by a Fourier series expansion which, as shown in (4), includes three terms.

$$E_{Torsion} = 1/2 \sum [V_1(1 + \cos \phi) + V_2(1 - \cos 2\phi) + V_3(1 + \cos 3\phi)] \quad (4)$$

Where V_1 , V_2 and V_3 are torsional barriers specified for the pair of atoms around which the torsion occurs. ϕ is the torsion angle (the rotation angle around the bond between the second and third atom in any serially connected four atoms).

Van der Waals interactions are described with the “Buffered 14-7” form [11]. The form of the potential is shown in (5). Van der Waals interactions are included whenever atoms i and j belong to separate domains or are

separated by three or more chemical bonds. R_{ij} corresponds to the distance between atom i and atom j .

$$E_{VdW_{ij}} = \epsilon_{ij} \left(\frac{1.07R_{ij}^*}{R_{ij} + 0.07R_{ij}^*} \right)^7 \left(\frac{1.12R_{ij}^{*7}}{R_{ij}^7 + 0.12R_{ij}^{*7}} - 2 \right)^7 \quad (5)$$

This form is used with an expression that relates the minimum energy separation R_{ii}^* (which can be assimilated close to the Van der Waals radius of atom i) to the atomic polarizability α (6), with specially formulated combination rules (7, 8), and with the potential depth ϵ_{ij} describing the minimum energy for a given atomic pair i and j .

$$R_{ii}^* = A_i \alpha_i^{1/4} \quad (6)$$

Where A_i is an experimentally defined constant.

$$R_{ij}^* = 1/2(R_{ii}^* + R_{jj}^*) + (1 + 0.2(1 - \exp(-12\gamma_{ij}^2))) \quad (7)$$

$$\gamma_{ij} = (R_{ii}^* - R_{jj}^*) / (R_{ii}^* + R_{jj}^*) \quad (8)$$

In order to limit the computation time of such a complicated energy, mainly responsible (like electrostatic energy) for the conformational change of both the ligand and the molecule, a significant approximation is made. Van der Waals and electrostatic energies influences are limited to 10 Å starting from the equilibrium position of the ligand in the binding site of the protein.

MMFF94 uses the buffered coulombic form as electrostatic interaction. As for Van der Waals energy, interactions are calculated when atoms i and j are separated by three or more chemical bonds.

$$E_{Elec_{ij}} = 332.0716q_i q_j / (D(R_{ij} + \delta)^2) \quad (9)$$

Where q_i and q_j are partial atomic charges of atoms i and j , R_{ij} is the internuclear separation. $\delta = 0.05$ Å is the electrostatic buffering constant and D the dielectric one.

B. Simulation

As said above, in the nature, a molecule and therefore a ligand or a protein is always in its minimum energy. Simulating the behaviour of such organic compounds devolves searching the global minimum of its force field. However, a molecule can have more than a thousand atoms, it appears clearly that the simulation should take a long time to reach the global minimum. It is possible to know the exact position of the protein’s atoms by nuclear magnetic resonance. Starting from these coordinates, the problem devolves then to reach a local minimum knowing that the global minimum will never be obtained. Energy minimization consists in finding a set of atomic coordinates that corresponds to a local minimum of the molecular energy function (such as the potential energy model). This is done by applying large scale non-linear optimization techniques to calculate a

conformation (near to the starting geometry) for which the forces on the atoms are zero.

Non-linear optimization algorithms typically have the following structure. Let x_k denote the vector of atomic coordinates at step k of the procedure and let E be the energy function. Then,

1. Test for convergence. If the convergence criteria are satisfied (see below), then x_k is returned.

2. Compute the search direction. Compute a non-zero vector p_k called the search direction. This is done with the Steepest Descent method ($p_k = -\text{grad}E(x_k)$), continued by the Conjugate Gradient method after a few iterations and finished by a Truncated Newton method when the gradient is reasonable.

3. Compute the step size. Compute a non-zero scalar a_k , called the step size, for which $E(x_k + a_k p_k) < E(x_k)$.

4. Set $x_{k+1} = x_k + a_k p_k$ and $k = k + 1$ and go to step 1.

The step size in step 3 is computed by using a safeguarded bicubic interpolation search along the search direction. In step 1, the optimization is done when any of the following three conditions are satisfied:

1. Root mean square gradient test: $|\text{grad}E(x_k)| < A\sqrt{n}$, where A is a predefined constant and n is the number of unfixed atoms.

2. Iteration limit test: $k > K$, where K is a predefined upper limit on the maximum number of iterations.

3. Progress tests: The following three conditions are simultaneously satisfied:

$$E(x_{k-1}) - E(x_k) < C(1 + |E(x_k)|) \quad (10)$$

$$|x_{k-1} - x_k| < C^{1/2}(1 + |x_k|) \quad (11)$$

$$|\text{grad}E(x_k)| \leq C^{1/3}(1 + |E(x_k)|) \quad (12)$$

In these conditions, C is a predefined constant indicating the number of significant figures in E that are required (the function test).

The necessary time to obtain a stable conformation is much larger than 1 ms implying that the forces feeling of this transformation could not be satisfying. In fact, a comprehensive haptic feedback needs a force feedback at the rate of 1 KHz. Considering that a pharmaceutical engineer wants to use different force fields to obtain the best docking conformation, rather than optimize a force field, we decided to use the response delay in the control law using the wave variables.

III. HAPTIC'S SPECIFICATION AND FORCE/POSITION COUPLING

A force/position control law is described on Fig. 2. Positions and orientations of the haptic device are sent to the simulation. Each position of each ligand's atom is modified

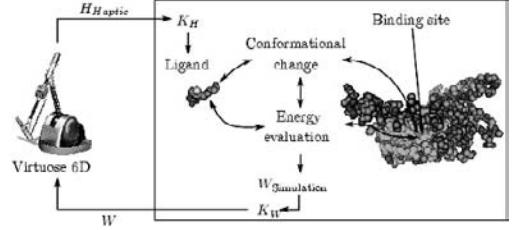


Fig. 2. Force/position coupling of a 6 DOF haptic device (*Virtuose* from *Haption Society*) with a docking simulation. The homogeneous matrix H_{Haptic} is sent to the simulation and a wrench W is sent back.

consequently as in (13). Then, the energy between the ligand and the binding site of the protein is evaluated, converted into forces and torques and sent to the *Virtuose*. During the energy evaluation, the protein and the ligand atoms' positions are once again modified by the minimization process's result. The global evolution of the ligand atoms' position is then described by (13), while the binding site evolution is only modified by the minimization process (14). Only the binding site and the ligand are flexible (to limit computation time).

$$H_{\text{Ligand}} = \underbrace{\begin{bmatrix} 1 & K_D \\ 0 & 1 \end{bmatrix}}_{K_H} H_{\text{Haptic}} H_{\text{Force Field}}^{\text{Ligand atoms}} \quad (13)$$

$$H_{\text{Binding site}} = H_{\text{Force field}}^{\text{Binding site atoms}} \quad (14)$$

Where H_{Ligand} and $H_{\text{Binding site}}$ represent the positions and orientations of the ligand and the binding site in the simulation, K_D is the displacement factor, H_{Haptic} is the position and orientation of the *Virtuose*, $H_{\text{Force field}}^{\text{Ligand atoms}}$ and $H_{\text{Force field}}^{\text{Binding site atoms}}$ are respectively the homogeneous matrix, representing the position variation induced by the force field, applied to the ligand and the binding site.

The wrench, reflecting the interatomic interactions between the ligand and the binding site, has to be sent to the *Virtuose* at the rate of one 1 KHz, to provide a good haptic feedback. Both the ligand and the protein are flexible, they change their conformation to a stable one while the ligand is moved.

A. Nano/Macro coefficients

The first problem to overcome is to convert a displacement in the simulation's nanoscale (\AA) to a macro one in the operator's scale (haptic displacement) and then to feel in the macro world the micro forces acting on the ligand. Two coefficients were introduced. The first, K_D (displacement factor), responsible for the macro to nano scaling, is determined as

$$K_D = x_{\text{Ligand}}^{\text{Nano displacement}} / x_{\text{Haptic}}^{\text{Macro displacement}} \quad (15)$$

where x_{Haptic} and x_{Ligand} are the position and the orientation of the haptic interface and the ligand, and the second, K_w (force

factor) a micro to macro scaling factor. K_w is determined as in (16)

$$K_w = \frac{\text{Maximal force/torque admissible on Virtuose}}{\text{Maximal force/torque of the simulation}}, \quad (16)$$

where the maximal force/torque admissible on *Virtuose* is 5 N and the maximal force/torque of the simulation is a user determined constant depending on the required precision.

B. Energy

As described in paragraph II, the force field describing the protein's behaviour uses the interaction energies. Consequently, a derivation of this interaction energy in the three space directions is made as a first approximation (highly approximative formulation of the forces starting from the energy, only allowing us, at first, to understand the profile of the forces during a docking). The effort is corrected in the displacement direction:

$$W_k^{\text{Simulation}} = \frac{E_k - E_{k-1}}{x_k^{\text{nano}} - x_{k-1}^{\text{nano}}} \quad (17)$$

where k is the iteration number and x^{nano} the position and orientation of the interface in the nano world. A singularity will appear if the interface displacement between step k and $k + 1$ is nil. Then, the force/torque sent to the interface is arbitrarily set to zero.

C. Results

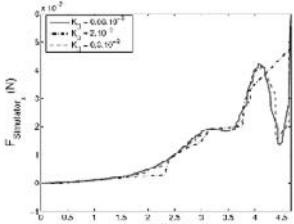


Fig. 3. Experimental results showing the influence of K_D on the forces' stability (on the x axis for the Van der Waals and electrostatic forces) during a docking of a biotin into a streptavidin complex.

Fig. 3 shows the forces (on the x axis) obtained during a ligand displacement ($\sim 5 \text{ \AA}$ on the x axis) in its binding site starting from its equilibrium position, with a displacement factor successively equal to 8.10^{10} , 3.10^{10} and 2.10^9 . A small displacement factor will lead to a force which can be easily interpreted because of its stability. The Van der Waals instabilities and the electrostatics forces can be then precisely depicted. But a high one will lead to forces with higher dynamic. In the first case, we can precisely feel the interaction forces but a docking is not possible (in the macro world, 1 meter corresponds to 0.08 \AA). In the second case, the docking is possible (1 meter corresponds to 2 \AA), but the simulation is unstable and the feeling unsatisfying.

The influence of K_w can be shown on Fig. 3. K_w makes the correspondence between the maximal force/torque admissible on the *Virtuose* and a desired maximal force/torque on

the simulation ($K_{w\text{-Max simulation}}$). If $K_{w\text{-Max simulation}} = 1.10^7$, all the forces grater than $F = 5.10^7 \text{ N}$ will be felt like a barrier. But all the forces smaller than this one will be felt according to this ratio. This coefficient has to be chosen according to the desired precision.

The last paragraph presents some solutions to overcome the problem of time delayed manipulation which is not passive [12]. The aim is to obtain a stable control of the simulation, and to have a better feeling of the forces taking into account the high dynamic shown above.

IV. PASSIVE CONTROL OF A DOCKING SIMULATION

A. Wave transformation

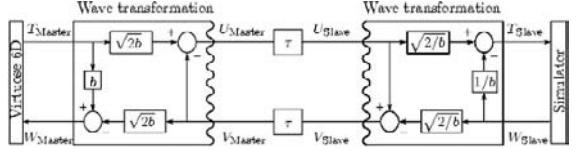


Fig. 4. Wave transformation (U and V) of informations (velocity and wrench) from master to slave in a time-delayed τ transmission. b is a stiffness factor.

Wave variables are a derivation of the well defined scattering parameters. Niemeyer [13] demonstrates that time delay is a passive element of a control chain if it is considered in the wave domain. If all components of the transmission are passive, as well as the haptic device and the simulation, then the entire process consisting in sending the information by the haptic device, its transformation in the wave domain, its interpretation by the simulator and its feedback, become stable and robust whatever the delay is.

In the wave domain, including a delay τ (and considering Fig. 4), the equations governing the transmission are:

$$U_{\text{Slave}}(t) = U_{\text{Master}}(t - \tau) \quad (18)$$

$$V_{\text{Master}}(t) = V_{\text{Slave}}(t - \tau) \quad (19)$$

In order to interpret the informations provided by the wave variables, it is necessary to successively encode and decode the wave. This is done by two bijective expressions, (20) and (21) for encoding which implies (22) and (23) to decode.

$$U_{\text{Master}}(t) = (bT_{\text{Master}}(t) + W_{\text{Master}}(t)) / \sqrt{2b} \quad (20)$$

$$V_{\text{Slave}}(t) = (bT_{\text{Slave}}(t) + W_{\text{Slave}}(t)) / \sqrt{2b} \quad (21)$$

$$T_{\text{Slave}}(t) = \sqrt{2/b}U_{\text{Slave}}(t) - 1/bW_{\text{Slave}}(t) \quad (22)$$

$$W_{\text{Master}}(t) = bT_{\text{Master}}(t) - \sqrt{2b}V_{\text{Master}}(t) \quad (23)$$

Where the wave impedance b is an arbitrary constant which determines the stiffness of the transmission, T , F , U and V are respectively the velocity and force, the forward and backward waves.

B. Application

The proposed approach, described below, is based on that the time delay is not between the two wave transformations but occurs only after having decoded the wave. The forward wave U is sent at the rate of the haptic device, 1 kHz. The simulator sends a response at the rate of 400 Hz. V is refreshed as soon as the simulator can compute a force.

1) Damping and wave variables: The molecular simulator described on Fig. 3 needs a position at its entry port. This position is applied to the ligand via a displacement factor. But the wave variables are expressed from the master's velocity. Our first approach was to send the master's position to the simulation and use the wave variables as a back carrier information wave (Fig. 5).

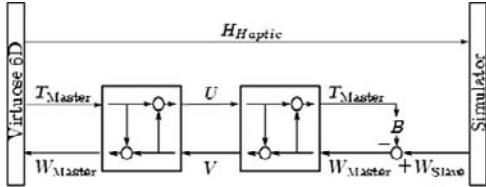


Fig. 5. Wave based control of molecular docking simulation. B is a user defined damping constant.

This wave is then considered as a damper (as it depends on the coefficient B , which is a user defined constant, and also on b) responsible for the dynamic attenuation of the forces send by the simulator (24).

$$W_{Master} = W_{Slave} - BT_{Master} \quad (24)$$

Considering an admittance local loop, the two waves U and V had to be expressed as in (25) and (26).

$$U = (bT_{Master}(t) - W_{Master}(t)) / \sqrt{2b} \quad (25)$$

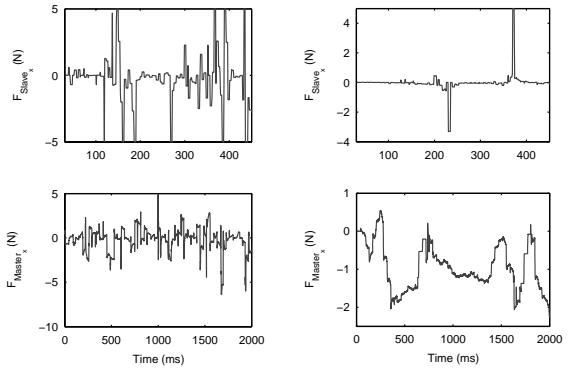
$$V = U + \sqrt{2/b}W_{Master} \quad (26)$$

These two expressions lead to the expression of the velocity (27) and the backward wave (28).

$$T_{Master} = \frac{1}{b+B} \left[\sqrt{2b}U + W_{Slave} \right] \quad (I.1)$$

$$V = \left(1 - \frac{2B}{b+B} \right) U + \left(\sqrt{\frac{2}{b}} - \sqrt{\frac{2}{b}} \frac{B}{b+B} \right) W_{Slave} \quad (I.2)$$

Two coefficients had to be chosen: the first one, b , determining the stiffness of the control loop and the waves' stability, and the second, B , responsible for the internal damping of the high forces' amplitude acting during the docking. There is an other meaning of the damping factor B . Indeed, the simulation is not passive as it would create energy. This coefficient could then dissipate it in order to make the control stable. An infinite value for B will dissipate all the energy ($V = -U$), the haptic device is blocked (all the incoming energy is sent back).



(a) $B = 0$, $K_D = 2.10^9$, $K_W = 5.10^7$ (b) $B = 50$, $K_D = 2.10^9$, $K_W = 5.10^7$
Fig. 6. Influence of coefficient B on the simulation's stability.

Fig. 6(a) shows the haptic device's response with $B = 0$. The energy is not dissipated and the only damping existing in the control is b (mainly responsible for the wave variables stabilisation). The docking is stable and possible but the intermolecular forces could not be conveniently interpreted. If $B = 50$ (Fig. 6(b)), the docking is possible and stable but all the forces are filtered because of the viscosity induced. To compare with the force/position control which is clearly unstable, this method, consisting in using the waves as a damper filtering the high forces' dynamic, also as a time delayed stabilisation method, could be a solution to the problem of molecular docking. By introducing viscosity and integrating time delayed simulator response in the control loop, the control becomes stable. However, even if the control is stable, the macro feeling of the micro forces should be difficult to understand because of the damping factor B . A new approach, allowing to have a better transparency in the bilateral control, is described below.

2) Wave variables control loop: For this control scheme, a modification of the simulator is needed. The haptic device sends a velocity to the simulator after having encoded it to a wave and decoded it. However, the simulation needs position data to manipulate the ligand. Integrating a velocity into a position will create a drift, the haptic device has to be regularly repositioned while the simulation is continuing (Fig. 7).

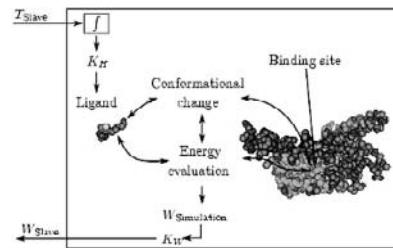


Fig. 7. Description of the molecular docking simulator. T_{Slave} and W_{Slave} are successively decoded from wave variables and encoded to wave variables (Fig. 4)

The velocity integration is done as follows:

$$[T] = \dot{H}_{Haptic} H_{Haptic}^{-1} \quad (29)$$

where $[T]$ is the velocity skew symmetric matrix determined from T_{Slave} . The discretisation of (29) leads to (32)

$$H_{k+1} = e^{([T])} H_k \quad (32)$$

where k is the iteration number and I the identity $[4 \times 4]$ matrix. H_{k+1} modify the position and orientation of the ligand as in (13).

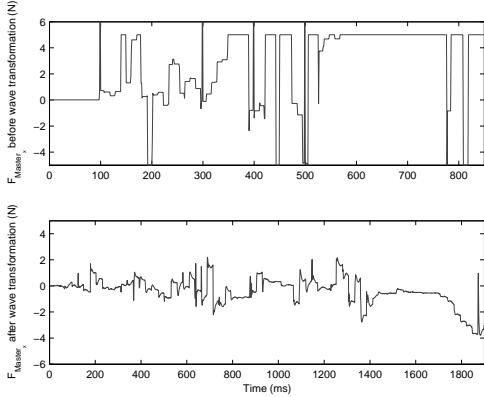


Fig. 8. Force feedback of the simulator, before wave transformation ($W_{Master} = K_w W_{Simulation}$), and after having decoded the wave. $K_w = 5.10^7$, $K_d = 1.10^9$.

Fig. 8 shows the haptic device's response regarding the simulation forces. F_{Slaves} is saturated at 5 N in order to protect the haptic device. As the forces become unstable, the waves act as a damper and the response is not as unstable as the excitation is. The control is inherently stable, the users only determine the wave's stability coefficient b . The main advantage of this method is that the forces sent back by the simulator are not as filtered as the previous method, making possible a good feeling of the micro forces.

V. CONCLUSIONS AND FUTURE WORKS

A. Conclusions

In this paper, a molecular docking simulation, with six degrees of freedom haptic feedback, is presented. Starting from initial observations - simulation based on the energy, long computation time for haptic manipulations, high forces' amplitudes - we have implemented two new methods for stable manipulations. They are both based on wave variables because it guarantees the stability in time delayed manipulation. The first one allows to overcome the problem of the high forces' dynamic dissipating the energy in a virtual damper, but the feeling of the forces is not quiet satisfying. The second one, based on the real wave variables allows to obtain a stable simulation, making possible the interpretation of the micro forces by the operator.

B. Future Works

The high forces' amplitude problem, deserves a particular attention. As a first approach, we only derivated the energy provided by the simulator but some singularities appeared. A solution could be to consider a quadratic potential $E = 1/2kp^2 \bullet gtr(R)$ where E is the potential, k and g are two positive constants and p and R are respectively the position and the orientation of the ligand. To find the forces and the torques means searching for the constants k and g in order to approach the real potential energy by the new quadratic one. The results have to be more stable than a simple derivation. The macro feeling of micro forces is not conveniently solved. A simple force factor K_w is not the best approach, because of the high dynamic of these forces. A variable force factor could be an interesting solution. Far from the binding site, a small force factor could be applied in order not to feel the high forces' amplitude. In the binding site, near the equilibrium position, a small force factor could be set therefore refining the ligand's position. The finality of this method is to provide a fully integrative and semi-autonomous program usable for Sanofi-Aventis, in order to accelerate the design of new drugs and make it more reliable.

REFERENCES

- [1] M.L. Teodoro, G.N. Philipps Jr, L.E. Kavraki, Molecular docking: A problem with thousands of degrees of freedom, *Proc. of the IEEE International Conference on Robotics and Automation*, 2001, pp. 960-966.
- [2] K. Kazerounian, From Mechanisms and Robotics to Protein Conformation and Drug Design, *Proc of ASME*, vol. 126, 2004, pp. 40-45.
- [3] J. Cortes, T. Simeon and al., A path planning approach for computing large-amplitude motions of flexible molecules, *Bioinformatics*, vol. 21, 2005, pp. i116-i125.
- [4] W.L. Jorgensen and J. Tirado-Rives, The OPLS potential function for Proteins. Energy minimization for crystals of cyclic peptides and crambin, *J. Am. Chem. Soc.*, vol. 110, 1988, pp. 1657-1666.
- [5] S.J. Weiner, P.A. Kollman and D.A. Case, A new force field for molecular mechanical simulation of nucleic acids and proteins, *J. Am. Chem. Soc.*, vol. 106, 1984, pp. 765-784.
- [6] B.R. Brooks, R.E. Bruckler, B.D. Olafson, D.J. States, S. Swaminathan, M. Karplus, CHARMM: A program for macromolecular energy, minimization, and dynamics calculations, *J. Comp. Chem.*, vol. 4, 1983, pp. 187-217.
- [7] J-H. Lii, N.L. Allinger, The MM3 force field for amides, polypeptides and proteins, *J. Comp. Chem.*, vol. 12, 1991, pp. 186-199.
- [8] N.L. Allinger, K. Chen, J-H. Lii, An improved force field (MM4) for saturated hydrocarbons, *J. Comp. Chem.*, vol. 17, 1996, pp. 642-668.
- [9] T.A. Halgren, Merck molecular force field. IV. Conformational energies and geometries, *J. Comp. Chem.*, vol. 17, 1996, pp. 587-615.
- [10] T.A. Halgren, Merck molecular force field. I. Basis, Form, Scope, Parametrization, and Performance of MMFF94, *J. Comp. Chem.*, vol. 17, 1996, pp. 490-519.
- [11] T.A. Halgren, Representation of van der Waals (vdW) Interactions in Molecular Mechanics Force Fields: Potential Form, Combination Rules, and vdW Parameters, *J. Am. Chem. Soc.*, vol. 114, 1992, pp. 7827-7843.
- [12] J-H. Lee, C-H. Cho, J-B. Song, C-S. Hwang, M. Kim, Haptic interface using delayed reflection wave: application to a passive haptic device, *proc. of the IEEE International Conference on Robotics and Automation*, 2005, pp. 2482-2487.

- [13] G. Niemeyer, Using Wave Variables in Time Delayed Force Reflecting Teleoperation, Phd, Massachussetts institute of technology, 1996.

A Model for Resonant Tunneling Bipolar Transistors

Buket D. Barkana and Hasan H. Erkaya

Eskişehir Osmangazi University, Electrical-Electronics Engineering Department,
26480 Eskişehir, TURKEY

bdbarkana@aol.com

hherkaya@ogu.edu.tr

Abstract

A model is proposed for the resonant tunneling bipolar transistor current voltage characteristics. The model is based on a model for the resonant tunneling diode and the traditional Ebers-Moll model of the bipolar transistor. A device structure was simulated, and characteristics that resemble that of the resonant tunneling transistor were obtained.

1. Introduction

The first resonant tunneling diode (RTD) was reported by Chang, Tsu and Esaki in 1973 [1]. Since then, detailed studies on resonant tunneling diodes led to the invention of resonant tunneling transistors (RTBT). Especially in the last ten years, many theoretical and experimental studies have been published in this area (Pan *et al.*, 2001 [2]; Cheng *et al.*, 1999 [3]; Tsai, 2001 [4]; Lacomb and Jain, 1996 [5]; Bigelow and Leburton, 1994 [6]; Taniyama *et al.*, 1994 [7]). In these studies, mostly AlGaAs, GaAs, and InGaAs materials were used, and the common emitter current gain was obtained around 140. The resonant tunneling devices can be used to design high performance electronic systems owing to their multi-state nature.

In this study, we suggest a simple model for RTBT that is based on the resonant tunneling phenomenon and traditional Ebers-Moll bipolar transistor model. The Ebers-Moll model is used to calculate current and voltage values. The resulting current-voltage characteristic of the RTBT structure is found to be similar to experimental results. Simulation was carried out on Matlab.

2. Structure of the Resonant Tunneling Diode

A resonant tunneling diode is a two-terminal quantum-effect device made of two undoped quantum

barriers and an undoped quantum well. A typical physical structure of the RTD is shown in Figure 1. For the simulation, the doping concentrations of both p- and n-type doped regions are assumed to be 10^{17} cm^{-3} . Layer widths of barrier regions and well region are assumed as 5 nm and 3 nm, respectively.

The current density through the RTD is given by Nag [8] as

$$J = \left(\frac{2e}{8\pi^3 \hbar} \right) \int (\nabla_{kl} E) T_u^* T_u [f(E) - f(E + |e|V)] d^3 k \quad (1)$$

where, k_l is the wave vector component perpendicular to the junction interface; E , electron energy; T_u , the transmission probability; V , applied voltage; $d^3 k$, the volume element in the wave vector; $f(E)$, the Fermi electron distribution function. The current-voltage characteristic of the RTD, which is obtained through the simulation, is shown in Figure 2.

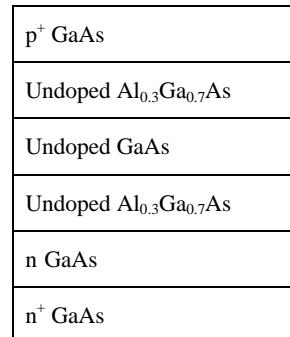


Figure 1. The structure of the resonant tunneling diode.

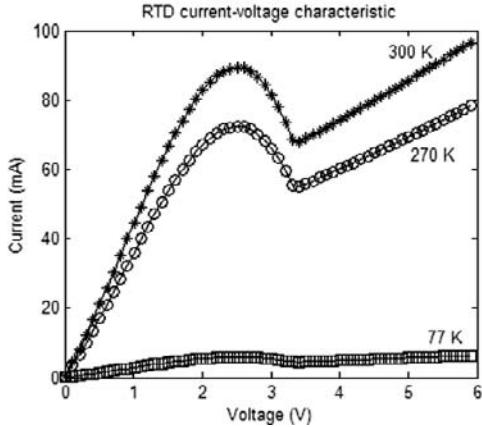


Figure 2. Current-voltage characteristic of the RTD.

3. A Model for the Resonant Tunneling Bipolar Transistor

In this section, a simple RTBT is proposed which is based on Ebers-Moll model. The model is given in Figure 3.

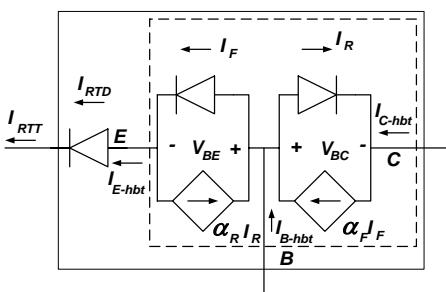


Figure 3. A circuit model for the Resonant Tunneling Bipolar Transistor

The base and collector currents of the RTBT are the same as that of the base and collector current of the heterojunction bipolar transistor (HBT). The current and voltage equations of RTBT can be expressed as follows:

$$I_{E_{RTT}} = I_{E_{RTD}} = I_{E_{HBT}} \quad (2)$$

$$V_{BE_{RTT}} = V_{RTD} + V_{BE_{HBT}} \quad (3)$$

$$I_{C_{RTT}} = I_{C_{HBT}} \quad (4)$$

$$I_{B_{RTT}} = I_{B_{HBT}} \quad (5)$$

The first step to find RTBT's current-voltage characteristic is to calculate the current, I_{RTD} , of the RTD for a given voltage, V_{RTD} . Here, I_{RTD} is also equal to the emitter current of the RTBT. Therefore, base-emitter voltage of the HBT can be found using Ebers-Moll model for the given I_{RTD} . This voltage value, $V_{BE_{HBT}}$, is expressed as

$$V_{BE_{HBT}} = V_T \ln \left[\frac{\left[\frac{\alpha_F I_{E_{RTD}}}{I_{S_{HBT}}} + \alpha_F + 1 \right]}{\left[1 - \alpha_F \cdot e^{-V_{CE_{HBT}}/V_T} \right]} \right] \quad (6)$$

$$V_{BC_{HBT}} = V_{BE_{HBT}} - V_{CE_{HBT}} \quad (7)$$

Collector and base currents can be calculated using the voltage value, $V_{BE_{HBT}}$:

$$I_{C_{HBT}} = I_{S_{HBT}} \left[\left(e^{V_{BE_{HBT}}/V_T} - 1 \right) - \frac{\left(e^{V_{BC_{HBT}}/V_T} - 1 \right)}{\alpha_R} \right] \quad (8)$$

$$I_{B_{HBT}} = I_{E_{RTD}} - I_{C_{HBT}} \quad (9)$$

Here, α_F and α_R are forward and reverse common-base current gains that are calculated for the BJT structure for the given bias conditions.

The physical properties of the RTBT in this study are assumed as shown in Figure 4. A similar structure was used experimentally by Wu *et al* in 1991 [9].

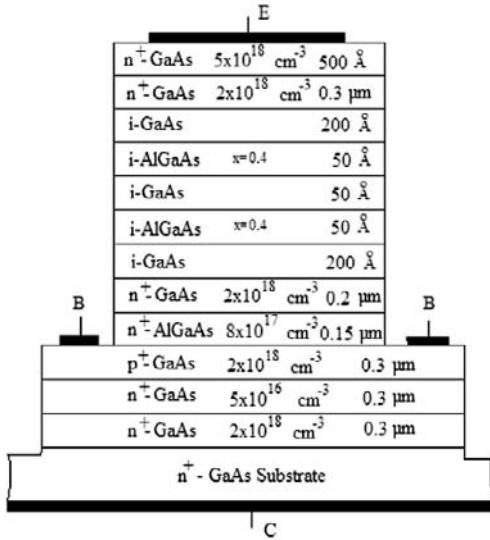


Figure 4. The physical structure of the RTBT.

4. Results

The simulation results for the current-voltage characteristics of the RTBT based on the model presented above are given Figure 5 and Figure 6. According to the characteristics in Figure 5, the device has the typical characteristics of the resonant tunneling transistor. The characteristics have the negative differential resistance region for the base-emitter voltage range 3.2 V – 4.0 V.

The collector current appears to be constant for a given base-emitter voltage regardless of the base collector voltage as long as the base-collector voltage is kept above 0.5 volts.

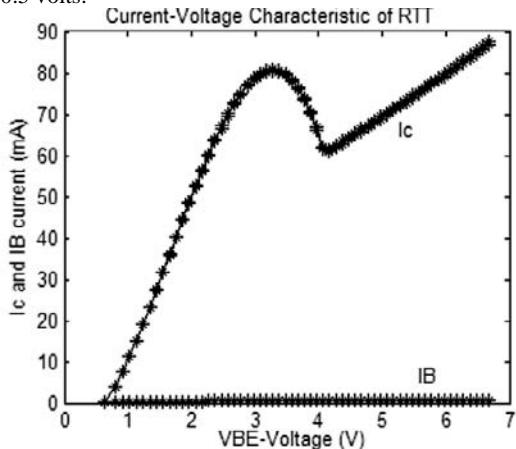


Figure 5. The collector and base currents versus base-emitter voltage of the RTBT for $V_{CE} = 1.5$ V.

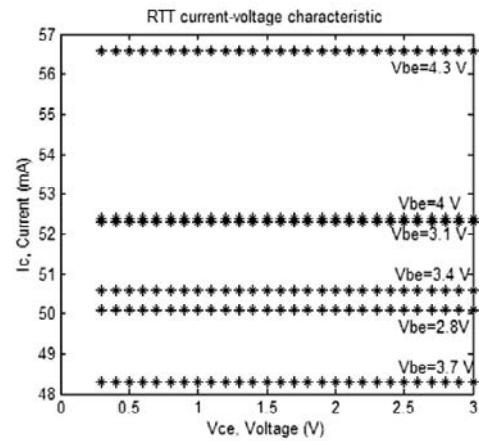


Figure 6. $I_C - V_{CE}$ Characteristics of the RTBT for various V_{BE}

5. Conclusion

The model that is consisted of a resonant tunnel diode and a bipolar transistor provides characteristics that resemble the characteristics of the resonant tunneling bipolar transistors.

REFERENCES

- [1] L. L. Chang, L. Esaki, and R. Tsu, "Resonant Tunneling in Semiconductor Double Barriers" *Appl. Phys. Lett.*, vol.24, p. 593, 1974.
- [2] H.-J. Pan, S.C. Feng, W.C. Wang, K.W. Lin, K.H. Yu, C.Z. Wu, L.W. Laih, and W.C. Liu, "Investigation of an InGaP/GaAs resonant tunnelling heterojunction bipolar transistor," *Solid State Electronics*, No.45, pp.489-494, 2001.
- [3] S.Y. Cheng, J.H. Tsai, W.L. Chang, H.J. Pan, Y.H. Shie, and W.C. Liu, "Investigation of an InGaP/GaAs resonant tunneling transistor (RTT)", *Solid-State Electronics*, Vol.43, pp.755-760, 1999.
- [4] J.H. Tsai, "Quantized Resonant Tunneling Phenomena of AlGaAs/InGaAs Heterojunction Bipolar Transistors", *Japanese Journal of Applied Physics*, Vol.40, pp. 5865-5870, 2001.

- [5] R. Lacomb and F. Jain, "A self-consistant model to simulate large-signal electrical characteristics of resonant tunneling bipolar transistors", *Solid State Electronics*, Vol.39, No. 11, pp 1621-1627, 1996.
- [6] J.M. Bigelow, J.P. Lepurton, "Self-Consistent Modelling of Resonant Interband Tunneling in Bipolar Tunneling Field-Effect Transistors", *IEEE Transactions on Electron Devices*, Vol.41, pp.125-131, 1994.
- [7] H.Taniyama, M. Tomizawa, A. Yoshii, "Two-dimensional analysis of resonant tunneling using the time-dependent Schrodinger equation", *Japanese Journal of Applied Physics*, Vol.33, pp.1781-1786, 1994.
- [8] B.R Nag, *Physics of Quantum Well Devices*, Boston: Kluwer Academic Publishers, Dordrecht, 2000.
- [9] J. S. Wu, C. Y. Chang, C.P. Lee, K.H. Chanh, D.G. Liu, and D.C. Liou, "Characterization of Improved AlGaAs/GaAs Resonant Tunneling Heterostructure Bipolar Transistors", *Japanese Journal of Applied Physics*, Vol. 30, No.2A, pp. L160-L162, 1991.

Developing secure Web-applications – Security criteria for the development of e-Democracy Web-applications

António Pacheco and Carlos Serrão

Abstract— One of the most important requirements in government websites is the security. The Data Protection Act, Human Rights Act and other legislation require that privacy is respected. Beyond this, Government websites must be secure to build trust and maintain the reputation of electronic government. This will be seriously damaged if websites are defaced, services are unavailable or sensitive information is released to the wrong people. Securing a Web application is difficult, not only because of various technical departments coordination involved, but also because most security tools are not designed to address the Web application as a whole, including how the different pieces of the application interact with each other. The potential for a security breach exists in each layer of a Web application. Traditional security solutions, such as access control or intrusion detection/prevention systems, are specialized to protect different layers of the Internet infrastructure, and are usually not designed to handle HTTP and HTML attacks. While these tools are useful for their specific functions, they do not address all of the issues that Web applications present. More important, using these tools can give administrators a false sense of confidence if they do not know that the other vulnerabilities exist. This paper is being performed in the context of the e-Voto project, a Portuguese project dealing with the complexity of the electronic voting systems, in particular to the dissemination of electoral results over the WWW. So, in this paper the authors present some recommendations to web applications development that manage and present important information like electoral results with medium-high security level.

Index Terms— E-Vote, Web security, Electoral results, E-Democracy

I. INTRODUCTION

Web application development is very different from other development environments. The Web browsers and the nature of HTTP pose security pitfalls not found in traditional client-server applications.

Carlos Serrão is with Adetti/ISCTE - Ed. ISCTE – Av. das Forças Armadas, 1600-082, Lisboa, Portugal; (e-mail: Carlos.Serrao@iscte.pt , Miguel.Dias@iscte.pt)

António Pacheco is with Marinha de Guerra Portuguesa, Direcção de Análise e Gestão de Informação, Lisboa, Portugal; (e-mail: guerreiro.pacheco@marinha.pt).

Web developers must know how web servers and browsers interact, the nature of Internet communications, and the attacks web applications undergo on the Internet.

The technical staff cannot rely on the fact that a Web Server (and/or web-applications) is secured by the usage of a firewall and network intrusion detection system. Security flaws in web applications easily bypass firewalls and other basic security measures. Many banking, military and e-commerce sites have learned that lesson on the hard way. It's easy for a medium-experienced software developer to create a web application that allows outsiders access to files on the server, gather passwords and customer information, and even alter the application itself despite firewalls and other security measures.

This document presents e-Democracy web application security problems. The examples are specific, the flaws and concepts described apply to all languages and platforms: such as .Net, ASP, PHP, Servlets, Cold Fusion and more.

II. E-DEMOCRACY WEB SITES SECURITY AREAS

A. The security of website

It needs to be stressed that most successful breaches of integrity on websites are made possible by misconfiguration of the web server itself and failure to install relevant security patches. The information in this section aims to raise awareness on correct configuration and patch application.

The security of a website is determined by the security of the following [9]:

- the web server application; the operating system of the web server computer;
- the local area network of the web server computer;
- ‘backend’ (eg database) applications supporting the web server;
- the authoritative domain name server for the web server network;
- remote web server administration, eg, use of FTP, use of server extensions (not addressed here), and
- physical and personnel measures in place to ensure that the web server environment is secure, but these are beyond the scope of this guidance.

In the sections below each area of security will be considered sequentially with recommendations for each. All of the recommendations should be followed if good website

security is to be achieved. This guidance presupposes that the web server is open to an untrusted user community and does not address the possibility of trusted users accessing or maintaining the website remotely. Most web servers provide remote file and directory authentication for such purposes, although the types and use of such authentication are beyond the scope of this paper.

B. The security of the Web server applications

A website or a web application is hosted by a web server. A web server is an application that accepts requests from client web browsers in the Hypertext Transfer Protocols (HTTP and HTTPS) and responds by sending web pages and other content to the client web browsers. A web page designer can manually generate these web pages or they can be automatically generated. Automatically generated pages may use interpreted scripting languages, such as Perl to produce the web pages by common gateway interface (CGI), or they may use proprietary server-side programming extensions such as Microsoft's Active Server Pages (ASP). Web server security therefore splits into two further areas:

- The security of the web server application itself;
- The security of any CGI scripts or server extensions.

For the security of the web server itself, the following steps are recommended:

- a)** As with any application, ensure that administrator monitor briefings from your CERT [5] and commercial sites such as bugtraq [4] on a regular and frequent basis and install any security patches relevant to the version of the web server that you are using and that address problems that the server is susceptible to.
- b)** When configuring the web server, ensure that any access controls that can be set within the web server application are set appropriately on all directories under and including the root directory of the web as follows:

- Ensure that no web directories or files within the web directory structure are modifiable or writable by anyone other than the web server administrator.
- Access to web pages should be read-only for users, although a web user will need permission to execute scripts or programs used to generate web pages dynamically.
- Web users should not be able to list the contents of directories, unless there is a clearly identified requirement.
- No access should be granted to other directories or programs in the web directory structure unless there is an explicit need.
- No access should be granted to the web server executable or to the web server configuration files.

- No access should be granted above the root of the web server directory structure.

c) Do not assign access control override privileges to the user as these can be abused by attackers to turn off access control.

d) Enable logging on the web server so that all server activity is logged. This should be analyzed on a regular and frequent basis by the organization's IT security officer for events indicative of an attack, for instance attempts to run non-existent scripts. The web server log should also contain all attempted and established connections, error messages, remote authentication attempts, all scripts run and any access control violations for files and directories under access control of the web server. This can be a complex and expensive activity so it may be considered more practical to use an Intrusion Detection System and analysis of these logs. For the security of CGI scripts and server extensions, the following steps are recommended:

- a)** Remove all sample scripts installed with the server.
- b)** Disable any server directives or extensions that enable scripts to run operating system level commands on the web server, for example, in a Unix environment, Server Side Includes.
- c)** In conjunction with your Departmental Security Officer or equivalent responsible officer ensure that a suitably qualified professional, external to your website development, checks all scripts that are used on the web server to ensure that they validate input to allow only expected types and lengths of input data and produce error messages otherwise. Care should be taken that special characters and empty values are treated adequately. Escapes to an operating command shell should never be permitted.
- d)** If possible, store all scripts in the same directory and forbid execution of scripts outside this directory.

C. The security of the "backend" applications supporting the web server

Any supporting 'backend' applications (eg databases) should be stored on another computer. Care needs to be taken that the web user account can only perform a specified set of actions on the 'backend' applications so that the security of those applications is not unduly compromised. For example, if a database application is used as a read-only source to web users, the web user account should have read only access, while if the database is updated by the web user account via web forms, the web user should be restricted to database update queries. This could be performed by a database application that provides access control by query type and data object (such as database and table) within the database application.

III. RECOMENDATIONS

At this point we will present the most important variables that change and interact with the most common e-Democracy web sites security level.

A. Sanitize browser input

Input fields displayed in web-page form, could be used to permit specific searches by users in E-Democracy web applications. When electoral results are presented, in some situations is important to user search by some fields like city or politic coalition. All input from web browsers, such as user data from HTML forms and cookies, must be stripped of special characters and HTML tags. This is by far the most common vulnerability in web applications. Everything from directory traversal problems to cross-site scripting problems can usually be traced to the simple lack of proper stripping of user input [2]. There are two separate dangers with browser input data: 1) Input containing special characters such as ‘!’ and ‘&’ could cause the web server to execute an operating system command or have other unexpected behaviour. 2) User input stored on the server, such as comments posted to a web discussion program, could contain malicious HTML tags and scripts. When another user views the input, that user's web browser could execute the HTML and scripts.

Special characters in form input

Characters such as ‘&’, ‘>’, ‘!’ and ‘\$’ (sometimes called “meta characters”) have special meaning to many operating systems. For example, both Unix and Windows interpret the symbol ‘<’ (“less than”) as meaning “read input from a file”. When an HTML form input is used to open files, send mail or interact with the operating system in any way, malicious users can enter meta characters hoping they will be passed to the underlying operating system, possibly accessing files or executing commands. “Invisible” characters are also a threat especially the NULL character (ASCII zero) and end-of-line characters [3]. Programs written in C use the NULL character to mark the end of strings. However, languages like Perl do not. Inserting a NULL character in an HTML form input can cause strings to be terminated early or to be unrecognized by simple pattern matching filters [4]. This “poisoned NULL” attack can cause interesting security problems when Web applications are built using both C and other languages.

Malicious HTML in stored data

Some web guest book and discussion board software allow users to format their comments with HTML tags such as ‘’ and ‘’. This is correct, but storing arbitrary HTML also allows users to insert Javascript, Java and DHTML tags. When another user reads the comments posted, the code can be executed on their browser, *as if developer web site had created it*. User-created HTML can contain malicious scripts, applet references and other techniques to access files, delete files, crash a user's computer or steal information. Stored HTML tags don't threaten developer web server security like metacharacters do [5]. Instead, they threaten the users of developer web application. The real danger is the one of trust. An outsider is allowed to store potentially dangerous HTML on developer server. A

Java applet or insecure Javascript functions that normally would be stopped could be allowed to run in the user's browser because it came from a trusted source.

Solutions

The best practice is to strip unwanted characters, invisible characters and HTML tags from user input. When stripping unwanted characters, the safest way is to check the input against a list of *valid* characters, not a list of invalid ones. Why? It's too difficult to determine all possible malicious characters... just when developer think he has thought of them all, a cracker invents an unexpected attack like “poisoned null” characters described above. It's also easier to simply check input against a list of characters ‘A-Z’ and ‘0-9’. All input should be sanitized, not just selected fields. All input can potentially percolate through to unexpected places. Even if developers are certain a particular input field cannot cause problems now, it might become possible in future revisions of the application. Rather than try to guess what input could be dangerous, it's simpler and more effective to just sanitize all input immediately when received from the browser. It's simple to strip unwanted characters from a string. However, input from web applications is not always plain ASCII or UTF-8. Characters in HTML form fields, cookies and CGI query strings can also be expressed as HTML Character Entities. For example, the symbol ‘<’ (“less than”) can be input using the HTML Entity code ‘<’ or in numeric format as ‘<’. Stripping ampersand (&) and semi-colon (;) characters from input will disable such sly attempts to bypass input filters, but if developer web application requires those characters it is best to decode any HTML character entities in all input to their corresponding characters before stripping. If web application is written in Perl using the CGI.pm library, all form input fields can be sanitized at the beginning of the program with a routine similar to the following:

```
use HTML::Entities ();
use CGI qw/:standard/;
$ok_chars = 'a-zA-Z0-9 ,.-';
foreach $param_name ( param() ) {
    $_ = HTML::Entities::decode( param($param_name) );
    $_ =~ s/[^\$ok_chars]//go;
    param($param_name, $_);
}
```

The above converts HTML character entities to plain characters then silently removes all characters except the ones listed in \$ok_chars from all HTML form input fields collected by CGI.pm. This method cripples shell metacharacters, the poisoned NULL attack, disables HTML tags and defeats attempts to hide metacharacters using HTML entities. The above code snippet works well, but instead of silently stripping input a more thorough solution would be to raise an alarm for the system administrator. When invalid characters are detected, it would be better to alert a system administrator and log the error and IP of the user to a file. Then developer would know when potential crack attempts are made and by whom.

When sanitizing input, keep in mind that user input is not just limited to HTML form fields. A malicious user can potentially alter everything a web browser normally sends.

HTML cookies and HTTP headers such as REMOTE_USER can be altered easily. It's not difficult to write a Perl script that poses as a web browser and sends altered versions of form input, hidden fields and other data complete with forged cookies and HTTP headers [7]. Never trust any input from a browser because all of it can be altered.

B. HTML directory

Most web applications (not only Electoral Results dissemination web-sites) use many types of files:

- **Static files:** HTML headers, footers, JPEG images and other raw non-changing content.
- **Parsed HTML:** static HTML mixed with executable code, such as PHP and ASP files.
- **Include files:** Libraries and routines shared by parsed HTML and other files.
- **Data files:** Database or flat text files written by the web application

Most beginning web developers dump all their files in the HTML directory, the "public_html" "htdocs" or "C:\inetpub\wwwroot" directory on the web server. Web servers use a "permission by directory" model: files are treated according to the directory they are in [3]. Every file in the HTML directory can be accessed by a web browser if the URL is known. Every file in the "cgi-bin" directory can be executed. If developer web applications write data files (such as a guest book application or message board), don't put the data files in the "cgi-bin" directory or "html" directory. Every file in "cgi-bin" can be executed, including data files. Every file in "/public_html" can be read by a browser. Never assuming an outsider will never guess the name of a file in those directories, because eventually they will. For example, if the developer web application places a data file named "card_numbers.dat" in "/public_html", any outsider who guesses the file name can view its contents in their browser. Keeping all data files in a common location also makes it easier to manage the web site. Developers have separate locations for HTML files, executable programs, shared library code and data. Separating the data files into sub-directories by application helps eliminate file naming problems, such as two different applications that create data files named "data.txt".

C. Hidden fields

Many CGI programs rely on so-called "hidden" form fields to store state information, settings and previous input data. However, HTML "hidden" fields are not hidden and not secure. Users can see them simply by viewing the HTML source of developer form in their browser. It's easy for a user to change "hidden" fields. They only have to same the HTML form to their computer, edit the HTML then re-submit the form. Contents of hidden fields should be sanitized and validated just like any other user input field. Hidden fields should not be used to set access modes or privileges for a CGI program (such as an 'admin' mode or 'paying user' privilege) without also using some form of user validation, such as

password and username access restrictions. A better way of preserving state information and settings is to store data in a file or database on the server then use an HTTP cookie or unique URL ID to reference the file [7]. This is more difficult to program, but important data stays on developer server.

D. POST / GET

When user need to use search or filter engine to obtains electoral results HTML forms can be submitted using either GET or POST methods. POST is preferred, especially when sending sensitive information. The GET method sends all form input to the web application as part of the URL. For example:

```
http://www.yourdomain.com/cgi-bin/cart.cgi?username=Pacheco&password=1234
```

When the web application is called using GET, the above input is visible on the browser's URL location window. However, a more dangerous problem is that URLs are logged in many places (The web server access log; The web browser's disk cache and history file; In firewall logs; In proxy server and web cache logs such as Squid [10]).

All this logging allows others to see the data sent from HTML forms using GET. The POST method sends form input in a data stream, not part of the URL. The data is not visible in the browser location window and is not recorded in web server log files. The POST method is also more practical. There's a limit to how many characters can be sent using the GET method, but POST can send an almost unlimited amount of data from an HTML form. However, even though POST information is generally not logged, like all other plain text information sent from a browser it can still be sniffed as it passes across the Internet. However, sniffing must be done in real time as information is sent across the Internet and requires the attacker to have physical access to the data lines between the web browser and web server. The risk of information being sniffed is far less than the risk of information being gathered from log files.

E. Validate on server

Developers know they must check that form input fields contain the correct data type, that required input is not missing and to perform other simple sanity checks. However, a disturbing trend recently has been to use Javascript or Java applets to validate user input. In a E-Government web application, HTML form fields are checked when the user submits the HTML form to the web server. If a mandatory field is blank or has the wrong type of input, the web application typically sends back an HTML page describing the errors and lets the user must submit the form again. Client-side validation lets this work be done in by the browser. Javascript or Java applets can be used to check inputs before the form is submitted to the web application, and not allow the form information to be sent until all fields are correct. This saves time and processing by the web application. It moves the overhead of input validation from the web application to

the browser. This technique saves load on the web server, but the problem is that anything running on the client end can never be trusted. Javascript in an HTML form can be changed or disabled by the end user very easily. Java applets can be disabled by the end user, or even decompiled and re-written. It's easy for a knowledgeable user to save an HTML form, disable the embedded Javascript, then use the modified form to submit bad data back to the web application.

When the application expects all input validation to have already been done by the web browser, and therefore doesn't double check the input, developer web app can be compromised. For this reason web applications should always validate form inputs on the server *even if they are also validated on the client*. Client-side input can never be trusted. Client-side validation should be used as a complement to server-side validation, a mean of catching simple input mistakes to reduce the number of times the web server has to validate input. Client-side validation should never be trusted as a replacement for additional server-side validation. Client-side validation is valuable for highly loaded web sites it offloads a lot of work from the server to the browsers. However if server load is not a factor, it's probably not worth the trouble of writing both client-side and server-side validation routines for HTML form input.

F. Real directory and File names

Never use actual directory or file names as parameters or construct names based on user input. Instead, use keywords that are *pointers* and store the actual file or directory names in a lookup table. For example, in a Perl program do NOT do this:

```
WRONG!> $datafile = param('datafilename');
WRONG!> $open DATAFILE $datafile or die;
```

Instead, do something like this:

```
BETTER> my %filelist = ( "name" => "/home/data/name.txt",
BETTER>   "address"  =>  "/home/data/address.txt" );
BETTER>   $keyword    = param('datafilename');
BETTER> open DATAFILE $filelist{$keyword} or die;
```

Using the above method, HTML form input is never passed directly to the 'open' command. If a malicious user tries to pass a bad value (such as '/etc/passwd'), it will fail to find a match in the associative array. Lookup tables also prevent a cracker from using a poisoned NULL attack to shorten strings. For flexibility, the locations of the files can be pulled in from an external configuration file, rather than be hard-coded into the application. However, make sure the config file cannot be accessed by web users (ie. put it in a separate data directory outside the html directory). If the web server is shared by many users, also ensure the data file can't be changed by other users on the server. If web application absolutely must be capable of opening ad hoc files based directly on browser input, rather than a predetermined list, never accept complete

path and filenames from HTML form input fields. Developer E-Government web application should at least prefix the input filename with an absolute path and strip slashes, backslashes, NULLs and sequential dots (".." and "...") from the input. For example:

```
$datadir = '/sites/internet/data';
$datafile = param('datafilename');
sanitize($datafile);
open DATAFILE $datadir . $datafile or die;
```

G. Log suspicious error

All applications should be written to trap errors. However, web applications are frequently attacked by crackers. It's a good idea to not only trap and recover from errors, but also to log events that may indicate an attack. Before opening a file for reading, a web application should check that the file exists and is readable. If the filename was constructed based on input from an HTML form, attempts to access a non-existent file or one it doesn't have privileges to read can indicate an attack. If a web application was written to be called with the POST method, it should raise an alarm if called using methods such as GET or PUT. Some web apps written to work when called by one method will fail when called by others. Even if developer app handles with all methods properly, many crackers try this form of attack. Detecting it will warn developer someone is trying to crack developer web application.

Denial of service attacks (where a malicious user tries to overload a server or application) can be detected by watching for repeated access from the same IP address. Multiple requests per second from the same IP could indicate a denial of service attempt, or that a cracker is running an automated script attempting to break the application.

IV. CONCLUSIONS

The present work as presented a comprehensive list of threads and countermeasures that can affect any web-application and in particular an e-Democracy application. Proponents of e-government and e-democracy suggest these initiatives will provide a variety of opportunities to improve governance and public participation on the democratic life. As discussed above, there are a number of forces driving the different e-government and e-democracy sectors. However, proponents of e-democracy suggest there are some overarching benefits that will result, either directly or indirectly, from these initiatives. E-Democracy is one means Parliament may use to try to achieve objectives related to these issues. As with many information technology-related projects, one of the anticipated benefits is improved efficiency. In e-government/e-democracy projects, this efficiency can assume many forms. Some projects seek to reduce errors and improve consistency of outcomes by automating standardized tasks. A related efficiency goal of many e-government/e-democracy initiatives is to reduce costs and layers of organizational processes by re-engineering and streamlining operating procedures. Similarly, some e-

government/e-democracy advocates suggest that reducing the amount of time spent on repetitive tasks will give those governmental employees an opportunity to develop new skills and advance their careers. All the above recommendations are methods of locking the "barn door", securing the way users normally access an E-Government/E-Democracy web applications.

However, securing the application itself is worthless if the web server itself has not been secured. Internet security begins with having secure servers and networks. That means the web server operating system and all software on it has the latest security patches installed, it sits behind a well-maintained firewall, and everything is monitored for break-in attempts. Many organizations believe skilled application developers are also skilled at system and network management. However, that is extremely rare. Being an application developer is a full time career, as is being a system administrator, network manager and security professional. Many of the well-publicized attacks on web sites targeted well-known operating system and network problems that were missed simply because the organization was focused on developing the web applications and design of the web site, or assumed their development team had all the answers. The "Code Red" worm that affected hundreds of thousand of Microsoft's IIS web server was able to spread largely because unskilled or overworked staff didn't patch a security hole in that product soon enough. Securing web applications requires a combined effort in many areas: application design, server management, network management and security auditing. Professionals specializing in one of these areas require a good knowledge of all the others, but in reality each area is a specialty that requires the attention of a focused individual or team. When the web sites content is so important as a electoral results, security is one of the most important variables of electoral process. High level of security is necessary to prevent different attacks to change or delete information output.

We will considerer all recommendations presented in this paper when implementing e-Voto project. First of all, it is essential to have totally server communications security. After that, we will develop the prototype and test some planned attacks over this server. When server security guaranteed, this paper recommendations will be restrict the development limits, and what the developers will be able or they will not be able to do. During the final version project developing they will be made forced tests against the main critical factors that the authors present in this paper. After all main recommendations pass the tests, developers know where they are the limits.

V. AKNOWLEDGMENT

The work that is described in this paper is being performed in the context of the e-Voto project, a Portuguese FCT project dealing with the complexity of the electronic voting systems.

REFERENCES

- [1] Garfinkel, Simson, 2001. Web Security & Commerce, Second Edition, O'Reilly
- [2] Scambray, Joel, 2005. Web Applications (Hacking Exposed), McGraw-Hill.
- [3] World Wide Web security FAQ: <http://www.w3.org/Security/Faq/www-security-faq.html>
- [4] CERT advisory 97.25.CGI: <http://www.cert.org/advisories/CA-1997-25.html>
- [5] CERT advisory CA-2000-02 <http://www.cert.org/advisories/CA-2000-02.html>
- [6] Secure Programming for Linux and Unix HOWTO (David A. Wheeler): <http://www.dwheeler.com/secure-programs>
- [7] Hidden form field vulnerability white papers (InfoSec Labs): <http://www.infoseclabs.com/mschff/mschff.htm>
- [8] Robert D. Atkinson and Jacob Ulevich, Digital Government: The Next Step to Reengineering the Federal Government, Technology & New Economy Project, Progressive Policy Institute, March 2000.
- [9] A Conceptual Overview, by Harold C. Relyea, and CRS Report RL31088, Electronic Government: Major Proposals and Initiatives, by Harold C. Relyea.
- [10] Paperwork Reduction Act Reauthorization and Government Information Management Issues, by Harold C. Relyea, for a more comprehensive analysis of PRA.
- [11] Government Information Technology Management: Past and Future Issues (The Clinger-Cohen Act), by Jeffrey W. Seifert, for a more comprehensive analysis of the Clinger-Cohen Act.
- [12] John M. Strate, Charles J. Parrish, Charles D. Elder, and Coit Ford, "Life Span Civic Development and Voting Participation," American Political Science Review, vol. 83
- [13] SQUID: <http://www.squid-cache.org>

Data acquisition and processing for determination of vibration state of solid structures – Mechanical press PMCR 63

Cătălin Iancu, PhD

University “Constantin Brâncuși” Târgu-Jiu, Romania
ciancu@utgjiu.ro

Abstract - In this paperwork is presented an experimental method for determination of vibration state of solid, three-dimensional structures, applied for mechanical press PMCR 63. First is presented the experimental equipment needed, then the real experiment and, in the end the interpretation of results. This kind of experiments are made in order to seek eventually resonance phenomenon and the results will be used as a comparison criterium for validation of analitic model built for further FEA analysis.

I. INTRODUCTION [1]

In the large category of conventional machines for plastic deformation, the mechanical presses have the largest use. Designing such equipment, with high productivity, and using automation, leads to a large utilization of presses. Notice that the mechanical presses are widely used among this type of equipment.

For the mentioned reasons have been developed modern analysis methods, finite element method being hardly used lately. So far the structural calculus using FEA method was very little or even not used for structures like mechanical presses, being eventually applied on static ground, existing the possibility to perform dynamic analysis.

In order to observe possible danger working regime and to identify possible excitement frequency nearby natural frequencies of press, and also to determine the bed deformation under loads developed on normal working conditions, have been conducted experiments on real structures, because deformation, as characteristic frequencies, will be used as a comparison criterium for validation of analitic model built for further FEA dynamic analysis.

II. REQUIRED EXPERIMENTAL EQUIPMENT [3]

- Piezoelectric transducer for acceleration Brüel & Kjær, type 4391;
- Load amplifier Brüel & Kjær, type 2635;
- Resistance transducer for linear stroke, type LK 15.
- Notebook equipped with analogue-numerical interface Keithley, type DAS 1602;
- Software for data acquisition and processing, wrote under TestPoint.

In fig.1 is a picture of the needed experimental equipment, presented before.



Fig.1. Experimental equipment

A. Accelerometer

The accelerometer is an electromechanical transducer, which gives an electrical signal according with the acceleration which is submitted to.

One of the most used accelerometer is the piezoelectric type, which in principle consist of two piezoelectric discs, with a seismic mass on top, pre-compressed through a lamellas system. The whole system is mounted inside a metallic case, which serves for the take up of mechanical motion.

When the accelerometer is subject to a mechanical vibration, the seismic mass will induce on piezoelectric discs a variable force, according to mass acceleration.

Based on piezoelectric effect, discs will load with an electrical charge according to the force applied on them, so according to mass acceleration.

The system mass-elastic lamella is practically an elastic mechanical system with one degree of freedom, characterized by a special resonance frequency. This is a particular characteristic of each accelerometer.

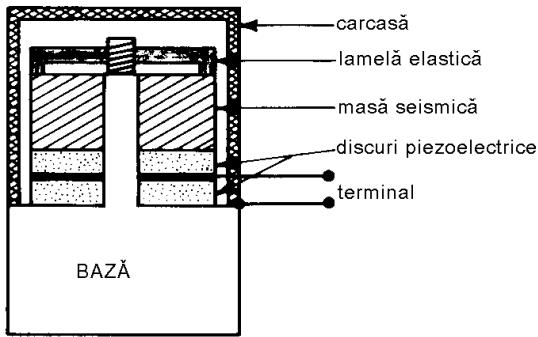


Fig.2. Diagram of a piezoelectric accelerometer

For frequencies lower than resonance frequency, the acceleration of the seismic mass will be approximately the same with the acceleration of the base of transducer, and so the electric charge output of transducer will be according to the acceleration, which the transducer is submitted to.

Accelerometer type 4391, made by Brüel & Kjaer, used on experimentation, has the main characteristics:

- current sensitivity: $1\text{pC}/\text{ms}^2 \pm 2\%$;
- frequency domain: $0,1\text{Hz} \dots 12\text{ kHz}$;
- resonance frequency: 40 kHz ;
- mass: 16 g .

B. Load amplifier

The load amplifier is introduced in the circuit for two reasons:

1°.-amplify the electric signal quite small, given by the piezoelectric transducer (which can be acceleration or force transducer);

2°.-transform the high impedance of the piezoelectric transducer to much lower impedance, in order for coupling to the other measurement and processing devices.

Load amplifier made by Brüel & Kjaer, type 2635, used on experimentation, has the main characteristics:

- current sensitivity, step selection from 0.01 mV/pC to 10 mV/pC ;
- frequency domain: $0,1\text{Hz} \dots 200\text{ kHz}$;

C. Resistance transducer for linear stroke.

This is a potentiometric transducer of a strong design, in order to resist heavy working conditions.

Resistance transducer for linear stroke type LK- 15, made by Novotechnik, used on experimentation, has the main characteristics:

- resistance: $5\text{ K}\Omega$;
- maximum supply voltage: 42 V ;
- active stroke: 150 mm .
- maximum speed: 10 m/s ;
- maximum acceleration: 200 m/s^2 ;
- resistance insulation (at 500 Vcc): $\geq 10\text{M}\Omega$.

D. Numerical acquisition interface

This interface makes the analogue-numerical conversion of the input electric signals, and transfers these signals to the computer in order to achieve numeric processing.

In principle an acquisition interface is characterized by: number of input channels, global frequency sampling, and resolution.

Numerical acquisition interface type DAS 1602, made by Keithley used on experimentation has the main characteristics:

- number of input channels: 8 differential / 16 Single End;
- global frequency sampling: 100 kHz ;
- resolution: 12 bit.

E. Computer notebook 586DX type 3005

F. Software for data acquisition and processing TestPoint-Keithley

TestPoint is a programming environment of high performance, object oriented, integrating data acquisition control, numeric analysis, matrix calculus, signal processing and graphic representation, in an easy way to handle [5].

The limitations that may occur using Test Point programming environment are subsequent to performances of computer used.

For graphic representation is used a specific graphics, with two cursors, being able to represent up to 6 curves in Cartesian coordinates, associated to one of 4 ordinates. The graphic representation has two slider-objects for selecting the upper and lower limits of representation domain and other two slider-objects for horizontal displacement of two cursors, data associated to curves in the cursors position being listed in a corresponding numbers of displays, having the same color as the curves.

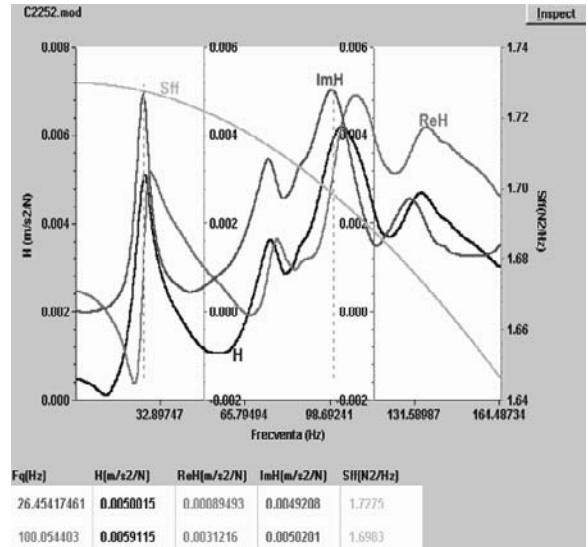


Fig.3. Example of TestPoint-Keithley software display

III. EXPERIMENTS ON NORMAL WORKING CONDITIONS

Using the experimental equipment described previously, have been conducted experiments for determination of vibration state of a mechanical press type PMCR-63, mechanical press with open bed, with nominal force 63 tf, in order to observe possible danger working regime and to identify possible excitement frequency nearby natural frequencies of press [1][2].

Also has been determined the bed deformation under loads developed on normal working conditions. Deformation, as characteristic frequencies, will be used as a comparison criterium for validation of analitic model built by FEA analysis.

Experiments have been conducted on a mechanical press type PMCR-63, made in 1999 la S.C. MIRFO S.A. Tg-Jiu, Romania, and working on normal condition at "AUTO SPARE PARTS Inc.", Topoloveni, jud.Argeș, Romania.

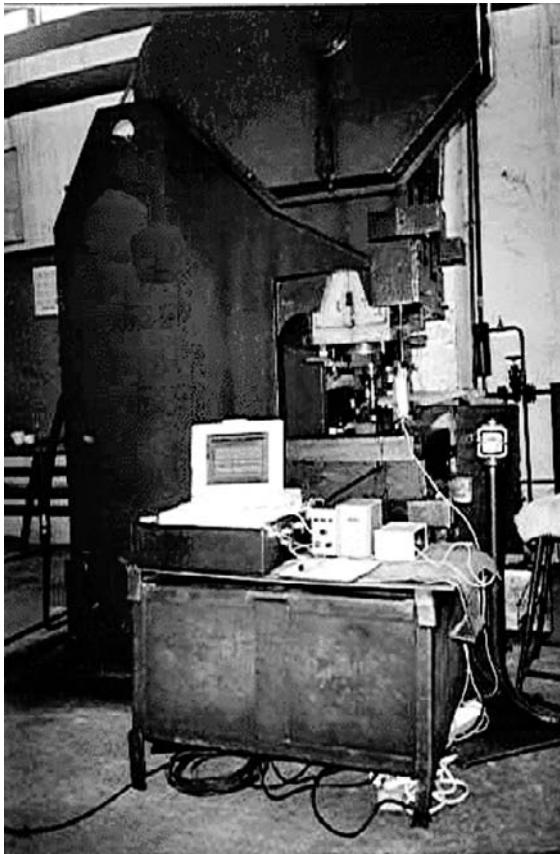


Fig. 4. Aspect of conducting experiments
(Disposition place of measurement points)

In fig. 4 is presented a picture taken while measurements had been conducted. By points 1, 2, 3, and 4 are represented the disposition place for the acceleration transducers.

For all the measurements bed deformation has been determined in single place, in the "C" zone.

On picture are represented:

- 1 - Measurement point nr.1- (disposition place);
- 2 - Measurement point nr.2- (disposition place);
- 3 - Measurement point nr.3- (disposition place);
- 4 - Measurement point nr.4- (disposition place);

It have been determined the following characteristics:

- vibration acceleration on horizontal-transversal direction;
- vibration acceleration on horizontal-longitudinal direction;
- vibration acceleration on vertical direction;
- bed deformation in the "C" zone.

Measurements have been conducted while press executes a combined operation of sheet metal stamping with punching on an auto item of steel sheet of 3-mm thickness.

IV. PROCESSING DATA AND NUMERIC RESULTS

In fig.5 are represented the characteristics of vibration accelerations and bed deformation, determined in measurement point nr. 1. The observation made hereby are equally the same for the other measurement points (2-4).

The order of curves is:

- Green** curve, over the whole display- bed deformation;
- Blue** curve, higher- vibration acceleration on horizontal-longitudinal direction;
- Red** curve, middle- vibration acceleration on vertical direction;
- Black** curve, lower- vibration acceleration on horizontal-transversal direction;

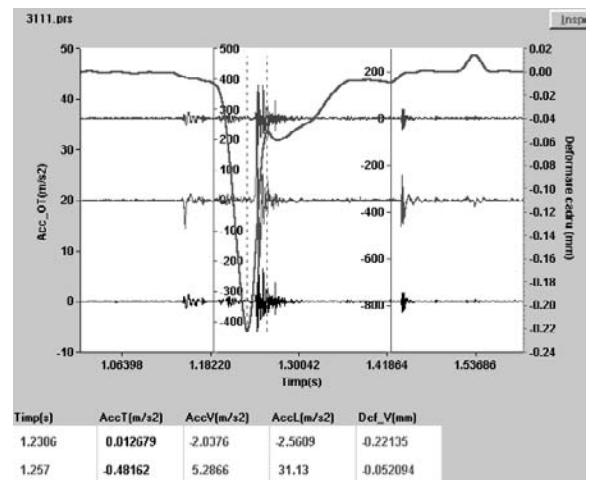


Fig.5. Characteristics determined in measurement point nr. 1

It can be observed that the bed deformation, measured in the maximum opening zone (**green curve**), has a maximum while effective cutting of sheet, a slight inertia on tempering, due to friction between the dies, and then go back to initial state, whole phenomenon during less than 0.5 sec.

For the real working conditions (sheet metal stamping, of 3-mm thickness), maximum deformation is about 0.225 mm.

The **blue curve** represents the vibration acceleration on horizontal-longitudinal direction. It can be observed two small vibratory zones in the extremities of measurement interval ($t=0, 5$ sec.), due to coupling-decoupling of press clutch.

Also it can be observed two vibratory zones of high amplitude, which boundary the jump of green curve (bed deformation), and represents the beginning of cutting process and respective the ending and dies spalling.

The same shape is remarked for vibration acceleration on vertical direction (**red curve**) and for vibration acceleration on horizontal-transversal direction (**black curve**), the correspondent amplitudes being slightly different, that proves the good rigidity of press.

In order to determine the spectral composition of functioning generated vibrations [2], it was done the Fourier transform of recorded accelerations.

In fig.6 is represented the modulus of Fourier transform of vibration acceleration on vertical direction, registered in measurement point nr.1.

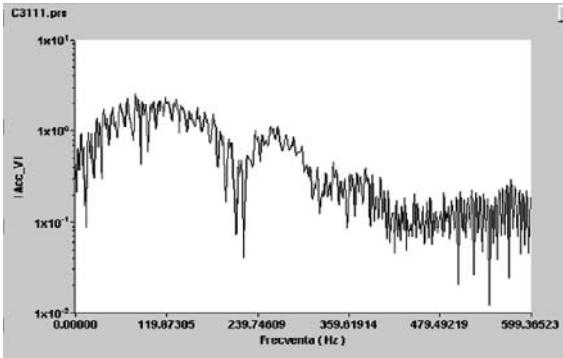


Fig.6 Modulus of Fourier transform of vibration acceleration on vertical direction

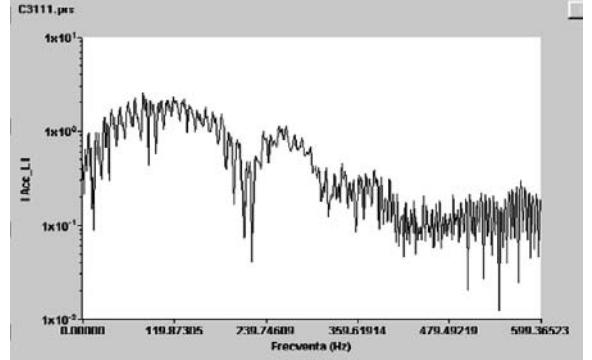


Fig.7 Modulus of Fourier transform of vibration acceleration on horizontal-longitudinal direction

In fig.7, shown above, is represented the modulus of Fourier transform of vibration acceleration on horizontal-longitudinal direction, registered in measurement point nr.1.

V. CONCLUSIONS

By examining whole characteristics [4] [6], presented in fig. 6 and 7 (and also for the other measurement points) it can be observed that the frequency spectrum has a relative uniform distribution in frequency range 1-550Hz, so in normal working conditions there aren't any resonance phenomenon.

Also it can be determined the natural frequencies, which will be used as a comparison criterium for validation of analitic model built for further FEA analysis.

REFERENCES

- [1]. Iancu C., “Contributions to dimensional optimization of mechanical presses in dynamic regime”, Ph.D. Thesis, University of Pitesti, Romania, 2001.
- [2]. Manea, I., “Introduction to modal analysis by practice and theory”, Ed. Scorilo, Craiova, Romania, 2000.
- [3]. ★★★★ User’s guide, DAS 1600/1400 Data Acquisition, 1997.
- [4]. ★★★★ Sound & vibration catalogue, Brüel & Kjaer, 1997.
- [5]. ★★★★ “TestPoint” Techniques & Reference, Capital Equipment Corporation, Massachusetts, USA, 1996.
- [6]. Randal, R.B., “Frequency Analysis”, Brüel & Kjaer, 1987.

Quality of Uni- and Multicast Services in a Middleware. LabMap Study Case

Cecil Bruce-Boye

University of Applied Science Lübeck
3 Stephensonstrasse
Lübeck, 23562 Germany

Dmitry A. Kazakov

cbb software GmbH
1 Charlottenstrasse
Lübeck, 23560 Germany

Abstract- The quality of service (QoS) is essential for a distributed data acquisition and control system. QoS depends on numerous factors, which are difficult to predict in advance. In this paper we present an empirical comparison of uni- and multicast based implementations of distributed middleware services. The LabMap® middleware offers both uni- and multicast data distribution services. Unicast is based on TCP, multicast on the PGM streams. We measured the performance of both transport layers on the typical 1-n case where multicast deployment would be possible. Our study shows that PGM is a useful complement to TCP transport, though its use should be carefully planned in advance.

I. INTRODUCTION

A typical distributed data acquisition and control system is a loosely coupled network of nodes capable to publish and subscribe system variables. For the applications running on the nodes the network is abstracted away through the middleware. The middleware provides: naming and identity services; data distribution and transport services; information services such as browsing and time services. Quality of these services (QoS) plays a decisive role for applications to enjoy advantages of the middleware.

Within the middleware the network is abstracted as a device with some network protocol supporting the services. Thus the concrete transport protocol is abstracted as well, to allow reuse of the middleware core implementation.

In the recent past there was little choice for a middleware working over the Ethernet. It was either TCP sockets for unicast or else UDP datagrams for broadcast connections. The choice was difficult, in particular, because of unreliability and lack of traffic control of UDP. Modern multicast technology presents an answer to UDP problems. It provides efficient filtering to protect an outside network from potentially massive traffic between distinct nodes. Traffic separation is achieved physically by switches. The corresponding network protocols are available for network traffic management control from the application side. Is the multicast technology mature to meet the requirements typical for automation and control application area of middleware technology?

We carried out an extensive empirical study of QoS based on uni- and multicast transport layers on the example of the

LabMap® middleware¹ [1]. One of the goals of the study was to justify empirical results of LabMap® deployment for hardware-in-the-loop scenario. [2]

II. RELATED WORKS

To the present time multicast in middleware, if implemented, was exclusively on the broadcast basis. For the CORBA (Common Object Request Broker) [3] there exist proposals for deployment of multicast [4], but no known implementations of. For unicast services QoS measures can be found in [16].

OPC (an initiative for open data connectivity) [5] also does not provide multicast layers.

The iBus middleware [6] provides multicast services, however its transport layer is not natively multicasting and any figures about performance are unknown to us.

Seppo Sierla conducted a QoS study of NDDS (Network Data Delivery Service) implementation of RTPS (Real-time Publish-Subscribe) middleware interface specification for unicast services [7].

Spread is a message distribution toolkit which supports multicast messages [8]. It is not a middleware, but it can serve as a reliable multicast transport layer for a middleware. Performance data on messages services are available for spread [9].

III. MIDDLEWARE ARCHITECTURE OVERVIEW

A. Networking

The middleware abstracts connections between nodes and represents them to the applications as publisher / subscriber relations. However, the efficiency of this abstraction highly depends on the nature of the underlying connections. In general to consider are:

- *Peer-to-peer* connections, like TCP/IP sockets. The advantage of a peer-to-peer connection is that it allows a straightforward packet filtering based on MAC (Media Access Control) addresses. An error correction mechanism is usually easy to implement, for example, by resending, because both sides are aware of each other's state. The disadvantage of peer-to-peer connections is that in the case

¹ LabMap® is applied for testbed automation by automotive vendors like AVL, Daimler-Chrysler AG, Opel, VW, MAN, Bosch AG.

- of $1-n$ and $n-1$ connections the overall overhead is a multiplicative of n .
- *Multicast* connections, like UDP datagram sent at the broadcast address. The advantage of multicasting lies in fixed overhead for $1-n$ connections. However using UDP might expose difficult QoS problems and middleware management problems. This problem, which is not specific to middleware, was recognized by the IETF (Internet Engineering Task Force) and a series of standards was designed to provide more efficient transport protocols suitable for $1-n$ connections. In particular IGMP (Internet Group Management Protocol) [10] and PGM [11] (Pragmatic General Multicast) are of especial interest for middleware.

B. Remote services

The policy of QoS is the requirements imposed by a subscriber on the published data. It is the expectations of the subscriber on QoS. The following policies are important:

- *On demand* - the subscriber explicitly requires data from the publisher. This type of policy is essential for implementation of events, commands, client-server queries, higher order services such as browsing.
- *Periodic* – the subscriber receives a data flow from the publisher. The subscriber specifies the data period. This type of policy is used for physical state data known to be defined at each moment of time. Usually the subscriber asks the publisher for the “native” data period because it is the physical limit and more frequent polling makes no sense. This policy is widely used, but exposed to various problems. The period should be twice as long as the “native” period, otherwise the subscriber will experience “oversampled” data. This sufficiently limits the system performance. When timestamps are supported, the subscriber can filter out repetitive data, however this would mean an additional burden for it.
- *Periodic on change* – the subscriber receives data only upon state change. Usually the state change is value or timestamp change. This type of policy does not suffer the problems typical for the periodic policy. Yet it sometimes makes application design more difficult, because the subscriber should synchronize on the data, which depending on the data sources might stay unchanged for a long period of time. In such circumstances, for the subscriber it might become difficult to detect data losses. Another problem is that the system load is less predictable under such event-controlled scenario. For mission critical applications that could be unacceptable due to possible time constraints violation. However, in some cases time constraints can still be satisfied due to physical / logical constraints a priory known for the system.

C. Local services

QoS is also influenced by the middleware notification services available to the subscribers. The services can be synchronous or asynchronous to the subscriber’s execution threads. For a service to be synchronous implies that the data

transfer may occur only on demand and also the subscriber is blocked until I/O completion. Such architecture is obviously flawed, so in all known implementations the synchronous services are only interfaces to the underlying middleware services, which themselves are natively asynchronous. The notification services can be:

- *Callbacks* – this notification service is usually performed from a separate execution thread, which requires interlocking and data exchange with the notified thread. Further callback can be blocking or non-blocking. A blocking callback prevents data loss. That is - if a next notification needs to happen during callback processing it is postponed until callback completion. Blocking callbacks is a great danger for the whole system because they may violate time constraints, strain system resources and deadlock. Non-blocking callback may suffer data losses.
 - *Synchronization objects* – this notification service is based on a waitable resource.
- There are many types of synchronization objects:
- *Event* is the most simple synchronization object. An event gets signaled upon notification. The subscriber can wait for the event. This solution may also suffer data losses and data corruptions.
 - *Semaphore* is a synchronization object that can be used to protect shared resources, such as data. The most used variant of semaphore is mutex. Mutex represents a very low-level mechanism exposed to various problems, from deadlock to priority inversion. Usually mutex and event are used as building blocks for higher-level synchronization objects, which are more reliable and safer to use. This notification service is based on a waitable resource.
 - *Queue* is a more elaborated synchronization object. As with the callbacks the queue may be blocking or not. Thus it is again a trade-off between time constraints and data consistency. Queue represents a 1-1 synchronization object.
 - *Blackboard* is a 1- n synchronization object. The notifications get published on the blackboard and interested threads may inspect the blackboard for the notification and enter waiting for a new notification.
 - *Protected object* is a higher-level primitive, which can be specialized into each of mentioned above objects. Protected objects are language supported and can be used only in interfaces written in higher-level languages providing concurrency primitives. Protected objects are known to be very efficient in terms of context switches [12]. The disadvantage is that they require language support, which a middleware interfacing to lower-level languages like C++ would lack.

IV. MULTICAST TECHNOLOGY OVERVIEW

Two issues are essential for middleware to take an advantage from multicasting: reliability of data streams and the topology of connections, which would allow an effective mapping of publisher-subscriber relationships to the multicast groups.

Fundamentally, multicast cannot handle bidirectional connections. This excludes commands and client-side requests

from multicast. In other words, only state data can be effectively transmitted using multicast. Unicast peer-to-peer connections will be still necessary for handling some bidirectional and all feedback traffic. This includes: I/O commands, time synchronization protocol, configuration requests, browsing and informational requests. For example, it is impossible to synchronize time on the basis of a unidirectional connection.

Another requirement for multicast connections to be effective is presence of logical 1- n connections. Otherwise, a peer-to-peer connection is expected to be more effective. The reason for this is that in a peer-to-peer connection both sides can maintain the connection state, because the information about it is fully known to them. On the contrary, in the case of multicasting neither the producer nor its consumers know the state. This requires additional protocol overhead to make consumers able to join broadcast without producer notification. For the middleware it means a more fat protocol of sending data. In LabMap®, for instance, incremental packets are periodically intermixed with full data packets within some definite time frame. The length of the frame will determine the time a consumer will need to establish a connection to the producer.

Differently to broadcasting, multicasting was designed with reliability in mind. There are several reliable multicasting protocols. PGM is one of them supported both by the hardware and OS vendors. In particular, PGM implementations exist for Windows® and Linux. For an application, like middleware, PGM provides a reliable data stream from producer to any of the consumers. The packets used in PGM are neither TCP nor UDP. The protocol takes responsibility for resending lost packets as necessary. Technically the multicast stream is buffered in the routing nodes. The negative acknowledgements from clients propagate up to the last routing node, which has the lost packet. The packet is then resent down to the client. The routing nodes keep the traffic window to make packet resending possible. The window size and length are configurable. This integrated error correction mechanism and efficient traffic filtering based on IGMP makes PGM superior to UDP for implementation of 1- n connections.

The LabMap® middleware provides reliable network transport layers for unicast and multicast, called LabNet and LabPGMNet respectively. LabNet is based on TCP/IP sockets. LabPGMNet uses PGM protocol.

V. TIME SYNCHRONIZATION

The middleware nodes are responsible for time stamping of the values of the variables and the events related to them. Time stamping requires globally applicable time stamps, which can be stored, restored and transmitted over the network. This inevitably requires applying UTC (Universal Coordinated Time) [13] timestamps rather than local political time.

The absolute accuracy of the time stamps is usually not required to be very exact. Normally, $\pm 1.0\text{s}$ would be suitable for all purposes. At the same time the relative accuracy within the distributed system need to be much better. The relative

clock readings on different nodes have to be far under the 1ms accuracy margin.

There are two scenarios of synchronizing timestamps in the system:

- Synchronization of the time sources. For example, by using synchronized atomic clocks, or by distributing time signals of the same clock among all participants.
- Translation of the time stamps to one base.

The first approach is more universal but also more expensive and fragile. It also presents a difficult maintenance problem by requiring an access to all participants. With the second approach the clocks of data sources remain intact, but the time stamps are adjusted as they arrive at the subscriber side.

LabMap® offers both options. We used timestamps translation in our experiments, because it is the most probable scenario.

VI. QUALITY OF SERVICE

QoS is characterized by:

- *Latency*, the time required to deliver the data from one the publisher to subscriber. It is composed out of many components as shown on fig. 1. The total latency experienced by the observer is $t_5 - t_1$. On fig. 1 t_1 is the issue time of a state change. The network interface becomes aware of the state change at t_2 . The change in the form of network packets arrives at the remote host at t_3 . The middleware there gets notified at t_4 . And finally, at t_5 the observer receives a notification.

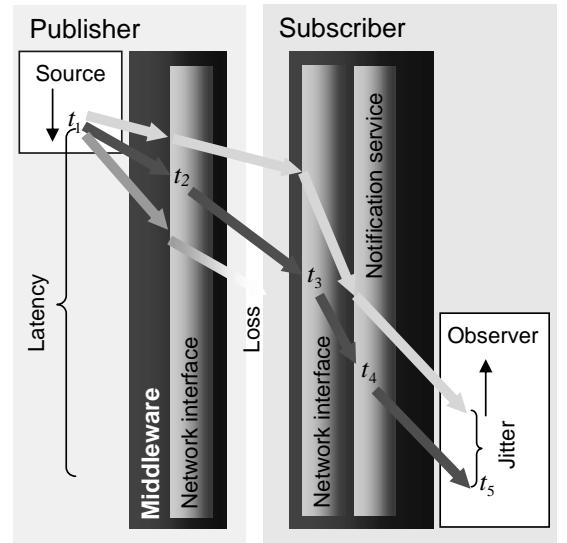


Fig. 1. Quality of service

- *Jitter*, the variation from one period to the next adjacent period of the periodic data delivery. For non-periodic data, jitter is variance of latency from its expected value. In some cases jitter is irrelevant provided the overall latency does not exceed some upper limit.

- *Data loss*, non-delivery. Data loss might be acceptable under some circumstances for periodic data.

VII. TESTBED AND PROCEDURE

The testbed network was comprised out of 6 identical computers running Microsoft® Windows® Server 2003 Standard Edition:

- Intel® Pentium® 4 Processor 519 (3.06 GHz);
- Mainboard with FSB 533 MHz;
- 750 MB DDR SDRAM PC400;
- 80 GB HDD;
- NET- 3COM 3C2000, gigabit network card;
- The computers were interconnected using CISCO Catalyst 3560 switch.

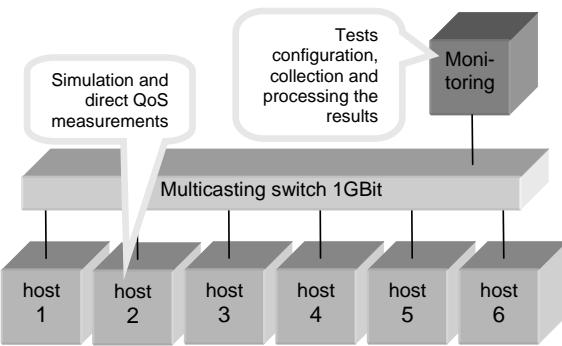


Fig. 2. Simulation configuration

Fig. 1 illustrates the simulation configuration. The hosts 1..6 simulated the nodes of a distributed control system connected via middleware. Each host ran the LabMap® middleware and a test application simulating data distribution and estimating QoS. The number of distributed variables was varied $n=1, 2, 5, 10, \dots, 20,000$ per node. We used floating-point variables in our experiments. The number of nodes s was varied $s=2, 3, 4, 5, 6$. Each test was executed once using the unicast transport layer and once using the multicast one. During the test each publisher application created n -variables, each of them was subscribed by s -subscriber nodes. The publishing period, i.e. the frequency in which the variables were changed on the publisher side was a parameter of the test. We used the periods $\Delta t=10, 50, 100, 200\text{ms}$. Further, each test pass was repeated multiple times (usually 1000) and the results of the repetitions were averaged.

The subscribers measured QoS directly by subtracting the notification time from the timestamp of the published variable value. Jitter was estimated as the standard deviation (σ) of the latency.

Data loss was controlled by using a definite pattern of published values. However, this was rather a plausibility check, because a total loss was not possible. LabMap® warranties delivery through degrading QoS, as long as the connection stays. For this reason we redefined data loss as a time

constraint violation, i.e. as an inability for the publisher to update a variable within its publishing period. When the publisher discovered that it published only p of n variables in Δt , then $n-p$ data losses were signaled.

All tests were performed in two variants:

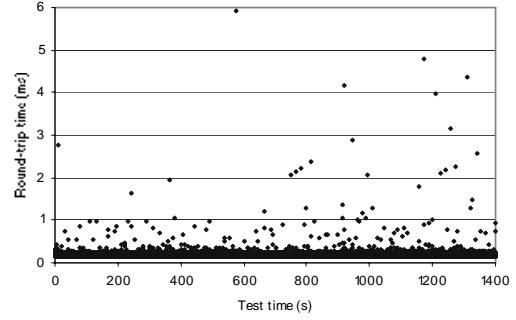
- Without additional system load. The nodes carried out only simulation of variables state changes, data distribution and QoS measures;
- Under stress load, when each node ran a numerical application.

For the load simulation we chose a public-domain implementation of Whetstone [14] by Painter Engineering, Inc [15]. It was modified in two aspects. The main program was changed to a subprogram wrapped by a C++ class derived from a task type. The object of the class started a thread, which ran in parallel to the QoS test's threads. This thread performed the benchmark. Another change was that the benchmark loop did not stop. The number of cycles passed were requested from outside. When a QoS test started the current counter of Whetstone cycles was queried and the time was noted. When a QoS test stopped the new counter was taken and the difference of the counters divided to the difference of the times gave the benchmark value.

The QoS test thread and the middleware process were given higher priority to one of the benchmark thread, in order to ensure service. So the benchmark measured during the test indicated free computation resources left.

VIII. TIME SYNCHRONIZATION MEASUREMENTS

Time synchronization measures were essential, because quality of time synchronization determined the accuracy of all further measurements. The major factor was the roundtrip time of the synchronization packets sent between the hosts. Fig. 3 represents typical roundtrip times experienced for



synchronization packets sent each 100ms.

The mean value of the roundtrip was about 200μs. Variance of the roundtrip is addressed to non real-time behavior of the system as a whole.

The time synchronization mechanism of LabMap® performs statistically. The estimation algorithm weights data samples according to the roundtrip time experienced. Thus samples

having longer roundtrip have lesser influence on the outcome than the values with shorter roundtrips. Further, the samples expire with time, i.e. the age of a sample reduces its weight. The reason for this is that clocks of the nodes have constant drift.

A half of the average roundtrip time should roughly correspond to the upper bound of time error.

An unexpected synchronization problem we stated in our experiments was rather poor quality of the hardware clocks. An estimated clock shift between two hosts had a constant trend. The trend depended on the computers and was up to $0.7\mu\text{s}/\text{s}$. All computers used in the test were of the same model from the same manufacturer.

IX. QUALITY OF SERVICE MEASUREMENTS

To reduce the dimensionality of the result space we combined the number of variables n , and the publishing period Δt into an integral parameter $n/\Delta t$, which characterize the number of middleware variables state changes per second. We discovered that the value of $n/\Delta t$ is a key factor that influences QoS. Within wide bounds, the number of variables can be safely increased when the publishing period is prolonged and reverse.

A. Losses

Fig. 4 and 5 represent losses by uni- and multicast correspondingly. As expected, multicast data distribution does not depend on the number of subscribers. The performance of

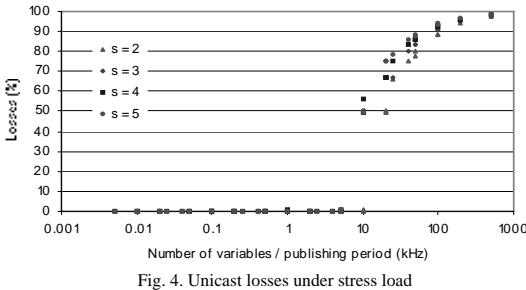


Fig. 4. Unicast losses under stress load

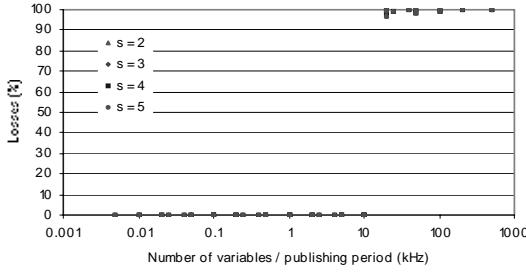


Fig. 5. Multicast losses under stress load

unicast distribution degrades with the number of subscribers. The maximal changes frequency in both cases was about 10^4 state changes per second. This practically means, that for

example 500 variables could be published no more frequently than in 50ms period.

An important observation about multicast distribution was an abrupt rise of losses in the transition area. It means that a multicast-based system should be planned more thoroughly to have more spare resources than a unicast-based system.

B. Latency

We refined latency measurement results to only the data for which no losses were observed. Otherwise, a non-delivery could eventually improve estimated latency results due to lesser data traffic, because the publisher discarded the changes it was unable to publish in time.

Table 1 represents the measured latency regression coefficients estimated for the model:

$$T_l(n, \Delta t) = a_l + b_l \frac{n}{\Delta t} \quad (1)$$

In (1) T_l is the latency as a function n (number of variables) and Δt (publishing period). The coefficients a_l and b_l describe latency as a linear function of.

The table represents the figures obtained with a stress load (outside brackets) and ones without load (in brackets) for different numbers of subscribers s . The coefficient a_l gives an impression of the best achievable performance. Without stress load it is about $250\mu\text{s}$ for both transport layers. The coefficient b_l determines how latency grows with the growth of the number of state changes per second. The figure 10^4 (state changes per second) determines the longest latencies to observe immediately before data loss would appear. Under stress, for unicast it is around 6ms, while for multicast it is 50ms. Without a stress load they are 1 and 25ms correspondingly. Here again, multicast shows to be more fragile than unicast.

TABLE I
LATENCY REGRESSION COEFFICIENTS

s	a_l (ms)		$b_l (10^{-3})$	
	unicast	multicast	unicast	multicast
1	0.998 (0.265)	0.244 (0.242)	0.521 (0.0526)	5.297 (2.349)
2	0.619 (0.151)	0.388 (0.230)	0.303 (0.0194)	5.248 (2.353)
3	0.544 (0.237)	0.246 (0.227)	0.223 (0.0866)	5.313 (2.352)
4	0.592 (0.185)	0.254 (0.213)	0.205 (0.0241)	5.284 (2.357)
5	0.710 (0.197)	0.211 (0.230)	0.178 (0.0233)	5.311 (2.361)

Unicast behavior clearly depends on the number of subscribers. b_l depends on s^3 almost linearly.

The results show an unexpectedly high influence of stress load, which indicates that the operating system resource sharing could be better. We expect that the performance under stress load could drastically improve on a dual-core machine.

C. Jitter

Fig. 6 and 7 represent jitter measurements under stress load. The jitter was estimated as the standard deviation of latency. As for the latency the results were refined from losses. We observed growth of jitter correlated with the growth of latencies.

Without stress load jitter was sufficiently lower. It was less than 1ms for unicast and less than 6ms for multicast.

Higher values under stress can be addressed to poor time sharing in the system.

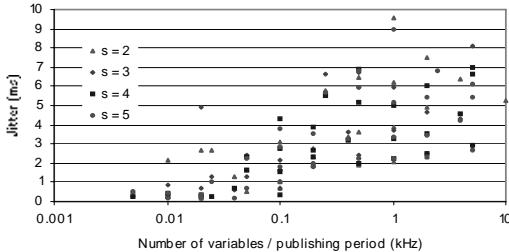


Fig. 6. Unicast jitter under stress load

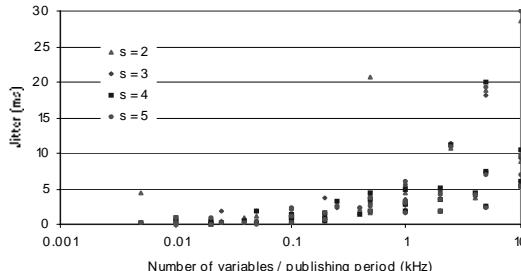


Fig. 7. Multicast jitter under stress load

D. Resources consumption

During the tests, we measured the stress load benchmarks to determine how much computational resources were left for the application logic while running the middleware. Table 2 represents the regression coefficients estimated for the model:

$$W(n, \Delta t) = a_w + b_w \frac{n}{\Delta t} \quad (2)$$

In (2) W is the number of whetstones per second as a linear function of the relation n (number of variables) to Δt (publishing period). The coefficients a_w and b_w , were estimated on both publisher and subscriber sides.

TABLE 2
WHETSTONE BENCHMARK REGRESSION COEFFICIENTS

s	a_w (10^6 whetstones $\cdot s^{-1}$)				b_w (10^3 whetstones)			
	unicast		multicast		unicast		multicast	
	Publ.	Subsc.	Publ.	Subsc.	Publ.	Subsc.	Publ.	Subsc.
1	0.735	0.742	0.740	0.743	-0.036	-0.047	-0.033	-0.059
2	0.741	0.739	0.739	0.743	-0.061	-0.048	-0.033	-0.059
3	0.741	0.741	0.739	0.743	-0.080	-0.053	-0.033	-0.059
4	0.740	0.741	0.738	0.743	-0.097	-0.053	-0.033	-0.059
5	0.738	0.741	0.738	0.743	-0.117	-0.055	-0.033	-0.059

As expected, there is no dependency on the number of subscribers for the unicast subscriber side and multicast in general. For unicast publisher benchmarks linearly depend on the number of subscribers. Performance of unicast and multicast is comparable in other respects. Unicast subscribers slightly outperform multicast ones. On the publisher side multicast pays off already with just two subscribers.

X. CONCLUSION

Modern multicast technology provides a viable alternative to traditional UDP-based approach to implementation of $1-n$ logical connections. The PGM multicast protocol is reliable and imposes an overhead and QoS comparable with TCP-based connections. In general for both TCP and PGM reliable data streams, latencies in order of $250\mu s$ are achievable. This opens a wide prospective for deployment of the middleware technology in the real-time and embedded application areas with very tight control cycles.

The Windows® operating system can be deployed for less demanding distributed control applications. The periods of 5ms are realistic and reliable. However, under a stress load the system may expose latencies up to 60ms.

For process automation the LabMap® middleware provides an attractive option of utilizing multicast technology with sufficient reducing network traffic and CPU load in the nodes. The middleware and network technologies are mature for developing software products analogous to LabMap® for real-time and embedded platforms.

REFERENCES

- [1] LabMap Handbook, <http://www.cbb-software.com/labmap.html>
- [2] C. Bruce-Boye, D. A. Kazakov and R. zum Beck, "An approach to distributed remote control based on middleware technology, MATLAB/Simulink - LabMap/LabNet framework", International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering CIS-E 2005
- [3] The Common Object Request Broker: Architecture and Specification, OMG Document 99-10
- [4] João Orvalho and Fernando Boavida, "Augmented Reliable Multicast CORBA Event Service (ARMS): A QoS-Adaptive Middleware," Interactive Distributed Multimedia Systems and Telecommunication Services: 7th International Workshop, IDMS 2000, Enschede, The Netherlands, October 2000. Proceedings
- [5] F. Iwanitz, J. Lange "OPC - Fundamentals, Implementation and Application", 2002
- [6] Professional Java Mobile Programming, Publisher: Wrox Press Ltd. ISBN: 1861003897
- [7] Seppo Sierla, "Middleware solutions for automation applications - case RTPS," Helsinki University of Technology Information and Computer Systems in Automation Espoo 2003 Report 9
- [8] Yair Amir and Jonathan Stanton, "The Spread Wide Area Group Communication System," Technical Report CNDS-98-4, The Center for Networking and Distributed Systems, The Johns Hopkins University.
- [9] Yair Amir, Claudio Danilov, Michal Miskin-Amir, John Schultz and Jonathan Stanton, "The Spread Toolkit: Architecture and Performance," Technical Report CNDS-2004-1
- [10] RFC 2236 - Internet Group Management Protocol, Version 2, 1997
- [11] RFC 3208 - PGM Reliable Transport Protocol Specification, 2001
- [12] Ada 95 Rationale: The Language, The Standard Libraries. John Barnes (ed.), Lecture Notes in Computer Science, vol 1247. Springer-Verlag, 1997, ISBN 3-540-63143-7
- [13] ITU-R Recommendation TF.460-4: Standard-frequency and time-signal emissions, International Telecommunication Union.
- [14] H. J. Curnow and B. A. Wichman, "A Synthetic Benchmark," Computer Journal 19 (1), February, 1976.
- [15] "C Converted Whetstone Double Precision Benchmark, Version 1.2, (22 March 1998)," Painter Engineering, Inc., http://www.netlib.org/benchmark/whetstone_c
- [16] Douglas C. Schmidt and Carlos O'Ryan "Patterns and Performance of Distributed Real-time and Embedded Publisher/Subscriber Architectures," Journal of Systems and Software, 2002.

Traffic Flow Analysis Over a IPv6 Hybrid Manet

Christian Lazo R.
Instituto de Informática
Universidad Austral de Chile
General Lagos N° 2086
Casilla 567, Valdivia, Chile
clazo@uach.cl

Roland Glöckler
Instituto Electrónica
Universidad Austral de Chile
General Lagos N° 2086
Casilla 567, Valdivia, Chile
rolandglockler@uach.cl

Sandra Céspedes U.
Departamento T.I.C.
Universidad ICESI
Calle 18 N° 122, Pance
Cali, Colombia
scespedes@icesi.edu.co

Manuel Fernández V.
E.T.S.I. Telecommunicación
Universidad de Vigo
Lagoas - Marcosende s/n
CP 36200, Vigo, España
mveiga@det.uvigo.es

ABSTRACT

The Mobile Ad-hoc NETworks (MANET) consist of a spontaneous association of a group of nodes that dynamically change their position and exchange data between each other, regarded as autonomous network segments with flat address schemes. However, its study has shown the benefits obtained by interconnecting them to fixed network segments and Internet. This article will revise by means of using a simulation tool, the behavior of the data transmissions between the fixed network segment, a reactive gateway and the IPv6 MANET, whose nodes show a high degree of mobility, such as vehicles in an urban environment.

KEYWORDS: MANET, Hibrid Network ,Internet, IPv6.

I. INTRODUCTION

The Mobile Ad-hoc NETworks (MANET) consist of a spontaneous and non-coordinated association of a group of nodes that dynamically change their position and exchange data between each other via wireless connections, without the participation or help of any external fixed network infrastructure.

The routing protocols used in MANETs have as main objective the maintenance of a communication between a pair of nodes (origin-destination) even when the position and speed described by their nodes change. When these are not directly connected, intermediate nodes forward the packets.

Currently the behavior of many of these routing protocols is investigated and some of them are in the process of standardization of the IETF (Internet Engineering Task Force). The protocols that already have been reached experimental RFC (Request For Comments) status are DYMO [2], OLSR [3], AODV [4], DSR [5] and TBRPF [6].

The MANET routing protocols deliver the necessary mechanisms to exchange data packets inside the network reach. In order to send packets toward external networks, such as a fixed network or Internet, some network component has to act as gateway and has to provide the mechanisms for the

interconnection with that domain [7]. The means to provide this connectivity for the gateway device generally is a wireless connection toward the MANET and a second connection to the external network segment.

The operation mode of the gateway interconnecting the two networks can be active, reactive or hybrid. However, the performance impact of these interconnection options is not clear yet [8], [9] since it is affected by several external factors, such as the mobility degree of the nodes, the hop count between the gateway and the communicating node, the routing protocol used inside the MANET and the partitioning degree of the network, among other factors.

The present article documents the results obtained with a simulation tool in the analysis of the behavior of data transmissions between a fixed network segment, a reactive gateway and an IPv6 MANET, composed by nodes with a high degree of mobility, just as the vehicles of an urban environment.

The outline of this work is the following. Section 2 discusses about the gateway strategies for the interconnection of the MANET and Internet, in the section 3 different mobility models are revised, in the section 4 the used routing protocol is described, in section 5 the network pattern implemented in the tests is explained and finally in section 6, the conclusions finalize the paper.

II. CONNECTION STRATEGIES

Although, the MANETs initially were conceived as solution for isolated networks, it could be seen that when interconnecting them to fixed networks (Internet) its development potential grew and the number of possible applications considerably increased. MANETs that are connected to fixed networks are also known as hybrid networks [7], [10]. In this type of networks, one or more nodes of the MANET additionally connect by means of any of its connected interfaces to a fixed network segment. This node is called gateway and it is the one that provides a path to Internet.

A MANET node has to be informed about the available packet forwarding gateways in order to be able to send or receive traffic from Internet. To carry out this process there are three proposed outlines [8] that operate similarly as a standard routing protocol.

A. Proactive Gateway

In this case the gateway floods the network periodically with messages indicating its existence and availability. In this case the nodes know permanently the gateway that can be used for information forwarding toward Internet. Using this outline, a low latency is achieved, but on the cost of a high bandwidth consumption inside the MANET.

B. Reactive Gateway

In this scheme the gateway plays a more passive role. Only when a node tries to send a packet to Internet, the process of requesting information of the present gateway is carried out.

C. Hybrid Method

In the hybrid approach a gateway informs their presence in proactive form only to the neighboring nodes (one distance hop). The more distant nodes are configured using the reactive mechanism described above.

III. MOBILITY MODELS

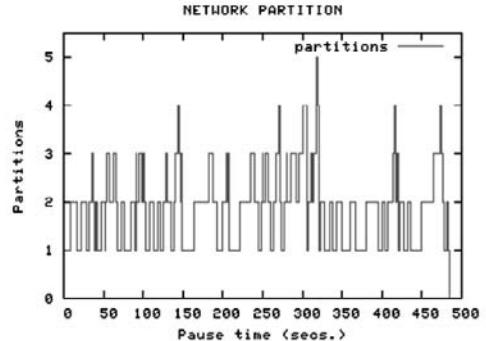
When we speak of mobility we should consider that the form, speed and trajectory of the movement described by the nodes, influence directly in the partitioning degree and connectivity level that the network achieves. Some of the measures of these variables are:

- Network Partition: indicates the number of network segments that exist for a group of nodes in a certain time (Fig. 1.).
- Space dependence: is the measure of how two nodes are dependent on each other in the movement; if two nodes have a similar speed and the same direction, then those nodes have high space dependence.
- Temporary dependence: is the measure of dependency between two nodes when their instantaneous speed is evaluated in magnitude and direction.

Considering their characteristics, MANETs are suited to give a connectivity solution to different scenarios and situations, therefore, each one of these scenarios should be represented with the pattern that comes closest to its reality at the moment of being evaluated by simulation. Among the main mobility models used by the investigation community we can mention [11]:

A. Random Waypoint

This mobility model is the most used one at investigation level. The nodes move at random speed whose values are in the range between 0 and $[V_{max}]$ and select a random destination. After arriving at the destination the node stops for



a time period [Pause] and again selects a next destination and a new speed.

Fig. 1. Network partitions during the simulation.

B. Rpgm

This group mobility model is used mainly to simulate the communication in battle fields, where a group leader moves at a speed $[V_{lider}]$ and the rest of the team moves next to him with similar speed and direction. The direction and speed of the rest of the team is adjusted periodically to the variations that the leader of the group executes. This model is characterized by high space dependence.

C. Freeway/Highway

The Freeway/Highway models are well suited to evaluate the behavior of the MANETs in vehicular network environments on freeways or highways. In this approach, three levels of speed (slow, medium and fast) are defined. Each level represents the displacement rails of the vehicles inside the freeway. The vehicles can change their displacement rail and consequently their speed in a gradual way, i.e., in order to pass from slow speed to fast, they have to pass through the medium speed first.

D. Manhattan Grid

The mobility pattern called Manhattan Grid is used to evaluate the behavior of MANETs in urban centers. This model allows representing pedestrians and vehicles moving in the streets of the city. Therefore, the pattern defines a grid where the lines and columns represent the streets, and the intersections the corners. In this model, nodes can move in a random way with medium speed $[V_{med}]$. When arriving to an intersection and under certain random probability, the nodes can stop and rotate in any direction (left - right) or continue on the same street (Fig. 2.).

This model imposes clear geographical restrictions on the node displacement, increasing this way the probability of partitions inside the network, just as indicated in Figure 1. On the other hand, it has the advantage of allowing the development of simulations with a high degree of similarity to the scenario found in urban environments. It also offers a

very high degree of space and time dependence because of the displacement pattern that the nodes describe.

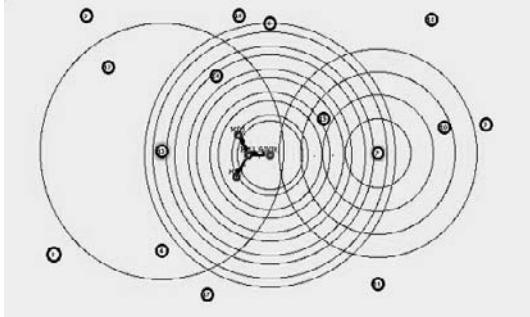


Fig. 2. Graphical network representation.

IV. ROUTING IN MANET

In the last years, many proposals of routing protocols for MANETs have been developed and presented for standardization [2], [3], [4], [5], [6]. Additionally, many comparisons have been carried out between them [12], [13], [14]. However, the consent is that the reactive protocols show the best performance and, therefore, have reached a better acceptance inside the IETF, specifically the case of the protocol Ad Hoc on Demand Distance Vector AODV[4]. Extensions have been developed for this protocol with the purpose of offering multiple paths (Routing Multipath) inside the MANET [15] and connectivity to Internet to the MANET domain [8].

A. Ad-Hoc On Demand Distance Vector

The AODV proposal bases on a reactive (or on-demand) protocol, based on distance vector routing that avoids the count-to-infinity problem and routing loops. For route control purposes it uses sequence numbers for each destination, this way it only maintains routes toward the nodes with those it maintains active communications. The routing table in the nodes keeps each entry for a while limited, so when this time expires, the routes are eliminated and a new process of route search should be started for the destination. Each entry is associated with a sequence number that is used to verify how new the route is in order to avoid loops.

B. Route Discovery

The route discovery process in AODV is initialized when a source node needs a route toward a destination node. If the sender does not find the path in their routing table, it increases the sequence number and floods the network with a *ROUTE REQUEST* message (RREQ). A neighboring node that receives the message checks if the message is duplicated, in which case it terminates. If the message is not a duplicate, then the node should create or update the inverse route toward

the node that transmitted the RREQ with the new sequence number . A node that receives the RREQ message can generate a *ROUTE REPLY* message (RREP) if it is the destination node or an intermediate node that previously knows the path to the destination node. The RREP message will be sent directly to the source node through the path discovered by the RREQ messages, after updating the corresponding sequence number. The intermediate nodes that receive a RREP create or update the route of the neighbor that sends it and the direct route toward the originator of the message of RREP. If the node that received the message RREQ cannot generate a RREP, then it forwards the RREQ message to its neighbors, with an updated sequence number.

C. Route Maintenance

In order to maintain the connection among the source and destination node, the nodes with active routes send periodical modified RREP messages with a TIME TO LIVE field equal to one (TTL=1) or HELLO messages. These messages are only received by the direct neighbors and they have the purpose of updating the route table. If the HELLO messages have not been received from a neighboring node for some time, it is assumed that this device is no longer available, therefore, the route is discarded and it is deleted from the routing table.

In the case that a destination cannot be reached or a loss of connectivity with a neighboring node is detected, a *ROUTE ERROR* message (RERR) is generated and the route discovery process is started again.

V. MODEL EVALUATION

The experiment to evaluate the behavior of the data transmissions between the fixed network and the MANET segments through a Gateway was conducted by simulation with the tool Network Simulator (NS-2) [16].

In this section we will describe the different parameters of the scenario used in our simulation:

A. Simulation Scenario

The examined scenario contains 3 fixed nodes in Internet, 15 mobile nodes using the net protocol AODV+ [8] and a gateway that interconnects both domains. The MANET topology is distributed on a rectangular area of 800m x 500m. The gateway works in reactive mode and is fixed to the center of the area (coordinates 400, 250). The mobile nodes move in random manner according to the mobility pattern "Manhattan Grid", with a medium speed of 20m/s (Figure 2). The mobile nodes and the gateway use omni-directional antennas offering a cover radius of 250m. The media access control is realized with the MAC layer 802.11. The fixed nodes in Internet and the gateway are interconnected by means of bi-directional connections at 5Mb/s and with 2 ms of latency.

B. Network Traffic

The traffic load on the network is composed of two data flows crossing the gateway and passing between both domains. In the first case, the network traffic goes from two nodes of the MANET environment to two nodes in the fixed net (manet to Internet). In the second case, the flow direction is reverted (Internet to manet), maintaining the correspondence among the nodes. For both cases the data transmission is realized with TCP and UDP flows.

For the nodes involved in sending and receiving the data flows, their packet size and the time of beginning and terminating the transmissions stay constant during the execution of the group of simulations.

C. Used Metrics

For the comparison of the behavior of the data transmissions among both networks, the following metrics were used:

End-to-End Delay (Delay)

The end-to-end delay is defined as the time difference between the packet generation and the arrival at their destination.

Packet Delivery Fraction (PDF)

This value corresponds to the percentage of successfully received packets by the destination node. It is calculated dividing the number of packets received by the number of packets generated.

Normalized Routing Overhead (NRO)

This value gives a measure of the overhead introduced by the MANET routing protocol and it is calculated as the fraction of control packets over data packets.

The first two metrics have direct relationship with the quality of service (QoS) measures of the Best-Effort service used in Internet and the last one with the overhead introduced by the MANET routing protocol.

VI. CONCLUSIONS

Table I shows statistical values obtained by the measurement series. They are ordered first by flow type (TCP, UDP) and then by the origin-destination segment (Fixed-mobile or Mobile-fixed). It can be observed that the data flow direction has little influence, regarding that for similar flows in different directions the behavior is quite similar. The small differences can be explained by the routes stored in the gateway at the moment of the transmission.

For the TCP flows, smaller Delay and Jitter values and better PDF rates can be observed; in contrast, UDP traffic obtains higher Delay and Jitter values and a lower PDF rate, that is, a higher latency compared to TCP and a lower rate of successfully received packets.

On the other hand, it can also be indicated that the PDF and the NRO are directly related, independent of the type and

direction of the flows, mainly due to the work executed by the routing protocol (AODV), to carry out the packet forwarding.

TABLE I
MEAN STATISTICS OF THE DATA FLOWS

	TCP		UDP	
	F-M	M-F	F-M	M-F
Delay	0.206878	0.194848	0.463238	0.549002
Jitter	0.11299	0.14191	1.29870	1.32829
PDF.	98.04781	97.73402	93.28205	92.59437
NRO	0.292047	0.115367	0.690216	0.477686

A. Delay

As can be seen in Figure 3(a), the behavior of the delay in UDP shows smaller instantaneous values than TCP, but a higher latency variation rate (Jitter) than the one shown by TCP figure 3(b), where the latency values are a lot more stable.

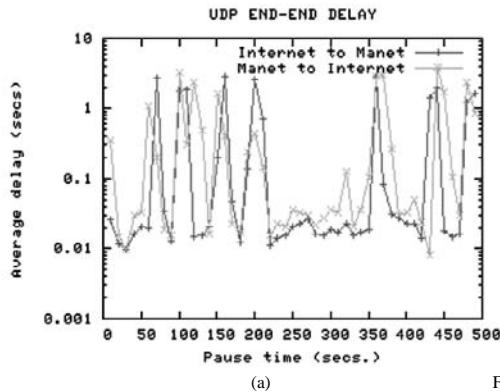
B. PDF

In general, the PDF is acceptable for both flows. Figure 4(b) shows the effect of the TCP error recovery mechanism and the relationship between the Jitter and the packet loss in the UDP flows which are produced by discarding some packets in the intermediate nodes.

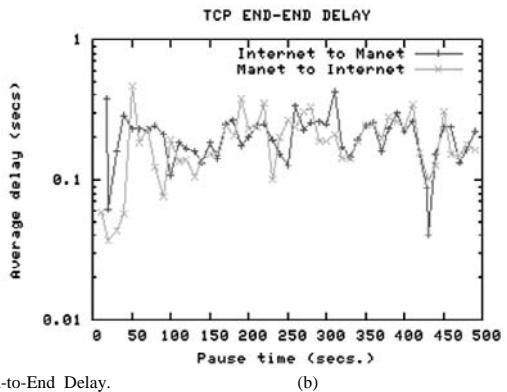
C. NRO

Figure 5(b) shows that that TCP has smaller network overhead rates. This can be explained in the behavior of the protocol itself, since the ACK sent by TCP helps to maintain routes up to date. Therefore, in this type of transmissions a smaller number of HELLO packets are necessary from the routing protocol. This way it is TCP who helps to maintain the routes stable, phenomenon that doesn't happen with the UDP transmissions just as can be appreciated in Figure 5(a).

In summary we can indicate that the behavior of both data flows in different directions indicates that TCP achieves a better performance compared to UDP in a network of these characteristics. The main reason is the error recovery mechanism included in the protocol, that reacts on the segment failures of the mobile segment and that interacts with the routing protocol mechanisms.

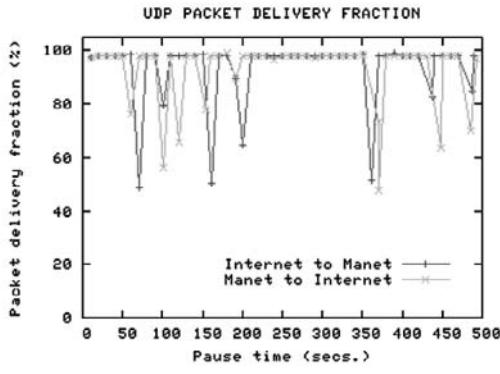


(a)

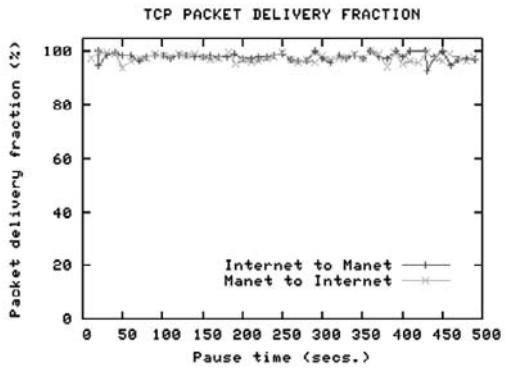


(b)

Fig. 3. End-to-End Delay.

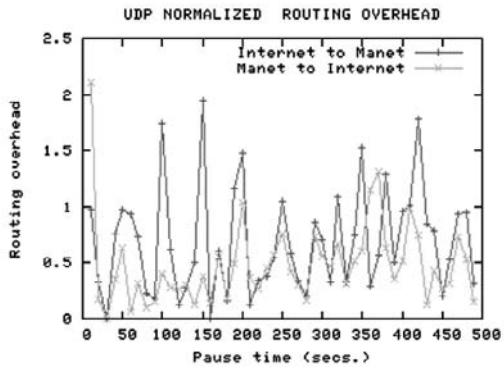


(a)

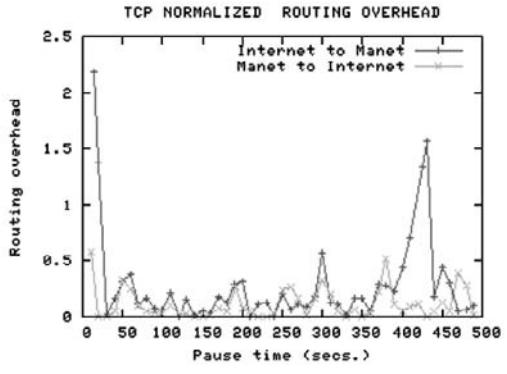


(b)

Fig. 4. Rate of Received Paquets.



(a)



(b)

Fig. 5. Routing Protocol Overhead.

ACKNOWLEDGMENT

This work was supported by the “Ministerio de Educación y Ciencia” (Spain) through the project TSI2006-12507-C03-02 of the “Plan Nacional de I+D+I”.

REFERENCES

- [1] S. Corson, J. Macker, “Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations”, IETF RFC 2501, January 1999.
- [2] I. Chakeres, C. Perkins, “Dynamic MANET On-demand (DYMO) Routing”, IETF Internet-Draft, work in progress, March 2006.
- [3] T. Clausen, P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, IETF RFC 3626, October 2003.
- [4] C. Perkins, E.Belding-Royer, S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing”, IETF RFC 3561, July 2003.
- [5] D. Johnson, D. Maltz, Y. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)”, IETF Internet-Draft, work in progress, July 2004.
- [6] R. Ogier, F. Templin, M. Lewis, “Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)”, IETF RFC 3684, February 2004.
- [7] R. Wakikawa, J. Malinen, C. Perkins, A. Nilsson, A. Tuominen, “Global Connectivity for IPv6 Mobile Ad Hoc Networks”, IETF Internet-Draft, work in progress, March 2006.
- [8] A. Hamidian, U. Körner, A. Nilsson, “Performance of Internet Access Solutions in Mobile Ad Hoc Networks” EuroNGI Workshop 2004: 189-209
- [9] P. Ruiz, A. Gomez-Skarmeta, “Enhanced Internet Connectivity for Hybrid Ad hoc Networks Through Adaptive Gateway Discovery,” *lcn*, pp. 370-377, 29th Annual IEEE International Conference on Local Computer Networks (LCN'04), 2004.
- [10] C. Jelger, T. Noel, A. Frey, “Gateway and address autoconfiguration for IPv6 adhoc networks” IETF Internet-Draft, work in progress, October 2003.
- [11] T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. *Wireless Communications F4 Mobile Computing (WCMC)*: Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, 2(5):483-502, 2002.
- [12] J. Broch, D. Maltz, D. Johnson, Y.C. Hu and J. Jetcheva, “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols,” *Proc. ACM/IEEE MOBICOM Conf.*, pp. 85-97, Oct. 1998
- [13] S.J. Lee, C.K. Toh, and M. Gerla, “Performance Evaluation of Table-Driven and On-Demand Ad Hoc Routing Protocols,” *Proc. IEEE Symp. Personal, Indoor and Mobile Radio Comm.*, pp. 297-301, September 1999.
- [14] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek and M. Degermark, “Scenario-Based Performance Analysis of Routing Protocols for Mobile Ad-Hoc Networks,” *Proc. ACM/IEEE MOBICOM Conf.*, p. 195-206, 1999.
- [15] M. K. Marina and S. R. Das, “Ad hoc On-demand Multipath Distance Vector Routing”, *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R) Special Feature on the First AODV Next Generation Workshop*, July 2002.
- [16] The VINT Project, “The Network Simulator-ns-2,” <http://www.isi.edu/nsnam/ns/>.

Designing aspects of a special class of reconfigurable parallel robots

Cornel Brisan

Technical University of Cluj-Napoca
C.Daicoviciu, 15, Cluj-Napoca, Romania

Abstract: This paper presents basic elements concerning modeling and simulation of parallel robots which are used for machine-tools development. The advantages of this new kind of machine-tools consist on their reconfigurability, on the possibility to improve accuracy of those machines etc. The main point of the paper is that few variants of parallel mechanisms with only one mobile platform and with number of degrees of freedom between 3 and 6 were emphasized. It must be also remarked that these variants are developed into modular manner in order to ensure full reconfigurability. The paper presents also numerical results obtained with the virtual models which were developed. Few prototypes which were developed are also presented.

I. INTRODUCTION

A good dynamic behaviour (high stiffness), a high accuracy and a good ratio between total mass and manipulated mass are just few advantages of parallel robots compared with serial type. However, the design, trajectory planning and application development of the parallel robot are difficult and tedious because the closed-loop mechanism leads to complex kinematics. To overcome this drawback, modular design concept is introduced in the development of parallel robots. Also, during the last period a new type of applications were developed. These new applications are related to the machine tools with parallel topology. Utilisation of parallel topology in the machine tools field creates the possibility for a reconfigurable design which is still an open problem and lacks theoretical base. One of the problems for reconfigurable robots is to determine the topology and geometry of the robot which is the suitable to fulfil a set of criteria. In the following sections we first present the modular topologic synthesis. Then, we describe the kinematics and an example is given.

II. MODULAR TOPOLOGIC SYNTHESIS

The structural synthesis of parallel mechanisms could be made if the relation of the number of degrees of freedom it is considered:

$$M = (6 - m) \cdot n - \sum_{k=1}^5 (k - m) \cdot C_k - M_P \quad (1)$$

where m is the number of common restrictions for all elements, n is the number of the mobile elements, k is the number of restrictions which define a joint (for example in the case of

prismatic joint $k=5$), C_k is the number of joints with $(6-k)$ degrees of freedom and M_P is the number of identical degrees of freedom.

In the case of parallel mechanisms without common restrictions and also without identical degrees of freedom the relation (1) it becomes:

$$M = 6 \cdot n - \sum_{k=1}^5 k \cdot C_k . \quad (2)$$

Let be N the number of mobile platforms and D_k – the number of joints with $(6-k)$ degrees of freedom which directly connect the platforms of the mechanism.

With these notations it results:

$$M = 6 \cdot (n_1 + N) - \sum_{k=1}^5 k \cdot (C_k + D_k) \quad (3)$$

where n_1 is the number of the elements which compose the loops which connect the platforms of the mechanism.

We can also assume (Fig.1) two types of basic modules (named basic legs) which can connect the platforms of the mechanism.

Let a_1 be the number of the loops with prismatic - universal - spherical (PUS) topology, let a_2 be the number of the loops with prismatic - rotational - spherical (PRS) topology, and also let a_3 be the number of the loops with prismatic - 2 universal - 2 spherical (P2U2S) topology.

In the case of parallel mechanisms which are used in the field of machine tools, it is common to consider:

$$N = 1, D_k = 0, k = \{1, \dots, 5\} \quad (4)$$

With these notations, the relation (3) becomes:

$$M = 6 - a_2 - 3a_3 \quad (5)$$

Also, each loop contains only one degree of freedom. Thus, it results:

$$M = a_1 + a_2 + a_3 \quad (6)$$

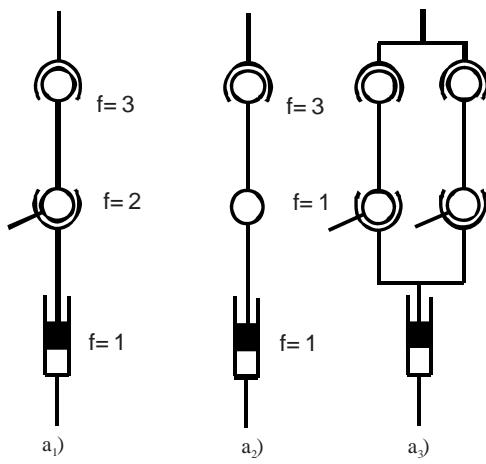


Fig.1. Adopted loops for PARTNER robots

Integer solutions of the equations:

$$\begin{aligned} M - 6 + a_2 + 3a_3 &= 0, \\ a_1 - M + a_2 + a_3 &= 0 \end{aligned} \quad (7)$$

gives all variants of parallel mechanisms with assumed hypothesis.

The system of equations (7) has many solutions. Also, if other parameters are taken into consideration (the order of the joints in the loop, the geometrical parameters of the loops etc) the topology problem becomes very complex.

The relation (7) defines the topology of parallel robots in a modular manner. If other parameters are taken into consideration (the order of the joints in the loop, the geometrical parameters of the loops etc) the topology problem becomes very complex.

Table 1 presents variants of **PARTNER robots**, solutions of (7), with $a_3=0$ and $6 \geq M \leq 3$.

TABLE 1.

SPECIAL VARIANTS OF PARTNER ROBOTS

No	M	a_1	a_2	Remarks
1	6	6	0	Stewart Platform
2	5	4	1	
3	4	2	2	
4	3	0	3	

Also, figure 2 presents kinematic loops of those variants.

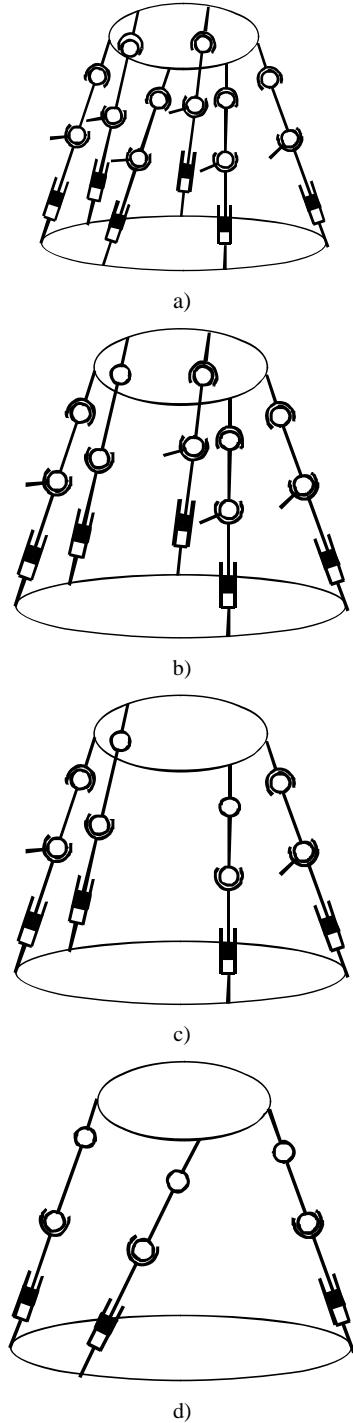


Fig.2. Special PARTNER robots

III. KINEMATICS

General algorithms used to solve direct kinematics in the case of parallel mechanisms consider that for each independent loop of the mechanism one vector equation can be write. Thus, a nonlinear system of scalar equations is obtained. Usually, this system of equations can be solved only with numerical methods and for that an accurate initial value of the solution it is required. Of course, this initial value of the solution is strongly related to the geometric parameters of the mechanism. When the geometric parameters of the mechanism are changed also the initial solution must be changed. According to that, the kinematics of the parallel mechanism will be developed in a modular manner, based on kinematics of the legs which connect the platforms and in order to ensure an analytical value for the initial solution. Each leg is in fact the right (or left) side of one independent closed loop and can be described by two coordinate systems: one attached to the frame and the other one attached to the mobile platform (Fig. 3).

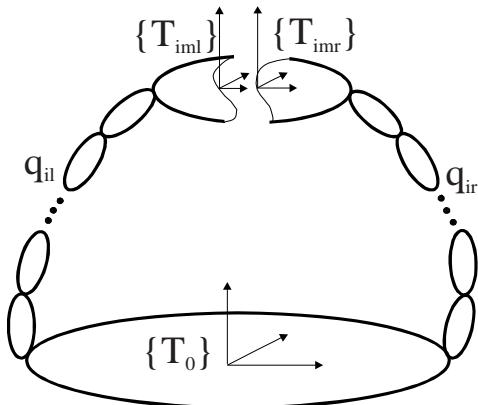


Fig. 3 Independent closed loop

The relationship between these coordinate systems is given by:

$$\mathbf{H}_{iml} = \prod \mathbf{A}_{il}(q_{il}), \quad (8)$$

for the left part of the independent loop and :

$$\mathbf{H}_{imr} = \prod \mathbf{A}_{ir}(q_{ir}), \quad (9)$$

for the right part.

\mathbf{H}_{iml} , \mathbf{H}_{imr} are absolute transformation matrices and $\mathbf{A}_{il}(q_{il})$, $\mathbf{A}_{ir}(q_{ir})$ are relative transformation matrices.

For an independent loop it results:

$$\mathbf{H}_{iml} = \mathbf{H}_{imr} \quad (10)$$

Matrix equation (10) leads to six independent scalar equations. For whole parallel mechanism, a nonlinear system of equations (with $6n$ independent scalar equations, where n is the number of independent loops) will be obtained. This system of equations can be solved only with numerical methods. Generally, the legs of the parallel component have the same topology. It results that the relative transformation matrices for the left and right part of each loop are formal similar. Therefore, for each topology of the legs, a formal mathematical entity (named **LMM** - Leg Mathematical Model) can be developed. Similarly a modular kineto-static model can be developed. This mathematical model leads to non-linear system of equations. Classic algorithms of numerical methods, e.g. Newton-Raphson, can be used in order to solve this system of equations.

Usually a virtual model must be designed in order to ensure a friendly way to cooperate with the customer. Related to the virtual parallel mechanisms and in order to ensure this property, the virtual model of LMM must include an automatic way to find an initial solution for the nonlinear system of equations.

Without lose the generality of the problem, a leg with PSU topology is considered (Fig.4a). An analytical solution of the initial values of the angular parameters of the joints of the leg means that a solution of the inverse geometric model for the initial position must be determined. This solution is also the initial solution for the nonlinear system of equations for the whole mechanism.

Thus, for the leg from figure 4a, it results:

$$\begin{aligned} \mathbf{H} &= \mathbf{A}_1 \cdots \mathbf{A}_6 \\ \mathbf{A}^{-1}_1 \mathbf{H} &= \mathbf{A}_2 \cdots \mathbf{A}_6 \\ \mathbf{A}^{-1}_2 \mathbf{A}^{-1}_1 \mathbf{H} &= \mathbf{A}_3 \cdots \mathbf{A}_6 \\ \mathbf{A}^{-1}_3 \mathbf{A}^{-1}_2 \mathbf{A}^{-1}_1 \mathbf{H} &= \mathbf{A}_4 \cdots \mathbf{A}_6 \\ \mathbf{A}^{-1}_4 \mathbf{A}^{-1}_3 \mathbf{A}^{-1}_2 \mathbf{A}^{-1}_1 \mathbf{H} &= \mathbf{A}_5 \cdot \mathbf{A}_6 \\ \mathbf{A}^{-1}_5 \mathbf{A}^{-1}_4 \mathbf{A}^{-1}_3 \mathbf{A}^{-1}_2 \mathbf{A}^{-1}_1 \mathbf{H} &= \mathbf{A}_6 \end{aligned} \quad (11)$$





Fig. 4. Virtual models of the modules

where H is the absolute transformation matrix, which describe the absolute position and orientation of the mobile platform (known for the initial position of the mechanism), A_i ($i=1,6$) is the relative transformation matrix. The elements of the A_i are functions of the joint coordinate (q_i for the prismatic joint and α_{ij} for all other joints of the leg). Using relations (11) a set of initial values for the parameters which describe the leg from figure 4a can be found.

IV. VIRTUAL MODELS

Based on relations (8),..., (11) and using MOBILE software package few kinds of virtual models may be developed. For example the mechanism shown in figure 5 has three degrees of freedom and five independent kinematic loops. This mechanism results for $a_1 = a_2 = 0$.

Thus, for each closed independent loop, the closing equations are:

$$\sum_{j=1}^4 \mathbf{a}_{ijL} = \sum_{j=1}^4 \mathbf{a}_{ijR}, \quad (12)$$

$$\mathbf{R}_{iL} = \mathbf{R}_{iR}$$

where \mathbf{R}_{iL} and \mathbf{R}_{iR} are the absolute orientation matrices, corresponding to the left and right side respectively of the closed independent loop.

The system of equations describe by (12) contains (in the case of all five loops) 30 unknowns.

These are the angular displacements (θ_{jiL} and θ_{jiR}) at the level of universal and spherical joints respectively. This system of equations can be solved with numerical methods. In order to find an initial solution (necessary for numerical methods) classical algorithm of inverse kinematics applied for open loop, which connects the mechanism platforms, can be used:

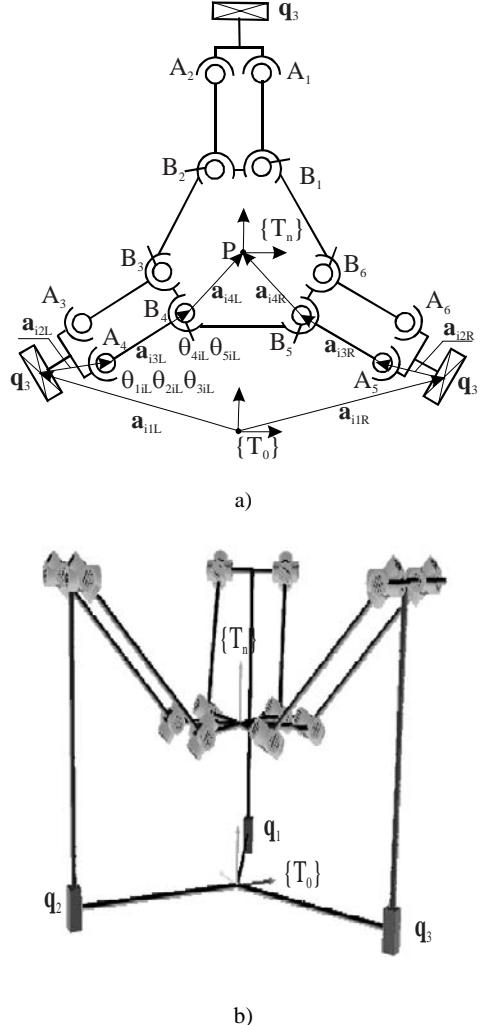
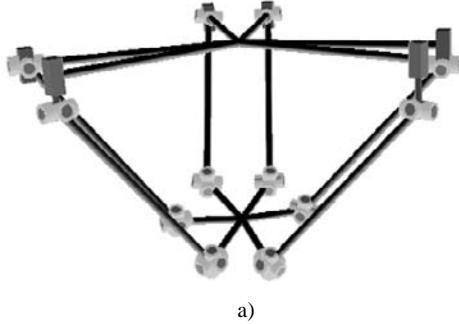


Fig. 5. a) Mechanism with 3 dof; b) Virtual model

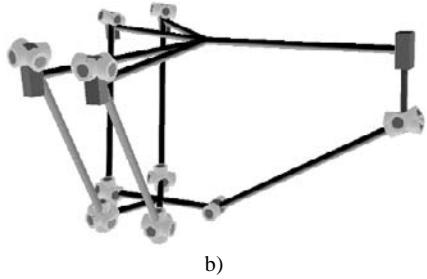
$$\prod_{j=1}^k \mathbf{A}_{jiL}^{-1}(\theta_{jiL0}) \mathbf{H}_0 = \prod_{j=k+1}^6 \mathbf{A}_{jiL}(\theta_{jiL0}). \quad (13)$$

where \mathbf{H}_0 is the absolute transformation matrix and \mathbf{A}_{jiL} are the relative transformation matrices.

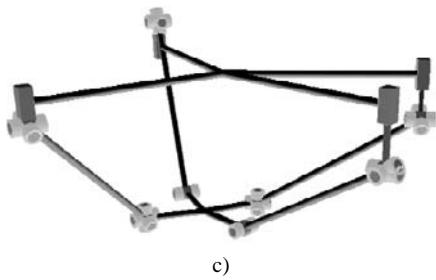
Also, figure 6 presents virtual models of the robots from figure 2.



a)



b)



c)



Fig. 6 PARTNER robots
a) with 6 dof; b) with 5 dof; c) with 4 dof; d) with 3 dof

Using these virtual models it is possible to get out also numerical results, those corresponding to assumed movements. Thus, Stewart platform, with concrete geometrical data were considered (Fig. 7).

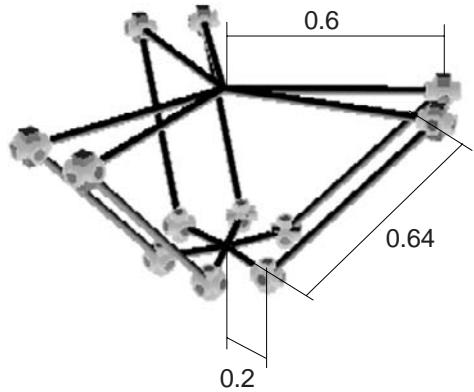
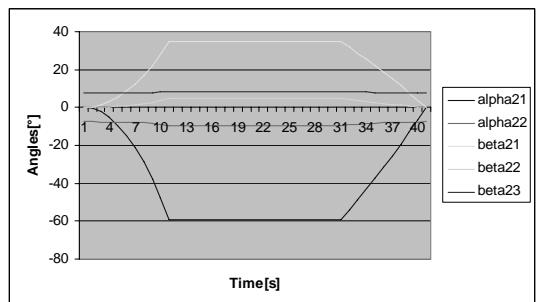
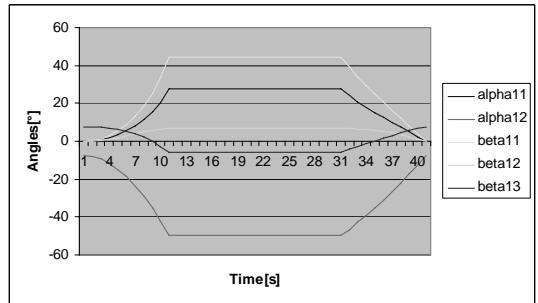


Fig. 7. Geometric data of Stewart platform

For this mechanism a subject of interest is the volume of work space and as consequence the values of the angles at the level of passive joints are object of interest. Figure 8 presents time variation for the angles of the passive joints for this mechanism (“alpha_{ij}” are the angles at the level of universal joint and “beta_{ij}” are the angles at the level of spherical joints).



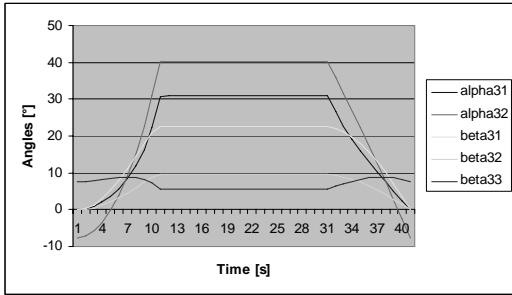


Fig. 8 Time variation of the passive angles in the case of Stewart platform

In addition, figure 9 presents few prototypes of the parallel robots from figure 6.



a)



b)



c)

Fig. 9. Prototypes of PARTNER robots
a) 4 dof; b) 5dof; c) 6 dof

V. CONCLUSIONS

The conclusion can be drawn as follows.

Based on assumed modules and on relation of the number of degrees of freedom for a mechanism, a topologic synthesis can be done.

The kinematics of the whole mechanism can be developed on a modular manner, each module based on the kinematics of one leg.

Solving inverse kinematics of one leg it is possible to find an analytical solution of the initial value of the solution of the system of equations, which solve the direct kinematics of the mechanism.

Analytical solution for the initial value of the solution of the system of equations corresponding to the direct kinematics of the mechanism increases significantly flexibility of the simulation model. Thus, it is possible to change automatically and interactive the geometric parameters of the mechanism during the simulation.

ACKNOWLEDGMENT

This paper was financial supported by Alexander von Humboldt Foundation

REFERENCES

- [1] Angeles, J., "Fundamentals of Robotic, Mechanical System", *Springer – Verlag*, 1997.
- [2] Brisan C., Handra-Luca, V., "Contributions to the Kinematic Structural Synthesis of the Parallel Robots", *International Conference on PKM*, Ann Arbor, Michigan USA, 2000, pp.71-78.
- [3] Carretero, J.A. s.a., "Kinematic Analysis And Optimization of a New Three-Degree-of-Freedom Spatial Parallel Manipulator," *ASME Journal of Mechanical Design*, Vol. 122, No. 1, 2000, pp. 17-24.
- [4] Hiller, M., "Multiloop Kinematic Chains and Dynamics of Multiloop Systems, in Kinematics and Dynamics of Multi-Body Systems" (ed. By J. Angeles and A. Kecskemethy), *CISM Courses and Lecture*, nr. 360, *Springer Verlag*, 1995.
- [5] Kecskemethy, A., "MOBILE -User's Guide and Reference Manual" *Gerhard-Mervator-Universität-GH Duisburg*, 1994.
- [6] Parenti, V., Castelli, A. "Classification and kinematic modelling of fully-parallel manipulators-a review" *Parallel Kinematic Machines: Theoretical Aspects and Industrial Requirements*, 1999, pp.51-68.
- [7] Pateli, A.J., Ehman, K.F. "Volumetric Error Analysis of a Stewart Platform Based Machine Tool" *Annals of the CIRP*, Vol 46,1997, pp.287-290
- [8] Pritschow, G., Tran, T.L., "Parallel Kinematics and PC-based Control System for Machine Tools" In: *Proceedings of 37th IEEE Conference on Decision and Control*, 16/18. December 1998,Tampa/Florida, USA, pp.2605-2610.
- [9] Pritschow, G.,Wurst, K.-H., "Systematic design of hexapods and other parallel link systems" In: *Annals of the CIRP* Vol 46, 1997, pp.291-295.
- [10] Pritschow, G.,Wurst, K.-H., "Modular Robots for flexible assembly" In: *Proceedings of 28th CIRP International Seminar on Manufacturing Systems "Advances in Manufacturing Technology - Focus on Assembly Systems*, May 15-17, 1996.
- [11] Ryu, S.-J., s.a., "Eclipse: an Over actuated Parallel Mechanism for Rapid Machining" *Parallel Kinematic Machines: Theoretical Aspects and Industrial Requirements*.1999, pp.441-454.
- [12] Song J. s.a., "Error Modeling and Compensation for Parallel Kinematic Machines" *Parallel Kinematic Machines: Theoretical Aspects and Industrial Requirements*. 1999, pp.171-187.
- [13] Wurst, K.-H., "LINAPOD-Machine Tools as Parallel Link Systems Based on a Modular Design" In: *Proceedings of 1st European-American Forum on Parallel Kinematic Machines*,1998, Mariland.

Performance Analysis of blocking Banyan Switches

D. C. Vasiliadis , G. E. Rizos , C. Vassilakis

Department of Computer Science and Technology

Faculty of Sciences and Technology

University of Peloponnese

GR-221 00 Tripolis

GREECE

dvas@uop.gr,georizos@uop.gr,costas@uop.gr

Abstract—Banyan Networks are a major class of Multistage Interconnection Networks (MINs). They have been widely used as efficient interconnection structures for parallel computer systems, as well as switching nodes for high-speed communication networks. Their performance is mainly determined by their communication throughput and their mean packet delay. In this paper we use a performance estimation model that is based on a universal performance factor, which includes the importance aspect of each of the above individual performance factors (throughput and delay) in the design process of a MIN. The model can also uniformly be applied to several representative networks. The complexity of the model requires to be investigated by time-consuming simulations. In this paper we study a typical (8X8) Baseline Banyan Switch that consists of (2X2) Switching Elements (SEs). The objective of this simulation is to determine the optimal buffer size for the MIN stages under different conditions.

Index Terms—Multistage interconnection networks, baseline networks, delta networks, crossbar switches, packet switching, performance analysis.

I. INTRODUCTION

MINs have been recently identified as an efficient interconnection network for a switching fabric of communication structures such as gigabit Ethernet switch, terabit router, and ATM switching. They are also frequently used for connecting processors in parallel computing systems. They have received considerable interest in the development of networks. A significant advantage of MINs is their low cost, taking into account the overall performance they offer. The important thing about an interconnection system is that it has the capacity to route many communication tasks concurrently. The situation where more than one packets claim the same communication resource is called a *conflict*. When a packet finds the next buffer position already occupied, then it cannot be routed and is thus blocked. The primary purpose of buffers in a SE is to prevent loss of packets due to routing conflicts.

For the estimation of MIN performance, a number of studies and approaches have been published. There are studies assuming uniform arriving traffic on inputs like [1,2]. [3] addresses non-Markovian processes which are approximated by Markov models. Markov chains are also used in [4] to compare MIN performance under different buffering schemes. Hot spot traffic performance in MINs is examined by [5], while [6] deals with multicast in Clos networks as a subclass of MINs. [7] uses mathematical methods for investigating group communication in circuit switched MINs, and employs Markov chains as a modeling technique. The throughput of finite and infinite buffered MINs under uniform and non uniform traffic can also be calculated. In the literature, there are also other approaches that focus only on non uniform arriving traffic [8,9]. [10] discusses approaches that examine the case of Poisson traffic on inputs of a MIN. Rehrmann [11], makes an analysis of communication throughput of single-buffered multistage interconnection networks consisting of (2X2) switches with maximum arrivals of packets 100%, using relaxed blocking model. Furthermore, there are studies that deal with self-similar traffic on inputs.

In this paper, we assume that packets are uniformly distributed across all the destinations and each queue uses a FIFO policy for all output ports. We study the performance of a Baseline Banyan Switch with blocking SEs that operates under different conditions. At first we present and analyze a typical (8X8) Baseline Banyan Switch. Then, we explain the performance criteria and parameters of this. Finally we present the results of our simulation experiments and provide the concluding remarks.

II. ANALYSIS OF A (NXN) BANYAN SWITCH

A MIN can be defined as a network used to interconnect a group of N inputs to a group of M outputs using several stages of small size Switching Elements (SEs) followed (or leaded) by link states. It is usually defined by, among others, its topology, routing algorithm, switching strategy and flow control mechanism. A Banyan Network was defined by [12] and is characterized by the property that there is exactly a unique path from each source (input) to each sink (output). The path can be encoded as a sequence of labels of the

successive outputs of the SEs. Thus, Banyan Switches are multistage self-routing switching fabrics. That means, each SE that accepts a packet in one of its input ports can decide in which of its output ports to forward this packet depending only on the destination address of it. A SE of stage k can decide in which output port to send it based on the k^{th} bit of the destination address and the k -bit shuffle algorithm. If the corresponding bit is 0, then the packet is forwarded to the upper output port and if the bit is 1 packet is forwarded to the lower output port.

A (NXN) Banyan Switch can be constructed by $n=\log_c N$ stages of $(c \times c)$ SEs, where c is the degree of them. At each stage there are exactly N/c SEs. Consequently, the total number of SEs of a MIN is $(N/c) * \log_c N$. Thus, there are $O(N \log N)$ interconnections among all stages, as opposed to the crossbar network which requires $O(N^2)$ links.

In this paper we study a typical Baseline Banyan Switch of dimension (8×8) that consists of 12 small SEs each of degree (2×2) . This type of Banyan Switches provides both benefits of Omega and Generalized Cube Switches (destination routing, partitioning and expandability). A configuration with finite size non-shared buffer queues is shown below in the figure 1. It is assumed to operate under the following conditions:

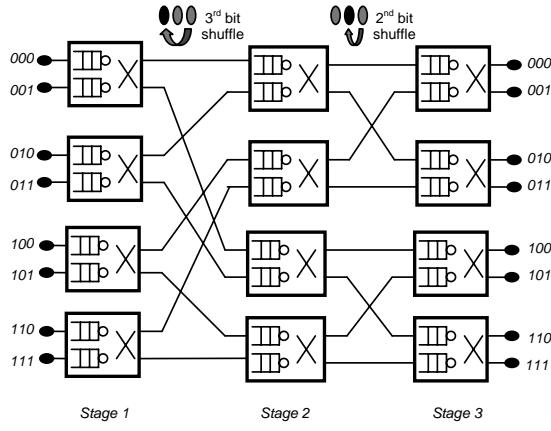


Fig.1 A (8×8) Baseline Banyan Switch

- The network clock cycle consists of two phases. In the first face flow control information passes through the network from the last stage to the first stage. In the second phase packets flow from one stage to the next in accordance with the flow control information.
- The arrival process of each input of the network is a simple Bernoulli process, i.e., the probability that a packet arrives within a clock cycle is constant and the arrivals are independent of each other.
- A packet arriving at the first stage ($k=1$) is discarded if the buffer of the corresponding SE is full.

- All SEs have deterministic service time.
- A packet is blocked at a stage if the destination buffer at the next stage is full.
- The packets are uniformly distributed across all the destinations and each queue uses a FIFO policy for all output ports.
- When two packets at the i^{th} stage contend for the same buffer at the $(i+1)^{\text{th}}$ stage and there is not adequate free space for both of them to be stored, there is a conflict. In this case, one of them will be accepted at random and the other will be blocked by means of upstream control signals.
- Finally, all packets in input ports contain both the data to be transferred and the routing tag. In order to achieve synchronously operating SEs, the MIN is internally clocked. As soon as packets reach a destination port they are removed from the MIN. So, packets cannot be blocked at the last stage ($k=3$).

III. PERFORMANCE EVALUATION METHODOLOGY

In order to evaluate the performance of a (NXN) MIN with $n=\log_c N$ intermediate stages of $(c \times c)$ SEs, we use the following metrics. Let T be a relatively large time divided into u discrete time intervals $(\tau_1, \tau_2, \dots, \tau_u)$.

- Average throughput* (Th_{avg}) is the average number of packets accepted by destinations per network cycle. This metric is also referred to as *bandwidth*. Formally, Th_{avg} can be defined as
- $$Th_{\text{avg}} = \lim_{u \rightarrow \infty} \frac{\sum_{i=1}^u n(i)}{u} \quad (1)$$
- where $n(i)$ denotes the number of packets that reach their destinations during the i^{th} time interval.

- Normalized throughput* (Th) is the ratio of the *average throughput* Th_{avg} to network size N . Formally, Th can be expressed by
- $$Th = \frac{Th_{\text{avg}}}{N} \quad (2)$$

- Average packet delay* (D_{avg}) is the average time a packet spends to pass through the network. Formally, D_{avg} can be expressed by

$$D_{\text{avg}} = \lim_{u \rightarrow \infty} \frac{\sum_{i=1}^{n(u)} t_d(i)}{n(u)} \quad (3)$$

where $n(u)$ denotes the total number of packets accepted within u time intervals and $t_d(i)$ represents the total delay for the i^{th} packet.

We consider $t_d(i) = t_w(i) + t_r(i)$ where $t_w(i)$ denotes the total queuing delay for the i^{th} packet waiting at each

stage for the availability of an empty buffer at the next stage queue of the network. The second term $t_n(i)$ denotes the total transmission delay for i^{th} packet at each stage of the network, that is just $n*nc$, where n is the number of stages and nc is the network cycle.

- *Normalized packet delay (D)* is the ratio of the D_{avg} to the minimum packet delay which is simply the transmission delay $n*nc$. Formally, D can be defined as

$$D = \frac{D_{\text{avg}}}{n * nc} \quad (4)$$

- *Universal performance (U)* is defined by the following relation of two above normalized opposing factors: one must be minimized (D) and the other must be maximized (Th). Formally, U can be expressed by

$$U = \sqrt{D^2 + \frac{1}{Th^2}} \quad (5)$$

It is obvious that, when the *packet delay factor* becomes smaller and/or the *throughput factor* becomes larger, the *universal performance factor (U)* becomes smaller. Consequently, as the *universal performance factor (U)* becomes smaller, the performance of a MIN is considered to improve. Because the above factors (parameters) have different measurement units and scaling, we normalize them to obtain a common value domain. Normalization is performed by dividing the value of each factor by the (algebraic) maximum value that this factor may attain. Thus, equation (5) can be replaced by the following equation:

$$U = \sqrt{\left(\frac{D}{D_{\text{max}}}\right)^2 + \left(\frac{Th_{\text{max}}}{Th}\right)^2} \quad (6)$$

where D_{max} is the maximum value of *normalized packet delay (D)* and Th_{max} is the maximum value of *normalized throughput*.

- *Universal performance ($U_{wd,wt}$)* with weight factors w_{wd}, w_{wt} includes the importance aspect of each factor in the design process of a MIN. Formally, $U_{wd,wt}$ can be expressed by

$$U_{wd,wt} = \sqrt{w_{wd} * \left(\frac{D}{D_{\text{max}}}\right)^2 + w_{wt} * \left(\frac{Th_{\text{max}}}{Th}\right)^2} \quad (7)$$

Effectively, the values of w_{wd} and w_{wt} will be chosen by the MIN designers to reflect the significance that the corresponding factor (*delay* and *throughput* respectively) has in the particular MIN.

The following parameters affect all the above performance aspects of a MIN.

- *Buffer size (β)* is the maximum number of packets that an input buffer of an SE can hold. In our case β is assumed to be $\beta=0, 2, 4$ or 8 .
- *Probability of arrivals (p_a)* is the steady-state fixed probability of arriving packets at each queue on inputs. In our simulation p_a is assumed to be $p_a = 0.1, 0.2, \dots, 0.9, 0.99$.

IV. SIMULATION AND PERFORMANCE RESULTS

The performance of MINs is usually determined by modeling, using simulation [13] or mathematical methods [14]. In this paper we estimated the network performance using simulations. We developed a general simulator for MINs in a packet communication environment. The simulator can handle several switch types, inter-stage interconnection patterns, loading conditions, and switch operation policies. We focused on an (8X8) Banyan Switch that consists of (2X2) SEs, using internal queuing. Each SE in all stages of the MIN was modeled by two non-shared buffer queues. Buffer operation was based on FCFS principle. When there was a contention between the packets in a SE, it was solved randomly. The simulation was performed at the packet level, assuming fixed-length packets transmitted in equal-length time slots, where the slot was the time required to forward a packet from one stage to the next.

The parameters for the packet traffic model were varied across simulation experiments to generate different offered loads and traffic patterns. Statistics such as *packet throughput* and *packet delays* were collected at the output ports. We performed extensive simulations to validate our results. All statistics obtained from simulation running for 10^5 clock cycles. The number of simulation runs was adjusted to ensure a steady-state operating condition for the MIN. There was a stabilization process in order the network be allowed to reach a steady state by discarding the first 10^3 network cycles, before collecting the statistics.

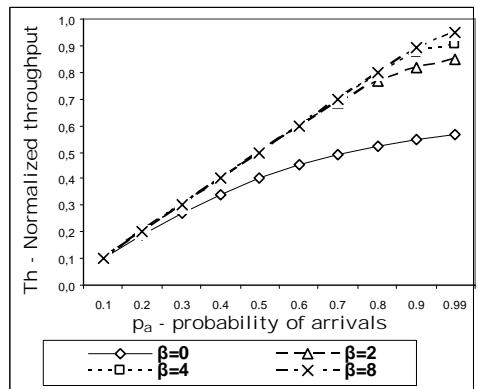


Fig.2 Normalized throughput vs. probability of arrivals

This section summarizes the results obtained from simulating the behavior of the MIN using various performance parameter value combinations. The objective of the simulation is to determine the optimal *buffer size* for the MIN stages under different conditions; optimality is determined by the value of the universal performance factor U , introduced above.

Figure 2 presents the relation between the *normalized throughput* performance metric and the *arrival probability* under different *buffer sizes*. This diagram clearly shows that using no buffer ($\beta = 0$) is not a good option, since approximately 42% of the network capacity is lost, mainly due to the excessive number of dropped packets. Analytical results of our simulation were validated by comparing them with earlier works. S.H. Hsiao and R.Y. Chen [1] present diagrams representing the *normalized throughput* (Th) of an ($N \times N$) Banyan Switch. It was investigated either by time-consuming simulations or approximated by mathematical models. In those diagrams, there is a comparison in *normalized throughput* (Th) with respect to number of stages under maximum value of *probability of arrivals* ($p_a=1$) with *buffer size* $\beta=0$ (only the processors of SEs have a single buffer). We notice that in the case of a 3-stage MIN, the *normalized throughput* ranges from 0.5 to 0.6. In our simulation the corresponding *normalized throughput* is ($Th \approx 0.57$).

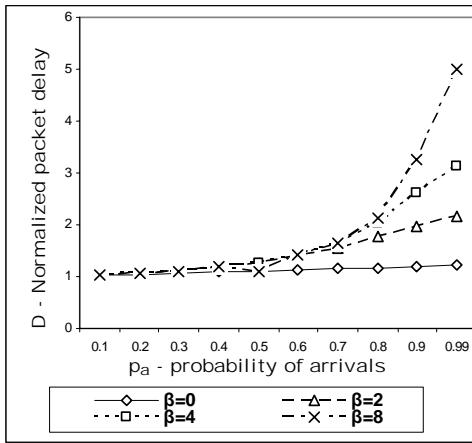


Fig.3 Normalized packet delay vs. probability of arrivals

Figure 3 illustrates the *normalized packet delay* for the various *buffer sizes* (0, 2, 4 and 8), when the *arrival probability* ranges from 0.1 to 0.99. It is clear that the *normalized packet delay* significantly increases for large *buffer sizes* (4 and 8) when the *arrival probability* exceeds 80%; however we should note that for small *buffer sizes*, the probability that a packet is dropped under heavy load (*arrival probability* > 80%) is also considerable [15].

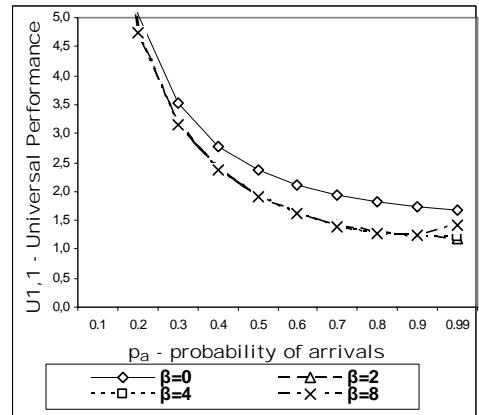


Fig.4 Universal performance factor with equal weights for individual factors

Figures 4-6 illustrate the relation of the combined *performance indicator* U to the *arrival probability* under different *buffer sizes*. Recall from section 3 that the combined *performance indicator* is itself parametric, allowing MIN designers to designate the importance of each individual factor (*packet delay* and *throughput*) through the use of weights. Thus, figure 4 depicts the case when the two factors are considered of equal importance ($w_d = w_t = 1$).

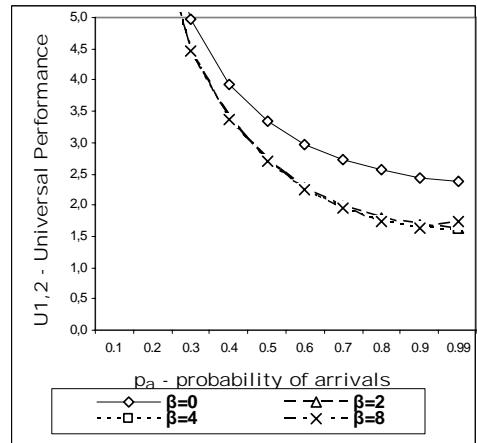


Fig.5 Universal performance factor with delay weight = 1 and throughput weight = 2

Figure 5 presents the case of a MIN where the overall *throughput* (and consequently, the exploitation of the available network capacity) is considered of greater importance; in this case w_d is set to 1, while w_t is set to 2.

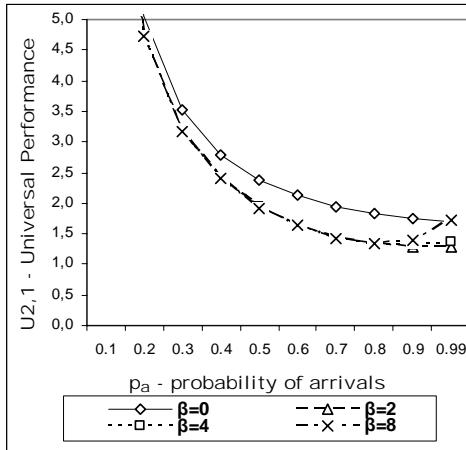


Fig.6 Universal performance factor with delay weight = 2 and throughput weight = 1

Finally, figure 6 illustrates the opposite case, where the minimization of *packet delays* is the primary consideration of the MIN designers.

V. CONCLUSION

The simulation results presented above provide useful insights for MIN designers regarding the network *throughput* and *performance parameters*, under different *loads* and *buffer sizes*. The combined metric *Universal Performance Factor* (U_{wd, w_t}) introduced in this paper gives an overall, single-dimension estimate of the network performance by allowing MIN designers to assign weights to individual *performance factors*; it is expected that MIN designers will choose weights accordingly to reflect the importance of each *performance factor* in the MIN operation.

An important finding from the simulation results is that the *Universal Performance Factor* deteriorates significantly when the switching element *buffer size* increases from 4 to 8. This happens because the *throughput* gains from increasing the *buffer size* from 4 to 8 are almost negligible, while the corresponding increment in the average *packet delay* within the MIN is considerable. This becomes more apparent when the w_d factor (i.e. the weight assigned to the *delay performance parameter*) is set higher than the w_t factor (the *throughput factor weight*).

At an application level, multimedia and streaming-oriented communications typically require small end-to-end packet delays, thus it is expected that in such contexts MIN designers will opt for small *buffer sizes*, with the values of 2 and 4 being the prevalent candidates. Especially for heavily loaded MINs, the choice of *buffer size* = 2 leads to the optimal value for the Universal Performance Factor. For MINs that do not exhibit such real-time requirements (and thus w_d will be equal to or

smaller than w_t), a choice of *buffer size* = 4 is acceptable, since network throughput is better exploited, while the additional end-to-end *packet delay* can be tolerated.

REFERENCES

- [1] S.H. Hsiao and R. Y. Chen, "Performance Analysis of Single-Buffered Multistage Interconnection Networks", 3rd IEEE Symposium on Parallel and Distributed Processing, pp. 864-867, December 1-5, 1991.
- [2] T.H. Theimer, E. P. Rathgeb, and M.N. Huber, "Performance Analysis of Buffered Banyan Networks", IEEE Transactions on Communications, vol. 39, no. 2, pp. 269-277, February 1991.
- [3] A. Merchart, A Markov chain approximation for analysis of Banyan networks, in Proc. ACM SIGMETRICS Conf. On Measurement and Modelling of Computer systems, 1991.
- [4] B.Zhou, M.Atiquzzaman, A Performance Comparison of Four Buffering Schemes for Multistage Interconnection Networks, International Journal of Parallel and Distributed Systems and Networks, 5, no. 1: 17-25, 2002.
- [5] M.Jurczyk, Performance Comparison of Wormhole-Routing Priority Switch Architectures, In Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications 2001 (PDPTA'01); Las Vegas, 1834.1840, 2001.
- [6] J.Turner, R. Melen, Multirite Clos Networks, IEEE Communications Magazine, 41, no. 10: 38-44., 2003
- [7] Y. Yang, J. Wang, A Class of Multistage Conference Switching Networks for Group Communication, IEEE Transactions on Parallel and Distributed Systems, 15, no. 3: 228-243, 2004.
- [8] M. Atiquzzaman and M.S. Akhtar, "Efficient of Non-Uniform Traffic on Performance of Unbuffered Multistage Interconnection Networks", IEE Proceedings Part-E, 1994.
- [9] M. Atiquzzaman and M.S. Akhtar, "Effect of Non-Uniform Traffic on the Performance of Multistage Interconnection Networks", 9th International Conference on System Engineering, Las Vegas, pp. 31-35, July 1993.
- [10] T. Lin, L. Kleinrock, "Performance Analysis of Finite-Buffered Multistage Interconnection Networks with a General Traffic Pattern", Joint International Conference on Measurement and Modeling of Computer Systems, Proceedings of the 1991 ACM SIGMETRICS conference on Measurement and modeling of computer systems, San Diego, California, United States, Pages: 68 - 78, 1991.
- [11] R. Rehrman, B. Monien, R. Luling, R. Diemann, On the communication throughput of buffered multistage interconnection networks, in ACM SPAA '96 pp. 152-161.
- [12] G. F. Goke, G.J. Lipovski, Banyan Networks for Partitioning Multiprocessor Systems, Proc. 1st Ann. Symp. on Computer Architecture, 1973, pp. 21-28
- [13] D. Tutsch, M.Brenner .MIN Simulate. A Multistage Interconnection Network Simulator.. In 17th European Simulation Multiconference: Foundations for Successful Modelling & Simulation (ESM'03); Nottingham, SCS, 211.216, 2003.
- [14] D. Tutsch, G.Hommel, Generating Systems of Equations for Performance Evaluation of Buffered Multistage Interconnection Networks, Journal of Parallel and Distributed Computing, 62, no. 2: 228-240, 2002.
- [15] D.C. Vasiliadis, G.E.Rizos Simulation for Multistage Interconnection Networks using relaxed blocking model. Proceedings of the ICCMSE 2006 conference, Greece, 2006.

DEMYSTIFYING THE DYNAMICS OF LINEAR ARRAY SENSOR IMAGERY

Dr. Koduri Srinivas

Data Processing Area National Remote Sensing Agency

Balanagar, Hyderabad, India

Email: srinivas_k@nrsa.gov.in

Abstract

The present study aims at demystifying the dynamics of spacecraft imaging system including state vector, viewing orientation, attitude parameters (roll, pitch and yaw) and other related parameters, as a digital solution, with a full force rigorous orbital photogrammetric model.

In this approach satellite orientation parameters are modeled as keplerian orbital parameters in continuous time domain, as against conventional approaches that use position and velocity vector parameters of the imaging platform in discreet time domain,. The attitude parameters are, however, modeled as polynomials in discreet time domain. This hybrid time domain model offers an excellent insight and a better understanding of the dynamics of linear array sensor imagery that is illustrated with a Spot 2 data set.

The study brings out that the key components associated with dynamics of push broom imagery are two keplerian parameters true anomaly and ascending node, attitude parameters (roll, pitch and yaw) and distance between space craft and imaged ground point.

Keywords: Remote sensing; SPOT; IRS satellites; geometric rectification; DEM, ortho-photo; image orientation; stereo images; continuous time domain model; unified theory of least squares and rigorous orbital photogrammetric model.

1. Introduction

Earth observation satellites (EOS) such as Spot, IRS series of satellites, Quickbird, and IKONOS scan the earth surface with an array of CCD elements in push broom mode, while satellites such as Landsat scan the same in whisk broom mode. For push broom imaging, direction of scan is along the flight direction of satellite, whereas for whisk broom imaging, direction of scan is perpendicular to the flight direction. Linear array sensors operating in push broom mode are widely used for acquiring images at high resolution for cartographic applications.

Up to the late 1970's, control engineering concepts have been used to model the movement of photo plates of analytical instruments as per the dynamics of aerial scanner. During the late 1980's, Kratky [16], Konecny [15] et al and others used analytical photogrammetric instruments for generating precision corrected products of Spot 2 with level 1B photo

products. These analytical instruments have been in vogue until the advent of digital photogrammetric workstations. Digital emulation of the dynamics of spacecraft imagery has been influenced by aerial scanner imagery wherein position and velocity information is modeled in discreet time domain. Other digital approaches have been based on rational polynomial functions, affine models and direct linear transformations. Several efforts have been made to understand the suitability of these models with respect to complexity, rigor and accuracy that are detailed in Dieter Fritsch et al., [7], and Dowman et al [6] and Daniela Poli [2].

Recent studies indicate that Kartky's approach is far superior to other models and this is largely due to his strict adherence to emulate the movement of photo plates of analytical photogrammetric instruments using keplerian parameters of Spot2 orbit. Eminent photogrammetrists such as Edward Mikhail [19], Toutin [26] etc have noted that there are several inadequacies by modeling satellite imagery with aerial scanner and other digital approaches. GP Rao et al [12], GP Rao [13] note the superiority of continuous time domain models from the simulation results of other disciplines such as control theory. In addition, these authors also indicate that Newton's, Faraday's, etc. are developed in continuous time domain and there is little possibility that these laws will be written in discreet time domain.

The focus of present study is on an analysis of dynamics of push broom spacecraft imagery based on Kartky's approach and as a digital photogrammetric solution in hybrid time domain with SPOT 2 data. This analysis is relevant for extraction of metric information from other linear sensor arrays such as IRS series of satellites, IKONOS and Quickbird. Accordingly, the paper is organized as six sections with this as an introduction. The need for rigorous orbital photogrammetric models is brought out as section 2. Sensor models based on discreet time domain and hybrid time domain are presented briefly as section 3. The parameters included for bundled adjustment are described in section 4. A critical analysis of pre-facto and post-facto parameters of the rigorous orbital photogrammetric model is presented as section 5 and is followed by a conclusion as section 6.

2.0 Need for Rigorous Photogrammetric Models

It is well known that the very narrow field of view associated with push broom linear scanners on earth observation satellites

(EOS) results in nearly parallel imaging rays along the direction of flight. This in turn causes a high correlation between projection centre coordinates and sensor view angle. Photogrammetric models of push broom imaging systems are, therefore, rather different, compared to standard approaches usually applied for full frame imagery such as aerial photographs. The rigorous models are based on photogrammetry co-linearity condition and are iteratively modified to include any external and internal orientation. The output of these models is used to generate data products such as geo-coded and ortho-rectified (terrain relief corrected) products.

Well modeled push broom imaging systems from missions such as Spot2 and IRS -1C/IRS-1D have been used for across track stereo viewing applications. Subsequently, missions such as IRS P5 and Spot 5 have incorporated multi camera imaging systems for an along track stereo viewing capability. This stereo viewing capability with an appropriate photogrammetric model, facilitates realization of height information on a pixel by pixel basis, generation of anaglyph products, DEMs, ortho-rectified products and 3D visualization. A critical analysis on the performance of various models for push broom imaging systems, has, therefore, been a subject matter of serious research.

3.0 Sensor Models

Differences between discrete and hybrid time domain models are brought out in this section. It is noted that a hybrid time domain system is a superset encompassing orbital parameters in continuous time domain and attitude parameters in discrete time domain. These hybrid time domain systems are more flexible and are well suited even for "step and stare" imaging platforms used for acquiring very high resolution data.

3.1 Sensor Models in Discrete Time Domain

In rigorous sensor model, physical properties of push broom sensor acquisition and photogrammetric co-linearity equations are used to describe the perspective geometry of imaging sensor on a line by line basis. Spacecraft sensor position, velocity and attitude information is available at fixed intervals of time as ephemeris and is used as an input with approximate values for modeling sensor exterior orientation (position, velocity and attitude).

Using the notation of Mikhale Edward et al [18], co-linearity equations for use with push broom imagery are as under:

$$U = m_{11} * (X_{Sat} - X_A) + m_{12} * (Y_{Sat} - Y_A) + m_{13} * (Z_{Sat} - Z_A) \dots (1)$$

$$V = m_{21} * (X_{Sat} - X_A) + m_{22} * (Y_{Sat} - Y_A) + m_{23} * (Z_{Sat} - Z_A) \dots (2)$$

$$W = m_{31} * (X_{Sat} - X_A) + m_{32} * (Y_{Sat} - Y_A) + m_{33} * (Z_{Sat} - Z_A) \dots (3)$$

$$x - x_p = 0 = U / W \quad \text{and} \quad \dots (4)$$

$$y - y_p = -f * V / W. \quad \dots (5)$$

where:

- i x_p, y_p and f are respectively principal point co-ordinates and focal length of the imaging sensor,
- ii x and y are the line and pixel number of the imaged ground point,
- iii X_{Sat}, Y_{Sat} and Z_{Sat} are satellite position coordinates associated with the ground control point A and
- iv X_A, Y_A and Z_A are co-ordinates of ground control point A..
- v The condition $x - x_p$ equal to zero describes a frame-let based perspective geometry.

The matrix $M = [m_{ij}]$ consists of rotations associated with sensor, view angle and attitude parameters and is realized in the following order:

$$M = [M_{View}] * [M_{Attitude}] * [M_{Sensor}] \quad \dots (6)$$

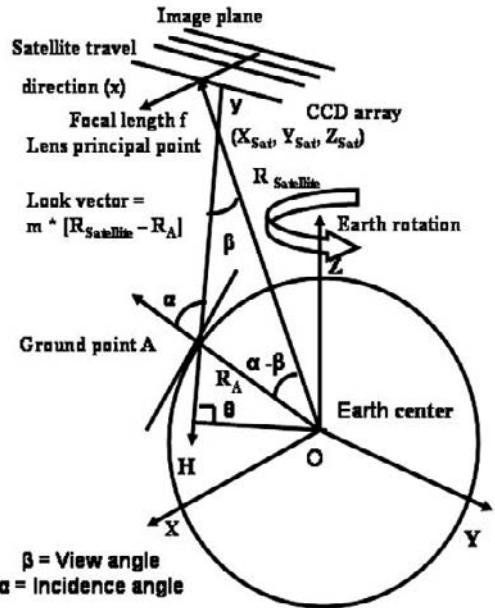


Fig 1: Linear Array Imaging Process

The components of attitude are modeled as drift rate changes associated with roll, pitch and yaw from the central line of the imagery. Similarly, the position, velocity and cross product of velocity and position form the components of sensor orientation and are calculated using ephemeris values of that imaging instance. In other words, the above parameters are modeled as 2nd order polynomials sampled at discrete time intervals. This model for satellite imagery has been influenced by the models traditionally used for aerial imaging systems.

3.2 Sensor Models in Hybrid Time Domain

In Kratky's [16] approach, satellite position is derived from known nominal orbit relations. Components of sensor orientation are right ascension of ascending node including earth rotation, inclination and traveled angle that is a sum of true anomaly and argument of perigee. In my model the composite rotation of these three matrices is as under:

$$\mathbf{M}_{\text{Sensor}} = \mathbf{M}_3 * \mathbf{M}_2 * \mathbf{M}_1 \quad \dots\dots(7)$$

Where:

- i \mathbf{M}_3 is a rotation matrix about Y axis for orbital traveled angle at the instance of imaging.
- ii \mathbf{M}_2 is a rotation matrix about X axis for inclination of orbit.
- iii \mathbf{M}_1 is a rotation matrix about Z axis for ascending node.

The attitude variations are modeled by either a simple linear equation or quadratic polynomial and on the lines undertaken for discreet time domain models.

Kratky's model has been extensively investigated, extended by Baltsavias et al [9] for SPOT, Baltsavias et al [10] for MOMS-02/D2 and Baltsavias et al [11] for IKONOS, Daniela Poli et al [4] for MOMS-02/Priroda and Dieter Fritsch et al [7] for Landsat TM and JERS-1 data. These recent studies indicate that this model is very accurate and yet is flexible enough to integrate the parameters of more complex new push broom instruments. Other hybrid time domain implementations include Gugan et al [14], O'Neill et al [20], Dowman et al [6], Westin, [24] and Toutin [25].

Dieter Fritsch et al [7] note that Kratky's rigorous photogrammetric bundle formulation includes imposing three additional constraints on geocentric distance "rs", traveled angle " τ " and the geographic longitude λ realized as elliptical orbit parameters. In other words, if one were to rephrase Dieter Fritsch and Dirk Stallman observations from a control engineer's perspective, the success of Kratky's model is based on adoption of continuous time domain / hybrid time domain systems for Keplerian orbital dynamics.

4.0 Bundled Adjustment with Unified Least Squares Solution

Sensor parameters of Spot 2 push broom panchromatic imagery and bundled adjustment details are listed in this section. There are 6000 CCD elements in the push broom linear array that facilitates acquisition of image data at a 10 meter spatial resolution per pixel. This sensor is steer able at +/- 27 degrees from nadir at steps of 0.6 degrees to facilitate across track viewing, has a line integration time of 1.5 milliseconds and admits of a swath width of 60kms. Orbits are determined regularly and the predicted ephemeris that is available along the video imagery.

The pre-facto and post-facto bundled adjustment values of 26 parameters comprising of full force model for Spot 2 scene acquired on 1st November 1988 with scene center at latitude 18.0092735 and long 73.5351357, are listed in table 1. Initial values of first eight parameters describing satellite orbit and imaging sensor are realized from satellite ephemeris files. The remaining eighteen parameters are realized as a part of the iterative bundled adjustment process with respect to translation (dx, dy and dz) and attitude (roll, pitch and yaw) in x, y and z dimensions. About seven ground control points were used as a part of bundled adjustment. It is noted that the translations are realized as refinements of keplerian parameters in continuous time domain while the attitude parameters are realized as 2nd order polynomials in discreet time domain whose sampling interval is a function of the detector integration time. All angular measurements are converted into radians and these parameters are listed as serials 1, 2, 3, 7, 18, 19, 20, 21, 22, 23, 24, 25 and 26 of table 1. The position and velocity parameters are converted to meters and are listed as serials 4, 9, 10, 11, 12, 13, 14, 15, 16 and 17 of table 1. The size of each CCD element is at 13 microns and the imaging sensor focal length of 1082mm is converted and listed as pixels in serial 8 of table 1.

Lee et al [13] have formulated the bundled adjustment equations corresponding to co-linearity equations by numerical differentiation. Our approach to formulate the bundled adjustment equations is, however, based on realizing the partial derivates as detailed by Slama et al in Manual of Photogrammetry [18] and in Mikhail et al [14]. These partial derivates are linearized according to first-order Taylor decomposition with respect to unknown parameters as functions of time. The resulting system of bundled adjustment equations is solved iteratively with a unified least square adjustment. There is no known major difference either in performance or on the accuracy of the estimated values from either of these two approaches. As already noted in section 2, there is a high correlation between projection centre coordinates and sensor view angle. The bundled adjustment solution, therefore, has to address other issues such as inversion of singular matrices for realizing the refinements to adjustment parameters. The mathematical details are not detailed here as the objective of the present study is to understand the dynamics of imaging platform through an analysis of pre-facto and post-facto bundled adjustment parametric values.

5.0 Analysis Of Spacecraft Parameters

Post-facto bundled adjustment analysis reveals that there is hardly any difference in the pre-facto and post-facto values of first eight parameters as listed in table 1. Likewise, the contributions of all translation parameters with an exception of dz0 are within a sub-pixel level. The contribution of dz0 corresponds to satellite to ground surface look-vector distance. The post facto values of attitude parameters describe orientation of imaging sensor and are, as expected, significantly different from pre-facto values

Table 1

#	Parameter Description	Pre-facto Values ^a	Post-facto Values * 1.0e+005
1	Right Ascension of Ascending Node	0.0000430934813	0.00004309348133
2	Inclination of orbit	0.0000021386431	0.00000213864318
3	Argument of Perigee	0.0000280836226	0.00002808362265
4	Semi major axis of orbit	0.0739927669678	0.07399276696788
5	Eccentricity of orbit	0.00000026549 857	0.00000026549858
6	Time At Frame Center	0.21428115234 400	0.21428115234400
7	Across Track View Angle	0.00000354301 838	0.00000354301838
8	Focal length in pixels	0.83230769230 769	0.83230769230769
9	dx0	0	0.00000596263014
10	dx1	0	0.00000000001572
11	dx2	0	0.00000000101476
12	dy0	0	0.00003954055208
13	dy1	0	0.00000000016379
14	dy2	0	0.00000000321556
15	dz0	0	8.24991705845123
16	dz1	0	-0.00000000019978
17	dz2	0	-0.00000004068430
18	do0	0	0.00003732575930
19	do1	0	0
20	do2	0	0
21	dp0	0	-0.00001177291907
22	dp1	0	0
23	dp2	0	0
24	dk0	0	0.00002426113540
25	dk1	0	0
26	dk2	0	0

Point ID	Residual parameters of 7 GCPs in pixels	
	Residual in X	Residual in Y
1	0.0006984	-0.00000024985699
2	-0.031852	-0.00000674963979
3	-0.055803	0.00014686304797
4	-0.089006	-0.00002321667466
5	0.1661612	-0.00012481995714
6	0.000555	0.00000052777432
7	0.009247	0.00000893070342
RMS Error Along Lines	0.0753	Not applicable
RMS Error Along Pixels	Not applicable	7.3497e-05

It is a common practice to list root mean square residual error (RMS error) in pixels as an indicator to convergence of bundled adjustment equations. Most of the models terminate their iteration process if RMS threshold fixed at a pixel level or at an acceptable integral multiple thereof is attained. CS Fraser et al [1], note that a 3D point positioning accuracy corresponding to 0.3 of the pixel footprint is possible but under practical test conditions accuracies of between 0.5and 2 pixels are more commonly encountered.

6.0 Conclusions

The output of post-pass Spot instrumentation is known for its excellent quality and its imaging process is a far simpler compared to other missions. Dynamics of this push broom scanner imagery has been specifically studied as a digital photogrammetric solution in hybrid time domain. The output listed as table 1 is that of a data set picked up at random.

For my model, RMS error has been separately computed as RMS error along lines and along pixels. It is noted that the RMS error along pixels is very small and can safely be equated as zero. The RMS error along lines is at second decimal of a pixel, which indicates that the model has attained a very high degree of convergence. In particular, it is interesting to note that even pixel no 5 that has got maximum root mean square residual error along lines, is also at a sub-pixel level.

The complete photogrammetric solution requires the full force 26 parameters listed in table 1. A careful analysis is indicative that the main contribution to the dynamics of imaging system is based on satellite movement along its orbital path and is described by true anomaly and right ascension of ascending node. The angular changes of these two parameters are included in co-linearity equations as linear changes with time. Further, as expected, attitude parameters also contribute significantly to orientation imaging sensor as with aerial photographs and aerial scanning systems. The look vector slant range to the pixel on earth surface is function of the altitude of spacecraft above ground and is an important parameter contributing to faster convergence of the photogrammetric model. Similar results are available for many other missions that acquire data at very high resolutions.

References

- [1] C.S. Fraser, E. Baltsavias, A. Gruen, "Processing of Ikonos imagery for submetre 3D positioning and building extraction," *ISPRS Journal of Photogrammetry & Remote Sensing*, vol. 56, pp. 177– 194, 2002.
- [2] Daniela Poli, "Orientation of satellite and airborne imagery from multi-line push broom sensors with a rigorous sensor model," *internet accessed "pdf" document*.

- [3] Daniela Poli, "Indirect geo-referencing of airborne multi-line array sensors: a simulated case study," *Proceedings of ISPRS Commission III Symposium Photogrammetric Computer Vision '02*, Graz, Austria, vol.34, part B3/A, pp. 246-251, 9-13, September 2002.
- [4] Daniela Poli, G. Seiz G, and E. P.Baltsavias, "Cloud-top height estimation from satellite stereo pairs for weather forecasting and climate change analysis," *IAPRS*, vol. 33, part B7/3, Amsterdam, pp.1162-1169, 2000
- [5] Daniela Poli, L. Zhang, A. Gruen, "SPOT-5/HRS stereo images orientation and automated DSM generation," *IAPRS*, vol. 34, Part B1, 2004.
- [6] I. J.Dowman, P.Michalis, "Generic rigorous model for along track stereo satellite sensors," *ISPRS Workshop High Resolution Mapping from Space*, Hannover, 4-6 October (on CDROM.), 2003.
- [7] Dieter Fritsch, Dirk Stallmann, "Rigorous photogrammetric processing of high resolution satellite imagery," *IAPRS*, vol.33, Part B1, Amsterdam, pp.313-321, 2000.
- [8] Pedro Ramon Escobal "Methods of orbit determination," John Wiley and Sons, Inc, New York, 1965.
- [9] Emmanuel P. Baltsavias, Dirk Stallmann, "Metric information extraction from Spot images and the role of polynomial mapping functions," *IAPRS*, vol. 29, part B4, pp. 358 – 364" 1992.
- [10] Baltsavias, E. P., Stallmann, D., Geometric potential of MOMS-02/D2 data for point positioning, DTM and orthoimage. *IAPRS*, Vol. 31, Part B4, Vienna, pp. 110-116, 1996
- [11] Emmanuel Baltsavias, Maria Pateraki, Li Zhang, "Radiometric and geometric evaluation of ikonos geo images and their use for 3d building modeling," *Joint ISPRS Workshop "High Resolution Mapping from Space,"* Hannover, Germany, 19-21 September 2001.
- [12] Ganti Prasad Rao, Hugues Garanier "Identification of continuous time domain systems; direct or indirect," on the occasion of Michael Faraday Birthday Celebrations, 22nd September 2006, (CDROM), IEEE Hyderabad, India, <http://ewh.ieee.org/r10/hyderabad>.
- [13] Ganti Prasad Rao, "Identification of continuous-time systems: a tutorial," on the occasion of Michael Faraday Birthday Celebrations, 22nd September 2006, (CDROM), IEEE Hyderabad, India.
- [14] D.J. Gugan, I.J. Dowman, "Accuracy and completeness of topographic mapping from SPOT imagery," *Photogrammetric record*, Vol. 12(72) pp. 787-796, 1988.
- [15] G. Konecny, P. Lohmann, H. Engel, E. Kruck, "Evaluation of SPOT imagery on analytical photogrammetric instrument," *PE&RS*, Vol. 53, No. 9, pp.1223- 1230, 1987.
- [16] V. Kratky "Rigorous stereo photogrammetric treatment of Spot images," *CNES, SPOT IMAGE*, International Conference on Spot Image Utilization, Assessment, Results, Paris, 23 – 27, November 1987.
- [17] C. Lee, H. J. Theiss, J. S. Bethel, and E.M. Mikhail, "Rigorous mathematical modeling of airborne push broom imaging system," *Photogrammetric Engineering & Remote Sensing*, vol. 66, no.4, pp. 385-392, 2000.
- [18] E.M. Mikhail, James S. Bethel, & Chris McGlone, J, "Introduction to modern photogrammetry," John Wiley & Sons, 2001.
- [19] E.M. Mikhail, "Is photogrammetry still relevant?" *ISPRS Commission III Symposium*, Columbus, OH, 1998.
- [20] M. O'Neil and I.J. Dowman, "A new camera model for the orientation of the SPOT data and its application to the OEEPE test of triangulation of SPOT data," *OEEPE Publication*, 26: 153-163, 1991.
- [21] J. Raggam, M.F. Buchroithner, and R. Mansberger, "Relief mapping using nonphotographic spaceborne imagery," *ISPRS Journal of Photogrammetry and Remote Sensing*, 44, pp. 21-36, 1989.
- [22] Radhakrishna Rao, Calyampudi, "Linear statistical inference and its applications," 2nd Edition, John Wiley and Sons, 1982.
- [23] C. Slama, C. Theurer, and S. Henriksen, (eds), "Manual of photogrammetry," 4th edition, American Society for Photogrammetry and Remote Sensing, 1980.
- [24] Theodore Westin, "Precision rectification of SPOT imagery", *Photogrammetric Engineering & Remote Sensing*, Vol. 56, No. 2, pp. 247-253, 1990.
- [25] Thierry Toutin, "Comparison of stereo-extracted DTM from different high-resolution sensors: Spot-5, EROS, IKONOS and Quickbird," *IEEE-TGARS*, 42(9), 2004, http://dweb.ccrs.nrcan.gc.ca/ccrs/db/biblio/paper_e.cfm?BiblioID=13383 (accessed on 9th May 2004).
- [26] Thierry Toutin, "Review article: Geometric processing of remote sensing images: models, algorithms and methods," *International Journal of Remote Sensing*, vol. 25, no. 10, pp. 1893–1924, 20 May, 2004.

On the Robustness of Integral Time Delay Systems with PD Controllers

Eduardo Zuñiga ¹, Omar Santos ² and M.A. Paz Ramos ¹

¹ Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Ciudad de México,
Calle del Puente 222, Col. Ejidos de Huipulco, Tlalpan, 14380, México D.F.

² CITIS, Universidad Autónoma del Estado de Hidalgo,
Carretera a Tulancingo, Km 2.5, Pachuca, Hgo., México.

a00970554@itesm.mx, omarj@uaeh.reduaeh.mx, marco.paz@itesm.mx

Abstract-We studied the robust stability of first-order integral systems in closed loop with a PD controller when general tables for tuning the controller are used. The frequency approach is used to obtain necessary and sufficient conditions for the robust stability of the characteristic equation in closed loop. The Linear Matrix Inequalities (LMI) approach is employed to obtain sufficient stability conditions when model non-linearities are considered.

I. INTRODUCTION

The robust stability analysis for time delayed systems has been widely studied in the last decades [8]. The time delay effect on the performance on the closed loop characteristic of the system when a control law is introduced may induce complex behaviors (instability, oscillations, undesired performance), therefore the study of the stability regions is a problem of great interest. Note that complete characterization of the corresponding stability regions is a very complex problem and still open in the general case [2]. Furthermore, a chaotic behavior may occur if the system is perturbed with a non-linear function that depends on the delayed state [5]. The Proportional Integral Derivative (PID) controller is one of the most popular strategies for control in industrial plants. The relatively easy implementation, robustness and the availability of an enormous set of rules and tables [15], [11], [13], [12] for tuning this type of controller makes the PID control the most adopted in a variety of applications. The robust stability of time delayed systems in closed loop with PID controllers has been studied in [6], [8] and [10]; however the papers that propose tables and rules for the PID tuning, for specific systems, do not present any robust stability analysis.

In this contribution, we present a robust stability analysis via the frequency approach for integral time delayed systems in closed loop with a PD controller. In addition, robust stability conditions are obtained when non-linear disturbances are considered in the model. The parameters of the controller for integral time delayed systems were obtained from two tables presented in [12] and [9]. The analysis can be extended to include other types of systems, for example, unstable first-order processes. Our contribution is organized as follows: in the first section we introduced our contribution, in section 2 we established the problem analyzed; the frequency domain analysis with illustrative examples is included in section 3,

section 4 deals with time domain analysis with an illustrative example, section 5 provide an analysis of the roots' behavior, and section 6 is dedicated to final comments.

II. PROBLEM FORMULATION

Consider the following integral time delayed system

$$\frac{Y(s)}{U(s)} = \frac{Ke^{-sh}}{s}, \quad (1)$$

when the input signal $U(s)$ is a PD controller, two constants must be determined: K_p and T_d . These constants can be obtained from the tables or rules when an optimization problem is solved considering a performance index. For example in [12] the ISE (Integral Square Error) and ITSE (Integral time square error) criteria are considered. The rules given in [12] are improved in [9], but neither [9] nor [12] present a robust stability analysis. So if there are variations in the system (1) parameters, it is interesting to estimate these variations on the parameters, which is shown in section 3. When the system presents non-linear perturbations or non-modeled dynamics, using the results given in [4], a time domain analysis is presented in section 4.

III. FREQUENCY DOMAIN ANALYSIS

In this section we analyze the robust stability of the system (1) in closed loop with a PD controller. Parameters space hypersurfaces are obtained using the Δ - partitions method [7]. We are considering the following system

$$\frac{Y(s)}{U(s)} = \frac{Ke^{-sh}}{s}, \quad (2)$$

where $Y(s)$ and $U(s)$ are the Laplace transformed of output $y(t)$ and input $u(t)$ respectively. Consider that input $U(s)$ is a PD controller, so we have that

$$U(s) = KpE(s) + K_d s E(s),$$

where $E(s)$ is the error signal given by $E(s) = R(s) - Y(s)$. So, we have that the characteristic equation (considering the transfer function of output $Y(s)$ and reference $R(s)$) is given by

$$s(1 + KK_d e^{-sh}) + KK_p e^{-sh} = 0. \quad (3)$$

Observe that the cuasipolinomiyal (3) is a neutral cuasipolinomiyal [1], [3]. As it is well know, [3], [8], a necessary condition for the stability of a neutral cuasipolinomiyal is that the atomic part has to be stable [3]; for equation (3) this necessary condition implies that

$$|KK_d| < 1. \quad (4)$$

Now, if we consider that the system (2) has K and h uncertain parameters, we want to obtain robust stability conditions for the parameters K and h if K_p and K_d are given.

Observe that when $h = 0$, according to the equations (3) and (4) the condition to conclude stability for the polynomial is that $KK_p > 0$, so, if we employ the roots' continuity principle with respect to the parameters [1], this implies that there exists an $h^* > 0$ such that the system (3) remains stable. We can use the **D**-partitions method to obtain the stability regions for the equation (3).

Now, according to the **D**-partitions method, the first boundary of the hyper-surfaces is when $s = 0$ in (3), if we assume that $K_d \neq 0$, it follows that

$$K = 0.$$

Another boundary is given when $s = j\omega$:

$$j\omega(1 + KK_d e^{-j\omega h}) + KK_p e^{-j\omega h} = 0,$$

it follows that

$$\begin{aligned} \omega - KK_p \sin(\omega h) + KK_d \omega \cos(\omega h) &= 0 \\ KK_p \cos(\omega h) + KK_d \omega \sin(\omega h) &= 0, \end{aligned} \quad (5)$$

direct calculations tell us that

$$\omega = \frac{KK_p}{\sqrt{1 - K^2 K_d^2}}. \quad (6)$$

The set of equations (set1) implies that

$$h = \frac{\cos^{-1}(-KK_d)}{\omega}, \quad (7)$$

combining the equations (w) and (h) we find that

$$h^* = \frac{\cos^{-1}(-KK_d)\sqrt{1 - K^2 K_d^2}}{KK_p}.$$

Now we are able to establish the following proposition.

Lemma 1. Assuming that $|KK_d| < 1$, the characteristic equation (3) is stable if and only if $KK_p > 0$ and $h \in [0, h^*]$, where

$$h^* = \frac{\cos^{-1}(-KK_d)\sqrt{1 - K^2 K_d^2}}{KK_p}.$$

We illustrate the use of Lemma 1 by analyzing the robust stability of the rules given in [12] and [9].

The rules for integral processes given in [12] when a ISE criteria is minimized are

PID parameter	ISE
K_p	$1.03/Kh$
T_i	-
T_d	$0.49h$

(8)

Using the conditions given in Lemma 1 we obtain that the regions for parameters K and h of the model (2) are defined as follows

$$K \in \left(0, \frac{|K_n|}{0.5047}\right), \quad (9)$$

and

$$h \in [0, h^*] \quad (10)$$

where

$$h^* = \frac{\cos^{-1}\left(-\frac{0.5047K}{K_n}\right)\sqrt{K_n^2 - K^2(0.2547)}}{1.03K} h_n,$$

K_n and h_n are the nominal values for the parameters in model (2). These nominal values are used for tuning the PD controller. Observe that the boundaries of the robust stability regions are defined by these nominal values. The analysis can be expanded to include the ITSE and ISTE criteria given in [12].

Now we analyze the robust stability of the model (2) parameters K and h when the following tables given in [9] are used

PID parameter	ISE
K_p	$0.0747/M$
T_i	-
T_d	$0.015h$

(11)

here, M is the slope for the open loop response and h is the delay. Using Lemma 1, we find the following conditions

$$K \in \left(0, \frac{|M|}{0.0011h_n} \right) \quad (12)$$

and

$$h \in [0, h^*] \quad (13)$$

Where

$$h^* = \frac{\cos^{-1}\left(-\frac{0.0011K}{M}h_n\right)\sqrt{M^2 - K^2(1.2 \times 10^{-6})}}{0.00747K}.$$

In the next section, we illustrate the robust stability conditions obtained for some plants.

ILLUSTRATIVE EXAMPLES

In this subsection, we illustrate the use of Lemma 1 for two given plants; the controllers were tuned with tables (8) and (11).

Example 1. Consider the following plant referred to [9]

$$G(s) = \frac{0.654}{s} e^{-10s}, \quad (14)$$

considering the nominal parameters $K_n = 0.654$ and $h_n = 10$, we can use the conditions (9), (10) (12) and (13) in order to obtain the following hyper-surfaces:

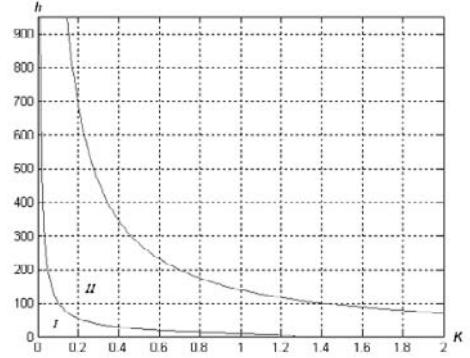


Fig. 1. Stability zones for plant (14).

Zone I is the systems (2) stability zone with a PD controller tuned using table (8). Zone II (which also includes zone I) is the stability region when table (11) is used. If we look closer, we can see that the pair $(0.654, 10)$ is on both stability zones:

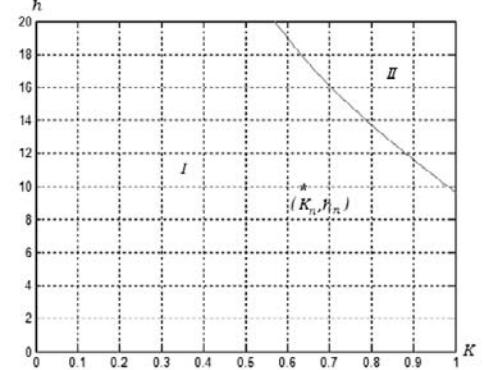


Fig. 2. Nominal values for plant (14).

Based on this example, we can conclude that the controller tuned as per table (11) is more robust than the controller tuned as per table (8).

Example 2. Now consider the following plant

$$G(s) = \frac{0.0506}{s} e^{-6s}. \quad (15)$$

The stability regions for closed loop systems are shown in the following figure

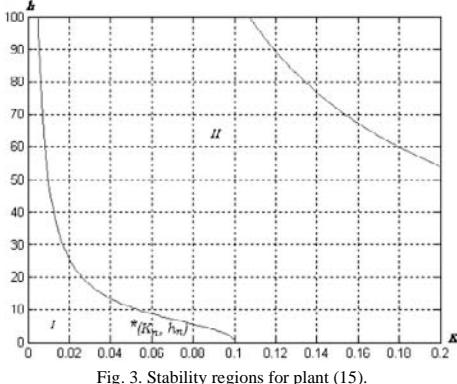


Fig. 3. Stability regions for plant (15).

Zones I and II correspond to tables (8) and (11) respectively. Again, region II includes region I; this implies that for this example the PD controller tuned as per table (11) is more robust than the controller tuned as per table (8).

In next section, we considered non-linear perturbances for the model. Using the results given in [4] we obtained sufficient conditions for robust stability.

IV. TIME DOMAIN ANALYSIS

In this section, we assumed that the model used had the following form

$$\begin{aligned} \dot{y}(t) = & Ku(t-h) + f(y(t), t) \\ & + g(y(t-h), t) + h(\dot{y}(t-h), t), \end{aligned} \quad (16)$$

where input $u(t)$ is a PD controller

$$u(t) = K_p e(t) + K_d \dot{e}(t),$$

$e(t)$ is the error signal, $e(t) = r - y(t)$. To simplify the expressions we assume that $r = 0$, which means that we want to carry output $y(t)$ to the origin. We assumed that constants K_p and K_d are calculated with the tables (8) and (11) for the nominal system:

$$\dot{y}_n(t) = -KK_p y_n(t-h) - KK_d \dot{y}_n(t-h). \quad (17)$$

Now, considering that the equation (17) is non-linearly perturbed, the equation (16) is

$$\begin{aligned} \dot{y}(t) = & -KK_p y(t-h) - KK_d \dot{y}(t-h) \\ & + f(y(t), t) + g(y(t-h), t) \\ & + h(\dot{y}(t-h), t), \end{aligned} \quad (18)$$

with initial function conditions

$$\begin{aligned} y(t+\theta) = & \varphi(\theta), \quad \dot{y}(t+\theta) = \dot{\varphi}(\theta), \\ \text{for all } \theta \in [-h, 0]. \end{aligned} \quad (19)$$

We denote with y_t the state of the system (18), defined as

$$y_t = y(t+\eta), \quad \eta \in [-h, 0], \quad \text{for all } t \geq 0$$

the uncertain system (non-linear) has non-linear time-varying perturbances $f(y(t), t)$, $g(y(t-h), t)$ and $h(\dot{y}(t-h), t)$ which satisfies

$$\|f(y(t), t)\| \leq \alpha \|y(t)\| \quad (20)$$

$$\|g(y(t-h), t)\| \leq \beta \|y(t-h)\| \quad (21)$$

$$\|h(\dot{y}(t-h), t)\| \leq \gamma \|\dot{y}(t-h)\| \quad (22)$$

where $\alpha \geq 0$, $\beta \geq 0$ and $\gamma \geq 0$ are given constants. For mechanical systems, we can interpret the non-linearities boundaries as the position $y(t)$ and velocity $\dot{y}(t)$. Observe that the system (18) is a neutral non-linear system. Observe that the inequalities (20), (21) and (22) can be rewritten as

$$f^2(y(t), t) \leq \alpha^2 y^2(t) \quad (23)$$

$$g^2(y(t-h), t) \leq \beta^2 y^2(t-h) \quad (24)$$

$$h^2(\dot{y}(t-h), t) \leq \gamma^2 \dot{y}^2(t-h) \quad (25)$$

We assumed that the nominal system (17) is stable, so we want to know the constants α , β and γ so that the perturbed system (non-linear) remains stable.

This type of system is considered in [4]. In fact, using the LMI approach, a Lyapunov-Krasovskii functional and the S-procedure [14] for the inequalities (23), (24) and (25), in [4], sufficient robust stability conditions are found.

Sufficient robust stability system (18) conditions are given for the next proposition. The proposition establishes delay dependent robust stability conditions.

Proposition 1. [4] *The system (18), with initial function condition (19) and disturbances, satisfying (23), (24) and (25), is asymptotically stable if $|KK_d| + \gamma < 1$, and there exists a*

real number X , and positive numbers P , R , S and Y so that the following LMI is satisfied

$$\begin{bmatrix} (1,1) & -XKK_p & PKK_d & P & P \\ * & (2,2) & 0 & 0 & 0 \\ * & 0 & (3,3) & 0 & 0 \\ * & 0 & 0 & -\varepsilon_1 I & 0 \\ * & 0 & 0 & 0 & -\varepsilon_2 I \\ * & 0 & 0 & 0 & 0 \\ 0 & * & * & * & * \\ 0 & * & * & * & * \\ * & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} P & 0 & 0 & (1,9) \\ 0 & -SKK_p & YK^2 K_p^2 & 0 \\ 0 & -SKK_d & YK^2 K_p K_d & 0 \\ 0 & S & -YKK_p & 0 \\ 0 & S & -YKK_p & 0 \\ -\varepsilon_3 I & S & -YKK_p & 0 \\ * & -S & 0 & 0 \\ * & 0 & -Y & 0 \\ 0 & 0 & 0 & -Y \end{bmatrix} < 0$$

Where

$$\begin{aligned} (1,1) &= -2KK_pP + R - 2KK_dQMP + \varepsilon_1\alpha^2 \\ (2,2) &= -R + \varepsilon_2\beta^2 \\ (3,3) &= -S + \varepsilon_3\gamma^2 \\ (1,9) &= h(X + P) \end{aligned}$$

Observe that the condition $|KK_d| + \gamma < 1$ is necessary for the neutral systems stability [8].

In the next subsection, we illustrated the use of Proposition (1) to obtain robust stability conditions for an example.

ILLUSTRATIVE EXAMPLE

In this section, we obtain explicitly the robust stability conditions using Proposition (1). The LMI Toolbox of Matlab is used to solve the LMI given in Proposition 1.

Example Consider the plant (14) in the time domain as the nominal plant

$$\dot{y}(t) = 0.654u(t-10). \quad (26)$$

The controller tuned with the Table (8) is

$$u(t) = -0.1574y(t) - 0.7717\dot{y}(t).$$

The closed loop is given by

$$\dot{y}(t) = -0.103y(t-10) - 0.5047\dot{y}(t-10). \quad (27)$$

Lemma 1 shows us that the system (27) is stable. Now we consider the non-linearities with boundaries given by (23), (24) and (25):

$$\begin{aligned} \dot{y}(t) &= -0.103y(t-10) - 0.5047\dot{y}(t-10) \\ &\quad + f(y(t), t) + g(y(t-h), t) \\ &\quad + h(\dot{y}(t-h), t). \end{aligned} \quad (28)$$

First, we consider that $\alpha = 0$, $\beta = 0.08$, $\gamma = 0.1$ and using the LMI Toolbox we found that the LMI given in Proposition 1 was feasible, therefore the system (28) is asymptotically stable. Now consider the following constants: $\alpha = 0.03$, $\beta = 0.05$, $\gamma = 0.1$, for these values, we found that the LMI is feasible, therefore the system (28) is asymptotically stable.

Consider the system (26), this time we tuned the PD controller with the Table (11), so we obtained the following controller

$$u(t) = -0.7515y(t) - 0.1127\dot{y}(t). \quad (29)$$

We know that the system (26) in closed loop along with the control law (29) is stable. If we consider the perturbed system we obtain

$$\begin{aligned} \dot{y}(t) &= -0.7515y(t-10) - 0.1127\dot{y}(t-10) \\ &\quad + f(y(t), t) + g(y(t-h), t) \\ &\quad + h(\dot{y}(t-h), t), \end{aligned} \quad (30)$$

when $\alpha = 0$, $\beta = 0.5$, $\gamma = 0.6$ we saw that the LMI given in Proposition (1) was feasible, therefore the perturbed system (30) is asymptotically stable. If we consider that $\alpha = 0.3$, $\beta = 0.2$, $\gamma = 0.6$ we found that the LMI is feasible, then the system (30) is asymptotically stable.

Clearly the PD controller tuned with the Table (11) is more robust under non-linear perturbances than the PD controller tuned with the Table (8).

V. ROOTS BEHAVIOR IN CLOSED LOOP ANALYSIS

Now, for the previously proposed plants we analyze the behavior of the roots, tuned according to the two tables shown. This analysis was based on data obtained using the software MAPLE specifically the “fsolve” function. With this tool we

swept the left semi-plane for roots, with this data we generated a graph that gave us the behavior of the roots for a given system.

It is well known that roots of the neutral quasipolinomyal behave chaotically in a certain radius close to the origin [1], and then they behave exponentially, until the real coordinate presents very small changes and stay trapped in a continuous chain. At this point we can assume that real coordinate distance to the intersection with cero will not change.

It is also well know that roots behave continuously with their respective parameters [1], so we can find out how robust our system will be depending upon the horizontal distance from the real part of the root to cero. So when plant disturbances appear, roots will have a bigger zone to move in before the system goes unstable.

Figure 4 shows the graph obtained for plant (14) and the behavior of its roots when the controller is tuned with the two given tables.

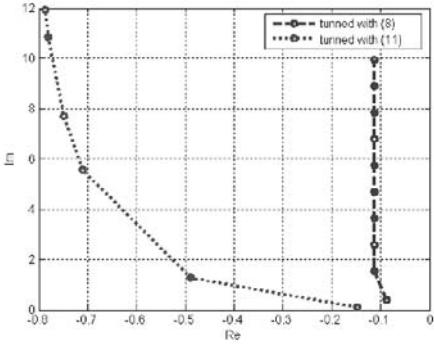


Fig. 4. Roots Behavior for the plant (14).

In this graph we can observe that the roots of the system tuned with table (8) are closer to the origin, which makes this system less robust than the other tuned with table (11). This shows a more robust root behavior because the zone where the roots' real part stays practically constant is considerably less likely to make the system unstable.

VI. CONCLUSIONS

An analysis of robust stability for the integral time delayed systems is presented. For the examples that we considered, the PD controller obtained from the table given in [9] presents a greater stability region than that generated with the PD controller tuned with the rules given in [12]. The approach can be extended in order to analyze the robust stability regions in other type of systems using other tables.

REFERENCES

- [1] Bellman, R. and Cooke, K. *Differential Difference Equations*, Academic Press, New York, 1963.
- [2] Diekman, O. et al. Delay equations, Functional, complex and non-linear Analysis, Appl. Math. Sciences series, 110, Springer Verlag New York, 1995.
- [3] Hale, J.K. and Verdun L. S. M. *Introduction to Functional Differential Equations*, Springer Verlag, New York, 1993.
- [4] Han, Q.L. and Yu, L. Robust stability of linear neutral systems with nonlinear parameter perturbations. IEE Proc. Control Theory Appl. vol. 151, 5, pp. 539-546, 2004.
- [5] Han der Heiden, U. et al. Existence of chaos in control systems with delayed feedback, J. Diff. Eqs. vol. 47, pp. 273-295, 1983.
- [6] Kolmanovskii, V. and Nosov, V. Stability of functional differential equations, Academic Press, London, 1986.
- [7] Neimark, J. D-subdivisions and spaces of quasipolynomials. Prik. Math. Mech. vol. 13 pp. 349-380, 1949.
- [8] Niculescu, S.I. Delay Effects on stability A robust control approach. Lectures Notes in Control and Information Sciences, 269, Springer Verlag, Germany, 2001.
- [9] Paz-Ramos, M.A. et al. Genetic rules to tune Proportional + Derivative controllers for integrative processes with time delays. In proceedings to the IEEE 15th CONIELECOMP'05, México, 2005.
- [10] Marshall, J. E. Control of time delay systems, The institution of electrical Engineers, London, 1979.
- [11] Poullin, E. and Pomerleau, A. PID tuning for integrating and unstable processes. IEEE Proc. Control Theory Appl. vol. 143, 5, pp. 429-435, 1996.
- [12] Visoli, A. Optimal tuning of PID controllers for integral and unstable processes. IEE Proc. Control Theory Appl. vol. 148, 2, pp. 180-184, 2001.
- [13] Wang, L. and Cluett, W.R. Tuning controllers for integrating processes, IEE Proc. Control Theory Appl. vol. 144, 5, pp. 385-392, 1997.
- [14] Yakubovich, V. A. S-procedure in nonlinear control theory. Vestn. Leningr. Univ. I. Mat. Mekh. 13, pp. 62-77, 1971.
- [15] Zhuang, M. and Atherton, D.P. Automatic tuning of optimum PID controllers, IEE Proc. Control Theory Appl. 140, 3, pp. 216-224, 199

Improvement of the Segmentation in HS Sub-space by means of a Linear Transformation in RGB Space

E. Blanco, M. Mazo, L.M. Bergasa, S. Palazuelos and A.B. Awawdeh

University of Alcalá/ Department of Electronics, Alcalá de Henares, Spain

edward@depeca.uah.es, mazo@depeca.uah.es, bergasa@depeca.uah.es, sira@depeca.uah.es, abdel@depeca.uah.es

Abstract – This paper presents an alternative that allows to improve the color image segmentation in the *HS* sub-space (*HSI* space). The authors propose to apply a zero order transformation in the *RGB* space which consists in adding a vector in the *RGB* space to control the separation between classes in the *HS* sub-space. This vector is considered optimum. To define it, the chromatic C_1C_2 sub-space (YC_bC_r space) is used. The proposal presented in this work has been designed to be applied in real-time on each consecutive frame of a sequence of color images. The effectiveness of this work has been tested and verified using applications where a reduced contrast between the background color and the color of the object to segment exists, and when the size of the object to segment is very small in comparison with the size of the captured scene. Furthermore, the process of segmentation is improved and, at the same time, the effects of the variations of the light intensity of the scene are considerably reduced.

I. INTRODUCTION

From the recent works on color segmentation we would like to emphasize those related to the segmentation of the skin natural color. In this field, S.L. Phung et al. [1] segmented the skin using a Bayesian classifier, obtaining satisfactory results even under adverse illumination conditions for different color spaces such as: *HSV*, *RGB*, YC_bC_r and *CIE-Lab*. R.-L. Hsu et al. [2] suggest the detection of face skin, considering a nonlinear subspace of YC_bC_r space that allows to compensate part of the luminosity variations. The trend to compensate part of these luminosity changes is the use of dynamic color models as done by L. Sigal et al. [3]. L. Sigal presents an overview of the works and researches done in the color skin segmentation field.

The most frequently used color spaces in this type of applications are *HSV* [3], [4] and normalized *rg* [5]-[7]. The perceptive color spaces as *HSV* and *HLS* are widely used in image processing, as well as *HSI*, where, in some works, only the Hue (*H*) and Intensity (*I*) components are used in the clustering process [8]. In other cases, as in [9], a threshold value for the Saturation (*S*) of each pixel based on its intensity is defined. This threshold is used before the clustering process to determine if *S* should be replaced by *H* or *I*.

In the sign language recognition field, N. Habil et al. [10] performed a pixel-by-pixel classification of the skin color with discriminant features of the C_bC_r plane, using the *Mahalanobis distance*, but he needs a fusion of motion cues to obtain good results. A similar segmentation is achieved in the work done by D. Chai et al. [11], where post-segmentation process steps have been applied, such as morphological

operations, in order to surpass the limitations of the segmentation. In [11], the YC_bC_r space has been used too. This color space is one of the most widely used in the segmentation process.

In the sign language recognition field, it is very important to detect the geometric form of the object to segment (face and hands edges). This is the reason why it is necessary to use strategies to enhance the contrast between the object and the background of the scene. This work aims to enhance the contrast by means of a class separation pre-process in the *HSI* space [12], by properly coloring the image with a color vector in the *RGB* space, taking into account the YC_1C_2 space [8], [13], [14].

This paper has been organized as follows: section II describes a general vision of the proposed algorithm to increment the separation between classes. Section III presents the criteria considered when separating the classes. Section IV details how to improve the separation between classes in *HS* plane starting from their location in the C_1C_2 plane. Section V presents the algorithm that performs the optimal class separation. Section VI describes how to obtain the color vector to add, and the effects it produces in the images. Section VII contains the experimental results, and section VIII the conclusions and future works.

II. ALGORITHM OVERVIEW

As mentioned before, the objective of this work is to improve the segmentation process by adding an optimal color vector to each one of the captured images in the *RGB* space. This vector is different from one image to another, looking for the maximum separation between classes in the *HS* plane (sub-space where the segmentation must be performed).

As it is known, an important property of the *HSI* space (perceptive space) is that it produces a maximum disconnection between the chrominance and luminance components. As a result, the luminance can be almost fully isolated, making the segmentation process more invariant to the changes in shades and illumination, as in [4]. For this reason, in our proposal, the analysis in the *HSI* space only considers the *H* and *S* chromatic components (*HS* plane).

If the original image is denoted by I , the optimal color vector to add by \mathbf{i}_r , and the colored image, resulting of the addition, by I_r , is fulfilled:

$$I_r = I + \mathbf{i}_r \quad (1)$$

The determination of the optimal color vector \mathbf{i}_r , for each captured *RGB* image, is done following the steps shown in

Fig. 1. These steps are:

1) From the captured *RGB* image (I), several significant samples (seeds) are obtained from both the object (class O) and the background (class B). We will refer to the object class in the *RGB* space as $O_{RGB} = \{\mathbf{r}_{O_k}\}$ $k=1,2,\dots,N$, while $B_{RGB} = \{\mathbf{r}_{B_q}\}$ $q=1,2,\dots,M$, will refer to the background class, where N and M are the number of pixel seeds taken for classes O and B, respectively.

2) For every O_{RGB} and B_{RGB} samples (in the *RGB* space), a transformation to the YC_1C_2 space is done. After this transformation, the resulting classes will be referred to as $O_{C1C2} = \{\mathbf{c}_{O_{k'}}\}$ and $B_{C1C2} = \{\mathbf{c}_{B_q}\}$.

3) Making use of the properties and relationship between the *HSI* and YC_1C_2 color spaces, the optimal location of the classes in the C_1C_2 space is obtained, by finding the optimal location of their respective mean vectors, $\mathbf{c}_{IO_{opt}}$ and $\mathbf{c}_{IB_{opt}}$.

4) From the $\mathbf{c}_{IO_{opt}}$ and $\mathbf{c}_{IB_{opt}}$ mean vectors, its corresponding ones in the *RGB* space, \mathbf{r}_{IO} and \mathbf{r}_{IB} , can be calculated. With these *RGB* vectors and the mean vectors of the original classes (O_{RGB} , B_{RGB}) represented by \mathbf{r}_O and \mathbf{r}_B , the optimal color vector can be calculated, as shown in (2) in the case of the O class:

$$\mathbf{i}_r = \mathbf{r}_{IO} - \mathbf{r}_O . \quad (2)$$

5) Once the optimal color vector has been obtained, the new colored image I_i can be calculated using (1).

Finally, the colored image I_i is transformed from the *RGB* space to the *HS* plane, where the segmentation is done. The color vector \mathbf{i}_r has its effects in the *HSI* space due to its nonlinearity.

III. CRITERIA FOR THE SEPARATION BETWEEN CLASSES

The Fisher Ratio (*FR*) is frequently used to measure the class separability in classification systems [15], [16]. This ratio simultaneously quantifies the inter-class and intra-class scatter. For a two-class system, it is interesting to achieve a large metric distance between the class means and a minimum dispersion within each class (leading to a high *FR*). In this work, the *FR* is used as a measurement index of the effectiveness of the separation between classes for pixel classification in the *HS* plane. In the case of a multi-class system, the generalized *FR* [17] is expressed by: $FR = \text{trace}(M_w^{-1} M_b)$, where M_b refers to the inter-class (*between class*) covariance matrix and M_w refers to the

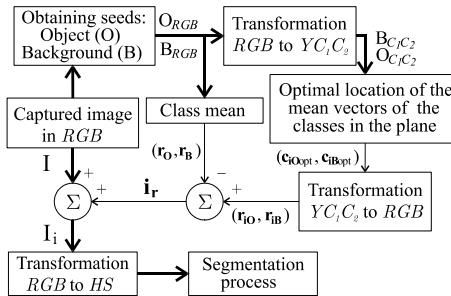


Fig. 1. General block-diagram of the proposed algorithm to define the optimal color vector.

internal (*within class*) dispersion matrix of the class. Due to the circular form of the trajectory of H component, this last equation cannot be directly applied. The reason is that for a two-class system (our case), the M_b does not represent a real distance between the H means of both classes. In addition, the M_w does not represent a real H variance in the discontinuity point when H moves from 2π to 0 in its trajectory. In order to solve this problem, a particular *FR* has been calculated separately [17] for each component in the *HS* plane, given by:

$$FR = FR_H + FR_S \quad (3)$$

where FR_H and FR_S represent the Fisher Ratio of the H and S components, respectively, given by (4):

$$FR_H = \theta_h / \sqrt{\sigma_{HO}^2 + \sigma_{HB}^2}, \quad FR_S = \|S_O - S_B\| / \sqrt{\sigma_{SO}^2 + \sigma_{SB}^2} \quad (4)$$

where θ_h is the separation angle between the hue means of both classes, $\|S_O - S_B\|$ is the distance between the saturation means of both classes, σ_{SO} and σ_{SB} are the standard deviations of the saturation for both classes, and σ_{HO} and σ_{HB} are the standard deviations of the hue.

IV. SEPARATION OF THE CLASSES IN THE *HS* PLANE STARTING FROM THEIR LOCATION IN THE C_1C_2 PLANE

This section details the most important relationships between the statistical mean and variance of the classes in the C_1C_2 and *HS* planes. Also, the effect of an increment in two vectors in *RGB* space on the projections of these vectors in the C_1C_2 and *HS* planes is analyzed.

A. Relationships between the *RGB* Space, and the *HS* and C_1C_2 Planes

Given a vector $\mathbf{r} = [R \ G \ B]^T$ located in the *RGB* space, the *HS* components of a vector \mathbf{h} [12] given by:

$$S = (1 - 3 \min(R, G, B)) / (R + G + B) \quad (5)$$

$$H = \begin{cases} \gamma, & B \leq G \\ 2\pi - \gamma, & B > G \end{cases}; \gamma = \cos^{-1} \left(\frac{R - 1/2G - 1/2B}{(R^2 + G^2 + B^2 - RG - GB - BR)^{1/2}} \right) \quad (6)$$

The components in the YC_1C_2 space [8], [13], [14] can be obtained from \mathbf{r} by:

$$\begin{bmatrix} Y \\ C_1 \\ C_2 \end{bmatrix} = \mathbf{Q} \begin{bmatrix} R \\ G \\ B \end{bmatrix}; \quad \mathbf{Q} = \begin{bmatrix} 1/3 & 1/3 & 1/3 \\ 1 & -1/2 & -1/2 \\ 0 & \sqrt{3}/2 & -\sqrt{3}/2 \end{bmatrix} \quad (7)$$

where \mathbf{Q} is the transformation matrix between spaces.

From (7), the components C_1C_2 of the vector \mathbf{c} are:

$$C_1 = R - 1/2G - 1/2B, \quad C_2 = \sqrt{3}/2G - \sqrt{3}/2B \quad (8)$$

From (8), the Chroma component C and the phase H of the vector in the C_1C_2 plane can be calculated using:

$$C = (C_1^2 + C_2^2)^{1/2} = (R^2 + G^2 + B^2 - RG - GB - BR)^{1/2} \quad (9)$$

$$H = \begin{cases} \alpha, & B \leq G \\ 2\pi - \alpha, & B > G \end{cases}; \alpha = \cos^{-1} \left(\frac{R - 1/2G - 1/2B}{(R^2 + G^2 + B^2 - RG - GB - BR)^{1/2}} \right) \quad (10)$$

Therefore, using (6) and (10) it can be demonstrated that a vector in the *RGB* space can be projected in the *HS* and C_1C_2 planes with the same phase shift but a different module, that is: $H = H'$ and $S \neq C$. It can also be demonstrated that the relationship between S and C is:

$$S = 2Cf(H)/3I; f(H) = \begin{cases} \cos(H - \pi/3) \Rightarrow (0 < H \leq 2\pi/3) \\ \cos(H - \pi) \Rightarrow (2\pi/3 < H \leq 4\pi/3) \\ \cos(H - 5\pi/3) \Rightarrow (4\pi/3 < H \leq 2\pi) \end{cases} \quad (11)$$

where I is the intensity (HSI space), which coincides with Y component, $f(H)$ is a weighting function that depends on the H component and $f(H) \in [0.5, 1]$. This $f(H)$ function generates a three lobe curve in the HS plane delimited by the discontinuities corresponding to the three color sectors of the plane: $0-2\pi/3, 2\pi/3-4\pi/3$ y $4\pi/3-2\pi$.

After all the above discussion, given two vectors in the RGB space, \mathbf{r}_O and \mathbf{r}_B , the resulting projection vectors in the C_1C_2 (\mathbf{c}_O and \mathbf{c}_B), and HS planes (\mathbf{h}_O and \mathbf{h}_B), it is fulfilled:

$$\theta_c = \theta_h = \theta, \quad \|\mathbf{c}_O\| = \|\mathbf{h}_O\|, \quad \|\mathbf{c}_B\| = \|\mathbf{h}_B\| \quad (12)$$

$$\|\mathbf{d}_c\|^2 = g_1(\mathbf{c}_O, \mathbf{c}_B, \theta_c) = \|\mathbf{c}_O\|^2 + \|\mathbf{c}_B\|^2 - 2\|\mathbf{c}_O\|\|\mathbf{c}_B\|\cos\theta_c \quad (13)$$

$$\|\mathbf{d}_h\|^2 = g_2(\mathbf{c}_O, \mathbf{c}_B, \theta_h, I_O, I_B, f(H)) \quad (14)$$

where θ_c is the angle between \mathbf{c}_O and \mathbf{c}_B , θ_h the angle between \mathbf{h}_O and \mathbf{h}_B ; \mathbf{d}_c is the distance vector between \mathbf{c}_O and \mathbf{c}_B , \mathbf{d}_h the distance vector between \mathbf{h}_O and \mathbf{h}_B ; and I_O and I_B are the intensity means of both classes, object and background, respectively, and corresponding to the \mathbf{h}_O and \mathbf{h}_B vectors.

On the other hand, it is important to note that when adding a vector \mathbf{i}_r to both \mathbf{r}_O and \mathbf{r}_B in the RGB space, the distance vector $\mathbf{d}_c = \mathbf{c}_O - \mathbf{c}_B$ in the C_1C_2 plane remains constant, so its magnitude ($\|\mathbf{d}_c\|$) and orientation (ϕ) are invariant. Therefore, adding \mathbf{i}_r in the RGB space results in a translation of the classes in the C_1C_2 plane. This effect can be achieved with a translation vector \mathbf{i}_c (corresponding to \mathbf{i}_r) directly added in the C_1C_2 plane.

Moreover, in the case of the C_1C_2 plane (13) is verified, where the values of θ , $\|\mathbf{c}_O\|$ and $\|\mathbf{c}_B\|$ depend on \mathbf{i}_r , given that $\|\mathbf{d}_c\|$ remains constant when \mathbf{i}_r changes.

In the case of the HS plane, it is necessary to say that if \mathbf{i}_r is added to the vectors \mathbf{r}_O and \mathbf{r}_B , contrary to what happens in the C_1C_2 plane, the difference vector \mathbf{d}_h also varies, therefore it is more difficult to model it. This is so, because \mathbf{d}_h depends (14) on the value of I_O and I_B and on the $f(H)$ function. In any case, (12) always holds.

Summarizing: to obtain the value of the color vector to be added in the RGB space, the authors suggest the use of the relationship between the \mathbf{h} vector components in the HS plane, and their corresponding \mathbf{c} vector components in the C_1C_2 plane, given by (10) and (11), and the relationship between pairs of vectors in these planes, given by (12, 13 and 14). Therefore, the proposed method is based on the analysis of the \mathbf{c}_O and \mathbf{c}_B vectors in the C_1C_2 plane and the properties of the difference vector \mathbf{d}_c (invariants).

B. Separation between the Means of Hue (Angular Separation)

The possibility of utilizing \mathbf{d}_h to obtain the separation between the hue means is rejected due to the discontinuities presented by \mathbf{d}_h because (14) is a function of (11). It is proposed to use C_1C_2 plane, where the distance function between the vectors \mathbf{c}_O and \mathbf{c}_B , ($\|\mathbf{d}_c\|$) (13) does not present discontinuities. Therefore, the proposed algorithm has been

parameterized as a function of the separation angle (θ) between the vectors already added with \mathbf{i}_r , \mathbf{c}_{IO} and \mathbf{c}_{IB} (" i " indicates that the color vector has been added).

In our case, the optimal angle θ_i is obtained from an observation function that measures the effectiveness of the separation between the classes in different locations in the HS plane. This function will be described in paragraph e of section V.

When the angle of separation θ_i is maximum, θ_i coincides with the angle whose bisector is a straight line p , that passes through the origin of coordinates and is perpendicular to the straight line, l , whose director vector is \mathbf{d}_c (Fig. 2). Therefore, the vector to add (\mathbf{i}_r) that causes the maximum difference of hue, makes the modules of both vectors \mathbf{c}_{IO} and \mathbf{c}_{IB} be equal ($\|\mathbf{c}_{IO}\| = \|\mathbf{c}_{IB}\|$) and the distance between the intersection point of the lines p and l , and the extreme of each vector be $\|\mathbf{d}_c\|/2$ (forced location). In Fig. 2, an example of the forced location of the vectors \mathbf{c}_O and \mathbf{c}_B after the addition of the color vector (\mathbf{c}_{IO} and \mathbf{c}_{IB}) is shown.

C. Separation between the Means of Saturation

Given two vectors, for example \mathbf{h}_{IO} and \mathbf{h}_{IB} , in the HS plane, we analyze how the value of the difference of saturation, $S_O - S_B = \|\mathbf{h}_{IO}\| - \|\mathbf{h}_{IB}\|$, varies when θ between both vectors changes. In our case as $\|\mathbf{c}_{IO}\| = \|\mathbf{c}_{IB}\| = C$, according to (11), the intensities (I_O, I_B) corresponding to both vectors \mathbf{h}_{IO} and \mathbf{h}_{IB} , and the value of the saturation weighting function $f(H)$ of each one, are the parameters that have a significant effect in the value of $S_O - S_B$. It is important to note that the saturation varies inversely with the intensity. According to this, it can be said that $S_O - S_B$ is determined by: a) the intensities of the vectors \mathbf{h}_{IO} and \mathbf{h}_{IB} (I_O, I_B), and b) the module and phase of \mathbf{d}_c (the invariants) since these ones determine the location of the vectors \mathbf{h}_{IO} and \mathbf{h}_{IB} along the curve $f(H)$ in the HS plane.

D. Analysis of the Dispersion of the Classes

In this paragraph we carry out an analysis of how the dispersions of saturation and hue of the classes in the HS plane are affected when they are translated in the C_1C_2 plane, as a result of the addition of the color vector (\mathbf{i}_r). This analysis will be necessary to obtain the class separation measure function.

1. Dispersion of the Hue (Angular Dispersion)

Knowing that the variation of the angular dispersion in the

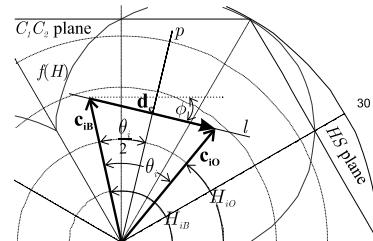


Fig. 2. Forced location of \mathbf{c}_{IO} and \mathbf{c}_{IB} vectors in the C_1C_2 plane, once the color vector has been added.

C_1C_2 plane corresponds with the variation of the dispersion of hue in the HS plane, and being C_1C_2 plane a Cartesian plane, the problem poses in the polar coordinates, taking these two considerations into account:

a) As it has already been indicated, in the C_1C_2 plane, the addition of \mathbf{i}_r produces translation of the classes and, therefore, variations of the modules of their mean vectors $\|\mathbf{c}_{iO}\|=\|\mathbf{c}_{iB}\|=C_i$. This causes that the angular dispersion of both classes is modified. The angular dispersion increases as the module of its respective mean vector decreases, due to the increment of the separation angle θ_i , according to: $C_i=\|\mathbf{d}_e\|/2\sin(\theta_i/2)$.

b) The geometric forms of the distributions of the classes are not predetermined, but they can vary, since the samples are randomly taken from the object and the background, implying that the dispersion varies. The reason is that for different translations of a class in the C_1C_2 plane, different orientations between the axis of maximum and minimum dispersion (represented by their uncertainty ellipse in a C_1C_2 plane) with respect to the orientation of their mean vectors (\mathbf{c}_{iO} or \mathbf{c}_{iB}) are generated.

As an example, Fig. 3 shows both classes, before a translation (O_{iC1C2} and B_{iC1C2}) and after it (O_{iC1C2} and B_{iC1C2}). It can be observed that the deviation of hue, σ_{HO} , of O_{iC1C2} is greater than the deviation of O_{iC1C2} (σ_{HO}), by the effect analyzed in the previous paragraphs (a and b). Nevertheless, the deviation of B_{iC1C2} is lower than the deviation of B_{iC1C2} by the effect analyzed in the a paragraph, since the module of \mathbf{c}_{iB} is greater than the module of \mathbf{c}_{iO} .

2. Dispersion of the Saturation

In fact, if all the vectors of the class have the same intensity, the dispersion of the saturation component is not directly affected by the effects of the translation of the classes in the C_1C_2 plane. The reason is that the saturation is a linear function of the components C_1 and C_2 , as it can be seen in (15). It is possible to demonstrate that (15) is the saturation (11) particularized for lobe 1 of $f(H)$.

$$S = C_1/3I + C_2/\sqrt{3}I \quad (15)$$

This characteristic of linearity makes the deviation of the saturation (σ_S) constant, since the distance between vectors in C_1C_2 plane remains constant independently of the addition of \mathbf{i}_r . Nevertheless, in the HS plane σ_S will be different for each lobe of $f(H)$ but will stay constant within each lobe. Evidently, if the vectors of the class have different intensity, the

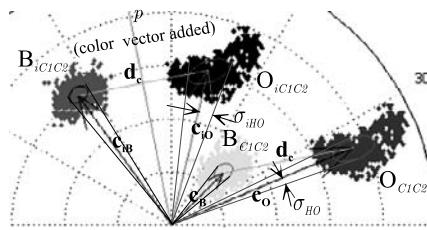


Fig. 3. Translation of the dispersions in the C_1C_2 plane and their different alignments with the mean vectors of each class.

dispersion of the saturation will not be constant for each location, not even within the lobes (there is a greater variation of σ_S when the dispersion of the intensity component is greater).

V. ALGORITHM FOR THE OPTIMAL LOCATION OF THE MEAN VECTORS OF BOTH CLASSES IN C_1C_2 PLANE

This section presents the strategy used for the obtaining, in C_1C_2 plane, of the mean vectors \mathbf{c}_{iOopt} and \mathbf{c}_{iBopt} that maximize the separation of the classes in the HS plane. The process consists of different phases, including an iterative algorithm to obtain a set of locations for the mean vectors of the classes (\mathbf{c}_{iO} and \mathbf{c}_{iB}) in C_1C_2 plane. The location of each vector will be parameterized by the angle formed between both vectors, θ_i . Therefore, we try to obtain a set of θ_m ($\theta_{i1}, \theta_{i2}, \dots$), each of them will have associated an index of measurement of separation between classes, that we will identify by β_{HSn} ($\beta_{HS1}, \beta_{HS2}, \dots$). From the function $\beta_{HSn}=f(\theta_m)$, the value of θ_m that produces the maximum separation between classes is obtained, θ_m optimal: θ_{opt} . The process begins obtaining in C_1C_2 plane the mean vectors of each class, i.e., $\mathbf{c}_O=E\{\mathbf{c}_{O_k}\}$ and $\mathbf{c}_B=E\{\mathbf{c}_{B_k}\}$. The invariants of vector \mathbf{d}_e are obtained from the vectors \mathbf{c}_O and \mathbf{c}_B , i.e., $\|\mathbf{d}_e\|=(d_{C1}^2+d_{C2}^2)^{1/2}$ and $\phi=\tan^{-1}(d_{C2}/d_{C1})$, where, $d_{C1}=C_{1O}C_{1B}$, $d_{C2}=C_{2O}C_{2B}$, and (C_{1O}, C_{2O}) and (C_{1B}, C_{2B}) are the components of the vectors \mathbf{c}_O and \mathbf{c}_B , respectively.

The iterative process consists of the following 5 steps:

a) *Forced location of the mean vectors in the C_1C_2 plane*
The original vectors \mathbf{c}_O and \mathbf{c}_B are relocated (forced) in the C_1C_2 plane using the invariants ($\|\mathbf{d}_e\|, \phi$), obtaining \mathbf{c}_{iO} and \mathbf{c}_{iB} with the following restriction:

$$C_i=\|\mathbf{c}_{iO}\|=\|\mathbf{c}_{iB}\|=\|\mathbf{d}_e\|/2\sin(\theta_i/2). \quad (16)$$

The Cartesian components of these vectors (Fig. 2), particularized for the vector \mathbf{c}_{iO} , are given by:

$$C_{1iO}=C_i \cos(H_{iO}), \quad C_{2iO}=C_i \sin(H_{iO}) \quad (17)$$

where H_{iO} is the angle of the vector that can be expressed by: $H_{iO}=\pi/2+\phi-\theta_i/2$. (18)

The iterative algorithm is initialized with an initial θ_i equal to θ , where θ is the angle formed by the vectors \mathbf{c}_O and \mathbf{c}_B . In each iteration (j) of the algorithm the value of θ_i is increased: $\theta(j)=\theta(j-1)+\Delta\theta$.

b) Verification of the \mathbf{c}_{iO} and \mathbf{c}_{iB} vectors locations validity

For each increase of θ_i , the validity of the locations of the vectors \mathbf{c}_{iO} and \mathbf{c}_{iB} is verified, checking if the values of the components of the corresponding vectors ($\mathbf{r}_{iO}, \mathbf{r}_{iB}$) in RGB space are lower than 1. If the locations are valid, the value of θ_i will be included in the set θ_m .

c) Calculation of the translation vector and translations of both classes in C_1C_2 plane

The translation vector \mathbf{i}_e is obtained for each value of θ_m . This \mathbf{i}_e is responsible of the translations of the classes from its original position to the forced location defined by θ_m . For the O class, this vector is given by: $\mathbf{i}_e=\mathbf{c}_{iO}-\mathbf{c}_O$. The translation of both classes in the C_1C_2 plane is made with \mathbf{i}_e . For the O class: $O_{iC1C2}=\{\mathbf{c}_{O_k}+\mathbf{i}_e\}; k=1,2,\dots,N$.

d) Classes transformation from the C_1C_2 plane to the HS

The classes in the *HS* plane (O_{iHS} and B_{iHS}) are obtained from the translated classes O_{iC1C2} and B_{iC1C2} , using (10), (15) and knowing that $I=Y$.

e) *The observation function: calculation of the measurement index of the separation between classes (β_{HSn}) in the HS plane*
As an observation function of the separation between the classes, a normalized index of measurement has been defined (β_{HS}) from the *FR* described in (3). To obtain the β_{HSn} associated to each θ_m we consider the mean and the dispersion of *H* and *S* of the classes, according to (4). Therefore, $\beta_{HSn}=k_h\beta_{Hn}+(1-k_h)\beta_{Sn}$, where, $\beta_{Hn}=(FR_H-1)/FR_H$, $\beta_{Sn}=(FR_S-1)/FR_S$, and k_h is a weighting factor between β_{Hn} and β_{Sn} that takes values between 0 and 1. The value of k_h is chosen depending on the weight that we want to give to *H* or *S*. Usually, *H* has a greater discriminating power than *S*, therefore $k_h > \frac{1}{2}$.

This iterative process is repeated until the first non valid value of θ_m is generated, being registered the pairs (β_{HSn} , θ_m). With this pairs (β_{HSn} , θ_m), the θ_m that produces the maximum index of measurement of separation between classes is selected. A cubic interpolation is performed around that local maximum to obtain the maximum of the interpolation index, β_{HSopt} , and its associated angle, θ_{opt} . Finally, with this θ_{opt} , the \mathbf{c}_{IOopt} and \mathbf{c}_{IBopt} vectors are obtained using (17).

Fig. 4 presents the curves of variation of β_{Hn} , β_{Sn} and β_{HSn} , as a function of $\theta_m/2$, for a particular case. The figure also shows the values of (θ_{opt} , β_{HSopt}) obtained with the interpolation.

VI. CALCULATION OF THE VECTOR TO ADD AND THE EFFECTS THAT PRODUCES ON THE IMAGES

The calculation of the vector to add, \mathbf{i}_r , is the goal of our proposal. This vector is the responsible of changing the color of the captured image in a suitable manner, so that the classes separate and the object class can be more easily segmented. Once the vectors \mathbf{c}_{IOopt} and \mathbf{c}_{IBopt} that represent the optimal location of the classes in the *HS* plane are obtained, the vectors \mathbf{r}_{IO} , \mathbf{r}_{IB} can be calculated. For example, for the object class *O*: if C_{1Oopt} and C_{2Oopt} are the C_1 and C_2 components of the vector \mathbf{c}_{IOopt} respectively, the vector \mathbf{r}_{IO} in *RGB* space is obtained by:

$$\mathbf{r}_{IO} = \mathbf{Q}^{-1}[Y_{IO} \quad C_{1Oopt} \quad C_{2Oopt}]^T \quad (19)$$

where, Y_{IO} is the intensity mean of the class object already translated in C_1C_2 plane. The \mathbf{i}_r vector is obtained with this \mathbf{r}_{IO} applying (2). Considering that the additions of the color vector

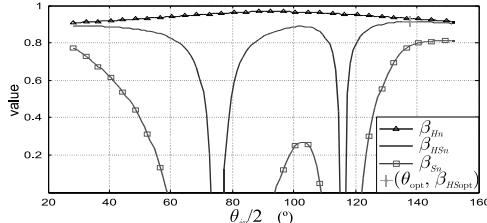


Fig. 4. Measurement indexes: β_{HS} , β_{Sn} and β_{Hn} as a function of $\theta_m/2$, and the point $(\theta_{opt}, \beta_{HSopt})$.

can be made without modifying the intensity values of the vectors of the classes after the addition, then $Y_{IO}=I_O$. In our case, it is not desired to control the saturation mean by I , but by $f(H)$. Therefore, the vector to add \mathbf{i}_r must have zero mean, i.e., $E\{\mathbf{i}_r\}=0$. The fact that $E\{\mathbf{i}_r\}=0$ implies that the intensity mean of the original image (I) and the colored one (I_c) are equal.

The effect of adding the vector \mathbf{i}_r to the original image in new image, I_c , is a greater concentration of the pixel colors around the mean color of one of the two classes. Namely, the addition of this vector contributes to the equalization of the histogram in *H* and in *S*.

As an example, Fig 5 shows the 2D histograms of image *I* (Fig 5.a) and of the colored image *I_c* (Fig. 5.b). In these figures the equalization of the histogram produced by the effect of the addition of the color vector can be clearly observed.

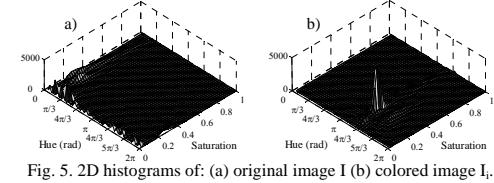


Fig. 5. 2D histograms of: (a) original image *I* (b) colored image *I_c*.

VII. EXPERIMENTAL RESULTS

Practical tests using a bank of real images of different scenes have been carried out to evaluate the effectiveness of the proposed method. The *Euclidean distance* has been used in the test segmentation process. We have utilized such a simple segmentation technique to show the advantages of our proposal. In the tests made, the following data have been used: $M=N=50$, $\Delta\theta=5^\circ$, $k_h=0.85$, interpolation interval $\Delta\Theta=\pm 3x\Delta\theta$. The problems derived from the cyclical nature of the hue in the segmentations have been solved via software.

The experimental results have been quantified by means of the *FR* defined in (3). Table 1 shows the values of *FR* for 4 cases of the bank of images.

Four examples of segmentation are shown in Fig. 6 (figures a, b, c and d) of the 4 cases of Table 1.

Four images are shown for each example, where: the superior left is the original image, the inferior left is the colored image,

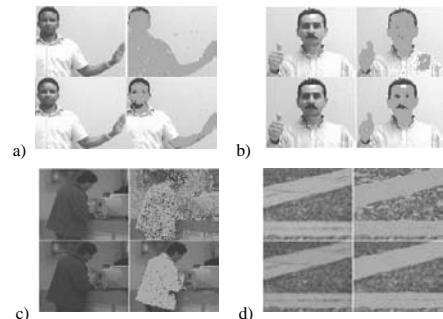


Fig. 6. Results of the segmentation for several persons and objects in different environments.

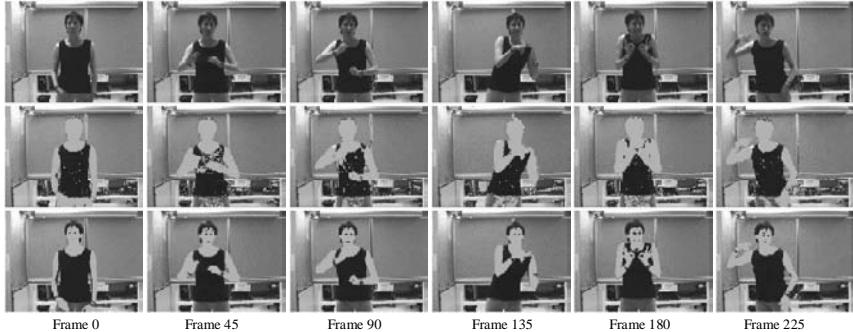


Fig. 7. Segmentation results, for frames 0, 45, 90, 135, 180 and 225 of an image sequence.

the right superior shows the segmentation of the original one, and the image of the right inferior part shows the segmentation of the colored image. As it can be observed, our proposal to add a color vector allows to obtain remarkable improvements in the segmentation process.

TABLE I

FR RESULTS FOR 4 CASES IN THIS WORK

Case	FR	FR (color vector added)	% Increase
1	18.93	35.48	87.40
2	13.72	25.31	84.42
3	2.62	8.62	228.54
4	5.23	10.03	91.57

Finally, in Fig. 7 the results of the skin-color segmentations of a sequence of images of a person generating the sign language are presented. The third row shows the results of the segmentations after adding the color vector proposed in this work.

VIII. CONCLUSIONS

A method to increase the separation between the classes to improve the segmentation process in HS sub-space has been proposed. The experimental results obtained demonstrate that adding color to an image guarantees good results in separating the classes and, therefore, better results when segmenting object. We should also take into account that the implementation of the system is simple and effective in real-time.

It is important to note that the shown images have been obtained directly from the classification process without additional steps, such as morphologic operations.

Currently our research is focused on the addition of a vector \mathbf{i}_r with mean different from 0, on applying higher order transformations that imply scales and rotations of the classes, and on modeling the dispersions of H and S as in [18].

ACKNOWLEDGMENT

The development of these studies has been funded by Ministry of Education and Science (MEC) in the project RESELAI (REF-TIN2006-14896-C02-01).

REFERENCES

- [1] S.L. Phung, A. Bouzerdoum and D. Chai, "Skin segmentation using color pixel classification: analysis and comparison", *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 27, Issue 1, pp. 148–154, Jan 2005.
- [2] R.-L. Hsu, M. Abdel-Mottaleb and A.K. Jain, "Face detection in color images", *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 24, No. 5, pp.606-706, May 2002.
- [3] L. Sigal, S. Sclaroff and V. Athitsos, "Skin color-based video segmentation under time-varying illumination", *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 26, No. 7, July 2004.
- [4] X. Zhu, J. Yang and A. Waibel, "Segmenting hands of arbitrary color," *Proc. Int'l Conf. Automatic Face and Gesture Recognition*, pp. 446–453, 2000.
- [5] J. Fritsch, S. Lang, A. Kleinehagenbrock, G.A. Fink and G. Sagerer, "Improving adaptative skin color segmentation by incorporating results from detection", *Proc. IEEE 11th Int'l Workshop on Robot and Human Interactive Communication*, pp. 337–343, 25–27 Sept. 2002.
- [6] M. Storrings, H.J. Andersen, and E. Granum, "Estimation of the illuminant colour from human skin colour," *Proc. Int'l Conf. Automatic Face and Gesture Recognition*, pp. 64–69, 2000.
- [7] M. Soriano, B. Martinkauppi, S. Huovinen, and M. Laaksonen, "Skin detection in video under changing illumination conditions," *Proc. Int'l Conf. Pattern Recognition*, Vol. 1, pp. 839–842, 2000.
- [8] C. Zhang and P. Wang, "A new method of color image segmentation based on intensity and Hue clustering", *Proc. IEEE 15th Int'l Conf. Pattern Recognition*, Vol. 3, pp. 613–616, 3–7 Sept. 2000.
- [9] S. Sural, Gang Qian and S. Pramanik, "Segmentation and histogram generation using the HSV color space for image retrieval", *Proc. IEEE Int'l Conference Image Processing*, Vol. 2, pp. II–589 – II–592, 22–25 Sept. 2002.
- [10] N. Habil, C. C. Lim and A. Moini, "Segmentation of the face and hands in sign language video sequences using color and motion cues", *IEEE Trans. Circuits and Systems for Video Technology*, Vol. 14, Issue: 8, pp. 1086–1097, Aug. 2004.
- [11] D. Chai and K.N. Ngan, "Face segmentation using skin-color map in videophone applications", *IEEE Trans. Circuits and Systems for Video Technology*, Vol. 9, Issue: 4, pp. 551–564, June 1999.
- [12] R.C. Gonzalez and R. E. Woods, "Digital image processing", Second Edition, Prentice-Hall Inc., New Jersey, pp. 299, 2002.
- [13] T. Caron and P. Lambert, "Color edge detector using jointly hue, saturation and intensity", *Proc. IEEE Int'l Conf. Image Processing*, Vol. 3, pp. 977–981, 13–16 Nov. 1994.
- [14] T. Caron and P. Lambert, "Symbolic fusion of hue-chroma-intensity features for region segmentation", *Proc. IEEE Int'l Conf. Image Processing*, Vol. 1, pp. 971–974, 16–19 Sept. 1996.
- [15] N. Vandebroucke, L. Macaire and J.-G. Postaire, "Color pixels classification in a hybrid color space", *Int'l Conf. Image Processing ICIP 98*, Vol. 1, pp. 176–180, 4–7 Oct. 1998.
- [16] N. Vandebroucke, L. Macaire and J.-G. Postaire, "Color image segmentation by supervised pixel classification in a color texture feature space. Application to soccer image segmentation", *Proc. IEEE 15th Int'l Conf. Pattern Recognition*, Vol. 3, pp. 621–624, 3–7 Sept. 2000.
- [17] S. Theodoridis and K. Koutroumbas, "Pattern recognition", Academic Press, San Diego, pp. 155–157, 1999.
- [18] S. Romaní, P. Sobrerilla and E. Montseny, "On the Reliability Degree of Hue and Saturation Values of a Pixel for Color Image Classification", The 14th IEEE International Conference on Fuzzy Systems FUZZ '05, pp. 306–311, May 22–25, 2005.

Obstruction Removal Using Feature Extraction Through Time for Videoconferencing Processing

*Elliott Coleshill, Dr. Deborah Stacey
University of Guelph, Guelph, Ontario N1G 2W1*

*Dr. Alex Ferworn
Ryerson University, 350 Victoria St. Toronto, Ontario, M5B 2K3*

Abstract:

A major problem with front projection displays used for video conferencing is the potential for undesirable shadows to be cast onto the display screen by presenters. This paper provides a new processing approach for removing cast shadows within videoconference applications. By using sequential images through time shadows can be detected and removed and the presentation contents reconstructed.

Key words:

Video Conferencing, Shadow Removal, Image Processing

1. INTRODUCTION

The increase in affordability and portability of high quality projectors and the general availability of high-speed Internet access has generated a surge of interest in videoconferencing systems research [1][2][3]. One of the most common first steps in many computer vision applications--like virtual videoconferencing--is the detection and removal of unwanted artifacts. The removals are often based on frame differences or background subtraction [4][5].

A challenge that arises from videoconferencing applications is shadow removal. Shadows are caused by

presenters standing in close proximity to the projector between the light source and the screen. Often, presenters are unaware that they are casting shadows the may interfere with the ability of the audience to see the projected image being blocked. There are many ways to detect and remove shadows. These include using multiple projectors and lights [6][7], using simple changes of intensity and saturation within the pixel colour values and other techniques. In this paper we propose a new method of removing shadows using sequential images through time to reconstruct presentation information obscured by shadows.

2. PROPOSED SOLUTION

Using a sequence of video frames taken through time, shadows can be detected and removed leaving the content of the presentation material on the display without distortion.

By using Mean Value Mapping, a tone/contrast map can be generated for each input video frame. A shadow caused by an obstruction usually creates a lower tone and contrast compared to the rest of the display. For each of the input frames all low tone and contrast areas are detected and removed. The final optimized image is then reconstructed using the remaining "good" information from each frame. We call this approach "Feature Extraction Through Time (FETT).

The use of FETT for removing obstruction shadows can be divided into the following steps:

1. Acquire Images

A series of frames are taken over time. Our approach relies on the motion of the presenter. During the time period the presenter's shadow will change due to this movement.

2. Perform Mean Value Tone Mapping

A grid is placed over each input frame where area [1,1] of frame-1 lines up with area [1,1] of frame-2 and so on. Mean mapping values are calculated for each image and are compared.

3. Generate New Image

The selected images and regions are then extracted from the original images and pieced together to generate a new image with removed.

3. RESULTS

A dataset of images has been generated with examples of how a presenter might cause occluding shadows on a display screen. Using the FETT method we have demonstrated how these shadows can be removed and replaced with the original content of the screen.

The first sets of tests were performed using the presenter's arm and hand as the obstruction causing the shadow. The test presenter moved their arm up and down over the screen as if they were pointing out details. Figure 1 (a) is a set of two frames taken with arm motion. It can be seen that every area of the screen is represented correctly within these two images. Using FETT Figure 1 (b) is generated with the arm/hand shadows removed.

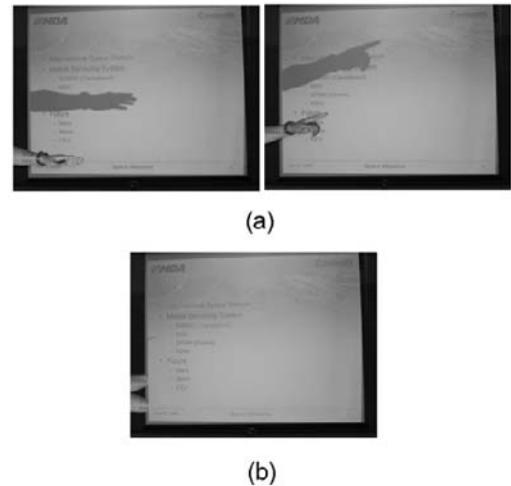
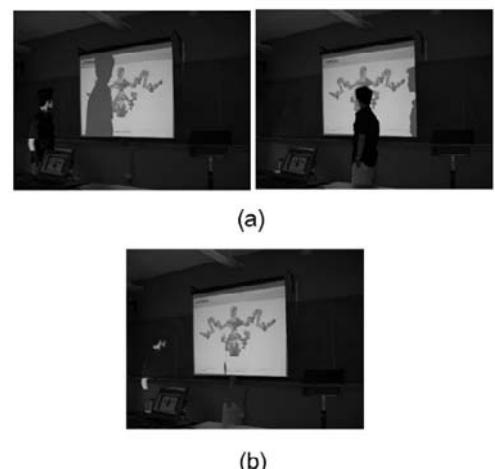


Figure #1: Hand/Arm Shadows

A second set of tests was performed using more complex patterns displayed on the screen as well as the presenter being visible within the field of view. If has been found that if the presenter is wearing dark clothing--causing them to show up as low tone and contrast areas within the image--FETT can filter them out as well. Figure 2 (a) is an example of two frames taken where the presenter is causing a shadow in one, and is blocking the screen with their body in the second. Using FETT a new image, Figure 2 (b) is generated removing the shadow and presenter and reconstructing the display and its content.



Figure#2: Presenter/Body Shadow Example

4. APPLICABILITY

FETT as described in this paper is designed to work using a sequence of images from a single camera view with no changes to the scene other than the presenter and his/her shadow. This algorithm maps the presentation display to a specific area of the scene and reconstructs that area based on the same area of another input image containing no shadows. If the camera is moved the reconstruction of the display will not be reconstructed correctly.

Future enhancements to this approach include the use of multiple cameras. Generating a sequence of images from different cameras located around the classroom to reconstruct the video display on the screen.

5. CONCLUSION

This paper proposes a new method for using a sequence of frames through time to extract occlusion shadows created by presenters for video conferencing applications. With the use of Mean Value Mapping techniques, shadows can be detected and removed and the presentation reconstructed. Using the remaining "good" pixel information, an optimized image can be generated with no shadows blocking the viewable presentation information.

6. REFERENCES

- [1] M. Draoli, G. Gambosi, and M. Lancia. "Videoconferencing on a LAN/MAN architecture: service evaluation and system dimensioning". IEEE Proceedings of ICCT'96, May 5-7, 1996. Volume 2 pp. 630-633.
- [2] K. Liao, and J. Roberts. "Videoconference Traffic and Network Design". IEEE Transactions on Communications. March 1987. Volume 35, Issue 3, pp. 275-282.

- [3] T. Turletti, and C. Huitema. "Videoconferencing on the Internet". IEEE/ACM Transactions on Networking (TON), June 1996. Volume 4, Issue 3. pp. 340-351.
- [4] A. Limton, H. Fujiyoshi, and R. Patil. "Moving Target Classification and Tracking from Real-Time Video". Proceedings of WACV'98, pp. 8-14, 1998.
- [5] A. Elgammal, D. Harwood, and L.S. Davis, "Non-parametric Model of Background Subtraction". Proceedings of ICCV'99 FRAME-RATE Workshop, 1999.
- [6] T. Cham, J. Rehg, R. Sukthankar, and G. Sukthankar. "Shadow Elimination and Occluder Light Suppression for Multi-Projector Displays". Proceedings of the CVPR'03. March 2003.
- [7] R. Sukthankar, T. Cham, and G. Sukthankar. "Dynamic Shadow Elimination for Multi-Projector Displays". Proceedings of CVPR'01. March 2001.
- [8] O. Schreer, I. Feldmann, and P. Kauff. "Fast and Robust Shadow Detection in Videoconference Applications". VIPromCom-2002. IEEE Symposium on Video/Image Processing. June 16-19, Zadar, Croatia. Pp. 371-375.

BLADE DESIGN AND FORMING FOR FANS USING FINITE ELEMENTS

F.D.Foroni

L.A. Moreira Filho

fernandoforoni@rocketmail.com

lindolfo@ita.br

ITA – Aeronautic Technological Institute, IEM
Praça Mal. Eduardo Gomes, 50 – Vila das
Acácias – S. J. Campos, Brazil – CEP 1228-900

M. A. Menezes

miguelm@ita.br, miguel@dem.feis.unesp.br

UNESP – São Paulo State University, Ilha
Solteira Engineering Faculty, DEM
Av. Brasil, 56 – Centro – Ilha Solteira – SP,
Brazil – CEP 15385-000

Abstract: The necessity of adapting the standardized fan models to conditions of higher temperature has emerged due to the growth of concerning referring to the consequences of the gas expelling after the Mont Blanc tunnel accident in Italy and France, where even though, with 100 fans in operation, 41 people died. However, since then, the defied solutions have pointed to aerodynamic disadvantages or have seemed non-appropriate in these conditions. The objective of this work is to present an alternative to the market standard fans considering a new technology in constructing blades. This new technology introduces the use of the stainless steel AISI 409 due to its good adaptation to temperatures higher than 400°C, particularly exposed to temperatures of gas exhaust from tunnels in fire situation. Furthermore, it presents a very good resistance to corrosion and posterior welding and pressing, due to its alloyed elements. The innovation is centered in the process of a deep drawing of metallic shells and posterior welding, in order to keep the ideal aerodynamic superficies for the fan ideal performance. On the other hand, the finite element method, through the elasto-plastic software COSMOS permitted the verification of the thickness and structural stability of the blade in relation to the aerodynamic efforts established

in the project. In addition, it is not advisable the fabrication of blades with variable localized thickness not even, non-uniform ones, due to the verified concentration of tensions and the difficulties observed in the forming. In this way, this study recommends the construction of blades with uniform variations of thickness.

Keywords: Fans, blades, aeronautic profiles, sheet metal forming, blade manufacturing, finite elements

1. INTRODUCTION

The finite element methods are techniques used for approximating differential equations to continuous algebraic equations by a finite number of variables. These techniques were firstly developed for structural problems, but they were extended to numerous cases. Its use on metal forming was first noticed on the 60's, but, the most import solutions were found in the last thirty years. During this period, many problems on this area of study were solved or, at least, better known. Due to that, it was used the elasto-plastic finite element software "COSMOS" to calculate the blade thickness, the blade panel thickness, maximum allowed rotation, fatigue cycles and the blade structural stability verifying displacements, stresses, as much as, the welding stability during the fan operation.

The present work is based in a product (fan) that is already existent on the market where the actual technology, in fiber reinforced plastic, and a work condition in ambient temperature was adapted to the use of stainless steel AISI 409. This material, as known in literature, is adjusted to work on temperatures around 400°C. This way, it was selected for use in fan blades, especially to the ones used for hot gases exhaustion in road tunnels and subways.

2. THE COSMOS SOFTWARE

The COSMOS software was chosen for this work because presents some advantages considering other finite element softwares, such as: linear static analysis, modal extraction and natural frequency calculation, fatigue analysis and non-linear analysis; wide tensile resources and material library with temperature properties, isotropic, orthotropic and anisotropic materials and multi layer composites and advanced non-linear analysis for big displacement problems and/or rotations, plasticity, viscous elasticity, elastic non-linearity and hipper elasticity (Drucker-Prager Criterion). Cemef (2005).

3. APPLICATION FOR THE FINITE ELEMENT METHOD ON THE FAN BLADE DESIGN

The software used for simulation was COSMOS, as previously described. The analysis were limited to the elastic behavior of the blade considering on this project only elastic displacements with stress level below the material yielding limit stress (60%).

It was considered a blade model with root nest and fist which were represented by solid elements (TETRA4 – with 4 nodes each), and the pressure side, trailing side and central stringer were represented as shell elements (SHELL4 – with 4 nodes each).

It was also considered a blade with 420mm length (z axis), with 225mm distance from blade root to rotating center and panel plates for pressure side and trailing side with 2mm thickness.

Table 1. Material Characteristic, Cemef (2002).

Material	Stainless Steel
E_x [GPa]	1,9
ν_{xy}	0,29
ρ_0 [kg/m ³]	8000
σ_e [MPa]	290
σ_f [MPa]	580

where E_x is Young's Modulus, ν_{xy} is Poisson Coefficient, ρ_0 is specific mass, σ_e is the yielding limit and σ_f is the fracture limit on x axis.

To avoid fatigue problems, it was considered a permissible stress for the material as considered $0,6 \times \sigma_e$, which results in Eq.1:

$$\sigma_{adm} = 174 \text{ MPa} \quad (1)$$

The foreseen application for this product was the fan operation. In this, the main loads are due to the bidirectional movement, in polar coordinates can be decomposed by axial load, tangent load and a momentum, Anderson (1991) as seen on the load cases LC1 and LC2 on Eq. 2 and Eq. 3. These loads are result of aerodynamic analysis and are shown on Table 2. These values result from the job and commercial conditions in order to supply the ventilation market needs.

$$LC1 = F_{ax} + F_{tg} + M_{arf} \text{ for } 1800 \text{ rpm} \quad (2)$$

$$LC2 = F_{ax} + F_{tg} + M_{arf} \text{ for } 3600 \text{ rpm} \quad (3)$$

where, F_{ax} is axial load, F_{tg} is tangential load and M_{arf} is the momentum suffered by the blades on application conditions LC1 e LC2.

The aerodynamic loads, for 1800 rpm (LC1), can be seen on Table 2.

Table 2 Aerodynamic Loads for 1800rpm
(LC1).Cemef (2002)

Radius	Profile Twist	Chord	Axial Thrust	Tangential Thrust	Momentum
r [m]	θ [°]	C [mm]	Fax [N]	Ftg [N]	Marf [N.m]
0,248	38,3	234,2	49,8	45,9	-4,4
0,294	32,0	243,1	64,1	52,0	-5,5
0,340	27,2	251,9	81,8	57,7	-6,8
0,386	23,6	260,8	103,2	64,7	-8,4
0,432	20,8	269,6	141,5	73,2	-10,3
0,478	18,7	306,2	189,2	91,0	-13,5
0,524	16,9	343,5	205,6	111,6	-17,7
0,570	15,4	316,8	216,6	112,1	-18,8

The rotation considered were the usually found on electric motors considering electric frequency as 60Hz. The loads considered for 3600 rpm (LC2) can be considered by the 1800 rpm loads (LC1) multiplying the factor on Eq.4.

$$\omega_1^2/\omega_2^2 = (3600)^2/(1800)^2 = 4 \quad (4)$$

Fig.1 shows the structure of the blade. It is made by a solid root nest and two evolving panels. However, due to the momentum suffered by the blade, a stringer was used in order to avoid the plate bending on the interface shell-solid. The stringer is welded in one shell and screwed in the other shell. Fig.1 also shows the load points according to Table 2 values.

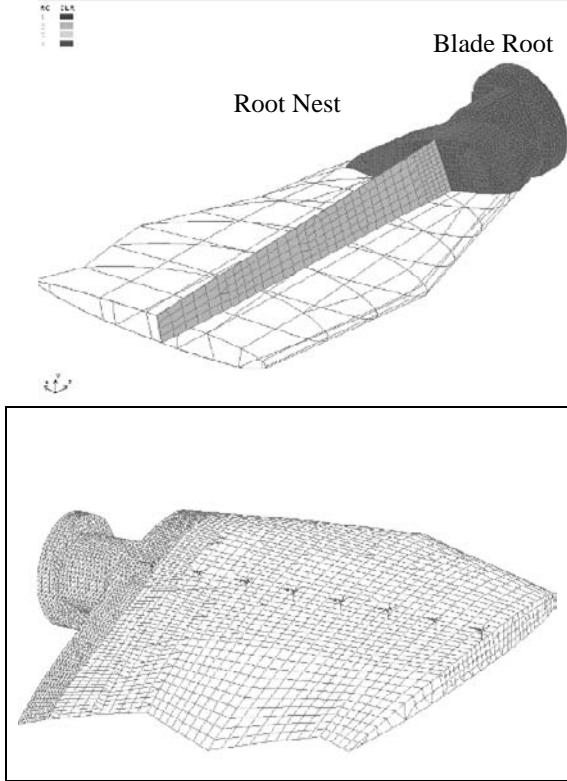


Figure 1. Blade structure and load points. Foroni (2005)

The root nest was projected as a cast solid to stand with the tensile concentration on this region, specially the centrifugal load. Due to that, the transition between the aerodynamic profile and the cylindrical fist is critical and will be constrained radial and axially as shown on Fig. 2 and Fig. 3.

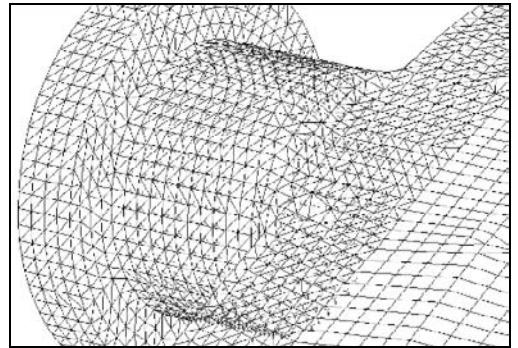


Figure 2. Root nest constraints- rotation constraint (radial direction) Foroni (2005)

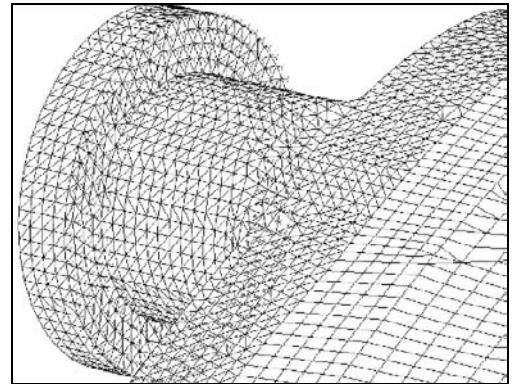


Figure 3. Root nest constraints- translation constraint (axial constraint). Foroni (2005)

4. RESULTS AND ANALYSIS - DISPLACEMENTS

The displacements calculated on the blade, considering the previously defined condition LC1 are shown on Fig.4, for the condition in which the blade are assumed rigid (undeformed condition)

and the condition in which the blade can be deformed. By Analysis of both cases, it's shown that the bigger displacements occur on the leading edge and close to the stringer, on the trailing edge, independently of the blade rigidity.

The leading edge displacements can be related to a bending rod by distributed loading. By the other hand it's important to observe that the bigger displacements on the positions external to the stringer, at the trailing edge can be explained by the reduction of thickness of the blade on these regions, or, the size of the aerodynamic profile, in order to comply with the aerodynamic and performance of the project.

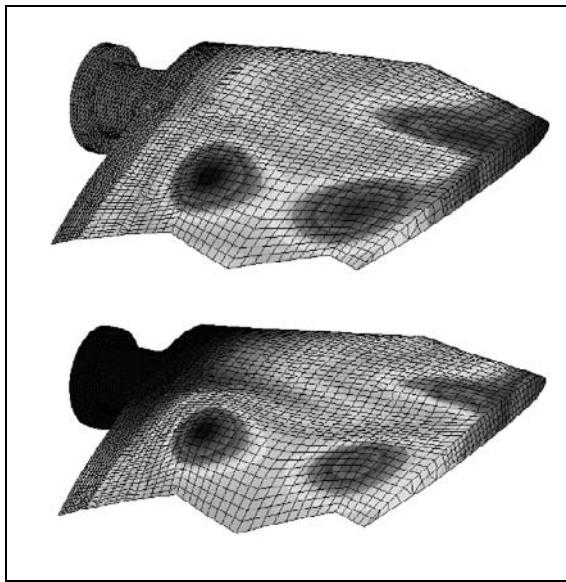


Figure 4. Displacements - LC1 - Undeformed configuration – Y axis (up) and Deformed configuration (down).

For LC2 (rotation 3600rpm), considering the Eq. 4 as a multiplying load factor for Table 2, results to similar displacement conditions. The displacements for LC2, the same way as for LC1 can be seen on Fig. 5.

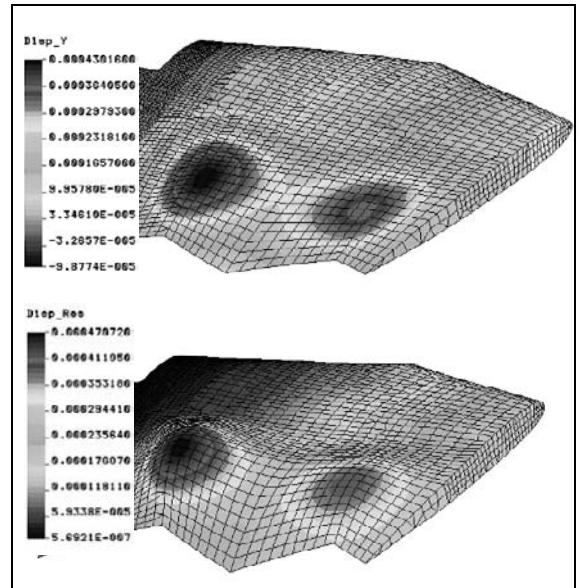


Figure 5. Displacements – LC2 - Undeformed configuration – Y axis (up) and Deformed configuration (down).

Analysing the values of displacements observed, by comparing Fig.5 and Fig.6, it is shown that the biggest displacements can be found on the deformed conditions in all positions. A similar observation can be taken by the LC2 condition. However, these results are based on the displacement level used for set up, which makes the entire blade work in traction considering the centrifugal forces as the most important ones.

Differently, for the LC2 condition (rotation 3600 rpm), it's observed the biggest displacements are most sensible on the positions external to the stringer, close to the trailing edge and they can be explained by the blade thickness reduction on these regions, showing how critical is the stress concentration in this project.

5. RESULTS AND ANALYSIS - STRESSES

The stresses, according to Von Mises method for isotropic or anisotropic with isotropic behavior ($R=1$), were calculated considering the

previously defined conditions LC1 and LC2 and are shown on Fig. 7 and Fig. 8. It's observed that the major stresses, on both cases, are located at the root nest, showing the effect of stress concentration due to the reduction of section on this position. This reduction allows the use of a fan with more blades, in which the geometry on the central hub, limits the air flow and influences the efficiency and effectiveness of the fan.

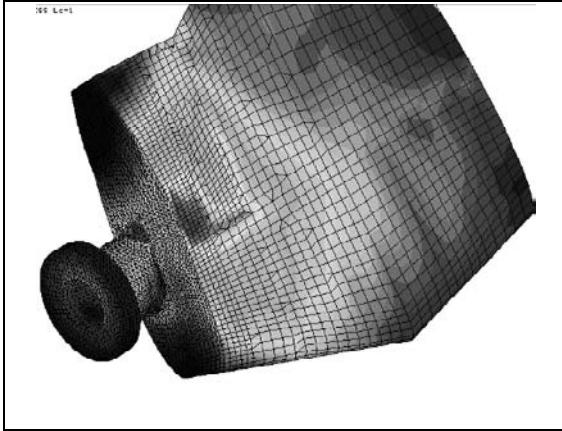


Figure 7. Stresses (Von Mises) in LC1 (144 MPa)

Figure 8, for LC2 shows a stress configuration with values four times bigger and with similar configuration that the case LC1, reinforcing the aerodynamic loads relation on Eq.4.

The stress results for the finite element simulation for 1800 rpm reached the value of 144 MPa as maximum stress. By the other hand, for 3600 rpm, at both positions the root nest and the hub fist, the stress values reached 560 MPa. Thus, as the max allowed stress for the material, considering fatigue life was established as 174 MPa (Eq. 1) it's validated the project only for the LC1 condition, and the LC2 condition, as presented, it's prohibited. This prohibition would be important not just by the surpass of the maximum allowed stress, but also because that at the root nest a mechanical anchorage, with

welding and rivet. This way, the welding stability would be a limit factor of the project.

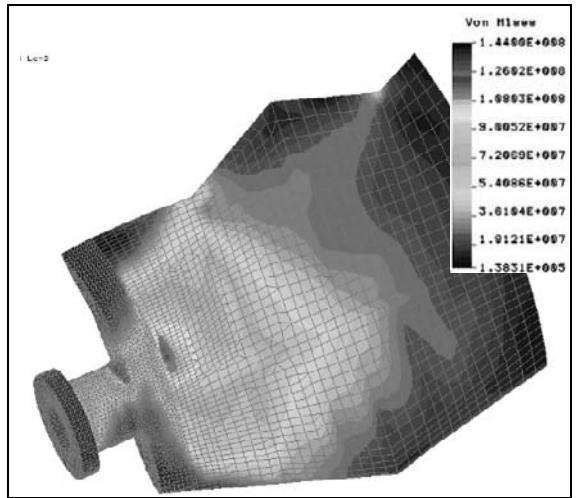


Figure 8. Stresses (Von Mises) in LC2 (560 MPa).

This finite element simulation dissuades the use of blades with localized variation of thickness, or non uniform. Due to this, and also to the difficulty of sheet forming with depth variation by deep-drawing, it's recommended the manufacturing of a blade with thickness variation uniform, or avoid the "bat" trailing edge format.

It should be remembered that the stresses and rotation can only be applied to the calculated diameter, being the tangential speed determining factor, or the multiplication result for rotation and radius. Besides that, the input data consider the blade operation on maximum torsion and loads, which is a limiting factor for aerodynamic issues. In addition, the torsional operation are always lower than the project, which demands the calculation of efforts for each pitch angles for the product validation.

Thus, the rotation of 3600 rpm can be used with the reduction of the fan diameter after posterior load calculation. The same way, blades with bigger length can be applied considering since that the efforts used on this simulation be

used as limitant. For this case, the fan rotation might be decreased.

The aerodynamic loads on Table 2, determines the aerodynamic project of the blade which are results of market analysis and fan adjustment to business needs. This way, this work is focused just on the structural part of the product.

6. CONCLUSIONS

It is shown that the biggest displacements can be found on the deformed conditions in all positions. A similar observation can be taken by the LC2 condition.

It's observed that the major stresses, on both cases, are located at the root nest, showing the effect of stress concentration due to the reduction of section on this position. This reduction allows the use of a fan with more blades, in which the geometry on the central hub, limits the air flow and influences the efficiency and effectiveness of the fan.

This finite element simulation dissuades the use of blades with localized variation of thickness, or non uniform. Due to this, and also to the difficulty of sheet forming with depth variation by deep-drawing, it's recommended the manufacturing of a blade with thickness variation uniform, or avoid the "bat" trailing edge format.

Acknowledgements

The authors would like especially to thank to the Tecsis Tecnologia e Sistemas Ltda by the experimental support.

REFERENCES

Anderson, J.R., 1991. *Fundamentals of Aerodynamics*, McGraw-Hill, p. 15-30.

CEMEF, 2002..*Análise estrutural Pá TLN 420*. Tecsis. p10.

CEMEF, 2005. *Cosmos*. In : <<http://www.cemef-engenharia.com.br/html/software.htm>>. Access in Spetember 6th, 2005.

Foroni, F.D., 2005. *Desenvolvimento de Processo de Conformação de Pás Metálicas de Alto Desempenho para Aplicação em Sistemas de Metrô e Túneis Rodoviários*. MSC Thesis, Instituto Tecnológico de Aeronáutica.

On the Application of Cumulant-based Cyclostationary Processing on Bearings Diagnosis

F.E. Hernández¹, Vicente Atxa², E. Palomino³, J. Altuna²

¹University of Pinar del Río, Martí 270, Pinar del Río, Cuba

²University of Mondragón, Loramendi 4, Mondragón, Spain

³Instituto Superior Politécnico José Antonio Echeverría, Calle 114, No. 11901, Marianao, Cuba.

Abstract-A false indication of failure in rolling element bearings can be reached when cyclostationary processing technique is used for machine condition diagnosis. This problem is due to the fact that the estimated second-order cyclostationary parameters can be altered by first-order cyclostationary signals such as vibrations no related to those produced by defective bearings. The goal of this work is to solve this problem by applying a cumulant-based approach. Four algorithms were implemented. In order to quantify the effectiveness of the algorithm applications, a new function, named Interference Rate Function, is proposed. The appreciable interference immunity in the estimated cumulant-based cyclostationary parameters demonstrated the veracity of the hypothesis.

I. INTRODUCTION

In the group of signal processing techniques applied on machine diagnosis through vibration analysis, the spectral analysis stands out from other techniques. In practical situations, the characteristics of the vibration to analyze (e.g., nonstationary, low signal to noise rate, etc.) does not make the use of this technique to be suitable [1]. In this case, cyclostationary processing technique emerges as one of the most promising procedure used for machine diagnosis.

Second-order cyclostationary analysis has proved to be effective on rolling element bearings diagnosis, as shown in [2], [3], [4] and [5], however, current applications of this technique carry a problem: an indication of failure existence can be achieved while faults in rolling element bearings do not exist. In other words, false alarms can occur. This problem appears when the rotating machine produces certain types of vibrations, for example, vibrations due to unbalances, misalignment, etc. From a different point of view, this problem occurs because of the moment-based approach of the traditional cyclostationary application, which makes the estimated second-order cyclostationary parameter be altered by those vibrations, which are in fact, first-order cyclostationary signals.

This problem can be solved by making the cyclostationary technique approach cumulants. That is why the goal of this work is to apply the cumulant-based cyclostationary processing on vibration analysis in order to resolve the problem of the first-order cyclostationary signals interference.

II. ABOUT THE APPLICATION OF CYCLOSTATIONARY ANALYSIS ON ROLLING ELEMENT BEARINGS DIAGNOSIS

A signal is cyclostationary of order n in the wide sense if and only if it is possible to find some n th-order nonlinear transformation of the signal that will generate finite-strength additive sine-wave components [6]. Frequencies at which spectral lines appear are called *nth-order impure cyclic frequencies* α , in opposition to those called *nth-order pure cyclic frequencies* β , to be explained below.

In general, the application of second-order cyclostationary processing on vibration analysis for diagnosis is based upon the estimation of the spectral parameter known as *correlation spectral density* (CSD), $\bar{S}_x^\alpha(f)_2$, which can be calculated in two ways: through the calculation of the *autocorrelation cyclic function*, and through the calculation of the *second-order cyclic periodogram* [6, 7]. The application of the cyclostationary theory to rolling element bearings failures starts from the assumption that the vibration generated when a failure exists is second-order cyclostationary, arising then a cyclic frequency equals to the *characteristic failure frequency*. The characteristic failure frequency is the main parameter used for diagnosing the bearings condition [8]. Although the procedure of failure detecting when applying cyclostationary theory is not clearly exposed in present references, it can be said that the CSD indicates the existence of a failure if it is not zero at the cyclic frequency α equal the characteristic failure frequency, f_c . That is, if $\bar{S}_x^{f_c}(f)_2 \neq 0$ for any f , then a local fault is present in the corresponding component of the rolling element bearings.

In this work, the experimentation is performed by simulating in computer the vibration produced by defective rolling element bearings. The simulation was based on the model described in [2]. Cyclostationary parameters were also calculated in computer. Matlab was the software used for implementing the corresponding mathematical functions and the signals to process.

The absolute value of the CSD, computed at a cyclic frequency $\alpha = 300$ Hz equals to the characteristic failure frequency of the damaged component of a rolling element bearings, is shown in Fig. 1a. In this case, the vibration is simulated following the characteristics of the model proposed

in [2]. Fig. 1b shows the absolute value of the CSD computed when two first-order cyclostationary signals (with two first-order cyclic components at 2100 Hz and 7570 Hz) are added to the signal simulating the vibration produced by defective bearings. It can be observed the effect of such first-order cyclostationary components on the estimation of the CSD.

The magnitude of the effect on the CSD produced by the first-order cyclostationary components can be measured through the following factor:

$$K_S^\alpha(f) = \frac{\left\| \bar{S}_x^\alpha(f)_2 \right\|_A}{\left\| \bar{S}_x^\alpha(f)_2 \right\|_B} - 1, \quad (1)$$

which is called Interference Rate Function (IRF), where “A” denotes the estimation of the CSD performed when first-order cyclostationary components are added, and “B” denotes the estimation of the CSD when first-order cyclostationary components are not added. A zero value at any frequency f in IRF implies this frequency is not being altered by first-order cyclostationary components. The IRF achieved by substituting the CSD computed and shown in Fig. 1 can be observed in Fig. 2.

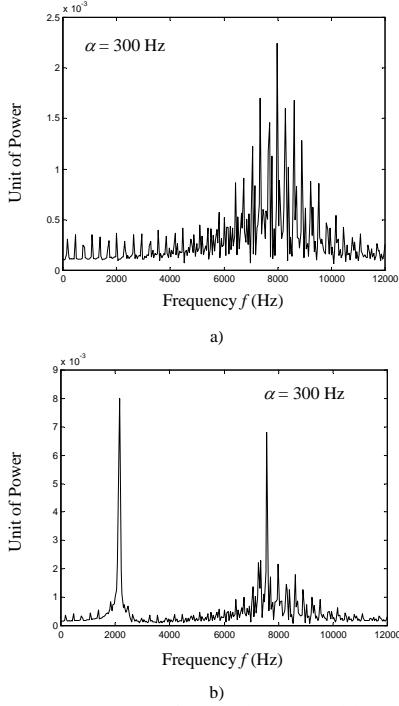


Fig. 1. Absolute values of the correlation spectral density of a) experimental signal simulating the vibration produced by defective rolling element bearings, and b) such a simulation signal having added two first-order cyclostationary components at 2100 Hz and 7570 Hz.

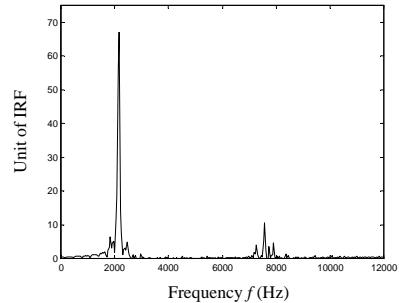


Fig. 2. Interference Rate Function computed via correlation spectral density.

The effect of first-order cyclostationary components on the second-order cyclostationary parameter can be reduced if cumulant-based cyclostationary analysis is applied. This work, in a similar way of moment-based cyclostationary analysis, consists in the calculation of a cyclostationary spectral parameter known as *second-order cyclic polyspectrum* (CP_2), $\bar{P}_x^\beta(f)_2$. Since interference caused by first-order cyclostationary components is not produced, it is said that the CP_2 is a second-order pure cyclostationary parameter and then, arising second-order cyclic frequencies β are considered as pure cyclic frequencies. The CP_2 can be also estimated in two ways: through the estimation of the *second-order cyclic temporal cumulant* [6], and through the convolution of the second-order cyclic periodogram (masked by a special function equal to one everywhere except at those frequencies that arise from impure sine waves, in which case it is equal to zero) with a smoothing window [6].

The procedure of applying the cumulant-based cyclostationary processing on bearing condition monitoring is the same as using the moment-based cyclostationary processing. The difference existing between these two approaches lies in the capability of the cumulant-based cyclostationary processing of providing a more robust estimation of the second-order cyclostationary parameters. However, it is necessary to take into account of the fact that in practical situations it is not possible to perform a precise estimation of the CP_2 as proposed in [6]. This matter is due to the impossibility of carrying out an accurate estimation of the frequencies at which first-order cyclostationary vibrations are produced by real machine in order to form the special window that masks the second-order cyclic periodogram.

III. IMPLEMENTED ALGORITHMS FOR SECOND-ORDER CYCLIC POLYSPECTRUM ESTIMATION

Firstly, an algorithm, based on the so called “general search problem” and presented by Spooner in [6], is adapted to be expressed by equations in reduced form. The IRF, in function of cumulant-based second-order cyclostationary parameters, can be expressed as:

$$K_p^\beta(f) = \frac{\left(\left|\bar{P}_x^\beta(f)_2\right|\right)_A}{\left(\left|\bar{P}_x^\beta(f)_2\right|\right)_B} - 1. \quad (2)$$

The application of the Spooner algorithm yields the IRF shown in Fig. 3a. In this case, interference reduction can be observed if such a result is compared with that obtained in moment-based approach and shown in Fig. 2.

Another algorithm, founded on the first-order cyclic spectral cumulants estimation, is proposed. This algorithm consists in:

- 1.-) Compute $X(f, \tau) = FFT_{t \leftrightarrow f}\{x(t)x(t+\tau)\}$.
- 2.-) Threshold detects the bins of X to find $\{\beta\}$.
- 3.-) Compute $\bar{R}_x^\beta(\tau)_2 = \langle x(t)x(t+\tau)e^{-j2\pi\beta t} \rangle$.
- 4.-) Compute $X(f, \tau) = FFT_{t \leftrightarrow f}\{x(t+\tau)\}$.
- 5.-) Threshold detects the bins of X to find $\{\alpha_1\}$.

- 6.-) Compute $R_x^{\alpha_1}(\tau)_1 = \langle x(t+\tau)e^{-j2\pi\alpha_1 t} \rangle$.
- 7.-) Compute $A^\beta(\tau) = \sum_{\alpha_0 + \alpha_2 \tau = \beta} R_x^{\alpha_0}(0)_1 R_x^{\alpha_2}(\tau)_1$.
- 8.-) Compute $\bar{C}_x^\beta(\tau)_2 = \bar{R}_x^\beta(\tau)_2 - A^\beta(\tau)$.
- 9.-) Compute $\bar{P}_x^\beta(f)_2 = FFT_{\tau \leftrightarrow f}\{\bar{C}_x^\beta(\tau)_2\}$.

Fig. 3b shows the IRF achieved as a result of applying this algorithm on second-order cyclostationary parameter estimation. It is clear that the interference is also reduced according to the result reached when applying moment-based cyclostationary parameter estimation as shown in Fig. 2..

Other algorithm is proposed by Napolitano and Spooner in [9]. This algorithm is based upon the median, and the positive outcome of its application on pure cyclostationary parameter estimation and interference reduction is shown in Fig. 3c.

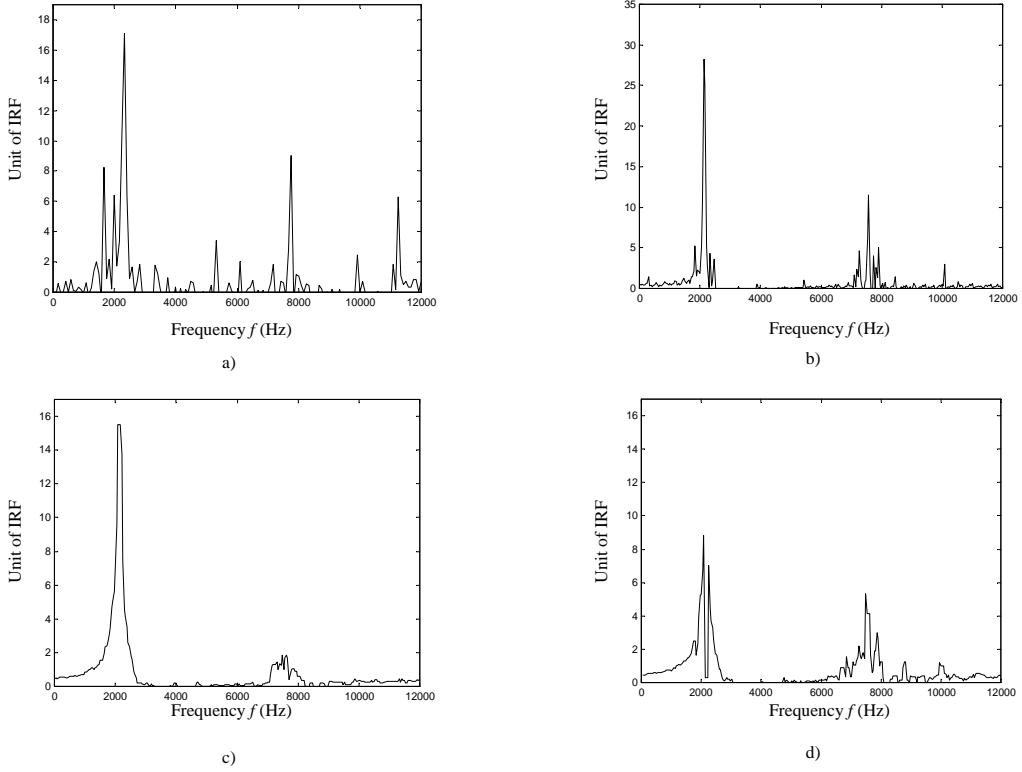


Fig. 3. Interference Rate Function computed via second-order cyclic polyspectrum, applying a) Spooner's algorithm, b) algorithm based upon first-order cyclostationary components, c) median-based algorithm, and d) median-based algorithm discarding the two most deviated components.

A low magnitude of interference caused by first-order cyclostationary components is shown in Fig. 3c. Even more, if some cyclostationary components inside the window that performs the median procedure are discarded, for example, two components (components that lie in positions very separated from the median value in the windows), the results achieved are enhanced, as shown in Fig. 3d.

IV. CONCLUSIONS

The cumulant-based cyclostationary processing, applied on diagnosis of rolling element bearings, allows to reduce the alteration produced by first-order cyclostationary components in the estimated second-order spectral parameter. Then false alarms occurrence is reduced too.

The best results were achieved by applying median-based algorithms in order to estimate the cumulant-based cyclostationary parameters.

The definition of a new function, named IRF, allowed to quantify the effect produced by first-order cyclostationary signals on the estimated second-order cyclostationary parameter, and then, to compare the results obtained by the application of different algorithms.

REFERENCES

- [1] F.E. Hernández, “Aplicación del procesamiento cicloestacionario de vibraciones, avanzado y de segundo orden, a la detección de fallos locales en cojinetes de rodamientos,” PhD dissertation presented at the Mechanic Department, Instituto Superior Politécnico José Antonio Echeverría, La Habana, Cuba, january 2006.
- [2] R.B. Randall, J. Antoni, and S. Chobsaard, “The relationship between spectral correlation and envelope analysis in the diagnostics of bearing faults and other cyclostationary machine signals,” Mechanical Systems and Signal Processing, vol. 15, pp. 945-962, 2001.
- [3] I. Antoniadis, and G. Glossiotis, “Cyclostationary analysis of rolling-element bearing vibration signals,” Journal of Sound and Vibration, vol. 248, pp. 829-845, 2001.
- [4] A. McCormick, and A.K. Nandi, “Cyclostationarity in rotating machine vibrations,” Mechanical Systems and Signal Processing, vol. 12, pp. 225-242, 1998.
- [5] J. Antoni, and R.B. Randall, “Differential diagnosis of gear and bearing faults,” ASME Journal of Sound and Vibration, vol. 124, pp. 165-171, 2002.
- [6] C. Spooner, “Higher-Order Statistics for Nonlinear Processing of Cyclostationary Signals,” in *Cyclostationarity in Communications and Signal Processing*, Ed. William Gardner, IEEE Press, 1994.
- [7] A.V. Dandawate, “Exploiting cyclostationary higher-order statistics in signal processing,” dissertation presented at the Engineering School of Applied Sciences, University of Virginia, 1993.
- [8] R.B. Randall, “State of the art in monitoring rotating machinery,” Annals of the International Conference on Noise and Vibration Engineering, Belgium, 2002.
- [9] A. Napolitano, and C. Spooner, “Median-Based Cyclic Polyspectrum Estimation,” IEEE Transactions on Signal Processing, vol. 48, pp. 1462-1466, 2000.

Application of Higher-order Statistics on Rolling Element Bearings Diagnosis

F. E. Hernández¹, O. Caveda¹, V. Atxa², J. Altuna²

¹University of Pinar del Río, Martí 270, Pinar del Río, Cuba

²University of Mondragón, Loramendi 4, Mondragón, Spain

Abstract-The aim of this work is to evaluate, in a theoretical sense, the current application of bispectrum on rolling element bearings diagnosis. A mathematical model of the vibration generated by defective rolling element bearings is used and substituted into bispectrum formulas. This work demonstrated that using this statistical tool in order to detect a local fault on rolling element bearings is not effective, contrasting with practical results achieved in other papers. In that sense, some arguments concerning such a contradiction are exposed.

I. INTRODUCTION

Many signal processing techniques have been applied on machine diagnosis via vibration analysis. Among them, spectral analysis is highlighted due to the low cost-to-benefit rate obtained from its implementation. However, in many applications, the characteristics of the vibration to analyze (e.g., nonstationary, low signal to noise rate, etc.) cause the worsening of the effectiveness of this technique, and, in such cases, it is justified the application of advanced signal processing techniques [1].

The vibration emitted by defective rolling element bearings is an example of signal with features that could make the spectral analysis perform an inappropriate fault detection task. That is why other signal processing techniques are being applied on the vibration analysis for bearings diagnosis. Higher-order statistical signal processing, in particular, the bispectrum, is one of the actual signal processing techniques, through which better practical results have been obtained [2-4].

The linear modulation process that appears in the vibration produced by defective rolling element bearings makes possible to infer that bispectrum is suitable to be applied. It is well known that higher-order statistical signal processing allows to detect phase-related spectral components, a feature of the modulation signals.

However, as it will be mathematically demonstrated in next sections, the employment of bispectrum for detecting rolling element bearings faults is irrelevant in the sense that no parameters related to the failure characteristic frequency of the bearings are obtained. Obviously, this theoretical result hardly contrasts with practical results actually achieved by different

authors, thus some criteria about this contradiction are presented.

II. USEFUL STATISTICAL FOUNDATIONS

All the features described are statistical because they are based on statistical distributions of the vibration samples. Such features are moments and cumulants.

The signal moments can be expressed as $m_n = E\{x^n\}$, where $E\{\cdot\}$ is the expectation operator which can be estimated (assuming that the signal is ergodic and stationary) using $m_n = \frac{1}{N} \sum_{i=1}^N x_i^n$ [5].

The signal moments are related to the probabilistic density function, $p(x)$, by the moment generating function, $\phi(s) = \int_{-\infty}^{\infty} p(x)e^{sx} dx$. The n th signal moment is calculated by evaluating the n th derivative of $\phi(s)$ at $s=0$, $m_n = \left. \frac{d^n \phi(s)}{ds^n} \right|_{s=0}$.

The second characteristic function is the logarithm of the moment generating function. The cumulants are calculated evaluating the derivatives of this function at $s=0$,

$$c_n = \left. \frac{d^n \ln(\phi(s))}{ds^n} \right|_{s=0}.$$

Cumulants have several useful properties that make their use more convenient than the use of moments. Firstly the higher-order cumulants of a Gaussian random variable are all zero. Secondly the cumulant of the sum of two random variables is the sum of the cumulant of the random variables. Therefore if a Gaussian random variable is added to a non-Gaussian random variable, the resulting signal's higher-order cumulants are the cumulants of the non-Gaussian signal.

A. Moment and cumulant functions and spectra

If a zero-mean real stationary random process, $x(t)$, is considered [6], the moment and cumulant functions, are expressed as follows:

$$m_1 = c_1 = \text{mean value}, \quad (1a)$$

$$m_2(\tau) = c_2(\tau) = E[x(t)x(t+\tau)], \quad (1b)$$

$$m_3(\tau_j, \tau_k) = c_3(\tau_j, \tau_k) = E[x(t)x(t+\tau_j)x(t+\tau_k)], \quad (1c)$$

and so on.

The term "higher-order" is used when the order is higher than two.

On the other hand, the Wiener-Khintchine relation can be generalized by transforming cumulant functions, which results in the spectral cumulant functions as follows:

$$c_2(\tau) \xleftarrow{1} C_2(f), \quad (2a)$$

$$c_3(\tau_j, \tau_k) \xleftarrow{2} C_3(f_j, f_k), \quad (2b)$$

and so on.

The elements $\xleftarrow{1}$ and $\xleftarrow{2}$ denote the one and two dimensions Fourier transform. The second-order cumulant spectrum is the traditional power spectral density and the third-order cumulant spectrum is known as bispectrum.

III. VIBRATION EMITTED BY DEFECTIVE ROLLING ELEMENT BEARINGS

The main function of rolling element bearings is to provide low friction conditions for supporting and guiding a rotating shaft.

The parts of the rolling element bearings are: rolling elements, inner race, outer race and cage. They remain in contact and their failures can be caused by manufacturing problems, inadequate usage or wearing.

One of the most important defects to detect on rolling element bearings is the local failure. This type of fault makes the bearings produce a vibration that corresponds to a linear modulation signal (see Fig. 1) which usually superimposes on other vibration sources in the rotating machine.



Fig. 1. Vibration produced by defective rolling element bearings.

IV. MODEL OF THE DEFECTIVE ROLLING ELEMENT BEARINGS VIBRATION

One of the models that better characterizes the vibration produced by defective rolling element bearings is the one provided by Randall *et al.* in [7]:

$$x(t) = \sum_i a_i s(t - iT_0 - \tau_i) + n(t), \quad (3)$$

where T_0 is the average time between impacts, $s(t)$ is the oscillating waveform generated by a single impact, $n(t)$ is a zero-mean stationary noise, τ_i is a zero-mean delta-correlated point process with probability density function $\rho_\tau(t)$, and a_i is a periodically delta-correlated point process.

V. PROCEDURE FOR DETECTING THE VIBRATION GENERATED BY DEFECTIVE ROLLING ELEMENT BEARINGS

Most of the techniques involved on bearings diagnosis by vibration analysis are based on the identification of some pattern related to the *failure characteristic frequency*. This frequency equals $1/T_0$; it depends upon mechanical characteristics of the rolling element bearings and can be calculated by well stated expressions [8, 9].

Practical results achieved by the application of the bispectrum on the detection of local faults in rolling element bearings, suggest that the procedure in this case consists of identifying bispectral lines separated at the failure characteristic frequency, $1/T_0$.

In this work, the bispectrum of the vibration generated by defective rolling element bearings is theoretically calculated, using the model described in section IV and substituted in the bispectrum expressions. It will be shown that in theory no bispectral lines can appear in the result, leading to a contradiction with those practical outcomes obtained by other researchers.

VI. THEORETICAL BISPECTRUM OF THE VIBRATION GENERATED BY DEFECTIVE ROLLING ELEMENT BEARINGS

The theoretical calculation of the bispectrum of the vibration produced by defective rolling element bearings is performed by substituting the vibration model in the third-order cumulant function, and then, by transforming the result (as expressed in (2b)).

In other words, the third-order cumulant function is written as follows:

$$\begin{aligned}
c_3(\tau_1, \tau_2) = & \\
= E \left\{ \left[\left(\sum_i a_i s(t - iT_0 - \tau_i) + n(t) \right) - m_1(t) \right] \cdot & \\
\cdot \left[\left(\sum_i a_i s(t - iT_0 - \tau_i + \tau_1) + n(t + \tau_1) \right) - m_1(t + \tau_1) \right] \cdot & \\
\cdot \left[\left(\sum_i a_i s(t - iT_0 - \tau_i + \tau_2) + n(t + \tau_2) \right) - m_1(t + \tau_2) \right] \right\} & \quad (4)
\end{aligned}$$

where $m_1(t) = \sum_i \bar{a}_i \tilde{s}(t - iT_0)$ is the mean value of $x(t)$ as calculated in [7] and $\tilde{s}(t) = s(t) * \rho_\tau(t)$.

The calculation of (4) results in:

$$\begin{aligned}
c_3(\tau_1, \tau_2) = & \\
= \left[\sum_i \bar{a}_i^3 s(t - iT_0) s(t - iT_0 + \tau_1) s(t - iT_0 + \tau_2) \right] * \rho_\tau(t) - & \\
- \sum_i \bar{a}_i \tilde{s}(t - iT_0 + \tau_1) \left[\bar{a}_i^2 s(t - iT_0) s(t - iT_0 + \tau_2) \right] * \rho_\tau(t) - & \\
- \sum_i \bar{a}_i \tilde{s}(t - iT_0) \left[\bar{a}_i^2 s(t - iT_0 + \tau_1) s(t - iT_0 + \tau_2) \right] * \rho_\tau(t) - & \\
- \sum_i \bar{a}_i \tilde{s}(t - iT_0 + \tau_2) \left[\bar{a}_i^2 s(t - iT_0) s(t - iT_0 + \tau_1) \right] * \rho_\tau(t) + & \\
+ 2 \sum_i \bar{a}_i^3 \tilde{s}(t - iT_0) \tilde{s}(t - iT_0 + \tau_1) \tilde{s}(t - iT_0 + \tau_2) & \quad (5)
\end{aligned}$$

Substituting the third-order cumulant function in (2b) results in the bispectrum. In this case, the starting expression is:

$$\begin{aligned}
C_3(f_1, f_2) = & \\
= \lim_{w \rightarrow \infty} \frac{1}{w} \int_{-w/2}^{w/2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} c_3(\tau_1, \tau_2) e^{-j2\pi f_1 \tau_1} e^{-j2\pi f_2 \tau_2} d\tau_1 d\tau_2 dt & \quad (6)
\end{aligned}$$

which leads to the final expression of the bispectrum of $x(t)$, as follows:

$$\begin{aligned}
C_3(f_1, f_2) = & \frac{1}{T_0} \sum_i \bar{a}_i^3 S(-f_1) S(-f_2) S(f_1 + f_2) - \\
& - \frac{1}{T_0} \sum_i \bar{a}_i \bar{a}_i^2 \tilde{S}(-f_1) S(-f_2) S(f_1 + f_2) P_\tau(f_1) - \\
& - \frac{1}{T_0} \sum_i \bar{a}_i \bar{a}_i^2 S(-f_1) \tilde{S}(-f_2) S(f_1 + f_2) P_\tau(f_2) - \\
& - \frac{1}{T_0} \sum_i \bar{a}_i \bar{a}_i^2 S(-f_1) S(-f_2) \tilde{S}(f_1 + f_2) P_\tau(-f_1 - f_2) + \\
& + \frac{2}{T_0} \sum_i \bar{a}_i^3 \tilde{S}(-f_1) \tilde{S}(-f_2) \tilde{S}(f_1 + f_2), & \quad (7)
\end{aligned}$$

where $s(t) \leftrightarrow S(f)$, $\tilde{s}(t) \leftrightarrow \tilde{S}(f)$ and $\rho_\tau(t) \leftrightarrow P_\tau(f)$ are transform pairs.

An inspection of the final bispectrum expression shows that no bispectral information in respect to the failure characteristic frequency, $1/T_0$, is achieved. In other words, the theoretical bispectrum does not result in discrete bispectral components equally spaced at the failure characteristic frequency.

VII. CONSIDERATIONS ABOUT THE PRACTICAL "EFFECTIVENESS" OF THE BISPECTRUM APPLICATION IN CONTRAST WITH THEORETICAL RESULTS

Despite the mathematical result reached in Section VI, several authors have previously presented the "benefits" of calculating the bispectrum of the vibration generated by a rotating machine in order to detect bearings failures [2-4]. In such works, when the bearings fault exists, bispectrum exhibits clear bispectral components separated at $1/T_0$, which is used as indication of failure existence. However, these components do not arise in the theoretical bispectrum, as shown in (7).

Attending to the practical difficulties in estimating the first-order moment of the vibration generated by defective rolling element bearings, it can be ensured that this contradiction is due to the fact that practical applications of the bispectrum are performed assuming that the mean value of $x(t)$ is constant and equals $\frac{1}{T} \int_{-T/2}^{T/2} x(t) dt$. A resulting practical bispectrum is shown in Fig. 2. Then it's clear to realize that the result of calculating the bispectrum in both a theoretical and a practical sense is not the same.

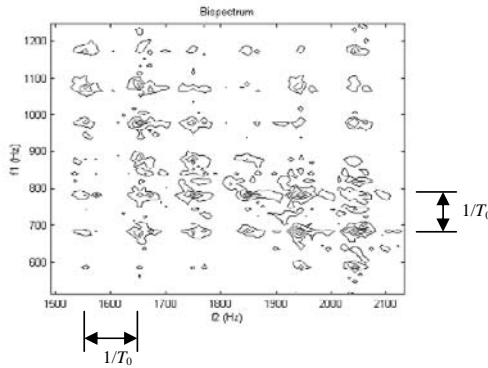


Fig. 2. Bispectrum of the vibration produced by a defective rolling element bearings (characteristic failure frequency equals to $1/T_0$).

VIII. CONCLUSIONS

This work demonstrated the theoretical inefficiency of calculating the vibration bispectrum in order to detect local faults in rolling element bearings. This conclusion constitutes a novel result since there are not previous references about it.

The contradiction in the results obtained by practical and theoretical applications of the bispectrum is evaluated in this paper. In fact, problems in the practical estimation of first-order moment of the vibration do not lead to the same results when applying both theoretical and practical bispectrum.

This study contributes to clarify the possibilities of applying advanced signal processing techniques on vibration analysis, specifically, the higher-order statistical processing.

REFERENCES

- [1] F.E. Hernández, "Aplicación del procesamiento cicloestacionario de vibraciones, avanzado y de segundo orden, a la detección de fallos locales en cojinetes de rodamientos," PhD dissertation presented at the Mechanic Department, Instituto Superior Politécnico José Antonio Echeverría, La Habana, Cuba, january 2006.
- [2] A.C McCormick, "Cyclostationary and higher-order statistical signal processing algorithms for machine condition monitoring," dissertation presented at Department of EEE, University of Strathclyde, United Kingdom, September 1998.
- [3] J. Piñeyro, A. Klempnow, and J. Lescano, "Effectiveness of new spectral tools in the anomaly detection of rolling element bearings," Journal of Alloys and Components, vol. 310, pp. 276-279, 2000.
- [4] F.E. Hernández, and V. Atxa, "Diagnóstico de maquinarias a partir del análisis de vibraciones," VI Seminario Anual de Automática, Electrónica Industrial e Instrumentación, Vigo, Spain, September 2003.
- [5] A. Papoulis, *Probability, random variables, and stochastic processes*, 3rd ed., McGraw-Hill, Inc., 1991, pp. 109-119.
- [6] B. Boashash, E.J. Powers, and A.M. Zoubir, *Higher-order statistical signal processing*, Longman House, Melbourne, Australia, 1995.
- [7] R.B. Randall, J. Antoni, and S. Chobsaard, "The relationship between spectral correlation and envelope analysis in the diagnostics of bearing faults and other cyclostationary machine signals," Mechanical Systems and Signal Processing, vol. 15, pp. 945-962, 2001.
- [7] N. Tandon, and B.C. Nakra, "Vibration and acoustic monitoring techniques for the detection of defects in rolling element bearings. A review," The Shock and Vibration Digest, vol. 3, pp. 3-11, 1992.
- [8] R.B. Randall, "State of the art in monitoring rotating machinery," International Conference on Noise and Vibration Engineering, Belgium, September 2002.

Extending RSVP-TE to support Guarantee of Service in MPLS

Francisco Javier Rodriguez-Perez, Jose Luis Gonzalez-Sanchez
University of Extremadura (Spain)
emails: {fjrodri, jlgs}@unex.es

Abstract-Independent Quality of Service (QoS) models need to be set up in IP and ATM integration and they are difficult to coordinate. This gap is bridged when MultiProtocol Label Switching (MPLS) is used for IP-ATM integration purposes. Guarantee of Service (GoS) allows MPLS to improve performance of privileged data flows in congested domains. We first discuss the GoS requirements for the utilization in conjunction with MPLS. Then we propose a minimum set of extensions to RSVP-TE that allow signaling of GoS information across the MPLS domain.

I. INTRODUCTION

Multiprotocol Label Switching (MPLS) is currently mainly used to provide Virtual Private Networks (VPNs) services [1] or IP-ATM with QoS integration purposes [2], combining ATM traffic engineering capabilities with flexibility of IP and class-of-service differentiation [3]. In this way MPLS bridges the gap between IP and ATM avoiding the need of setting up independent QoS models for IP and for ATM, which are difficult to match. ATM switches can dynamically assign Virtual Path Identifier/Virtual Channel Identifier (VPI/VCI) values which can be used as labels for cells. This solution resolves the problem without the need for centralized ATM-IP integration servers. This is called Label-Controlled ATM (LC-ATM) or IP+ATM.

Like ATM Virtual Circuits (VCs), MPLS Label Switched Paths (LSPs) let the headend Label Edge Router (LER) control the path its traffic takes to a particular destination [4]. This method is more flexible than forwarding traffic based on destination address only. LSP tunnels also allow the implementation of a variety of policies related to network performance optimization [5][6]. For example, LSP tunnels can be automatically or manually routed away from network failures or congestion points. Resource ReSerVation Protocol (RSVP) is a signaling mechanism used to reserve resources for these LSP tunnels throughout a network. So MPLS reserves bandwidth on the network when it uses RSVP to build LSPs. Using of RSVP to reserve bandwidth for a particular LSP introduces the concept of *consumable resource* in the network, that allows to RSVP nodes to find paths across the domain which have bandwidth available to be reserved. Unlike ATM, there is no forwarding-plane enforcement of a reservation. A reservation is made in the control plane only, which means that if a Label Switch Router (LSR) makes an RSVP reservation

for 10 Mb and later it needs 100 Mb, it will congest that LSP. The network attempts to deliver that 100 Mb, damaging performance of other flows that can have even more priority, unless we attempt to police the flows using QoS techniques. Although RSVP with Traffic Engineering (TE), (performance optimization of operational RSVP networks), is expected to be an important application in this problematic [7] an extended RSVP-TE protocol can be used in a much wider context for performance improvement. In this way, MPLS-TE is providing fast networks but with no local flow control, so assuming that devices are not going to fail or there will be no data loss. However, resource failures and unexpected congestion cause a great part of lost traffic. In these cases, upper layers protocols will request lost data retransmissions at end points, but the time interval to obtain retransmitted data can be significant. For some types of services with special requirements of delay and reliability, as stock-exchange data or medical information, MPLS is not able to ensure that performance will not be worse due to lost traffic end-to-end retransmissions.

In this work we describe a set of extensions to MPLS RSVP-TE signaling required to support GoS over MPLS. This technique will allow to offer Guarantee of Service to privileged data flows [8], allowing discarded packets due to congestion to be locally recovered, avoiding in this way, as far as possible, end to end retransmissions requested by upper layers.

Following section shows what is GoS and how it can be applied to privileged flows in an MPLS domain. In the third section we study the RSVP-TE extensions to transport GoS information through a MPLS domain. In fourth section an analysis of the proposal is shown and finally this article concludes indicating the contributions of the research.

II. GOS OVER MPLS

The GoS capacities for a MPLS privileged data flow is the capacity of a particular node to local recovering of discarded packets belonging to the data flow. This work proposes up to four GoS levels (see Table I), codified with two bits; so each packet can be marked with this information throughout all the route. A greater GoS level implies a greater probability that a packet can be found in the GoS buffer of any node it has been passing through. Thus the need of end to end retransmissions is avoided, recovering lost data in a much rather local environment.

TABLE I
GoS LEVELS CODIFICATION

GoS ₁	GoS ₀	Meaning
0	0	No GoS packet.
0	1	Level 1 of GoS.
1	0	Level 2 of GoS.
1	1	Level 3 of GoS.

Implementation of GoS levels is carried out by means of the MPLS packet header, in the network level header and upper layers headers too. The main implied levels in an MPLS communication are *Network*, *Link* and level 2+ or MPLS. However, we have to bear in mind the possibility of marking the whished GoS levels in *Transport* layer for *Application* level packets. Thus, following the TCP/IP model, data is marked with GoS at *Application* level directly by user and after that, the process would mark the TCP segments to be encapsulated in IP packets, which finally would receive a label to be switched across the MPLS domain.

In *Application* level, a GoS capability session can be started selecting a particular port when opening a TCP socket. For example, in order to use email service we access to the port 110 or we use port 22 to SSH services. In this way, GoS use three ports to open TCP sessions, mapped with each one of the three GoS available levels. This will cause the *Transport* and upper levels to be marked with GoS.

In *Transport* level, there are six reserved bits in the TCP header since initial TCP research. For a long time these bits have not been used, but in recent years, several bits have been used to mark some options of *Differentiated Services*. There are still four available bits to be used by GoS.

In *Network* level, the GoS mark has been implemented in the IP *Options* field, which has a size of up to 40 bytes. However only the first byte of this field is needed to codify the two bits for GoS. To mark a packet with GoS in MPLS level, the *label* field has value 1, which has been defined as a special value for MPLS labels. The *EXP* field (see figure 1) can transport the two bits needed for GoS. This mark will be set by the ingress Label Edge Router (LER), a node that allows to enter to the MPLS domain. By the other hand

A. GoS packets identification

In GoS nodes, a temporal buffer called NonStop-Forwarding Memory for GoS PDUs (NMGP) is needed. Moreover, GoS packets buffered in these nodes must also be identified to allow a GoS packet which satisfy a local retransmission request can be found. So privileged PDUs will be indexed in these buffers, allowing all sent and received GoS packets are globally identified in the MPLS domain, for nodes which request local retransmissions recognize each packet whose retransmission is needed as well as for upstream nodes to find stored GoS marked packets.

The IP address from *Network* layer allows to identify each node in a network topology so it can identify data flows, but it can not identify each packet sent by a particular node. An *id* identifier will go with each GoS packet and will be assigned by

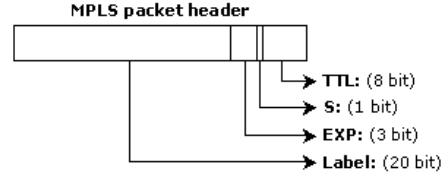


Fig. 1. MPLS packet header structure.

the sender node that generates it. A four octets identifier allows to recognize up to $2^{32} = 4.294.967.296$ packets sent by a node. After that, it would start to assign *ids* from the beginning, perhaps allowing the existence of two packets with the same identifier. However it is very likely that before starting to repeat identifiers, the other repeated packets have already left the MPLS domain, what is less likely if indexing is lesser than 2^{32} . In summary, the *Network* level address of the sender, together with the four bytes *id* will be considered as the unique identifier for a GoS packet. This *id* field will also be marked in the *Options* field, after the GoS level field (see figure 2).

B. GoS Path Marking and Local Recoveries

We consider a domain $G(U)$, with a set of nodes U and a data flow $\varphi(G)=\varphi(x_i, x_n)$ in $G(U)$ across a path $LSP_{i,n}$, with origin in node x_i and destination in node x_n , with $\{x_i, x_n\} \subset U$. Node x_n only knows incoming port and incoming label of every arrived packet of $\varphi(G)$, i.e., x_n only knows that x_{n-1} is the sender of $\varphi(x_i, x_n)$. It could know which node is the sender of a packet basing on label information, but this is not a reliable strategy because node x_{n-1} could use flow aggregation mechanisms to merge k flows coming from other nodes into a unique flow, in the form:

$$\varphi(x_{n-1}, x_n) = \sum_{i=1}^k \varphi_i(x_{n-1}, x_n) \quad (1)$$

By the other hand, if x_n , due to congestion, do not keep Flow Conservation Law:

$$\sum_{j=1}^k p_{nj} < \sum_{i=1}^k p_{in} , \quad (2)$$

being p_{ij} the traffic volume sent from x_i to x_j through x_n ; so node is discarding one or more packets. In this case x_n cannot find any node to request local retransmissions of lost packets. It is very important to know the set of nodes by which a particular GoS packet has passed through and this is known as *GoS Path Marking*. Thus, x_n will know that discarded traffic can have been stored in upstream GoS nodes in $LSP_{i,n}$. The first node to request a local retransmission will be the starting node of the *GoS Plane*, i.e., its previous GoS neighbor. To get this stack of GoS nodes we have to obtain the set of nodes X such that $X \subseteq LSP_{i,n} = \{(x_i, x_{i+1}), (x_{i+1}, x_{i+2}), \dots, (x_{n-1}, x_n)\} \subseteq U$,

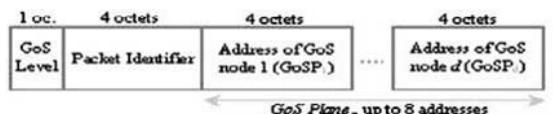


Fig. 2. IP Options field format for characterization of GoS packets

of $G(U)$ domain, with maximum *diameter* $d(x_i, x_n) = n - i$ such that X are *GoS* capable. In this way, with packet discarding, a local retransmission could be requested to any node belonging to X , avoiding requests to the head end and bringing a lesser increment of global $\varphi(G)$ in the domain.

Path marking at MPLS level implies using of several bits from the label, making that Non-*GoS* nodes ($LSP_{i,n} - X$) do not know how to handle *GoS* traffic. So working at network level is a better strategy, i. e., *GoS* nodes of $LSP_{i,n}$ mark its network level address in the IP *Options* field of the *GoS* privileged packets. This stack of network address of nodes that have switched the packet is known as *GoS Plane* and the number of elements of this stack is the *diameter* (d) of the *GoS Plane*. Maximum value of d is $\max d = ((OS \cdot BU)/BpA)$, where OS is the IP *Options* field size (40 bytes); BU is the number of bytes used in the *GoS* proposal for packet characterization (1 byte for *GoS* level and 4 bytes for packet identification); BpA (*Bytes per Address*) is the number of bytes needed to codify an IP address (4 bytes). The value $d = 8$ is the maximum supported *GoSP diameter*. The objective of *GoS* is not to propose the replacement of all the nodes in a MPLS domain but the incorporation of several *GoS* capable MPLS nodes. In this way, in case a local retransmission was necessary in a node, there is a *GoS Plane* of at most 8 nodes to go upstream, increasing possibilities of finding lost packet. Moreover, *Internet Effective Diameter* (*IED*), that is defined as the maximum number of indispensable hops that are needed to reach to any other node in Internet [9], shows that rounding to 4, approximately 80% of the pairs of nodes in Internet are reachable in this distance. If we consider an effective diameter of 5, it covers more than 95% of the pairs of nodes so a *GoSP diameter* of at most 8 nodes is a suitable size.

The last d *GoS* nodes which have switched a particular *GoS* packet is always known. This stack will also be marked in the *Options* field, after the *GoS* level field and after the four bytes packet identifier. So, in order to support *GoS*, the IP *Options* field of a packet will be formatted like in figure 2 is shown.

III. GOS SIGNALING

The specification of RSVP-TE [1] defines extensions to the Resource reSerVation Protocol (RSVP) in order to make network resources reservations and to distribute labels, establishing LSPs with traffic engineering capabilities. Among these extensions are the ability to specify a strict path to be followed by an LSP or supporting of state recoveries [10].

RSVP messages are composed of header and a set of objects. Among these objects are the Explicit Route Object, the Sender Template Object or the Hello Object. This message enables RSVP switches to detect when neighbor nodes are not reachable, so this mechanism provides a very local and effective failure detection. When such a failure is detected it is commonly handled as a link layer communication failure. This Hellos mechanism is intended to be mainly used when failure detection mechanisms provided by the link layer are not sufficient for timely node failure detection.

The Hello extension is designed in the way that one side can use the mechanism while the other side does not. Neighbor failure detection may be initiated at any configured failure detection intervals and at any time, e.g., when nodes first learn about each other or when they are sharing *Resv* or *Path* state too. It is an optional RSVP message and there are two types of *Hello* objects: *Hello Request* and *Hello Ack*. Nodes with no Hello capabilities or not configured for it, can ignore this messages. In this way, reception of Hello messages must not alter the typical operation of any node.

The IP source address is the IP address of the sender node. The IP destination address is the IP address of the neighbor node which receive the Hello. It is intended for use between immediate neighbors, so messages which are being exchanged between immediate neighbors should be set the IP *Time To Live* field of all outgoing messages to 1. However, it could be used as *keepalive* between non neighbors nodes. In this case IP destination address would be the address of a remote node and TTL field would be set to a suitable value bigger than 1.

A. RSVP-TE Hello Message Operation

A node may periodically generates a Hello message containing a *Hello Request* object for each neighbor who's status is being tracked. The periodicity is set in a *Hello Interval* field and default value is 5 ms. For every *Hello Request*, neighbor must send a *Hello Ack*. If no messages are received, via either requests or acks from a neighbor within a configured number of *Hello* intervals (default for this is 3,5 intervals), then a node presumes that it cannot communicate with the neighbor.

When *Hellos* exchanging starts, sender fills in the *Source Instance* field (see figure 3) with a value representing its per neighbor. This value must not change while the agent is exchanging *Hellos* with the neighbor. In the *Destination Instance* field the sender also fills with the *Source Instance* value most recently received from the neighbor. If no value has ever been received from the neighbor or it considers communication to the neighbor have been lost, then it is set to zero (0). The generation of a message should be suppressed when a *Hello Request* was received from the destination node within the *Hello Interval*.

On receipt of a message containing a *Hello Request* object, the receiver must generate a message containing a *Hello Ack* object. The receiver also compares *Source Instance* field value of the sender with the previously received value to verify that the neighbor has not reset. If previous value was zero, and new received value is non-zero, then it considers that neighbor has reset and updates itself with the new value. If non-zero values differ or *Source Instance* field is zero, then the node must treat the neighbor as if communication has been lost. The receiver of a *Hello Request* also compares received *Destination Instance* field with the *Source Instance* field value most recently transmitted to that neighbor. If the neighbor continues to advertise a wrong non-zero value after the configured number of intervals, then node considers that communication has been lost. On receipt of a message containing a *Hello Ack*

(see figure 4), the receiver verifies that neighbor has not reset, comparing *Source Instance* of the sender with the previously received value. If previous was zero, and received value is non-zero, then it considers that neighbor has reset and updates itself with the new value. If non-zero values differs or the *Source Instance* field is zero, then the node treats the neighbor as if communication has been lost. The receiver of a *Hello Ack* object also verifies that neighbor is not advertising a wrong value in the *Destination Instance* field, in such case node treats the neighbor as if communication has been lost. When communication is presumed to be lost as described above, a node may re-initiates *Hello* exchange. Thus, it uses a *Source Instance* value different than the one advertised in the previous *Hello* message and must continue to be advertised to the neighbor until a new reset or reboot occurs, or until another communication failure is detected. If a new instance value has not been received from the neighbor, then node advertises a zero value in the *Destination Instance* field.

B. GoS Extended Hello Operation

In [10] an extension for *Hello* message is proposed for handling nodal faults, relates to the case where a node losses its control state (e.g., after a restart) but does not loose its data forwarding state, as well as for control channel faults, relates to the case where control communication is lost between two nodes. The format of this extended Hello message is:

```
<Hello Message> ::= <Common Header> + [<INTEGRITY>]
+ <HELLO> + [<RESTART_CAP>]
```

In this work a GoS Hello message is proposed with following format:

```
<Hello Message> ::= <Common Header> + [<INTEGRITY>]
+ <HELLO> + [<GoS>],
```

which, besides a Hello object, also includes an object with a GoS request or a GoS ack. GoS nodes will use information of Source and Destination Instances to test connectivity with neighbors in GoSP as explained above. Formats of *GoS*

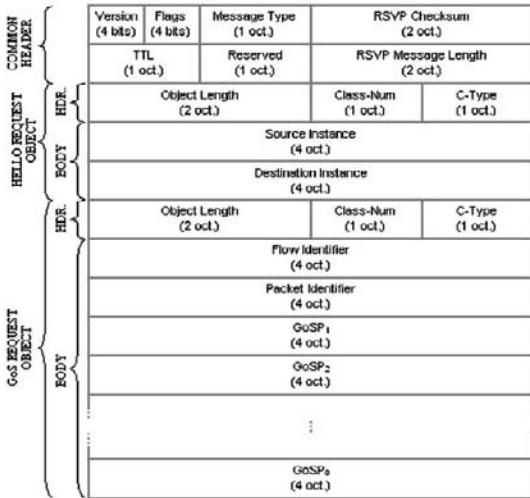


Fig. 3. GoS extended Hello message format, with *GoS Request* object

COMMON HEADER	Version (4 bits)	Flags (4 bits)	Message Type (1 oct.)	RSVP checksum (2 oct.)	
	TTL (1 oct.)	Reserved (1 oct.)	RSVP Message Length (2 oct.)		
HELLO ACK OBJECT	Object Length (2 oct.)		Class-Num (1 oct.)	C-Type (1 oct.)	
	Source Instance (4 oct.)				
GoS ACK OBJECT	Destination Instance (4 oct.)				
	Object Length (2 oct.)		Class-Num (1 oct.)	C-Type (1 oct.)	
BODY			GoS Ack (4 oct.)		

Fig. 4. GoS extended Hello message format, with *GoS Request* object

Request object and *GoS Ack* object are in figures 3 and 4.

The usual state of a GoS node is *data forwarding* state, switching labels and forwarding data packets to the next node. There are only two events that change this state in the GoS node. One of them is detection of a discarded GoS packet. In this case node is able to capture GoS characterization information of discarded packet (see figure 2) and change its state to *request of local retransmission*, to send a extended Hello message with a GoS Request to the first node of GoSP (GoSP₁). When the GoS Hello message is received with an GoS Ack of GoSP₁, it changes to the forwarding state again. The other event that make state changing is receiving from any downstream GoS node an extended Hello message with a GoS Request for a local retransmission. Here the node changes its state to *NMGP search*, to accede to its temporal buffer trying to find the requested packet, according to the information received in the GoS request. If it finds in NMGP the requested packet, it send a GoS Hello message with a GoS Ack object indicating that packet was found and it will be locally retransmitted. After this, it changes to *local retransmission* state, to get the GoS packet from NMGP and retransmit it. After this it will return to initial *forwarding* state. In case of not find the packet in NMGP buffer, it will send a GoS Ack object indicating that packet was not, changing to *request of local retransmission* state, sending a GoS Hello message with the GoS request to the next GoSP node, if it is not the last one. This new GoS request message to the next node in GoSP is shorter than previous one, since that a node does not find the requested GoS packet in the NMGP and it has to request it to next node of GoSP, it first will remove its address of GoS Request object, to simplify the message (see figure 3). So with a bigger crossed diameter in the plane GoS, the GoS messages to send will be simpler.

IV. ANALYSIS AND EVALUATION OF THE PROPOSAL

In this section we will show an analysis of GoS benefits with respect to the delay of packages belonging to privileged flows. We consider an MPLS domain $G(U)$ network with a set X of n nodes and a set U of links. Let δ_{ij} the delay of link $(x_i, x_j) \in U$ and let $\delta(x_i, x_j)$ the delay of a path between two nodes x_i and x_j which can be non-neighbors. Our objective is to minimize the delay used by such packets when are transmitted between two any nodes of the path $LSP_{i,n}$ of $U(G)$:

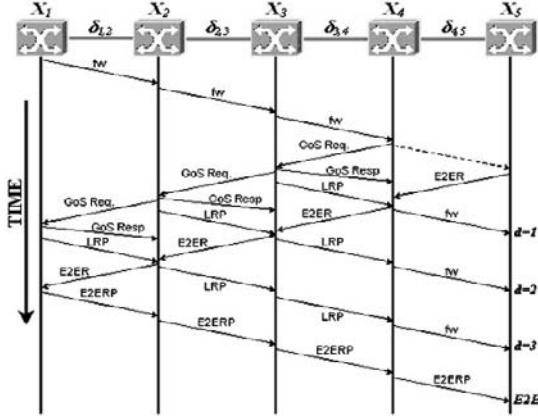


Fig. 5. Operation after a packet discard in intermediate node X_4 , using 3 GoSP diameters to get a local retransmission and compared with an ideal case of end to end recoveries (Fw: packet forwarding; E2ER: end to end retransmission request time; LRP: locally recovered packet).

$$\min \delta(x_i, x_j) = \sum_{i=1}^n \sum_{j=1}^n \delta_{ij} x_{ij}, \quad (3)$$

$$\text{subject to: } \sum_{l=2}^n x_{il} = 1 \quad (4)$$

$$\sum_{i=1}^n x_{il} - \sum_{j=1}^n x_{lj} = 0, \quad l = 2, 3, \dots, n-1 \quad (5)$$

$$\sum_{l=1}^{n-1} x_{ln} = 1, \quad (6)$$

where $\delta_{i,i} = 0, \forall i \in N$; $x_{i,j} = 1, \forall (x_i, x_j) \in LSP_{i,n}$ and $x_{i,j} = 0, \forall (x_i, x_j) \notin LSP_{i,n}$.

A. End to End Retransmissions

Let x_n a non-GoS congested end node. In case of packet discarding by x_n , then function *Discarding Detection Time* (DDT_{e2e}) between two nodes of $LSP_{i,n}$ is:

$$DDT_{e2e}(x_i, x_n) = \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1}. \quad (7)$$

Minimal delay of the end to end ($e2e$) retransmission is:

$$\delta_{e2e}(x_i, x_n) = 2 \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1}. \quad (8)$$

So total delay $\Delta_{e2e}(x_i, x_n)$ to get discarded flow in x_n is got from (7) and (8):

$$\Delta_{e2e}(x_i, x_n) = 3 \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1} \quad (9)$$

B. If Congested End Node x_n is GoS Capable

Let x_n a GoS congested end node. In case of packet discarding by x_n , then *Discarding Detection Time* (DDT_d) between source and sink nodes of path $LSP_{i,n}$ is:

$$DDT_d(x_i, x_n) = \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1} \quad (10)$$

Minimal delay of local retransmission using a *GoSP* with diameter d (δ_d) is:

$$\delta_d(x_i, x_n) = 2 \sum_{l=n-d}^{n-1} \delta_{l,l+1} x_{l,l+1}, \quad (11)$$

subject to: $0 < d < n-i$

If diameter in Eq. (11) was $n-i$, then if $l = n-d = n-(n-i) = n-n+i = i$, we get that:

$$2 \sum_{l=n-d}^{n-1} \delta_{l,l+1} x_{l,l+1} = 2 \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1}, \quad (13)$$

i.e., it would be and $e2e$ retransmission.

Moreover, if in Eq. (11) *GoSP diameter* was bigger than $n-i$, then it would be trying to get a retransmission from a previous node to x_i , but this one is the source of data flow, so it is unfeasible. Thus, total delay $\Delta_d(x_i, x_n)$ to get discarded traffic from initial instant of transmission is got from (10) and (11):

$$\Delta_d(x_i, x_n) = \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1} + 2 \sum_{l=n-d}^{n-1} \delta_{l,l+1} x_{l,l+1} \quad (14)$$

At this point we test if (14) $<$ (9):

$$\sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1} + 2 \sum_{l=n-d}^{n-1} \delta_{l,l+1} x_{l,l+1} < 3 \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1} \quad (15)$$

$$2 \sum_{l=n-d}^{n-1} \delta_{l,l+1} x_{l,l+1} < 2 \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1} \quad (16)$$

So according to Eq. (8) and Eq. (11), we only need to verify in Eq. (16) that $\delta_d(x_i, x_n) < \delta_{e2e}(x_i, x_n)$. The only condition that distinguishes the members of (16) is the set of values of variable l . We only need to demonstrate that l takes a lesser number of values in $\delta_d(x_i, x_n)$ than in $\delta_{e2e}(x_i, x_n)$:

$$n-1-(n-d) < n-1-i; \quad n-1-n+d < n-1-i; \\ -1+d < n-1-i; \quad -1+1+d < n-i; \quad d < n-i, \quad (17)$$

We get that the problem is kept in feasibility zone, since Eq. (17) is one of the restrictions of (12). Thus, it has been demonstrated that $\Delta_d(x_i, x_n) < \Delta_{e2e}(x_i, x_n)$. So, Eq. (14) offers delay benefits: Eq. (14) – Eq. (9) > 0 , improving (3):

$$\Delta_{e2e}(x_i, x_n) - \Delta_d(x_i, x_n) = 2 \sum_{l=i}^{n-d-1} \delta_{l,l+1} x_{l,l+1} \quad (18)$$

Consider an MPLS domain with a congested sink node. We have joined four GoS nodes in the LSP to improve performance of a privileged flow $\phi(x_i, x_n)$. Figure 6 shows a comparative between no congested traffic, $e2e$ case (using $e2e$ retransmissions) and three cases of local retransmissions (with $d=1$, $d=2$ and $d=3$). At 1320 ms, only 213 packages have been correctly received in the sink node. In *GoSP diameter*=3 case, sink node has already received 270 packets node, with $d=2$ 370 packets and in case of using $d=1$, sink has received 627 packets in the same interval of time.

C. If a Congested Intermediate Node x_{DD} is GoS Capable

Let x_{DD} a GoS congested intermediate node. In case of packet discarding by x_{DD} , then *Discarding Detection Time* (DDT_d) between source and congested node x_{DD} is:

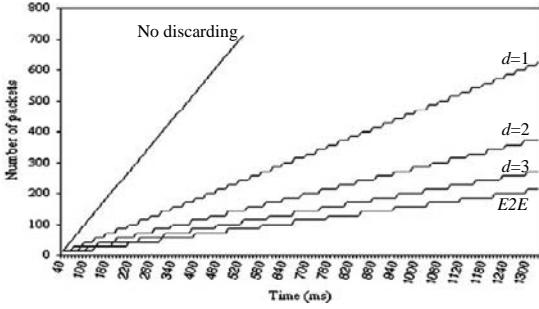


Fig. 6. Delay comparative between, local retransmissions and E2E, with congestion only in sink node

$$DDT_d(x_i, x_{DD}) = \sum_{l=i}^{DD-1} \delta_{l,l+1} x_{l,l+1} \quad (19)$$

Minimal delay of the *e2e* retransmission is:

$$\delta_d(x_i, x_{DD}) = 2 \sum_{l=DD-d}^{DD-1} \delta_{l,l+1} x_{l,l+1}, \quad (20)$$

subject to: $0 < d \leq DD - i$, (21)

If diameter in Eq. (20) was bigger than $DD - i$, then it would be trying to get a retransmission from a previous node to x_i , but this one is the source of data flow, and this is unfeasible. (In this case, retransmission from source node x_i ($d = DD - i$), brings improvement with respect to *e2e*, because x_{DD} is a previous node to x_n , i.e.: if $DD < n \Rightarrow DD - i < n - i$, so it is a local retransmission. So total delay $\Delta_d(x_i, x_n)$ to get discarded traffic from initial instant of transmission is got from (19) and (20):

$$\begin{aligned} \Delta_d(x_i, x_n) &= DDT_d(x_i, x_{DD}) + \delta_d(x_i, x_{DD}) + \sum_{l=DD}^{n-1} \delta_{l,l+1} x_{l,l+1} = \\ &= DDT_{e2e}(x_i, x_n) + \delta_d(x_i, x_{DD}) \end{aligned} \quad (22)$$

At this point we test if $(22) < (9)$:

$$\sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1} + 2 \sum_{l=DD-d}^{DD-1} \delta_{l,l+1} x_{l,l+1} < 3 \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1}. \quad (23)$$

Optimizing, we get:

$$2 \sum_{l=DD-d}^{DD-1} \delta_{l,l+1} x_{l,l+1} < 2 \sum_{l=i}^{n-1} \delta_{l,l+1} x_{l,l+1} \quad (24)$$

So according to Eq. (8) and Eq. (11), again we only need to verify in Eq. (24) that $\delta_d(x_i, x_n) < \delta_{e2e}(x_i, x_n)$. As in Eq. (17) we get that the problem is kept in feasibility zone. So Eq. (22) offers delay benefits: Eq. (22) – Eq. (9) > 0 , improving Eq.(3):

$$\Delta_{e2e}(x_i, x_n) - \Delta_d(x_i, x_n) = 2 \left(\sum_{l=i}^{DD-d-1} \delta_{l,l+1} x_{l,l+1} + \sum_{l=DD}^{n-1} \delta_{l,l+1} x_{l,l+1} \right) \quad (25)$$

Consider an MPLS domain with a path LSP_{in} . The last $n-i$ nodes are discarding packets. Figure 7 shows a comparative between no congested traffic, *e2e* case (using *e2e* retransmissions) and three cases of local retransmissions (with $d=1$, $d=2$ and $d=3$). At 3730 ms, only 171 packages have been correctly received in the sink node. In *GoSP diameter=3* case, sink node has already received 213 packets node, with

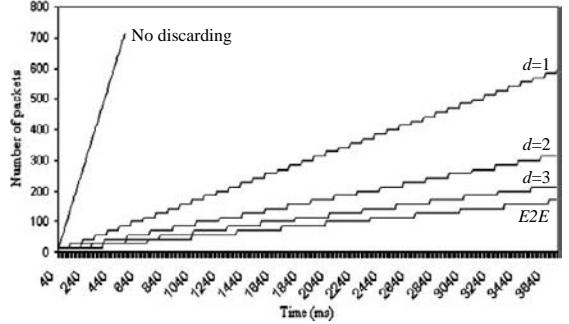


Fig. 7. Delay comparative between, local retransmissions and E2E, with congestion in last $n-1$ nodes

$d=2$ 313 packets and in case of using $d=1$, sink has received 598 packets in the same interval of time.

V. CONCLUSION

This work proposes GoS as a traffic local recovery technique in an MPLS domain in order to improve performance of privileged data flows. We have first discussed the requirements for GoS over MPLS. We have then shown that by introducing a limited number of RSVP-TE protocol extensions it is possible GoS signaling to such privileged data flows that require reliability. The proposed technique has been analysed and demonstrated the benefits due to local retransmissions of discarded traffic with respect to end to end retransmissions.

REFERENCES

- [1] Geng Yanhui, et al. "A novel approach to improve the performance of MPLS-based VPN," The 8th Russian-Korean International Symposium on Science and Technology, July 2004, pp. 35-39 vol. 1.
- [2] Taesang Choi. "Design and implementation of an information model for integrated configuration and performance management of MPLS-TE/VPN/QoS," IFIP/IEEE 8th International Symposium on Integrated Network Management. March 2003, pp. 143-146.
- [3] Young-Tak Kim. "DoomiMan for guaranteed QoS provisioning in next generation Internet," IEEE/IFIP Network Operations and Management Symposium, April 2004, pp. 877-878 Vol.1.
- [4] Ionescu-Graff, et al. "Quantifying the value propositions of MPLS evolution; why and when to migrate to a converged MPLS core?," 11th Int. Tel. Network Strategy and Planning Symp., June 2004, pp.45-50.
- [5] Butenweg, S. "Two distributed reactive MPLS traffic engineering mechanisms for throughput optimization in best effort MPLS networks," 8th IEEE Int. Symposium on Comp. and Comm., 2003, pp. 379-384.
- [6] Fowler, et al. "QoS path selection exploiting minimum link delays in MPLS-based networks," Proceedings IEEE Systems Comm., Aug. 2005.
- [7] Suryasaputra, R. Kist, A. A. Harris, R.J. "Verification of MPLS traffic engineering techniques," 13th IEEE International Conference on Networks, Nov. 2005.
- [8] Fowler, S. Zeadally, S. "Priority-based congestion control in MPLS-based networks," Adv. Industrial Conference on Telecommunications. IEEE AICT/SAPIR/ELETE, July 2005, pp. 332-337.
- [9] G. Siganos, "Powerlaws and the AS-level Internet topology," ACM/IEEE Transactions on Networking, Aug. 2003, vol. 11, pp. 514-524.
- [10] RFC3473: GMPLS Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions, January 2003.

This work is sponsored in part by the Regional Government of Extremadura (Education, Science and Technology Council) under GRANT N° PDT05A041

Operators Preserving Products Of Hurwitz Polynomials And Passivity

Guillermo Fernández-Anaya and José-Job Flores-Godoy
Departamento de Física y Matemáticas, Universidad Iberoamericana
México, D. F. 01490 MÉXICO

Abstract-In this work it is presented a new class of operators on polynomials which preserve realness of roots and interlacing relationships; certain products of Hurwitz polynomials are preserved. In particular, sufficient conditions to preserve complex Hurwitz polynomials and strictly passivity are given. A new property of the operator derivative for Hurwitz polynomials and strictly passive rational functions is presented.

I. INTRODUCTION

As is pointed out in [1] and [2] the concept of positive realness of a transfer function plays a central role in Stability Theory. The definition of rational Positive Real functions (PR functions) arose in the context of Circuit Theory. In fact, the driving point impedance of a passive network is rational and positive real. If the network is dissipative (due to the presence of resistors), the driving point impedance of the network is a Strictly Positive Real transfer function (SPR function). Thus, positive real systems, also called passive systems, are systems that do not generate energy. The celebrated Kalman-Yakubovich-Popov (KYP) lemma [1], established the key role that strict positive realness plays in the design of Lyapunov functions associated to the stability analysis of Linear Time Invariant (LTI) systems with a single memory-less nonlinearity. For Hurwitz polynomials some work has been made based in the properties of “hyperbolic” polynomials i.e., polynomials with only real zeros, but almost nothing using results on preservation of properties in “hyperbolic” polynomials. In the case of preservation of passivity based in these properties, as we know no work has been made.

In this paper based in a new class of operators on polynomials which preserve realness of roots and interlacing relationships, certain products of polynomials closed under Hurwitz property are preserved. In particular, sufficient conditions to preserve complex Hurwitz polynomials and strictly passivity are given. For instance, a new property of the operator derivative for Hurwitz polynomials and strictly passive rational functions is presented.

II. PRELIMINARIES

This section presents the notation and definitions which will be used throughout the paper.

Let \mathbb{Z} and \mathbb{Z}^+ denote the integers and positive integers respectively, \mathbb{R} be the field of real numbers; \mathbb{C} the complex plane, \mathbb{C}^+ the open right-half complex plane; \mathbb{C}^- the left-half complex plane; for $z \in \mathbb{C}$ such that $z = \sigma + j\omega$, with $\sigma, \omega \in \mathbb{R}$ and $j = \sqrt{-1}$ the imaginary unit; the real part of

$z \in \mathbb{C}$ is denoted by $\operatorname{Re}\{z\} = \sigma$; Let $R[s]$ be the ring of real polynomials and $R(s)$ be the field of real rational functions. Let H be the set of Hurwitz stable polynomials. The degree of a polynomial $p(s)$ is denoted by $\deg[p(s)] = n$, with $n \in \mathbb{Z}^+$. Let \mathbb{R}^n be the vector space on \mathbb{R} with vectors of n components. Similarly, for the vector space \mathbb{R}^m .

Consider the rational function

$$G(s) = \frac{n(s)}{d(s)} = \frac{a_n s^n + \dots + a_0}{b_m s^m + \dots + b_0}$$

the relative degree of $G(s)$ is the integer $\deg[d(s)] - \deg[n(s)] = m - n$, when $m - n \geq 0$, $G(s)$ is said to be a proper rational function.

A. Preliminary Definitions

In this subsection, we give a list of basic definitions used in this work.

Definition 1. An n^{th} degree polynomial with real coefficients $p(s) = s^n + a_1 s^{n-1} + \dots + a_0$ is Hurwitz stable if all its roots, i.e., $p(s) = 0$ have negative real part. Also a simple root is a root from the polynomial with multiplicity one. \square

Definition 2 ([3]). The Hadamard product of two polynomials $p(s), q(s) \in R[s]$, is defined by

$$p \circ q = a_k b_k s^k + a_{k-1} b_{k-1} s^{k-1} + \dots + a_0 b_0$$

with

$$p(s) = a_n s^n + a_1 s^{n-1} + \dots + a_0$$

$$q(s) = b_m s^m + b_1 s^{m-1} + \dots + b_0$$

where $k = \min(n, m)$. \square

Let $p_0(s)$ and $\delta(s)$ be polynomials and define S to be the set of $\lambda \in \mathbb{R}$ for which $p_0(s) + \lambda \delta(s)$ is stable. In general, little can be said about the set S . For certain polynomials $\delta(s)$, known as convex directions, the set S is an interval.

Definition 3 ([4]). A polynomial $\delta(s)$ is a convex direction if for all polynomial $p_0(s)$ with $\deg[p_0(s)] \geq \deg[\delta(s)]$ we have that the stability of the polynomials $p_0(s)$ and $\delta(s) + p_0(s) \triangleq p_1(s)$ imply the stability of $p_0(s) + \lambda \delta(s)$ for all $\lambda \in \mathbb{R}$. Equivalently, the polynomials $p_0(s)$ and $p_1(s)$ are stable if and only if the set of polynomials

$$\{p(s) : p(s) = \lambda p_1(s) + (1-\lambda) p_0(s), \lambda \in [0, 1]\}$$

is stable. Directions $\delta(s) = p_1(s) - p_0(s)$ for which this proposition is true are called convex directions. \square

Now we recall some definitions of products which will be useful in the sequel.

Definition 4 ([3]). The circle-point product (\odot) of two standard real polynomials

$$f(s) = f_n s^n + \dots + f_0$$

$$g(s) = g_n s^n + \dots + g_0$$

is the polynomial

$$(f \odot g)(s) = \sum_{k=0}^n k! f_k g_k s^k$$

\square

In the following definition we introduce a new product of polynomials.

Definition 5. The Wagner product (\otimes) of two real polynomials $f(s)$ and $g(s)$ is the polynomial

$$(f \otimes g)(s) \triangleq \sum_{k \geq 0} \alpha_k \beta_k s^k (1-s)^{d-2k}$$

with

$$\alpha_k = \frac{[(1-s)^{-n_f} f(s)]^{(k)}}{k!}, \quad \beta_k = \frac{[(1-s)^{-n_g} g(s)]^{(k)}}{k!}$$

where $n_f \triangleq \deg[f(s)]$, $n_g \triangleq \deg[g(s)]$ and

$$d = \deg \left[\sum_{k \geq 0} \zeta_k \eta_k s^k (1+s)^k \right]$$

with

$$\zeta_k = \frac{[(1+s)^{-n_f} f\left(\frac{s}{1+s}\right)]^{(k)}}{k!}, \quad \eta_k = \frac{[(1+s)^{-n_g} g\left(\frac{s}{1+s}\right)]^{(k)}}{k!}$$

The Wagner product is bilinear. \square

Definition 6. A real polynomial $f(s)$ can be decompose in its even part $f_e(s)$ and its odd part $f_o(s)$ as

$$f(s) = f_e(s^2) + s f_o(s^2)$$

\square

Definition 7. Define the linear operator $\bar{\otimes}_h(f(s)) : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ as

$$\bar{\otimes}_h(f(s)) \triangleq (h \otimes f_e)(s^2) + s(h \otimes f_o)(s^2)$$

Notice that

$$\bar{\otimes}_h(f(s)) \neq h \otimes (f_e(s^2) + s f_o(s^2))$$

However, the operator $\bar{\otimes}_h$ is linear. \square

III. PASSIVITY PRESERVING OPERATORS AND PRODUCTS

In this section the main results are given. The results are based on the definitions of products and operators of the previous section.

Theorem 8. If $h(s)$ has all its roots in the interval $(-\infty, 0)$, it is simple-rooted, and $f(s)$ is a Hurwitz stable polynomial, then $\bar{\otimes}_h(f(s))$ is a Hurwitz stable polynomial. \square

Proposition 9. If the real polynomial $h(s)$ has all its roots in the interval $(-\infty, 0)$, and $f(s)$ is a Hurwitz stable polynomial, then $\bar{\otimes}_h(f(s))$ is a Hurwitz stable polynomial. Where the linear operator $\bar{\otimes}_h(f(s)) : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ is defined as

$$\bar{\otimes}_h(f(s)) \triangleq (h \odot f_e)(s^2) + s(h \odot f_o)(s^2)$$

\square

Corollary 10. For each fixed Hurwitz stable polynomial $f(s)$. The linear operator $\Delta_f : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ defined as

$$\Delta_f(g(s)) \triangleq \sum_{k=0}^n \lambda^k f_k g^{(k)}(s)$$

preserves Hurwitz stable polynomials, for each fixed $\lambda \in \mathbb{R}^+$. \square

The linear operators $\bar{\otimes}_h$, $\bar{\otimes}_h$, Δ_f , map Hurwitz real polynomials into Hurwitz real polynomials.

Theorem 11. If $\phi : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ is a linear operator that preserves simple roots and negative real roots. Then the operator $\bar{\phi} : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ defined as

$$\bar{\phi}(f(s)) \triangleq \phi(f_e)(s^2) + s\phi(f_o)(s^2)$$

preserves Hurwitz stable polynomials and it is linear. \square

The linear operators $\bar{\otimes}_h$, $\bar{\otimes}_h$, Δ_f , can be considered as particular cases of Theorem 11.

Definition 12 ([5]). A rational function $q(s)$ of zero relative degree is strictly positive real (SPR0) if and only if $q(s)$ is analytic in $\text{Re}[s] \geq 0$ and $\text{Re}[q(j\omega)] > 0$ for all $\omega \in \mathbb{R}$.

Theorem 13. If $\phi : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ is a linear operator that preserves simple-roots and negative real roots. Then the operator $\bar{\phi} : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ defined as

$$\bar{\phi}(f(s)) \triangleq \phi(f_e)(s^2) + s\phi(f_o)(s^2)$$

1) Preserves complex Hurwitz stable polynomials i.e., if $b(s) = f(s) + jg(s)$ is a complex Hurwitz stable polynomial, then the complex polynomial $\bar{\phi}(b(s))$ is Hurwitz stable.

2) Preserves SPR0 functions i.e., if $\frac{p(s)}{q(s)}$ is a SPR0 function, then $\frac{\bar{\phi}(p(s))}{\bar{\phi}(q(s))}$ is a SPR0 function. \square

Notice that with linear operators preserving Hurwitz stable polynomials is possible to build new classes of products of Hurwitz stable polynomials. Two such examples are the following, let $f(s)$ and $g(s)$ be Hurwitz stable polynomials, and $\phi, \varphi : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ linear operators preserving Hurwitz stable polynomials. Define the product $\circ_{\phi, \varphi}$ of Hurwitz stable polynomials as

$$f(s) \circ_{\phi, \varphi} g(s) \triangleq \bar{\phi}(f(s)) \circ \bar{\varphi}(g(s))$$

where \circ is the Hadamard product as seen in Definition 2. The product $\bullet_{\phi, \varphi}$ of Hurwitz stable polynomials as

$$f(s) \bullet_{\phi,\varphi} g(s) \triangleq \bar{\phi}(f(s))\bar{\varphi}(g(s))$$

The products $\circ_{\phi,\varphi}$ and $\bullet_{\phi,\varphi}$ are linear in each component, associative and preserve Hurwitz stability, but they are not commutative.

Corollary 14. Let $\delta(s) = p_1(s) - p_0(s)$ be a convex direction with $\deg[p_1(s)] = \deg[p_0(s)]$ i.e., the set of polynomials

$$\{p(s) : p(s) = \lambda p_1(s) + (1-\lambda)p_0(s), \lambda \in [0,1]\}$$

is stable. Let $\bar{\phi} : \mathbb{R}[s] \rightarrow \mathbb{R}[s]$ be a linear operator defined as in Theorem 13, then

$$\bar{\phi}(\delta(s)) = \bar{\phi}(p_1(s)) - \bar{\phi}(p_0(s))$$

is a convex direction. \square

The last corollary is a clear consequence for convex directions.

Example 15. The Gauss-Lucas Theorem states that if a polynomial $p(s)$ has its zeros contained in some given convex set K , then its derivative $\frac{dp(s)}{ds}$ has all its zeros in K as well (unless $p(s)$ is constant). In particular, if all the zeros are real, then also all the zeros of the derivative are real. For instance, if all zeros of $p(s)$ are real and negative, then so are the zeros of the derivative (see [5]). In consequence, it is clear that the derivative operator $(\frac{d}{ds})$ is a linear operator preserving simple-roots and negative real roots. In particular consider the following polynomial:

$$p(s) = (s+1)^4(s+2)^3(s+3) \quad (1)$$

with

$$p_e(s) = s^4 + 72s^3 + 417s^2 + 350s + 24$$

$$p_o(s) = 13s^3 + 222s^2 + 489s + 140$$

Applying the derivative operator $(\frac{d}{ds})$ to the Hurwitz stable polynomial $p(s)$ we obtain

$$\begin{aligned} (\frac{d}{ds})[p(s)] &= 4s^6 + 39s^5 + 216s^4 + 444s^3 + 834s^2 \\ &\quad + 489s + 350 \end{aligned}$$

Notice that $(\frac{d}{ds})[p(s)]$ is a Hurwitz stable polynomial by Theorem 11.

Now consider the polynomial

$$\begin{aligned} q(s) &= 2s^8 + 17s^7 + 75s^6 + 232s^5 + 420s^4 + 493s^3 \\ &\quad + 352s^2 + 147s + 25 \end{aligned} \quad (2)$$

with

$$q_e(s) = 2s^8 + 75s^6 + 420s^4 + 352s^2 + 25$$

$$q_o(s) = 17s^7 + 232s^5 + 493s^3 + 147s$$

Applying the derivative operator $(\frac{d}{ds})$ to the Hurwitz stable polynomial $q(s)$ we obtain

$$\begin{aligned} (\frac{d}{ds})[q(s)] &= 8s^6 + 51s^5 + 225s^4 + 464s^3 + 840s^2 \\ &\quad + 493s + 352 \end{aligned}$$

Notice that $(\frac{d}{ds})[q(s)]$ is a Hurwitz stable polynomial by Theorem 11.

Let the rational function $G(s) = \frac{p(s)}{q(s)}$, with $p(s)$ and $q(s)$ given by (1) and (2) respectively. Notice that $G(s)$ is a SPR0 function. Applying the operator $(\frac{d}{ds})$ in the numerator and the denominator, we obtain

$$\begin{aligned} \frac{(\frac{d}{ds})[p(s)]}{(\frac{d}{ds})[q(s)]} &= \frac{2s^8 + 17s^7 + 75s^6 + 232s^5 + 420s^4 + 493s^3 + 352s^2 + 147s + 25}{8s^6 + 51s^5 + 225s^4 + 464s^3 + 840s^2 + 493s + 352} \end{aligned}$$

Observed that $\frac{(\frac{d}{ds})[p(s)]}{(\frac{d}{ds})[q(s)]}$ is a SPR0 function by Theorem 13.

CONCLUSIONS

In this paper we present new linear operators which preserve products of (real and complex) Hurwitz polynomials and strictly passive rational functions. We believe that these results provide an insight into the theory of stability and passive real functions preserved by these products. This can also be extended in several directions. A possible application of the results presented in this paper is in robust stability theory.

REFERENCE

- [1] K. S. Narendra and A. M. Annaswamy, *Stable Adaptive Systems*. Prentice-Hall. Englewood Cliffs, NJ, USA, 1989.
- [2] K. S. Narendra and J. H. Taylor, *Frequency domain criteria for absolute stability*. Academic Press. New York, NY, USA, 1973.
- [3] J. Garloff and D. Wagner. Hadamard products of stable polynomials are stable. *Journal of mathematical analysis and applications*, 202:797-809, 1996.
- [4] S. P. Bhattacharya, H. Chapellat, and L. H. Kell. *Robust Control: The Parametric Approach*. Prentice-Hall, New York, NY, USA, 1995.
- [5] A. Aleman, D. Beliaev, and H. Hedenmalm. Real zero polynomials and Pólya-Schur type theorems. *J. Anal. Math.*, 94:49-60, 2004.

A computer aided tool dedicated to specification and verification of the MoC and the MoF

N. Hamani, N. Dangoumau, and E. Craye

Laboratoire d'Automatique, Génie Informatique et Signal (LAGIS),
Ecole Centrale de Lille, BP.48 59651 Villeneuve d'Ascq cedex, France
Phone: 0033-(0)3 20 33 54 55; fax: 0033-(0)3 20 33 18 99; e-mail: nadia.hamani@ec-lille.fr

Abstract— In this paper, we extend our modeling approach by introducing verification methods so that the design process will be carried correctly. The Model of Component (MoC) and the Model of Function (MoF) are the basic models of our modeling approach. Thus, we formalize some properties of these models and we present the corresponding verification methods. A computer aided tool for specification and verification is developed to illustrate our approach.

I. INTRODUCTION

Operating modes of Automated Production Systems (APS) are characterized by coherence and safety constraints. The main difficulty is to insure mode changing while guaranteeing the system coherence. The solution to this problem relate to modeling methods as well as verification means. Several approaches are proposed in the literature [6]. These approaches focus on modeling, without dealing with verification of the proposed models. That is why we extend in this paper our modeling approach of *mode handling* [3][5] by developing formal verification tools so that this design process will be performed correctly. We introduce some properties of the obtained models and we propose some verification methods using graph theory. The aim is to handle the verification stage of the design process.

In the following section we present briefly the main characteristics of our modeling approach for *mode handling*. We extend this process by integrating appropriate verification methods. Section 3 presents some properties of the MoC and the MoF and the corresponding verification methods. In section 4, we illustrate our propositions through an application example.

II. A MODELING APPROACH FOR MODE HANDLING

We proposed in [3] a modeling method for *mode handling* of APS. The system is modeled using a Functional Graph (FG) obtained according to an analysis approach based on production goals. We should determine the main goals for which the system was designed and the sub goals that allow to reach them; each sub goal can be decomposed in the same manner until obtaining the initial goals. These are the leaves of the graph; they are related to the resources which perform the initial goals. The behavior of the resources and the functions is then specified. For each function or resource, several concurrent families of modes are determined according to a multipoint of view method. The obtained

models representing the behavior of the resources and the functions are respectively called Model of Component (MoC) and Model of Function (MoF). They are the basic models of this design approach. The behavior represented by these models is characterized by a set of concurrent state-transition graphs (the set is called a family of modes and the graphs are called modes). The incompatibilities and constraints are taken into account in the design process by the addition of some specifications to respect them; called mechanisms.

1) *Specification of the modes*: This specification process is based on the point of view concept, which allows characterizing a resource according to the observer's criteria. For example from the exploitation point of view, the system is characterized according to two points of view: production and maintenance. These points of view can be characterized by other points of view. The method determines a set of families of modes and generic modes representing the behavior of a production system [3].

2) *Specification of the Models of Component*: The specification of the MoC (Fig. 1) follows three steps:

1st step- *specification of the static part*: This step consists in listing the states that can take the system. The modes which characterize an elementary component are the same ones as those which characterize a production system.

2nd step- *specification of the dynamic part*: This step consists in determining at first the initial states of the model then the change-of-state conditions. A matrix form called Matrix of the Change-of-state Conditions (MCC) is used to represent these conditions within a mode.

3rd step- *study of the coherence of the modes*: This study begins with the development of the Matrix of Coherence of the Modes (MCM) (also called Matrix of Compatibility) which characterizes the incompatibilities of the states. When two states are incompatible their simultaneous activation is not possible and this should be taken into account in the specifications. We distinguish forbidden states and transient states. The forbidden states correspond to situations that should not occur. So any switching to these states must be forbidden. The transient states are states from which we can only go through without staying (the switching is considered as instantaneous). The activation of such states causes then a switching to compatible states. In order to guarantee the coherence of the MoC, a specification solution called mechanism is proposed for each case. Then it is necessary to

report the specifications resulting from the mechanisms on the final MoC.

Following the previous steps, the final MoC is obtained. The example represented in Fig. 1 shows two families of modes: production and maintenance. The family of production modes includes: shutdown mode (PS), working mode (PW), Functioning mode (PF), and production mode (PP). For instance, PF mode contains two states: normal state (PF-n) and degraded state (PF-d). A meaningless state is represented in each mode. The notation proposed in [3] is used in this paper for representing the states, the modes and the families of modes.

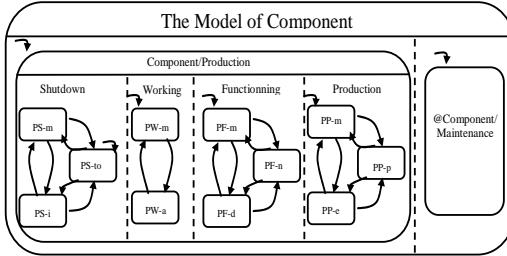


Fig. 1. Example of a Model of Component [3].

3) Specification of the Models of Function: A function is characterized by its availability, its using context (the configurations and their versions) and the states (behavior) of the corresponding subsystem according to its modes. The states of the subsystem are obtained in the same manner as for the MoC. Fig. 2 shows an example of a MoF.

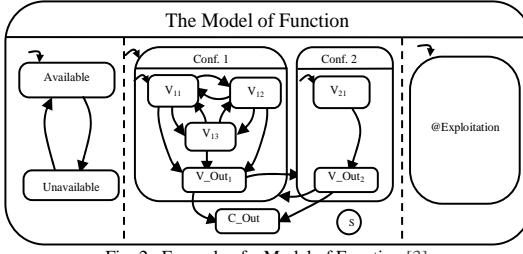


Fig. 2. Example of a Model of Function [3].

For clarity reasons, the change-of-state conditions are not represented in Fig. 1 and Fig. 2.

4) Integration rules: Some rules are defined in order to handle the interactions between the models designed in the previous stages. These rules depend on the kind of the relationships that characterize the functional modeling (necessity, alternative), the considered point of view (production, maintenance) and the current context (configuration and version) [3].

III. FROM SPECIFICATION TO VERIFICATION

The specification of the behavior of the resources and the functional subsystems is carried out using the MoC and the MoF. The following concepts are used to represent both the MoC and the MoF [3]: For static part: families of modes, modes, states. For dynamic part: initial state, change-of-state conditions, events. For mode coherence: incompatibility,

switch and forbidden mechanisms.

We use the mathematical model of state-transition graphs to formalize the MoC (resp. the MoF), this will be explained in subsection III.B. First, we present in the following the specification and the verification process (Fig. 3) of the MoC (resp. the MoF). These models fulfilling some properties can then be integrated for the design of the mode handler.

A. The analysis and verification process

We start with representing each mode determined in the specification stage. The constrained modes are then organized in families of modes. The constraints are taken into account through the incompatibilities between the states listed in the MCM. The families of modes are then integrated to obtain the MoC (resp. MoF). At this stage, we should verify that the graphs representing the modes are correctly specified (i.e. properties of the modes). Then it is necessary to check the coherence of each family of modes (i.e. properties related to the coherence of the families of modes).

If one of the properties related to the modes or the families of modes is not verified it is necessary to reconsider the method of implementing the incompatibilities or the earlier steps i.e. the structural and functional decomposition of the APS and the determination of the modes.

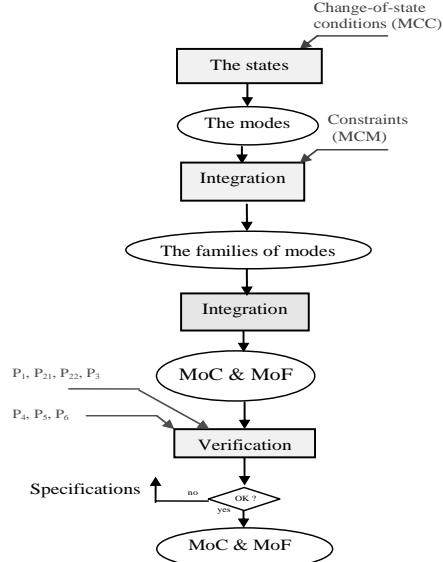


Fig. 3. Modeling and verification of the MoC and the MoF.

The obtained MoC (resp. MoF) verify the required properties and can be re-used for the design of the mode handler. This verification process allows an early correction of specification errors; otherwise they lead to a considerable cost of correction of the final model.

B. Specification of the modes using state-transition graphs

The specified modes can be represented using directed state-transition graphs. The states correspond to the tops of the graph and the transitions correspond to the edges. Each

transition is labeled and the label corresponds to change-of-state condition. Therefore, handling the modes and consequently the states of an entity is carried out using labeled transition systems, each one represents a mode.

Definition 1. The states of an entity (or a system) in a mode are represented by a directed state-transition graph. Each top of the graph represents a state in a mode and the label corresponds to the change-of-state condition.

The formal definition of a labeled state-transition system is given below [2].

Definition 2. A labeled state-transition system on an alphabet A is a quintuplet $[S, T, \alpha, \beta, c]$ where:

- $[S, T, \alpha, \beta, c]$ is a directed graph,
- S is a set of states (instead of nodes),
- T is a set of transitions (instead of edges),
- α and β are two applications of T in S that to each edge, associate its origin $\alpha(t)$ and its goal $\beta(t)$.
- c is an application of T in A: $c(t)$ is called the label of the transition t.

In our model, the alphabet A corresponds to the combinations of events that cause mode changing of an entity.

The change-of-state conditions in a mode are listed in a Boolean matrix known as incidence matrix of the graph [4]. There are as many matrices as modes taken into account.

The definition given below presents some concepts related to graph theory [1][4]. We need these concepts later.

Definition 3. We call incidence matrix of a graph $G = [S, T, \alpha, \beta, c]$ the matrix $W(G)$ such as:

$$W(G) = w_{ij} \text{ with} \\ \begin{cases} w_{ij} = 1 & \text{if } (i, j) \in T \\ w_{ij} = 0 & \text{otherwise} \end{cases}$$

$(i, j) \in T$ corresponds to the directed transition (of top i towards the top j).

For verification, we use the calculations below related to the incidence matrix:

- The out-degree of top i, noted $d^+(i)$ is the arithmetic sum of the edges number outgoing of top i.
- The in-degree of top i, noted $d^-(i)$ is the arithmetic sum of the edges number entering the top i.
- A graph transitive closure is represented using the matrix: $\hat{W}(G) = W^{[0]} + W^{[1]} + W^{[2]} + \dots + W^{[k]}$..., where

$$\begin{cases} W^{[0]} = I & \text{(Boolean matrix unit)} \\ W^{[1]} = W \end{cases}$$

With $k > n-1$ (n is the order of the incidence matrix W). In practice, we stop as soon as: $W^{[k+1]} = W^{[k]}$. We use a practical calculation of transitive closure with the Boolean theorem of the binomial [1], which is written as follows: $[I + W]^{[k]} = I + W + W^{[2]} + \dots + W^{[k]}$. The terms to be calculated are:

$$[I + W]^{[2]}, [I + W]^{[4]} \dots \text{until: } [I + W]^{2^{p+1}} = [I + W]^{2^p}$$

- Some properties need to use change-of-state conditions in the incidence matrix. In this case, we will have:

$$w_{ij} = \begin{cases} c_{ij} & \text{si } (i, j) \in T \\ 0 & \text{otherwise} \end{cases}$$

$(i, j) \in T$ corresponds to the directed transition (of top i towards the top j).

The constraints between the modes belonging to the same family are represented using a matrix form as shown in the following.

Definition 4. The constraints are taken into account through compatibility relations between states. They are specified in the MCM [3] in which the lines and the columns represent the states. $MCM_{(e_{ik}, e_{jl})}^{(m_i, m_j)}$ represents the compatibility of the states e_{ik} and e_{jl} (with $e_{ik} \in m_i, e_{jl} \in m_j$). This matrix is built as follows:

$$MCM_{(e_{ik}, e_{jl})}^{(m_i, m_j)} = 1 \text{ if the states } e_{ik} \text{ and } e_{jl} \text{ are compatible,}$$

$$MCM_{(e_{ik}, e_{jl})}^{(m_i, m_j)} = 0 \text{ if not.}$$

For example, the states PS-m and PW-a belonging respectively to PS and PW modes, are compatible whereas the states PS-m and PF-m belonging respectively to PS and PF modes are incompatible.

C. Properties and verification

A top-down approach is used for the specification of the MoC and the MoF. We start with the identification of the families of modes, the modes and then the states. The verification is a bottom-up process as explained in the following.

The state-transition graphs representing the modes belonging to the same family (definition 1) are constrained. Thus, the expression of properties and their verifications are carried out in three steps.

- We consider first the state-transition graphs that represent each mode belonging to the same family: some properties being verified are introduced and the corresponding verification methods are presented. This stage concerns the state-transition graphs specified for each mode and taken independently from each other.

- After considering the modes separately, we introduce in a second stage the properties related to the modes belonging to the same family.

- A MoC (resp. a MoF) is characterized by a set of families of modes. It is assumed that the families of modes are not constrained so we introduce the properties related to these models.

1) The modes: In this stage, we verify the structural properties of the state-transition graph representing a mode. The verification of these properties uses mainly the incidence matrix of the graph defined above (definition 3). Some properties will be presented in the following.

Property 1. Deadlock-freeness

Every state within a mode must be deadlock-free.

Verification: We have to verify that whatever the top i of the graph, its out-degree $d^+(i)$ is not null.

$$\forall G = [S, T, \alpha, \beta, c], \forall i \in S, d^+(i) \neq 0$$

- In the incidence matrix, for a given top, the corresponding line should not contain only zeros. So there is at least an edge whose initial extremity is the top i.

Property 2.1. Reachability

Every state within a mode must be reachable.

Verification: We have to verify that whatever the top i of the graph, its in-degree $d^-(i)$ is not null.

$$\forall G = [S, T, \alpha, \beta, c], \forall i \in S, d^-(i) \neq 0$$

- In the incidence matrix, for a given top, the corresponding column should not contain only zeros. So there is at least an edge whose final extremity is the top i.

Property 2.2. Mutual reachability

Every state within a mode must be reachable starting from any other state in the same mode.

Verification: We have to verify that the graph is strongly connected by calculating its transitive closure.

$\forall G = [S, T, \alpha, \beta, c]$, if there is a path between any pair of distinct tops of G, the graph is strongly related.

- All the elements of the transitive closure matrix of a strongly connected graph are equal to 1.

Note: the previous property is not mandatory in all design cases [5].

Property 3. Determinism

Every mode must be deterministic.

Verification: We have to verify that for any top i of which the degree is strictly higher than 1, the labels (the logical expressions) of the transitions cannot be simultaneously true. It is supposed here that two uncorrelated events cannot be simultaneous.

For verification, we use change-of-state conditions according to the incidence matrix (definition 3).

- In this matrix, for the transitions whose top is i, the change-of-state conditions should not be simultaneously true.

2) The families of modes: The structural properties listed above have to be checked for each mode. The incompatibilities of the modes belonging to the same family are taken into within the specification of the state-transition graphs (the change-of-state conditions). We consider the modes within their family and we propose the corresponding properties. At first we introduce the following definition.

Definition 5. At a given moment, the states, which do not belong to the same mode, are simultaneously active in a family of modes.

This is guaranteed by the principles of modeling: the concurrency of the modes belonging to the same family. The following property adds a condition on this definition.

Property 4. Compatibility

Each state should be simultaneously active at least with another state of each one of the other modes in the same

family.

Verification: We have to verify that any state of any mode is compatible with at least one state of the other modes of the same family.

$\forall e_{ki} \in m_k, \forall i, \exists j$ such as $e_{ij} \in M_l (k \neq l)$ is compatible with e_{ki} where e_{ki} and e_{ij} are two states of two distinct modes m_k and $m_l (k \neq l)$ respectively and belonging to the same family.

- In the MCM, for two distinct modes, the line corresponding to each top i should not contain only zeros.

Now we consider the constraints that exist between the states of the modes belonging to the same family in the MoC (resp. the MoF). The constraints are represented by the incompatibilities, which are taken into account in the specification stage. The incompatibilities are provided by the designer and specified in the MCM (definition 4). Thus, we need the list of incompatible states as well as the kind of the mechanisms used to specify the incompatibilities (forbidden and switch mechanisms).

Given two incompatible states A_1 and B_1 ; when using the mechanisms, three solutions can be used to forbid the simultaneous activation of these two states [3]. The forbidden and switching mechanisms are used in Fig. 4. For forbidding, the addition of constraint ‘and not B_1 ’ do not enable switching to B_1 if the state A_1 is already active. For switching, if the state A_1 is active, the condition b_{21} which allows the activation of the state B_1 provokes a change-of-state to A_2 thanks to ‘/’.

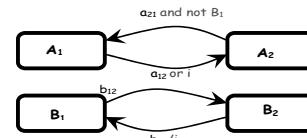


Fig. 4. The forbidden and switch mechanisms.

The method implementing these specifications on the set of concurrent modes of the same family is detailed in [3]. It is based on the asynchronous product of the graphs representing the modes.

The properties being verified on the MoC (resp. le MoF) depend on the kind of the mechanism, more precisely on the change-of-state conditions. Thus, for each state of each incompatible states pair, a forbidden or a switching solution is implemented. The following properties concern these two kinds of mechanisms. To this aim, we look at the change-of-state conditions of the transitions entering and/or outgoing of these states according to the mechanism. The properties correspond to the specifications of Fig. 4. We chose this case because it is specified with both solutions.

Property 5. Reachability - forbidden mechanism

When the forbidden mechanism is used, if one of the states is active the other state remains unreachable (and reciprocally if the forbidden solution is used in the two directions).

Verification: We have to verify that for any forbidden states pair, if one state is active, the change-of-state conditions

associated with the entering transitions of the other state are invalid (and reciprocally).

- In the incidence matrix, if one of the two forbidden states is active, the column corresponding to the other state should include only transitions that are invalid (and reciprocally if the forbidden mechanism is used in the two directions).

Property 6. Reachability-switching mechanism

When the switching mechanism is used, if one of the states is active, the activation of the other state provokes instantaneously a switching of the first state to a compatible state (and reciprocally if switching is caused in the two directions).

Verification: We have to verify that at least one of the outgoing change-of-state conditions from the supposed active state becomes instantaneously valid at the moment of the activation of the other state.

- In the incidence matrix, if one of the two transient states is active, the column corresponding to the other state must include a transition, which instantaneously provokes the switching of the state presumed active. The line corresponding to this last state contains a transition, which instantaneously becomes valid and switches the state to a new compatible one.

3) The MoC (resp. the MoF): According to the point of view concept, a MoC (resp. MoF) is characterized by a set of families of modes. We assume that there is no constraint between those families. Thus the integration of the families of modes in the MoC (resp. the MoF) does not require the addition of particular specifications. As a result the properties verified on the families of modes are unchanged.

Remark. In the same manner, the proposed analysis and verification process can be applied to the specifications related to the *alternatives* and *availability* parts of the MoF. Indeed, the properties related to the graphs representing the modes remain valid for the graphs representing the *alternatives* and the *availability*.

Table I summarizes the proposed properties. Their significance and the corresponding mathematical properties of state-transition graphs are given. To illustrate our approach a computer aided tool implementing all the steps from specification to verification is currently developed with Java (using Jbuilder 9). Fig 5 represents the main user interfaces of the tool.

IV. EXAMPLE

Let us consider a loading robot of a flexible manufacturing cell to illustrate our approach. The MoC of this example is represented in Fig. 6. The figure shows two families of modes: production and maintenance; only production family is represented. PF mode includes a meaningless state (PF-m), normal state (PF-n) and out of order state (PF-o).

Taken the modes separately, only the verifications made for PF mode are presented. The other modes of MoC are

verified in the same manner. We present then the verifications related to the modes belonging to the same family.

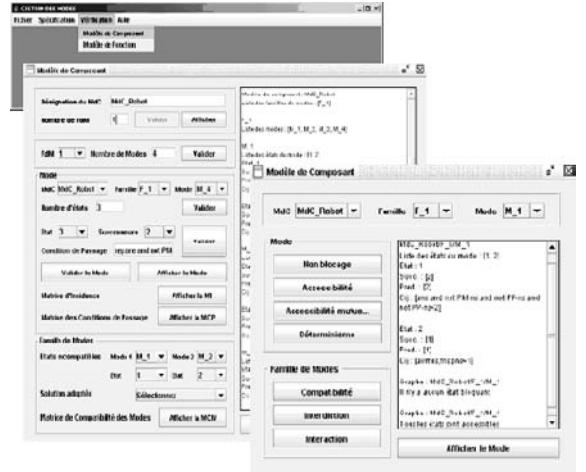


Fig. 5. User interface of the design aided tool.

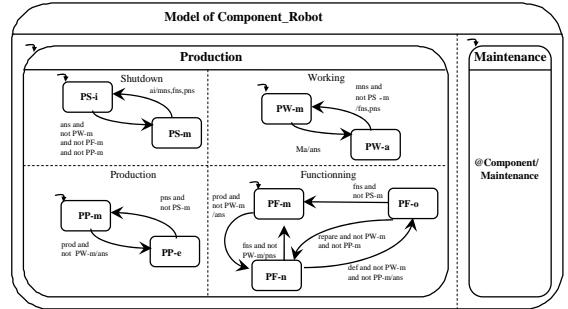


Fig. 6. The production family modes of the MoC_Robot.

The incidence matrix associated with PF mode is given in table II. The incidence matrix of PF mode is completed with change-of-state conditions; we obtain the matrix of table III.

TABLE II
PF MODE INCIDENCE MATRIX

States	PF-m	PF-n	PF-o
PF-m	0	1	0
PF-n	1	0	1
PF-o	1	1	0

TABLE III
CHANGE-OF-STATE CONDITIONS OF PF MODE

States	PF-m	PF-n	PF-o
PF-m	0	prod and not PW-m/ans	0
PF-n	fns and not PW-m	0	def and not PW-m and not PW-m/ans
PF-o	fns and not PS-m	repare and not PW-m and not PW-m/ans	0

Table IV represents the MCM of the MoC_Robot, which we use to verify property 4. Properties 5 and 6 use the incidence matrices completed with change-of-state conditions.

For PF mode, **properties 1**, **2.1** and **2.2** are proved because the out-degrees as well as the in-degrees are not null. In addition, all the elements of the transitive closure matrix are equal to 1. **Property 3** is proved because if there is more than one change-of-state condition in the line corresponding to any state, they are never simultaneously true. For example, the transitions that start from PF-0, have the change-of-state conditions '*fns and not PS-m*' and '*repare and not PW-m and not PP-ms*' that are not true at the same time because the events '*fns*' and '*repare*' are not correlated. **Property 4** is proved because for two distinct modes, the line corresponding to each top does not contain only zeros.

According to MCM (Table IV) the MoC of the robot has 12 incompatible state pairs. In order respect the incompatibility of the states pair (PW-m, PP-e) in the specifications, the designer chooses both forbidding and switching mechanisms. For PW mode, **property 5** is proved because if PW-m is active the condition '*prod and not PW-m/ans*' which allows PP-e activation in PP mode is invalid. PP-e is unreachable as long as PW-m is active because it is conditioned by '*not PW-m*'.

For PP mode, **property 6** is proved because if PP-e is active, the condition ‘*mns and not PS-m/fns,pns*’ which allows PW-m activation in PW mode causes instantaneously PP-e switching to PP-m. So, if the condition, which enables PW-m activation, is true, the one that switches PP-e (i.e. ‘*pns and not PS-m*’) to PP-m is also true. PP-m is compatible with PW-m. PW-m and PP-e are called transient states.

All the properties are proved for the production family of the MoC_Robot. If one of the properties is not proved it is necessary to reconsider the specification stage as needed.

V. CONCLUSION

For safety requirements of *APS mode handling*, models must be provided with adequate verification methods and tools. In this paper, we extend our modeling approach by introducing adequate verification methods. We proposed some properties for the design process of the MoC and the MoF. The properties are independent of the context and should be respected whatever the modeled system is. The approach is based on graph theory. We illustrated it through an example of a loading robot. A computer aided tool was developed to help the designer for the specification and the verification of the models dedicated to *mode handling*.

This study will be continued to verify other properties within the design process. The verification approach can be extended to deal with the model representing the behavior of the APS.

REFERENCES

- [1] A. Alj, R. Faure, *Éléments de la théorie des graphes, Guide de la recherche opérationnelle*, T.1. Les fondements, France: Masson, 1986.
 - [2] A. Arnold, I. Guessarian, *Mathématiques pour l'informatique*, France: Masson, 1993.
 - [3] N. Dangoumau, "Contribution à la Gestion des Modes des Systèmes Automatisés de Production," Ph.D. dissertation, Université des Sciences et Technologies de Lille, Lille, France, 2000.
 - [4] M. Gondran, M. Minoux, *Graphes et Algorithmes*, Collection de la Direction des Etudes et Recherches d'Electricité de France, Ed. Eyrolles, 1995.
 - [5] N. Hamani, N. Dangoumau, E. Craye, "Design analysis and verification of the Model of Component," in *Proc. 10th Int. Multi-Conf. on Advanced Computer Systems (ACS 03)*, Miedzyzdroje, Poland, 2003, pp. 271-285.
 - [6] N. Hamani, N. Dangoumau, E. Craye, "A comparative study of Mode Handling approaches," in *Proc. 35th Int. Conf. on Computers & Industrial Engineering (CIE 05)*, Istanbul, Turkey, 2005.

TABLE I
THE PROPERTIES OF THE MoC (RESP. OF MOF)

Properties	Designation	Correspondence with the properties of state-transition graphs
Modes	P ₁	Deadlock freeness the out-degree $d^+(i)$ of each top i of the graph is not null
	P ₂₁	Reachability the in-degree $d^-(i)$ of each top i of the graph is not null
	P ₂₂	Mutual reachability the graph is strongly connected
Families of modes	P ₃	Determinism each top of the graph which has more than one outgoing edge, the labels cannot be simultaneously true
	P ₄	Compatibility in the MCM, for two distinct modes, the line corresponding to each top i should not contain only zeros
Families of modes	P ₅	Reachability- forb. mec. if one of the states is active, the other state is unreachable
	P ₆	Reachability-swit. mec. if one of the states is active, it should be switched from the moment of the activation of the other state

TABLE IV
MCM OF THE PRODUCTION FAMILY OF MoC-ROBOT

Directionality Based Preventive Protocol for Mobile Ad Hoc Networks

Hetal Jasani, Yu Cai

hjasani, cai@mtu.edu

School of Technology

Michigan Technological University

Houghton, MI 49931

Kang Yen

yenk@fiu.edu

Department of Electrical and Computer Engineering

Florida International University

Miami, FL 33174

Abstract

Novel preventive link maintenance scheme based on directional antennas has been proposed to extend the life of the link for Mobile Ad Hoc Networks (MANET). We use the ability of directional antennas to orientate radio signals into the desired directions. To be more specific, preventive orientation warning is generated and sent to previous node in the path to initiate directional pattern. Link is considered in danger when received packet power is close to minimum detectable power. We call orientation handoff to the process of changing the pattern of antenna from omnidirectional to the directional. We do a comparative performance study between omnidirectional and directional antennas for DSR (on-demand routing protocol) using simulation with OPNET. By using directional antennas, substantial gain is achieved in terms of end-to-end delay, aggregate throughput, and routing overhead. The proposed scheme is general and can be used with any other on-demand routing algorithms.

Key words

Directional Antennas, Mobile Ad Hoc Networks, Dynamic Source Routing (DSR), and Medium Access Control (MAC) Layer, On-Demand Routing Protocols.

I. INTRODUCTION

Typically, omnidirectional antennas have been used to communicate with other nodes for communication in Mobile Ad Hoc Networks (MANET). Omnidirectional antennas may not be efficient due to the limited range of communications. Directional antennas may be useful to increase network efficiency by directing the transmitted power in the desired direction towards target location. Due to the mobile nature of Ad Hoc Network nodes in their applications, it is important to observe the effect of directional antennas on network layer. We propose novel scheme of link life extension by using directional radiation pattern, which helps to avoid or delay route rediscovery operation in routing protocol. Route rediscovery operation is expensive process in terms of network resources and control overhead. Recently, there has been increasing interest in developing protocols at link layer and network

layer for Ad Hoc Networks where nodes are equipped with directional antennas [3, 4, 6, 8, 10, 12, 14]. Previous researchers have shown, directional antennas based communications increase throughput because of better spatial reuse of the spectrum [5, 7, 8, 11, 13]. By exploiting capabilities of directional antennas, we propose a novel preventive link maintenance scheme that yields better throughput, lower end-to-end delay, and decrease routing overhead.

In traditional routing algorithms of wired, wireless and mobile networks, a change of path (route) occurs in one of two cases: (i) a link along the path fails; or (ii) a shorter path is found. A link failure is very expensive since: (i) multiple retransmissions/timeouts are required to detect the link failure; (ii) a new path has to be found and used (in on-demand routing) since spare path may not be readily available. In wired networks, route rediscovery is not very expensive since paths don't fail very frequently. Routing protocols in mobile and wireless networks also follow the same model although they have significantly higher frequency of path disconnections. For each link break (in IEEE 802.11 standard), three MAC (Medium Access Control) layer retransmissions (total of four time-outs including the original transmission) are required before a link is considered broken. A preventive link maintenance scheme proposed here initiates local recovery action early by detecting that a link is likely to break soon and uses directional antenna pattern to prevent link failure and thus extend the life of the link and reduce the cost of link failure. The scheme maintains connectivity by proactively establishing a "higher quality" link when the quality of a link in use becomes suspect. Note the similarity to on-demand protocols: we replace link failure, with the likelihood of failure as the trigger mechanism for directional antenna orientation instead of sending RERR (Route Error packet) to source node, which initiates costly operation of route rediscovery for new path from source to destination. We study the effectiveness of proposed preventive link maintenance scheme by simulating with OPNET software [1] for DSR routing algorithms [2, 16]. Our scheme can be used for any other kinds of routing algorithm.

II. RELATED WORK

Recently there have been several papers that have looked into the problem of data link layer and routing layer design for Mobile Ad Hoc Networks where nodes are equipped with directional antennas [4, 6, 8]. Most of the work towards the use of directional antennas has concentrated on MAC layer. The directional antenna models used in various papers include switched beam antennas (the antenna is sectored and one of these sectors is used depending on the direction of the communicating node), multi-beam antennas (here more than one beam can be used simultaneously), and adaptive antenna arrays.

Bao, et al. [6] developed slotted scheduling-based MAC protocols for networks, in which nodes are equipped with directional antennas. The directional antenna considered is a multi-beam adaptive array antenna, which is capable of forming multiple beams. Assumption for the protocols was that nodes could engage in several simultaneous transmissions. Authors developed the neighbor-tracking scheme that is then used to schedule transmissions by each node in a distributed way. Nasipuri, et al. [4] proposed a directional CSMA/CD mechanism that utilizes a switched beam antenna array and assumes that the gain of the directional antenna is equal to the gain of an omnidirectional antenna. The transmitters use omnidirectional antennas to transmit RTS frames and the receiver antennas remain in omnidirectional mode. Assuming the receiver is idle; it receives the RTS and transmits CTS, again using an omnidirectional antenna. The transmitter estimates the angle of arrival (AoA) of the CTS being received and transmits data using the directed antenna beam. Since the transmissions and receptions involving omnidirectional antenna patterns are susceptible to collisions, this mechanism suffers from high probability of packet error. The authors used a switched beam antenna array that could only switch among a limited number of antenna patterns.

Choudhury, et al. [8] and Takai, et al. [7] have suggested the use of directional virtual carrier sensing (DVCS), in which a Directional Network Allocation Vector (DNAV) is constructed. The DNAV table stores the angle of arrival of RTS packets along with the duration of data transmission in any given direction. Thus, when the medium access control layer receives a packet from an upper layer, along with the angular profile of the destination node with respect to the source node, the DNAV table is consulted to determine whether the angle overlaps with any of the ongoing transmissions. If there are no overlaps, the packet is transmitted; otherwise, packet transmission is deferred in accordance with a back off mechanism.

Ramanathan [11] proposed the scheme for considering higher transmission range using beamforming

antennas. He discussed the issues more related to MAC layer and didn't discuss the issues related to the performance of the network layer. Very little work [9,15] related to the work presented in this paper has been published on preventive maintenance using directional antennas. Preemptive routing [15] proposed keeps track of signal strengths and look forward to route repair procedures before a link breaks. Router Handoff [9] is the strategy of finding another path preemptively before link actually breaks and pass routing information to another suitably situated node after local recovery. However, both work don't utilize the ability of directional antennas for the routing performance improvement. In this paper, we focus on preventive link maintenance scheme for improving the performance of reactive routing protocols such as DSR.

III. ANTENNA MODEL

A directional antenna module is implemented in OPNET [1]. There are two separate modes of operations of this model: omnidirectional and directional [8]. In normal operation, the omnidirectional mode is used, while the directional mode is used for both transmission as well as reception after preventive orientation warning has been generated due to decreasing signal strength in received packet. Nodes can interchange the modes with negligible latency or delay. We use multiple directional antennas (N) to avoid the sweeping operation and sweeping delay [17] that presents in the case of single switched beam antenna. Use of multiple directional antennas would also solve the deafness problem [17] since other antenna elements would be available to listen other communication in other directions.

In Omnidirectional mode, a node is capable of receiving signals from all the directions with a gain of G_O . In the Directional mode, a node can point its beam towards a specified direction with gain G_d (with G_d typically greater than G_O). Moreover, the gain is proportional to the number of antenna beams (i.e., inversely proportional to the beam-width). Since more energy can be concentrated towards a particular direction, this results in an increased coverage and transmission range. Though it is not feasible to have a complete non-overlapping pattern practically, we assume the non-overlapping pattern for directional antennas. To model antenna side lobes, we assume that the energy contributed to the side lobes is uniformly distributed in a circular area. For simulation purpose, we also assume that the side lobe gain is fixed and is set to a very small value.

IV. PREVENTIVE LINK MAINTENANCE SCHEME

We propose a novel directional link maintenance scheme based on signal strength. We name it Preventive Link Maintenance (PLM) scheme since we take preventive

action before link actually breaks. We replace weak omnidirectional link with high quality directional link to extend the life. More specifically, the scheme consists of two components: (i) detecting that a link is likely to be broken soon; and (ii) establishing a directional link to it. Determining when link quality is no longer acceptable (which generates a preventive link maintenance warning) is a crucial component of the proposed scheme. The link quality can incorporate several criteria such as signal strength, the age of a link, and rate of collisions. In this paper, we assume the link quality to be a function of the signal strength of received packets. Since most link breaks can be attributed to link failures due to *node motion* in a typical ad hoc scenario, the signal strength offers the most direct estimate of the ability of the nodes to reach each other. We should keep in mind that signal power variations due to fading and similar temporary disturbances do not generate erroneous preventive link maintenance warnings and hence creation of directional link.

If directional link is established successfully before the omnidirectional link breaks, the cost of overhead for detecting a likely broken omnidirectional link (the retransmit/timeout time) is eliminated using preventive link maintenance. In other words, the cost for creating directional link is justified since the route recovery is initiated locally before the current link actually breaks. Eventually, it helps to improve the performance in terms of reduced latency (end-to-end delay), higher throughput, and reduced routing overhead.

When the signal power of a received packet drops below an *orientation threshold*, the preventive link maintenance warning is generated. The value of this threshold is significant to the effectiveness of the algorithm – if the value is too low, there will not be sufficient time to create directional pattern before the link breaks. However, if the value is too high, the warning is generated too early with negative side effects of unnecessary computing for creating directional link. Likewise, the moving nodes may change direction and the current link never breaks, rendering the preventive action an unnecessary overhead. Generating the preventive link maintenance warning is complicated due to fading that can cause sudden variations in the received signal power.

The decision to create directional link is made by a node based on measured signal strengths of its neighbors with whom it forms part of an active route. We maintain power information at nodes in terms of the *received power*. The decision to create high quality directional link because of weak signal strength is made when one end of the link senses that the *received power* has dropped below an *Orientation Threshold* and preventive link maintenance warning is generated. Operation of switching to the directional link from an omnidirectional link is called an *Orientation Handoff*. We incorporate *Orientation Handoff*

into the DSR protocol by making these changes: Each node maintains a *Neighbor Received Power List* containing the received signal strength for last three received packets originating from each neighbor. This list is updated whenever a packet is received. We measure and store three measurements of packet power to check the consistency and take decision accordingly to avoid generating false warnings.

Every node that is part of an active route, checks its predecessor link and next link strengths for each route while receiving the date packet during normal communications (using omnidirectional antennas). If a node detects that *either* the previous or next link strength along an active route is predicted to fall below the *Orientation Threshold*, it initiates *Orientation Handoff*. If orientation with directional antennas cannot achieve strong link creation, no action is taken and the route is allowed to fail and consequently, standard DSR route repair procedure is followed.

Use of time varying directional antenna patterns is envisioned to help in the establishment of directional links in multihop wireless networks that might otherwise not be possible with the use of omnidirectional antennas. We establish the links using directional antennas depending on the condition (signal strength) of the links within network between active nodes. Creation of directional link requires a priori knowledge of the location of the neighbor nodes or transmission/receiving direction. In this paper, we assume that wireless nodes can employ the techniques such as GPS to determine the direction of communications by having position information of nodes and can use that information to orient their antennas.

While establishing the link, the transmitter and receiver may fall into one of the following scenarios. 1) If the transmitter and the receiver are neighbors and the link between them is established by using an omnidirectional antenna, nodes are called *near neighbors*. 2) If two nodes are not near neighbors, they may be *far neighbors*; the link between them is established by using directional antenna. In this scenario, the source and destination node may establish a directional link between *far neighbors* by orienting their receiver and transmitter antennas towards each other. In this case, link is called an *extended link* and neighboring nodes are called *far neighbor*. The decision to establish an extended link between *far neighbors* for data transmission, instead of relying on multiple hops, depends on a number of factors, such as delay in establishing the link, feasibility of a directed link and the cost of the link in terms of its effect on aggregate throughput in the network.

The establishment of an extended link between *far neighbors* requires communications between the transmitter and receiver nodes through immediate link (when they are near neighbors) to allow appropriate orientation of transmitter and receiver antennas. This signaling

information must be exchanged during omnidirectional communications. The neighboring nodes can use an established omnidirectional link to send antenna orientation commands before it gets too late (because of weakening link) for establishment of extended directional link. The establishment of extended links can result in decreasing the end-to-end delay between end nodes (source and destination) since directional link between those intermediate nodes would eliminate (or reduce) the costly operation of route rediscovery. Depending on communication traffic load and relative positions of other nodes, the extended link will have the varying effect of increasing the overall network throughput.

We keep updating the *Neighbor Received Power List* on all the nodes while using directional link. In some mobility pattern, it may be possible to go back and use omni directional antenna when received signal strength is more than orientation thresholds for at least three consecutive received packets.

V. DPMAC PROTOCOL

We modified 802.11 standard protocol [10] to facilitate our proposed PLM scheme. We call it DPMAC, a directional Preventive MAC protocol, for the purpose of evaluating routing over directional antennas. The design of DPMAC is based on the notion of reserving the wireless channel before actual data is transmitted using directional communication. Directional channel reservation is performed using a RTS/CTS handshake with orientation warning flag set (between any two node: lets say *A* & *B*) after orientation warning is received by transmitting node from receiving node. During the omnidirectional communications, DPMAC reserved the channel using RTS/CTS handshake when orientation warning flag is cleared.

When orientation warning is received from node towards destination, transmitting node has to reserve the directional channel by doing RTS/CTS handshake with orientation flag set on it. More specifically, DPMAC specifies the beam to be used for data transmission only after orientation warning is received/generated. To do this, DPMAC maintains a direction look-up table, a cache, containing fields; *NeighborId*, *AntennaBeam*. Once orientation warning is received, the antenna system beamforms in the direction of the intended node and senses the channel using the specified *AntennaBeam*. Note that even though node *A* was using the channel in the omni mode while sending previous data packets, carrier sensing has to be performed again, to beamform in a particular direction to continue data transmission. This is necessary because the directional beamforms have a higher gain. If node *A* senses the carrier busy by using its directional beam, it postpones RTS transmission until the medium is

once again idle. If the medium is free, node *A* proceeds through the steps of waiting for a DIFS period and backing off for a random interval (similar to the steps in IEEE 802.11 [10]) before it transmits the RTS with orientation warning flag set.

Node *B*, while idle, listens to the carrier in omni mode and receives the RTS meant for it. The RTS is received with omnidirectional gain G_o and received signal strength, P_r . While the RTS is being received in the *Omni* mode, node *B* is susceptible to collision due to signals arriving from other directions. Channel is reserved via normal 802.11 protocol. When P_r is below the orientation threshold, routing layer will generate orientation warning towards transmitting node (source node). DPMAC at node *B* will send ACK in omni mode with orientation flag set on it. When node *B* receives the RTS with orientation warning flag set, it now determines the antenna beam on which the received signal power of the RTS was maximum, and uses that same beam to send back a CTS with orientation flag set on it. Node *B* may also use the location./position information stored in the direction look-up table to beamform towards the transmitting node after it has received this flagged RTS. The CTS is transmitted in the directional mode of operation with orientation flag set on it. Sending back the CTS is also preceded by carrier sensing and waiting for SIFS duration, as in 802.11. Node *A* in the meantime remains beam-formed towards *B* and receives the CTS directionally, with directional gain G_d . Once the RTS/CTS handshake is accomplished, node *A* starts the data transmissions directionally to node *B*. Node *B* receives the data packet using the same beam that it used for sending the directional CTS.

VI. PERFORMANCE EVALUATION

A. Simulation Environment

Now, we illustrate simulation scenario that uses the developed antenna models along with OPNET [1] to characterize network performance. The wireless communication channel is modeled by 13 pipeline stages including antenna gains, propagation delay, signal-to-noise ratio, calculation of background noise and interference noise, transmission delay, etc. This powerful simulation environment enables designers to create realistic wireless scenarios. In this work, we have modified the MANET node model to make it to work with four individual antennas. We have used predefined and fixed beams and created an antenna pointer model. The antenna gain pattern specified in the Antenna Pattern Editor is used to provide the gain values. Model includes four different antennas to cover four different directions. The antenna patterns have directional gain of 10 dBm with 90° beamwidth. Orientation threshold of 3 dBm was chosen.

We use the network of 50 nodes placed randomly over area of 2500 x 2500 sq. meter. We have 5 random

sources of CBR (constant bit rate) each of which generates 1024 bytes data packets to a randomly chosen destination at a rate of 2 to 50 packets per second with starting time lag of 10s. All five sources start data transmission with different times. All connections/communications end when simulation ends. We use random waypoint mobility model to simulate different patterns of mobility (speed of nodes and pause time). The DPMAC is used as MAC layer protocol for simulation. Simulations are run for 600 seconds and all results are averaged over 5 different seeds. We compare our results with original DSR.

B. Simulation Results and Discussions

In this subsection, we analyze the simulation results in terms of aggregate throughput, end-to-end delay (latency), and routing overhead. Aggregate Throughput is the total number of bits transmitted from one node to other nodes in the network per unit of time. It is the total traffic sent and received in bits per second for entire network. We collected this statistic in our simulation scenario and compared with original DSR (with omnidirectional antenna nodes). Our PLM scheme performs better in different scenarios since preventive link maintenance scheme allows link to live longer than omnidirectional case. An establishment of directional link postpones the route rediscovery process and also reduces frequent disconnection. Figure 1 shows that aggregate throughput is higher in our scheme using directional antenna. Aggregate throughput (performance) of entire network for our scheme is about 75% higher than original DSR for higher packet/data rate.

End-to-end delay (latency) of packets for the entire network is the time elapsed between the creation of the packet at its source and its destruction at its destination. It is almost half in case of our scheme when we have five flows communicating simultaneously in compare to smaller number of simultaneous flows. In other words, the average end-to-end delay per packet increases much more sharply for original DSR algorithm than our scheme as shown in Figure 2. It can be concluded that routing performance improves when we have many simultaneous connections. It is also because of the number of directional antennas (four) we use in our simulation.

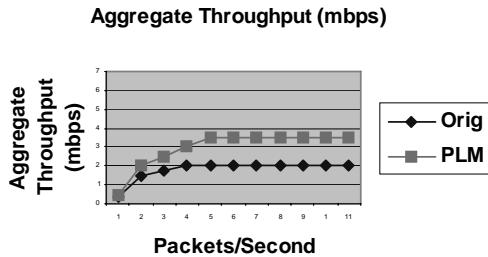


Figure 1. Aggregate Throughput

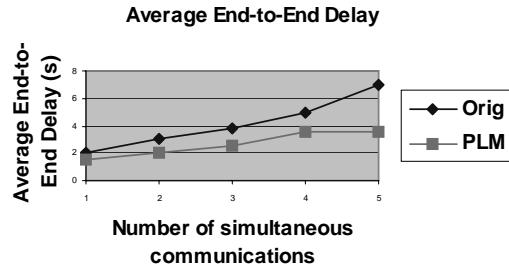


Figure 2. Average end-to-end delay (latency)

Routing overhead per received packet is the ratio of the total number of routing control packets (including RREQ, RREP and RERR) generated/forwarded to the data packets received correctly at the destination. Figure 3 shows that routing overhead is about 40% to 60% less than original DSR. For high mobility scenario, original DSR produce larger routing overhead where as our scheme has lower routing overhead. Routing overhead increases as speed of mobile node increases, but the increment is slight. In summary, our results are encouraging to use PLM scheme for MANET.

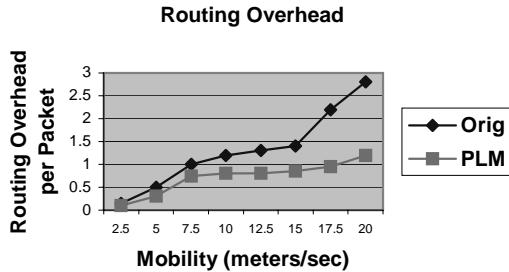


Figure 3. Routing Overhead per Packet

VII. CONCLUSIONS

Directionality based preventive link maintenance scheme is proposed to improve the performance of mobile ad hoc networks. The MAC is modified accordingly to incorporate the proposed scheme using directional antenna. A directional antenna module is implemented in OPNET simulator with two separate modes of operations: omnidirectional and directional. The antenna module has been incorporated in wireless node model and simulations are performed to characterize the performance improvement of DSR Ad Hoc routing protocol. Link breakage happens due to the node movement and subsequent reducing signal strength of receiving packets.

Performance improvement is achieved by orienting neighboring nodes antennas towards each other by using the position/location information of nodes or Angle of Arrival information. It helps ad hoc network to avoid or postpone costly operation of route rediscovery while using on-demand routing protocols. We compare the simulation results of PLM scheme with omnidirectional scheme (original DSR algorithm) by collecting the statistics of aggregate throughput, end-to-end delay, and routing overhead. Use of directional antennas has been found encouraging for on demand routing protocols of MANET using our proposed preventive link maintenance scheme.

REFERENCES

- [1] Online Documentation, “OPNET Modeler”, <http://www.opnet.com/>, Date visited: February 2006
- [2] D.B. Johnson, D.A. Maltz, Y.-C. Hu and J.G. Jetcheva, “The dynamic source routing protocol for mobile ad hoc networks,” *IETF Internet draft (November 2001) draft-ietf-manet-dsr-06.txt*
- [3] H. Dajing, J. Shengming and R. Jianqiang, “A link availability prediction model for wireless ad hoc networks,” *Proc. of the International Workshop on Wireless Networks and Mobile Computing*, Taipei, Taiwan, April 2000.
- [4] A. Nasipuri, S. Ye, J. You and R. Hiromoto, “A MAC protocol for mobile ad hoc networks using directional antennas,” *Proc. of the IEEE Wireless Communications and Networking Conference*, Chicago, Illinois, Vol. 3, September 23-28, 2000, pp. 1214-1219.
- [5] Z. Huang and C. Shen, “A comparison study of omnidirectional and directional MAC protocols for ad hoc networks,” *In Proc. of IEEE Globecom'02*, 2002.
- [6] L. Bao, and J.J. Garcia-Luna-Aceves, “Transmission scheduling in ad hoc networks with directional antennas,” *In ACM/SIGMOBILE MobiCom 2002*, 23-28 Sept. 2002.
- [7] M. Takai, J. Martin, R. Bagrodia and A. Ren, “Directional virtual carrier sensing for directional antennas in mobile ad hoc networks,” *Proc. of the ACM MobiHoc'02*, Lausanne, Switzerland, June 9-11, 2002, pp. 183-193.
- [8] R. Choudhury, X. Yang, R. Ramanathan and N. H. Vaidya, “Using directional antennas for medium access control in ad hoc networks,” *Proc. of the MOBICOM*, Atlanta, Georgia, September 23-28, 2002, pp. 59-70.
- [9] Abhilash P., Srinath Perur and Sridhar Iyer, “Router Handoff: An Approach for Preemptive Route Repair in Mobile Ad Hoc Networks,” *Proc. of High Performance Computing*, 2002.
- [10] IEEE, “Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications”, IEEE Standard 802.11, June 1999.
- [11] R. Ramanathan, “On the performance of ad hoc networks with beamforming antennas,” *Proc. of the ACM MobiHoc*, Long Beach, California, October 4-5, 2001, pp. 95-105.
- [12] S. Roy, D. Saha, S. Bandyopadhyay, T. Ueda, and S. Tanaka, “A network aware MAC and routing protocol for effective load balancing in ad hoc wireless networks with directional antenna,” *In ACM MobiHoc'03*, June 2003.
- [13] S. Horisawa S. Bandyopadhyay, K. Hausike and S. Tawara, “An adaptive MAC and directional routing protocol for ad hoc wireless networks using ESPAR antenna,” *In ACM/SIGMOBILE MobiHoc'01*, Oct 2001.
- [14] M. Sanchez, T. Giles and J. Zander, “CSMA/CA with beam forming antennas in multi-hop packet ratio,” *Proc. of the Swedish Workshop on Wireless Ad Hoc Networks*, March 5-6, 2001.
- [15] T. Goff, N.B. Abu Ghazaleh, D. Phatak and R. Kahvecioglu, “Preemptive Routing in Ad Hoc Networks,” *In Proc. of ACM SIGMOBILE*, Rome, pp.43-52, 2001
- [16] D. Johnson, D. Maltz, “Dynamic source routing in ad hoc wireless networks,” edited by T. Imielinski and H. Korth, Kluwer Academic Publisher, pp. 153-181, 1996.
- [17] R. Choudhury, N. H. Vaidya, “Performance of Ad Hoc Routing using Directional Antennas,” *Journal of Ad Hoc Networks - Elsevier Publishers*, November, 2004.

The Problem of Accurate Time Measurement in Researching Self-Similar Nature of Network Traffic.

I.V. Sychev
IEEE Conference Publishing
21 Ignatevkoe shosse
Blagoveschensk, 675027 Russia

Abstract-This publication gives new results in short time measurement of networking flow. A new method for realistic measurements in short time experiments is designed.

I. INTRODUCTION

The main idea is that long memory property of self-similar (fractal) traffic is able to help forecasting traffic for the purpose of quality of service (QoS) provision. But for pragmatic mathematical forecasting and modeling it needs an accurate information of the real process, especially in measuring high resolution time. Common information about researched types of experiments is presented in part II. At the part III necessity and reasons of building new measurement system are presented. In the same part readers can find general results of measurements. Part IV describes main evidence of pseudo-fractal (caused by measuring error) property in short time experiment. Part V provides explanation of the experimental environment to ensure that the main idea of time measuring in networking has no influence from hardware. And general conclusions are presented in part VI.

II. NETWORKING MEASUREMENT EXPERIMENTS

References [1-11] describe two kinds of networking traffic measurement experiments:

- Long time experiments, as in [6], [9]; collecting traffic for years (using a special database) with integral time resolution (e.g. all traffic every 300 seconds, when 300 seconds is the smallest fragment of measurement).
- Short time experiments, as in [1], [2], [3], [4], [7], [10]; when every traffic package is captured; in these experiments timestamps should have high resolution.

It is very attractive to use short time experiment, since it economizes human time and machine resources - but only if the timestamps are correct. Note that in modern personal computer (PC) it is possible to receive more than one package at 18,20648... Hz – this is the normal PC clock time resolution.

In the referenced articles conclusions are mostly made on the basis of short-time range experiments. Moreover, the experiments use only one measuring device.

There are two kinds of PC traffic measurement systems:

- standard OS equipment programs and hardware;
- special programs and hardware designed for measuring

purpose.

When data are measured, the majority of researchers build traffic simulation systems; then measurements are compared with simulated data and the difference is observed.

The author of this article proposes three stage experiments: fractal traffic simulation, measurements using standard methods and experiments with programs and hardware especially designed for measuring purpose.

Main points of work on the experiments are:

To design a new traffic measuring method to reduce the disadvantages of well known means for network-flow analysis.

To design a new measuring system. Field experiments analysis might ensure traffic self-similarity property.

To design an imitation model of informational systems with client-server architecture, and take into account self-similar data flow.

To compare the designed model with traditional exponential models of queue theory and define fields of models preferred usage.

III. SPECIAL REAL TIME TRAFFIC MEASURING SYSTEM

Results cannot be considered reliable if they are significantly influenced by the measuring device.

Multi-user multitasking operating systems are interrupted by running processes and thus delay networking tasks unpredictably. Furthermore, reprogramming hardware clocks (for monitoring purpose) for faster run may cause problems with other running programs. Possibly programmers avoid reprogramming the clock and simply randomize the timer resolution that is left (for identification purpose). Therefore there is no guarantee that timestamps have high resolution. This may lead to non-realistic conclusions about self-similarity of traffic.

For traffic measuring purpose it's suggested to use device with only one task – measurement.

A new measuring system was built for ISO/OSI level 2 and level 3 to determine whether the flow of traffic is realistic or not.

In experiments with the standard way of time measuring (using PC clocks) it was noted that the error of such measurements is additive by time. This error comes from processing the interrupt routine. Also an error appears as the result of extra interrupts (timer calls) while networking

interrupts are processed. The best solution of this problem is to get timestamp data at the moment of the networking event and to avoid the usage of the PC timer. The proposal is to use the Pentium instruction “Rdtsc”: it returns the count of ticks since processor reset (64 bit) and does not depend on the CPU load. For accurate measurements the program “M2” was built. The program is copyrighted by Federal service for intellectual property patents and trademarks, Russian Federation, (Rospatent, www.fips.ru). The full name is “The program for research of properties of self-similar traffic in real time in Ethernet 10/100BaseT network, with time resolution 10⁻⁶ seconds”. Registration No of the program is: 2006613266.

This M2 program functions to:

- capture time of received packages
- capture time of packages in the net card buffer
- send measured data to the program-receiver

The program also has the following properties:

- uses a counter of completed CPU ticks from the beginning of its run (that is much more reliable than using timer interrupts);
- uses 32-bit registers;
- interacts with the package driver of a net cards for 10 and 100 megabits per second.

Time is converted from CPU ticks to SI units; the time resolution is 10E-8 seconds. Conversion depends on the frequency of the CPU. Frequency does not give accurate values as it depends on temperature, power block voltage and electro magnetic emissions; apparently, there are three ways of possible correction:

- extra software for CPU frequency measurements. Disadvantage of this method is that there is no guarantee that a measured value will not change during the experiment.
- “on the fly” measurement to calculate CPU frequency while running a measurement program. Disadvantages of this method are excessive data for the transfer of measured values and additionally the complexity of the measuring software.
- calculation of a correction by the approximating the flow dynamic; this is the most accurate method, especially in approximating the difference of two measuring systems.

It is proposed to compare the difference in time of the “tcpdump” program and M2 after the conversion of tcpdump data to SI. A fragment of measured data is presented in table 1. Though clock start moment in M2 and tcpdump differs, it has no sense to synchronize the starting moment of both systems: in order to eliminate the difference we can use simple method of constant value subtracting.

Presented data fragment contains data about measured time from 10 packages (numbers of packages are 50 to 60) that can be seen on fig. 1 and fig. 2 (x-axis). This fragment was picked randomly, since including all the measured data would overwhelm frames of this publication. All the presented data are SI units (seconds).

TABLE I
THE DATA FRAGMENT

Package number	M2	Tcpdump	Subtraction
50	1127,92351204	54259,46316700	53131,53965496
51	1128,10860877	54259,56316800	53131,45455923
52	1128,29372190	54259,66316700	53131,36944510
53	1128,44797460	54259,76316700	53131,31519240
54	1128,63308064	54259,86316700	53131,23008636
55	1128,78733035	54259,96316700	53131,17583665
56	1128,94159743	54260,06317600	53131,12157857
57	1129,09585066	54260,18316800	53131,08731734
58	1129,25010479	54260,28316700	53131,03306221
59	1129,40437384	54260,38316700	53130,97879316
60	1129,55862778	54260,48316700	53130,92453922

Graphic shown on Fig. 1. is a linear increasing or decreasing function (before correction) of index i=1..N, where “j” is the number of received/sent packages. The values of this function are the times of receiving/sending a package. From these values we subtract the corresponding values of a linear approximation. Thus, as corrected CPU frequency we use the projection on the axis.

The result of projection is shown on Fig. 2, and presents a pseudo-fractal (self-similar) process caused by measuring error of the tcpdump system.

IV. EVIDENCE OF PSEUDO-FRACTAL PROPERTY

Obviously pseudo-fractal property in short time experiment appears as a result of inaccurate time measuring. Wrong conclusions can be made when using the well-known “tcpdump” as in works in [1],[2],[3],[4],[5]. Reference [4] describes an algorithm of correction tcpdump package lose, but there is no information on time measuring. In the reference [5] the same form pulsations on very small time ranges (6 seconds) are described and named self-similar. That is most probably not realistic.

Fig. 2 shows pulsations that seem to be self-similar not only visually, but can be proved statistically on some segments, e.g. using the Hurst parameter described in [1],[4],[7],[9],[10],[11]. Description of Herst parameter mathematic runs out of this paper frames, but it is sufficiently represented in abovementioned references.

For calculating the Hurst parameter pi was taken as the proportional coefficient on a flow of 654 measurements.

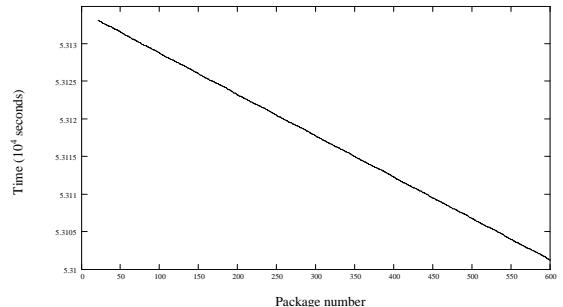


Fig. 1. Difference between two measurement systems.

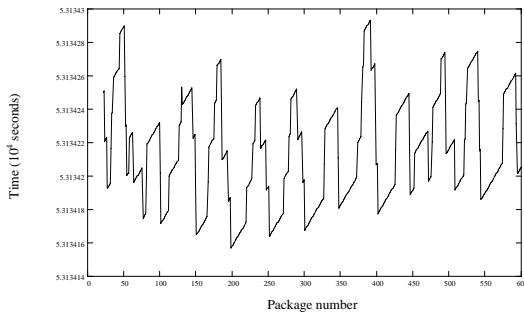


Fig. 2. Difference after correction of the processor frequency.

The data represented by Fig. 2, have Hurst parameter 0.12015, range (R) 4.283919 and standard deviation (S) 1.713238. The obtained data show obvious anti-persistent property of the flow. Thus first, the flow can be predicted with a degree of high probability and, second, the flow can be classified as self-similar.

The described error of traffic measurement is the most probable reason for wrong conclusions about traffic flows' self-similarity property in short-time experiments.

V. THE EXPERIMENTAL ENVIRONMENT

A scheme of network components connection, shown on fig. 4, does not require special equipment and made of standard components.

Qualitatively new result described in part IV does not depend on the net topology. The major idea of presented installation is to use additional measuring systems functioning in the client-server channel. In case of accurate real time operating system usage proposed mechanism can be integrated in operating system of client and server.

Tests of hardware for installation were conducted in the following sequence: IBM GL300 PCs, then Advanced Logic Research (ALR) SD i486, then different laptops and finally Intel Pentium-4 based computers.

Software M2 on host-3 and tcpdump on host-4 are running in promiscuous mode and capture all transmitted packages between host-1 and host-2. The collected data is transferred by extra link. Then it is transmitted by portions in certain guaranteed time (this time is extremely small in comparison with time of experiment duration, and therefore can be disregarded) to the data receiver machine that simultaneously can be a client of analyzed network connection. Fig. 3. presents appearance of installation.



Fig. 3. Appearance of the installation.

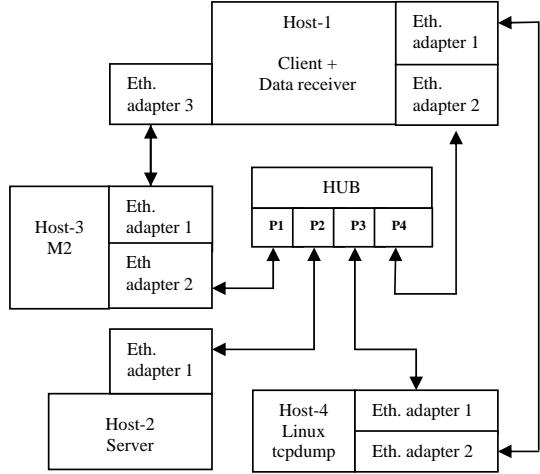


Fig. 4. Measurement system.

VI. CONCLUSIONS.

Obtained knowledge can be effectively used for enhancing QoS in global networks. Moreover, it can assist scientists to defeat research based on non-realistic data.

Conducted work gave the following outcomes:

- possible networking experiments and their stages are analyzed;
- new method of accurate time measurement in networking traffic is designed, and the program product that realizes the method is described;
- the opportunity of usage of Herst parameter – well-known metric for determining self-similarity property of process – is shown;
- discovered possibility of wrong interpretation of obtained data;
- shown basic points for realistic conclusions in conducting small-time measurement experiments.

REFERENCES

- [1] D.E.Sokolov, N.G.Trenogin. Net traffic fractal features in client-server informational system, SybSTU, 2003.
- [2] V.V.Platov, V.V.Petrov. Research of self-similar structure of teletraffic, 2004.
- [3] V.V.Petrov. Teletraffic structure and algorithm of quality of service with self-similar influence, dissertation, Moscow, 2004.
- [4] Peter Haga, Peter Pollner, Gabor Simon, Istvan Csabai, Gabor Vattay, Self-generated Self-similar Traffic, Communication Networks Laboratory, Eotvos Lorand University, 2004.
- [5] Vern Paxson, Experiences With Internet Traffic Measurement and Analysis, ICSI Center for Internet Research International Computer Science Institute and Lawrence Berkeley National Laboratory, 2004.
- [6] Will E. Leland, Murad S. Taqqu, Walter Willinger, Daniel V. Wilson, "On the Self-Similar Nature of Ethernet Traffic", 1993.
- [7] Vitaly Petroff, "Self-Similar Network Traffic: From Chaos and Fractals to Forecasting and QoS", 2003.
- [8] Sergejs Ilnickis, "M/M/1 and G/M/1 systems with a self-similar input traffic", 2004.
- [9] Sergejs Ilnickis, "Research of the network server in Self-similar traffic environment", 2004.
- [10] Kihong Park, Walter Willinger, "SelfSimilar Network Traffic: An Overview", 2000.
- [11] Pradeep Ramakrishnan, "Self-Similar Traffic Models", 1999.

Wi-Fi as a Last Mile Access Technology and The Tragedy of the Commons

Ingrid Brandt, Alfredo Terzoli, Cheryl Hodgkinson-Williams
Departments of Computer Science and Education, Rhodes University
Tel: 046 603-8291 Fax: 046 636-1915
I.Brandt@ru.ac.za, A.Terzoli@ru.ac.za, C.Hodgkinson@ru.ac.za

Wi-Fi.

Abstract—With an alarmingly low teledensity in South Africa, just 12%, and not much hope of further wired infrastructure at the local loop level, as the costs incurred are high compared to potential revenue, wireless connectivity could be a great asset and service in South Africa. However, the use of unlicensed spectrum in building wireless networks can be comparable to “The Tragedy of the Commons”, the result of selfish behaviour towards common and limited resources. This paper evaluates the use of 802.11 wireless technologies in building a broadband wireless network and the effects of high amounts of interference on such a network. The paper concludes that for urban areas 802.11 technologies using unlicensed spectrum is not advisable, unless used in point-to-point links, while its use in rapid rural development (where there is less interference) is very promising.*

I. INTRODUCTION

IN 2002 the total teledensity in South Africa was just 12% with most fixed line telephones located in urban, historically white, residential and business areas, while black rural areas continued to experience teledensities commensurate with the rest of rural Africa, which is around 1% [1]. According to the Genesis report published in 2005 [2], of the 2.8 million lines that Telkom rolled out in compliance with its exclusivity agreement with government, 70% have now been disconnected due to non-payment, leaving South Africa with approximately 5 million fixed lines for 42 million citizens.

In order for more South Africans to benefit from the Information Age and the empowerment that it provides, more and more wireless technologies could be employed in order to affordably connect more South Africans to the Internet and a world of information. Wireless technologies can be easily deployed in areas where teledensity is low and at lower cost than wired alternatives [3], [4]. We should begin to see more telecommunication providers making use of wireless technologies in providing their services to their customers – in both rural and urban areas. Extremely popular today is the IEEE 802.11 range of technologies, commonly referred to as

II. WHAT IS Wi-Fi?

The IEEE 802.11 standard, commonly referred to as Wi-Fi, is part of a family of standards for local and metropolitan area networks. This family of standards deals with the Physical (PHY) and Data Link layers (also known as the Medium Access Control (MAC)) as defined by the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Basic Reference Model. These standards define the protocol and compatible interconnection of data communication equipment via the air – radio or infrared – in a local area network (LAN) using the Carrier Sense Multiple Access protocol with Collision Avoidance (CSMA/CA) medium sharing mechanism [5]. They define the PHY and MAC layers so that they are compatible with the existing standards for higher layers (Logical Link Control and higher) [6], allowing stations to move and roam freely through a wireless LAN (WLAN) and still appear stationary to the Logical Link Control (LLC) sub-layer and above. This allows existing network protocols such as TCP/IP to operate transparently over IEEE 802.11 WLANs [7].

IEEE 802.11b (1999) extends the IEEE 802.11 standard (1999) by building on the data rate capabilities to provide 5.5 Mbps and 11 Mbps payload data rates in addition to the 1 Mbps and 2 Mbps rates [8]. The IEEE 802.11g (2003) further extends the 802.11 standard and the 802.11b extension by building on the payload data rates of 1 and 2 Mbps that use Direct Sequence Spread Spectrum (DSSS) modulation and by building on the payload data rates of the 1, 2, 5.5 and 11 Mbps that use DSSS, Complementary Code Keying (CCK) and optional Packet Binary Convolutional Code (PBCC) modulations. The extended rates of 802.11g provide additional payload data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps [9]. For more detail about the IEEE 802.11 standard, and its “b” and “g” extensions, we recommend reading [5], [8], [9].

802.11 technologies operate in the 2.4 GHz Industrial, Scientific, Medical (ISM) band. The band is divided into evenly sized portions of spectrum, referred to as channels [10]. Each channel is 22 MHz wide and its starting frequency is separated from the next channel’s starting frequency by only 5MHz. Thus, adjacent channels overlap and can interfere with

*This work was undertaken in the Distributed Multimedia Centre of Excellence at Rhodes University, with financial support from Telkom SA, Business Connexion, Converse, Verso Technologies, Tellabs, Stortech, THIRP, and the National Research Foundation.

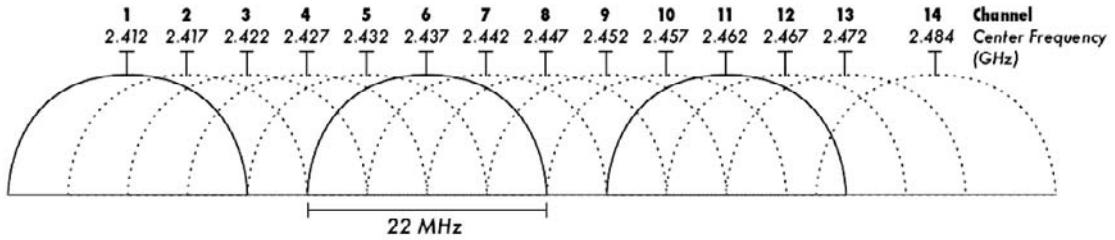


Fig. 1. Channels and center frequencies for 802.11b and 802.11g. Note that channels 1, 6, and 11 do not overlap.

one another. There are only 3 channels that do not overlap and therefore can be used in networks that are adjacent [10]. Figure 1, taken from [10], depicts available channels for 802.11b and 802.11g networks.

There are several advantages and disadvantages to using 802.11 technologies in connecting South Africans to telecommunication services. The advantages of using the IEEE 802.11 standards are low cost, standardisation and interoperability. Standardisation and interoperability make such networks cost-effective and easy to deploy and manage. The greatest disadvantage of 802.11 as a WAN or MAN wireless network is that it is specifically designed to be a LAN network standard and thus not particularly suited to covering distances longer than 100 m [5]. As a result of this another important disadvantage of 802.11 emerges, namely interference. Interference problems within the 802.11 radio frequency range tend to be substantial as many other household appliances operate in the same range [11] such as microwaves, electric door openers, car alarms, cordless phones and Bluetooth devices. More importantly, in building wider area networks, other telecommunication operators also using 802.11 technologies use the ISM band [10]. This can result in large amounts of interference and an unreliable signal, especially in non-point-to-point communication links.

As a result of 802.11 technologies making use of unlicensed spectrum and being so affordable, interference on 802.11 networks tends to be the most obvious obstacle to providing reliable broadband connectivity because it is so widely used. One is reminded of “The Tragedy of the Commons” with respect to the use of 802.11 technologies in unlicensed spectrum.

III. THE TRAGEDY OF THE COMMONS

“The Tragedy of the Commons” is a well known paper written by Garrett Hardin in 1968 and published in Science [12]. Hardin extended the original parable published by William Forster Lloyd in his 1833 book on population. The parable illustrates how unrestricted access to resources such as pastures, the ocean or, we believe, radio frequency (RF) spectrum eventually dooms these resources because of over-exploitation [13]. This over-exploitation occurs because the benefits of exploitation accrue to individuals, while the costs of exploitation are distributed between all those exploiting the

resource. While Hardin, like William Forster Lloyd, was primarily interested in population and especially in the problem of human population growth, he also commented more generally on the use of resources such as the atmosphere and oceans.

Hardin uses the example of the pasture that is shared by local herders in order to make his point clear and understandable. In this example, he assumes that the herders wish to maximize their yield and so will increase their herd size whenever it is possible to do so. The utility of each additional animal has both a positive and a negative component:

- Positive: the herder receives all the proceeds from each additional animal
- Negative: the pasture is slightly degraded by each additional animal

The crucial aspect is that these two components are unequally divided. The individual herder gains all of the positive aspect while the negative aspect is shared between all the herders using the pasture [12], [13]. Thus for an individual herder weighing up these aspects, the rational course of action is to add the extra animal as the positive outweighs the negative. Whenever faced with this choice the herder will always add yet another animal. However, since all the herders reach the same conclusion, over-grazing and degradation of the pasture will be the long-term result. Nonetheless, the rational response for any individual will remain the same each time the decision is faced because the gain is always greater to an individual than the distributed cost. Therein lies the tragedy: the inevitability of it all (unless the “rational” response considers the whole system and not just the individual interest). Thus each herdsman is locked into a system that compounds him to increase his herd without limit, in a resource that is limited [12].

One method of preventing over-use is through regulation. However, Hardin suggests that this “policing of the commons” tends to favour selfish individuals over those whom are more far-sighted [13]. In order to avoid over-exploiting the commons Hardin concludes by quoting Hegel, “Freedom is the recognition of necessity [12].” He suggests that when we interpret freedom as the freedom to do as we please, we create the tragedy of the commons. However, if we recognise resources as commons in the first place and relinquish our freedom to exploit them, realising that they require management then “we can preserve and nurture other and more precious freedoms [12].” Recognising that our commons

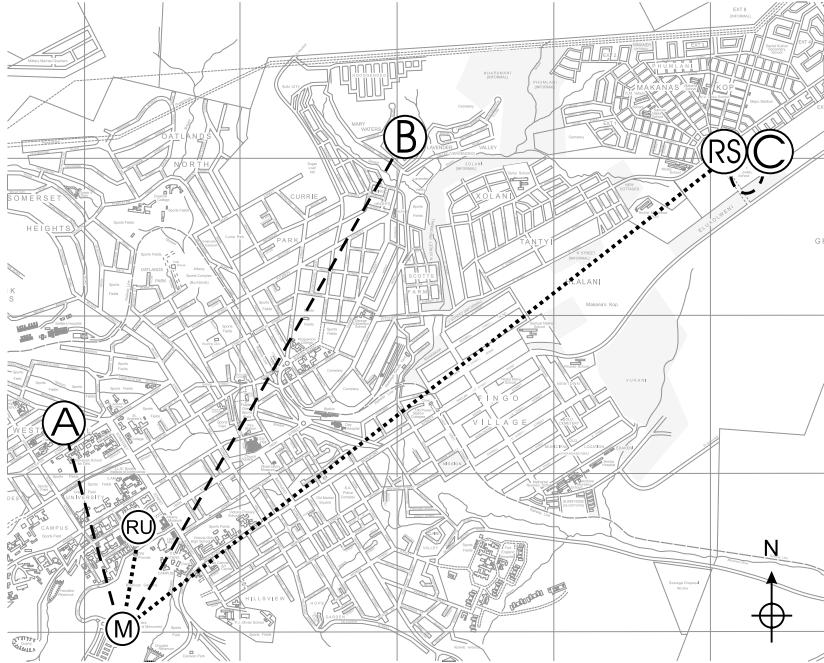


Fig. 2. Grahamstown with wireless network nodes. RU: Rhodes University; M: 1820 Settlers Monument; A: site A; B: site B; C: site C; RS: repeater station

require management would hopefully result in commons not being over-exploited but rather utilised for the common good. By managing our commons well and stipulating in what manners they can be used it is possible to avoid over-exploitation without having to stop making use of the commons altogether.

IV. WI-FI IN THE LAST MILE

At Rhodes University a research team has been working on the problem of integrating ICT into the secondary schools and their curricula. One of the problem areas that schools in South Africa face today is the issue of how they connect the computers in their schools to the Internet. A solution to this problem is to use wireless technologies. To this end the Telkom Centre of Excellence in the Computer Science Department at Rhodes University has been investigating the use of IEEE 802.11b and 802.11g based wireless LAN technologies as a means of connecting these schools to the University and then to the rest of the Internet [14], [15].

The investigation of IEEE 802.11 standards began in 2003 with 802.11b and changed in 2004 to the faster 802.11g. We wanted to cover distances much greater than 100 m as we wished to be able to connect schools that were as far as 10 km from Rhodes University. In order to achieve this we placed an access point with an omni-directional antenna on the 1820 Settlers Monument. The Monument stands approximately 620 m above sea-level (much higher than the buildings in the

town) and is situated on the south western hills, relative to the centre of town (see Figure 2). For the experiment, we replaced the access point's (AP) standard 2 - 3 dB antenna with an 8 dB omni-directional antenna and used 12 dB directional antennas connected to wireless Ethernet bridges at client sites.

The schools in Grahamstown East are unable to see the Monument and thus connections were impossible. We thus decided to experiment with building a wireless repeater station on top of a water tower at one of the schools which could see the Monument (RS in Figure 2, which is 5 km away from the Monument). The repeater consisted of a high gain 22 dB directional antenna aimed at the Monument, on the south-western side of town, connected to a wireless Ethernet access point configured in bridging mode and another access point with an 8 dB omni-directional antenna. This repeater station allowed clients in Grahamstown East to access the Monument via the repeater. A more detailed explanation of this wireless network can be found in [15]. The results of all the experimentation were very promising and interesting in terms of what we learnt about the possibilities of using Wi-Fi technologies in providing last mile access.

During initially testing phases we were able to obtain transfer rates of 2.6 Mbps at site A (1.2 km from the Monument), a client site within the city bowl, and 4 Mbps at site C (see Figure 2). After time these promising results began to taper off as we began to notice a marked increase in the amount of interference in the town. As discussed in section II

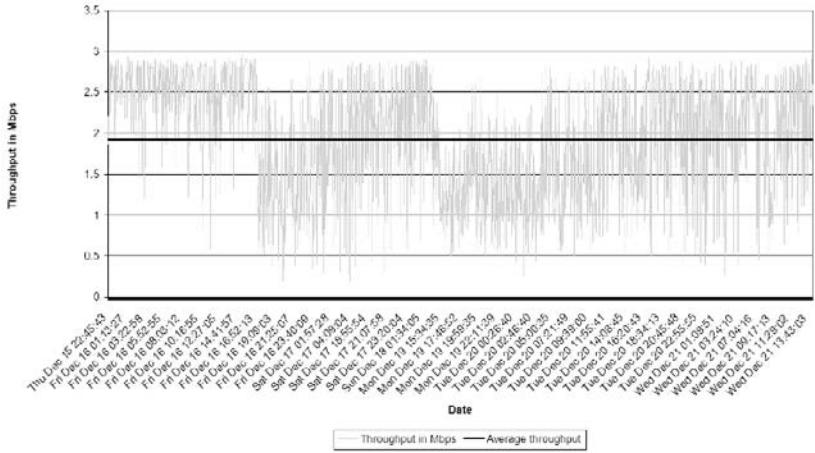


Fig. 3. Throughput from the Monument AP to site C, via the repeater station, in Mbps. The solid black line indicates the average throughput on this wireless link

we are aware that other telecommunication service providers making use of the same 2.4 GHz ISM band will interfere with each other. As interference in Grahamstown increased, we experienced a marked decrease in the quality of the wireless network. On the links closer to the Monument, such as that of site A, we noticed degradation in the signal with slower transfer rates, increased delay and increased packet loss.

On longer distance links, such as that from the Monument to site C and the repeater station, the effects of interference were much more severe. We found that the repeater station was able to make an association with the AP at the Monument on layers one and two of the IEEE 802.11 protocol, but at layer three, IP traffic could not be transferred as the usable signal was too weak. In Figure 4 it can be seen that there was a 100% packet loss when pinging the repeater station. While trying to associate with the Monument AP from the repeater station we were able to “see” wireless AP beacons from the additional wireless networks creating the increased interference. Figure 5 shows the results of a scan for beacons run from the repeater station. The increase in the number of wireless networks resulted in an increased interference for our original wireless network, which explained the degradation in the network performance.

While the connection at site A was not as good as it had been before, the link from the repeater station to the Monument was unusable and thus we needed a method to work around the interference. To that end we replaced our original AP equipment (which had a signal output of 63 mW) with newer equipment whose signal transmission strength was 100 mW. Furthermore, we added a 22 dB directional antenna at the Monument in order to build a direct, point-to-point connection from the Monument to the repeater station. These hardware improvements allowed us to overcome the increased interference in the town.

Eventually the marked increase in interference tapered off again down to a fairly reasonable level and we were then able to add other test sites to our network. With the then decreased interference in the 2.4 GHz band we were able to add site B which is 3.5 km from the Monument to the network. The average throughput to site A was 2.4 Mbps, site B was 1.8 Mbps and site C was 1.9 Mbps. Figure 3 depicts the throughput at site C and provides an example of the graphs generated by throughput testing. This test site was connected to the Monument via the repeater station. Its improved throughput over site B is probably due to the fact that site C is approximately 50 m from the repeater station and the link between the repeater station to the Monument employs two high gain, 22 dB directional antennas. While site B also has a directional antenna of 22 dB, it is communicating with an omni-directional antenna of only 8 dB and thus radio conditions will be worse than the repeater-to-Monument link.

When the interference caused by the additional networks were removed, the original network again was able to successfully provide broadband connectivity in the same way it had prior to the increased interference. These results depict how easily a wireless network operating in unlicensed spectrum can be affected by interference from other networks operating in the same spectrum, especially when employing the use of omni directional antennas in a point-to-multipoint network. Further complications result when the technology has not been designed to overcome such interference, as is the case with 802.11 technologies.

Furthermore, from these results, we can see that when there is little or no interference it is possible to obtain good quality broadband connectivity using 802.11 technologies and that it is possible to overcome signal degradation due to interference by employing directional, point-to-point links only.

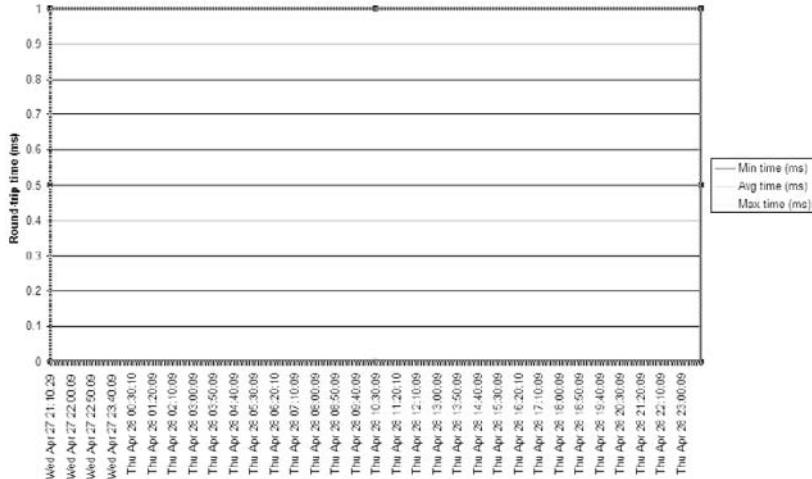


Fig. 4. Returned ICMP ping packets from the repeater station, note there were no ping packets returned (100% packet loss)

Traffic will be disrupted during the channel scan => BSS'es from the selected wireless mode

BSS	Type	Channel	RSSI	BSSID	WEP	SSID
Ad-hoc	2.412	(1)	19	02:02:36:b4:2c:0e	ON	*Mk7lnK#
AP BSS	2.412	(1)	5	00:0f:3d:df:c5:dc	OFF	Rhodes
AP BSS	2.422	(3)	39	00:0f:3d:9f:f6:e7	OFF	scw2
AP BSS	2.437	(6)	14	00:02:6f:35:62:db	ON	amcctai
Ad-Hoc	2.437	(6)	4	02:02:c7:56:58:a5	OFF	PJO
AP BSS	2.437	(6)	15	00:02:6f:37:0a:4b	ON	
AP BSS	2.452	(9)	10	00:0f:3d:df:47:e8	OFF	scw
AP BSS	2.462	(11)	21	00:02:6f:32:26:77	ON	#Ap93kM*
AP: 6, Ad-Hoc: 2. Total BSS: 8						

Fig. 5. Wireless beacons “seen” from the repeater station.

V. SOLUTIONS TO THE TRAGEDY OF THE COMMONS

According to Gardin [12] the solution to the tragedy of the commons is that we should relinquish our freedom to exploit the commons. Does this mean then that we should not make use of 2.4 GHz spectrum and other unlicensed spectrum in providing wireless broadband? We believe the answer depends on the geo-social context. In urban areas, where there is a high density of people, unlicensed spectrum should not be used for long distance connectivity because there will more than likely be a higher concentration of service providers who will want to use such spectrum in order to save on costs. This higher concentration will result in a marked increase in interference which will degrade the signal and network quality for all whom use the unlicensed spectrum.

That is not to say that it is impossible to circumvent interference issues. When using 802.11 (Wi-Fi) technologies it is possible to have more than one operator in the same area if those operators are using point-to-point links in order to connect two sites together. Point-to-point links are more immune to interference than point-to-multipoint links. There

are also some technologies that are designed in order to operate in unlicensed spectrum, in such a way that they are immune to higher interference ratios, such as is claimed for the Motorola Canopy product [16]. Furthermore, as technological advances take place in the fields of software radios and intelligent antennas, it is conceivable that systems may eventually be trained to know what is signal and what is interference, making wireless networks more robust and immune to interfering sources [17], [18].

802.11 technologies can however be extremely useful as a first phase in providing broadband connectivity to people living in rural areas with only one (or more often none) network operator. Here interference sources will mostly likely be relatively limited and thus allow a service provider to connect local communities to a broadband network that can provide them with telephony, data and possibly video services.

VI. CONCLUSION

The use of unlicensed spectrum, such as the 2.4 GHz ISM band which is used in 802.11 (Wi-Fi) technologies, has its place in WAN applications, but we believe that place is in

rural development and not in urban areas - unless point-to-point links are implemented - where there is an increased chance of such networks being susceptible to high interference from other similar networks.

When network operators build wireless networks in urban areas or use wireless technologies to build critical networks they should strongly consider the use of licensed spectrum or point-to-point links in order to insure that their network(s) will not be susceptible to interference from other surrounding wireless networks.

REFERENCES

- [1] A. Gillwald, "Under-serviced Area Licences in South Africa: Steps to achieving viable operators," Feb. 2002, last Accessed Apr. 2006. [Online]. Available: <http://link.wits.ac.za/papers/usal.pdf>
- [2] Genesis Analytics, "Telecommunications prices in South Africa: An international peer group comparison," Occasional Paper No 1/2005, Apr. 2005.
- [3] W. Drew, "Wireless networks: new meaning to ubiquitous computing," *The Journal of Academic Librarianship*, 2003, last Accessed Apr. 2006. [Online]. Available: <http://people.morrisville.edu/~drewwe/wireless/jal-wireless.pdf>
- [4] D. Essex. (1999, Oct.) Wow! Wireless Works! Last Accessed Apr. 2006. [Online]. Available: http://www.healthcareinformatics.com/issues/1999/10_99/cover.htm
- [5] LAN/MAN Standards Committee of the IEEE Computer Society, "Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE-SA Standards Board - The Institute of Electrical and Electronics Engineers, Inc., Tech. Rep., 1999.
- [6] F. Bellotti, A. D. Gloria, D. Grosso, and L. Noli, "WLESS-frame: a simulation-based development environment for 802.11 stations," *Computer Networks*, vol. 36, pp. 625-641, 2001.
- [7] N. Baghaei and R. Hunt, "Review of quality of service performance in wireless LANs and 3G multimedia application services," *Computer Communications*, vol. 27, pp. 1684-1692, 2004.
- [8] LAN/MAN Standards Committee of the IEEE Computer Society, "Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band," IEEE-SA Standards Board - The Institute of Electrical and Electronics Engineers, Inc., Tech. Rep., 1999.
- [9] —, "IEEE Standard for Information technology – Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band," IEEE-SA Standards Board - The Institute of Electrical and Electronics Engineers, Inc., Tech. Rep., 2003.
- [10] C. Aichele, R. Flickenger, C. Fonda, J. Forster, I. Howard, T. Krag, and M. Zennaro, *Wireless Networking in the Developing World: A practical guide to planning and building low-cost telecommunications infrastructure*. Limehouse Book Sprint Team, 2006, last Accessed Apr. 2006. [Online]. Available: <http://wndw.net/index.html>
- [11] A. Gumaste and T. Antony, *First Mile Access Networks and Enabling Technologies*. 800 East 96th Street, Indianapolis, IN 46240 USA: Cisco Press, 2004.
- [12] G. Hardin, "The Tragedy of the Commons," *Science*, vol. 162, no. 3859, pp. 1243-1248, Dec. 1963, last Accessed Apr. 2006. [Online]. Available: <http://www.sciencemag.org/scient/sotp/pdfs/162-3859-1243.pdf>
- [13] Wikipedia, the free encyclopedia. (2006) Tragedy of the commons. online encyclopedia. Last Accessed Apr. 2006. [Online]. Available: http://en.wikipedia.org/wiki/Tragedy_of_the_commons
- [14] B. Whittington, G. Halse, and A. Terzoli, "Secure, extensible and heterogenic wireless networks: A model for community orientated wireless Internet in South Africa," Computer Science Honours thesis, Rhodes University, Grahamstown, South Africa, 2003.
- [15] I. Brandt, A. Terzoli, and C. Hodgkinson-Williams, "Wireless Communication for Previously Disadvantaged Secondary Schools in Grahamstown, South Africa," in *SATNAC 2005, Convergence - Can technology deliver?*, Sept. 2005. [Online]. Available: <http://ings.rucus.net/Brandt.pdf>
- [16] Motorola. (2004) Canopy Wireless Broadband Platform. Last accessed Jun. 2004. [Online]. Available: <http://motorola.canopywireless.com/>
- [17] M. Haardt and Q. Spencer, "Smart antennas for wireless communications beyond the third generation," *Computer Communications*, vol. 26, pp. 41-45, 2003.
- [18] J. T. Bernhard, G. H. Huff, S. Zhang, and G. Cung, "Reconfigurable Portable Antenna Systems For High-Speed Wireless Communication," 2003, last Accessed Apr. 2006. [Online]. Available: <http://hcac.hawaii.edu/tcwct03/papers/s07p05.pdf>

Study of Surfaces Generated by Abrasive Waterjet Technology

J. Valíček¹, S. Hloch², M. Držík³, M. Ohlídal⁴, V. Mádr.¹, M. Lupták², S. Fabian², A. Radvanská², K. Páleníková¹
¹VŠB – TU Ostrava, ²TU of Košice, ³ILC Bratislava, ⁴Brno University of Technology

Abstract - The paper deals with results obtained by means of contactless optical shadow method and by commercial methods, namely by using an optical commercial profilometer MicroProf (FRT) and a contact profilometer HOMMEL TESTER T8000. The main emphasis is put on the analysis of results for defining the process of creation of a new surface generated by the stream of abrasive waterjet, including its geometric parameters and mechanisms of cutting tool-material interaction. New possibilities of the surface quality evaluation and optimizing the technological parameters selection of the cutting process appear.

I. INTRODUCTION

With the development of technology, the scientists and the technologists in the field of manufacturing are facing more and more challenging problems. The demand for the highest accuracy and surface finish, the challenge to produce critical surfaces and complex shapes, have necessitated the use of non-traditional machining techniques. The use of such non-traditional machining techniques is found to be the best option for manufacturing complex dies and aerospace components with the required high precision and accuracy. Competition and scientific progress requires introduction of technologies that perform challenging claims of modern production in automation field, from economy, environmental and energy efficiency point of view. Abrasive waterjet cutting represents all of these claims. The abrasive waterjet cutting technique is considered to be a flexible tool in the processing of a wide range of materials without time loss by tool changing and with minimal risk to occupational health and environment [17]. Nowadays represents cold precise, computer controlled shape cutting without any strain. These attributes poses this technology to the position of permanent use in the future, that represents excellent perspective for expansion in volume sectors, especially there, where the materials with excellent utility properties are used [16]. Abrasive waterjet (AWJ) technology has greatly altered the tooling and manufacturing industry, resulting in the dramatic improvement in accuracy, quality, and productivity. However, such techniques are not favourably nourished due to the difficulties and complexities involved in setting their process factors which enters to the cutting process. The nature of the mechanisms involved in the domain of AWJ machining is still not well understood but is essential for AWJ control improvement.

II. RELATED WORKS

The unevenness of surfaces created by machining [1-6] traditional or newly developed technologies (for example

machining by ultrasonic, laser, plasma, waterjet or abrasive waterjet technologies) is a property, which is precisely standardised. From the manufacturing and technical point of view, we are interested in the technological property of workpieces. This property influences the durability and reliability of components, arc energy releases (waste of energy), wear resistance and the economics of machines and equipment. The scale of the basic metrology operation is defined by the standards determining the required quality class [7], [8]. These operations lead to correct results for surfaces created by traditional technologies. The physical basis of the formation (creation) of new surfaces by non-conventional technologies is different; therefore the geometrical characteristics of the created surfaces will differ. Good agreement has been confirmed by comparison of the results obtained using the newly developed measurement method with the commercial method. The principle of the measurement method SM, design and optical scheme adjusted for measurement of cut surfaces by abrasive waterjet have been published for example in works [9], [10], [11]. We would like to briefly present some results obtained from the measurement by the SM method for the purpose of the surface roughness control.

III. EXPERIMENTAL SET UP

A two dimensional abrasive waterjet machine Nessap 1000-V, was used in this work with the following specification: work table x-axis 800 mm, y-axis 1000 mm, z-axis discrete motion, with maximum traverse speed 250 mm.min⁻¹. A high-pressure intensifier pump PTV-37-60. Pump with maximum pressure 415 MPa was used. A Paser III. cutting head manufactured by Flow Inc. was used. The following target materials have been used (AISI 309, EN Fe 510 DD1, EN Fe 360 BFN a DIN GS - 20 Mn 5). The properties of each sample are: the length of 20 mm, the width of 20 mm, and the height of 8 mm. Cut surfaces of the square samples have been prepared up at the following speeds of the cutting head (50, 100, 150 a 200 mm.min⁻¹) where each side of the sample was created by different traverse speed. The surface quality of each side of samples has been measured by an optical method using a CCD camera on 22 geometric lines with a vertical step of 0.364 mm (fig. 1). Fig. 2 shows basic set-up of the optical method of shadow visualization by CCD camera where α is lighting angle, amplitude – frequency spectrum is obtained from surface created at the cutting speed 200 mm.min⁻¹, for AISI 309 material. The optical signal about light and shadows surface distribution have been analysed by

means of the Fourier transformation analysis, spectral decomposition and frequency band filtration with the aim of obtaining RMS (Root Mean Square) light reflection intensity from the surface and transforming equations between RMS and surface roughness parameters, particularly a surface roughness profile parameter, the average roughness R_a [μm].

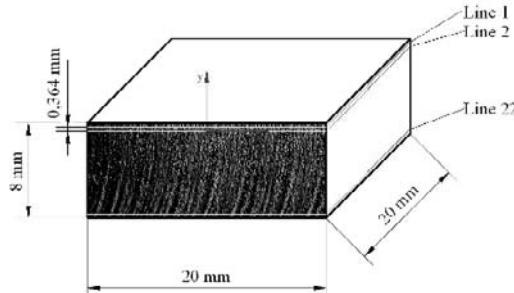


Fig. 1. Experimental sample and measurement lines, material AISI 309, cutting surface created at cutting speed $200 \text{ mm} \cdot \text{min}^{-1}$.

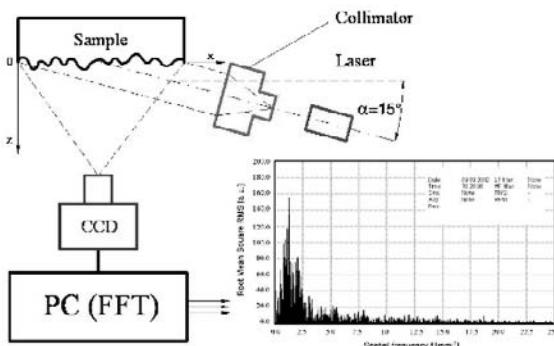


Fig. 2. Basic set-up of the optical method of shadow visualization by CCD camera where α is lighting angle, amplitude – frequency spectrum is obtained from the surface created at the cutting speed $200 \text{ mm} \cdot \text{min}^{-1}$, material AISI 309.

Distribution of the surface roughness profile is considered to be most important because it provides complex information about the mechanical effect of selection of the technological factors, about material properties and about interaction of the cutting forces with the machined material.

TABLE I
THE SPATIAL FREQUENCY RANGE DIVIDED INTO A SPECTRUM

Order	f mm^{-1}	λ mm
I	$f \leq 2.5$	$\lambda \geq 0.4$
II	$2.5 < f \leq 20$	$0.4 > \lambda \geq 0.05$
III	$f > 20$	$\lambda < 0.05$

From the practical point of view the spatial frequency range can be divided into a spectrum composed of three parts, namely: $(0 - 2.5) \text{ mm}^{-1}$ – the waviness, $(2.5 - 20) \text{ mm}^{-1}$ – grooving and slotting, which is hard to distinguish from the roughness $(20 - 100) \text{ mm}^{-1}$ (tab. 1). It can be seen in real

equations that the kinetic energy of the abrasive waterjet decreases with the cutting depth raising, and hence the surface roughness values increase or amplitudes and the frequencies decrease. It is caused by the cutting mechanism where the tensile and shear stress change to compression stress. At specimens cut using the AWJ, the low frequency RMS (1) (i.e. the waviness) preponderates over the high frequency (i.e. the surface roughness). Hence as shown in (fig. 3) containing a chart of the RMS relationship with the depth, the high frequencies remain constant at a given depth. At a given depth the low frequency (i.e. the surface waviness) increases.

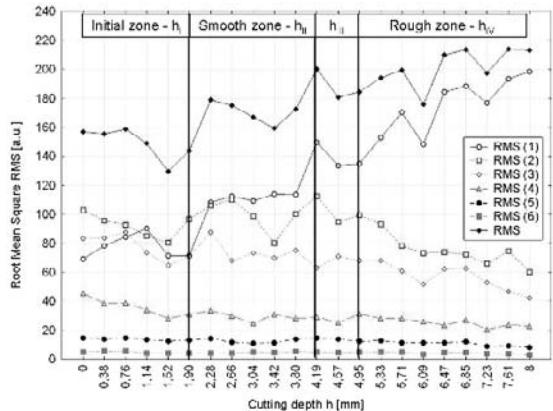


Fig. 3. Spectral surface decomposition obtained from surface created at cutting speed $200 \text{ mm} \cdot \text{min}^{-1}$, for material AISI 309, where h_I is depth of initial zone, h_{II} is depth of smooth zone, h_{III} is depth of transition zone and h_{IV} is depth of rough zone.

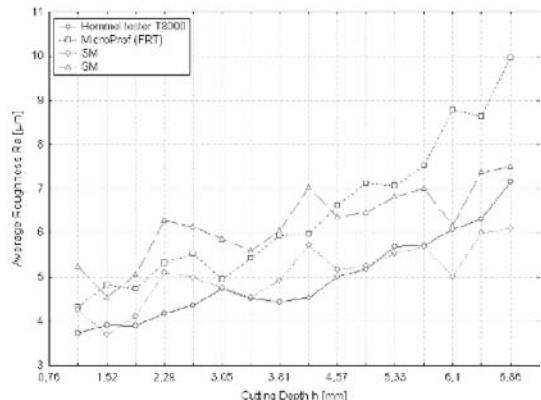


Fig. 4. Comparison of the results obtained by measurement by means of optical profilometer MicroProf (FRT) and contact profilometer HOMMEL TESTER T8000 for stainless steel AISI 304, at cutting speed $200 \text{ mm} \cdot \text{min}^{-1}$.

On measurement lines 1-22, the RMS parameter has been measured at the following six different frequencies: $0-2.5 \text{ mm}^{-1}$ (RMS(1)), $2.5-5 \text{ mm}^{-1}$ (RMS(2)), $5-10 \text{ mm}^{-1}$ (RMS(3)), $10-15 \text{ mm}^{-1}$ (RMS(4)), $15-20 \text{ mm}^{-1}$ (RMS(5)), $0-25 \text{ mm}^{-1}$ (RMS(6)). The frequency steps selected and used in the above-mentioned manner simulated „cut off“ of the contact profilometer used for decomposition of the surface structure

into individual sub-components. Fig. 4 shows the comparison between SM, optical commercial profilometer MicroProf (FRT) and contact profilometer HOMMEL TESTER T8000. As main surface geometry parameters have been proposed average roughness R_a [μm], stream deflection Y_{ret} [mm] and deviation angle D [$^\circ$] (fig. 5). They are defined in figure 6, 7 and 8. The character of the distribution of topographical elements divided surfaces generated by AWJ into cutting wear area h_c [mm] and deformation wear area h_d [mm], according to Hashish [12], [13].

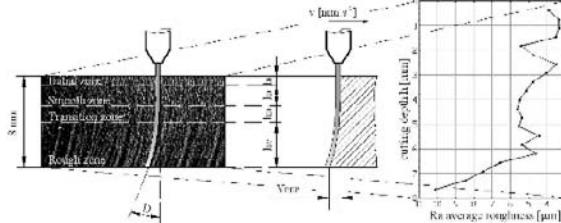


Fig. 5. Photographs of the surface, material AISI 309, magnification 1:12, cutting speed, $200 \text{ mm} \cdot \text{min}^{-1}$ and proposed main parameters of the surface profile.

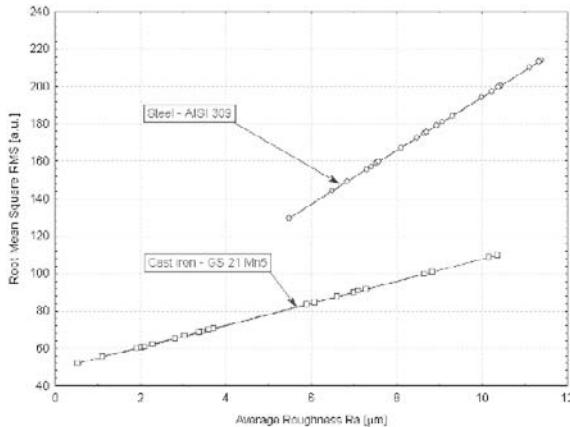


Fig. 6. Influence average roughness on RMS for AISI 309 and Cast iron – GS 21 Mn5.

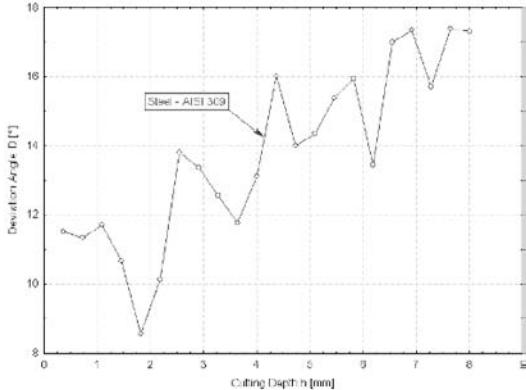


Fig. 7. Influence of depth h on deviation angle $D = \arctg(Y_{ret}/h)$.

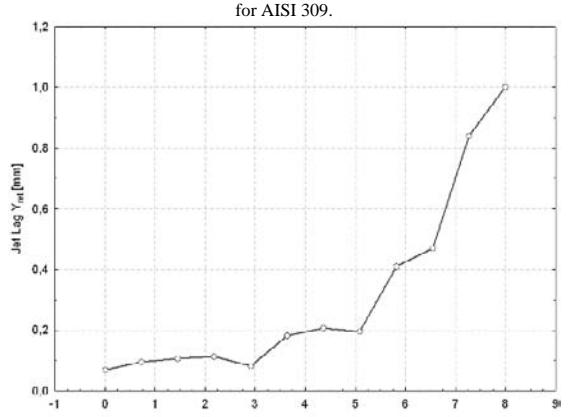


Fig. 8. Influence of cutting depth material on jet lag (stream deflection) Y_{ret} for AISI 309 $Y_{ret} = 0,022 \cdot R_a \cdot h_{rel}$.

V. PROPOSAL OF THE DATA BANK FOR AWJ TECHNOLOGY CONTROL

Relevant questions dealing with the influence of surface roughness on functional reliability and product service life are not new. This solution is given low attention. A quantitative answer about the behaviour of that problem for next development of the science and technology is still missing. The prediction is quite impossible because the present surface roughness evaluation does not characterize functional surface in its entirety, it does not determine its estimation. Objective technical knowledge of production structure and texture of a thin surface film and its quantitative description of complex topographical function call for a lot of experimental measurements, analyses and scientific effort. The solution for that relatively young and still unconventional technology must begin by systematic measurement of parameters structuring related to geometric distribution of the surface topography elements, their storing and statistical and analytical processing in terms of the AWJ technology process and material characteristics. The conceptual structure of the databank is characterized in figure 9. The main input and output factors are sorted according [14], so that hydraulic factor, material factors, shapes and MESH of abrasive and technical factors of the stream and hydro-devices creates an output of energy characteristic of the stream. Material and dimension properties of the specimens depended on the energetic load and claims for the exacting character and quality of work. Material parameters like tensile strength, pressure, torsion strength, modulus of elastic compression, weight, Poisson number, ultrasonic wave propagation speed, chemical composition, will represent, beside the main technological factor, the basic inputs. The material constants determine mechanical behaviour of the material and character of induced power, tension and deformation field. Examination of the mathematical function among input material, technological and the output – geometrical surface parameter is the base for its mutual affecting in the control system. The

machining realized by AWJ is process difficult in terms of technology. The project preparation, optimisation and the overall result of the AWJ machining are influenced by a number of factors. Partial influence of the factors is mutually connected; some statistical-mathematical methods, such as factor analysis that is presented for example in current works of Hloch [15-17] have been applied to their optimisation and selection. Besides the cutting surface topographical parameters, the total energy consumption, performance parameters and manufacturing costs will be observed. The data will be systematically updated and statistically and analytically evaluated in order to be fully usable for the prediction of the geometrical surface state and for the project of optimisation of the main AWJ process factors, which covers all kinds of materials used most frequently in technical professions.

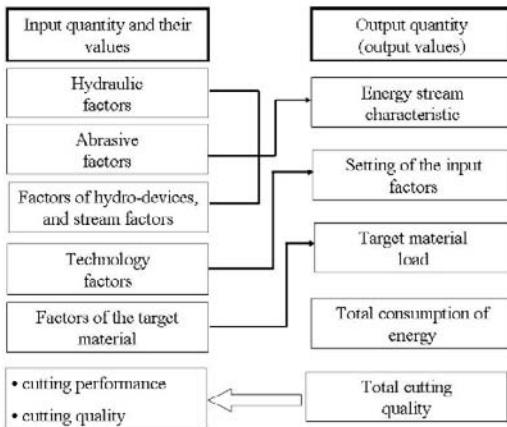


Fig. 9. Databank conceptual structure.

CONCLUSION

Based on the good results of comparison of the data measured by a new optical method SM with the data obtained by a commercial optical set and by a contact profilometer. The main optical quantity RMS has been estimated and defined and, besides the cutting depth h , the main interpreted parameters R_a , Y_{ret} and D . It is a new structured geometrical property of the surface that will be systematically stored in the databank after each measurement. In terms of the development of the AWJ technology, the above described procedure only lays foundations for solution of much more difficult problems relating to interaction between a flexible cutting tool and the target material, and for knowledge of the theoretical relations to the technological factors of the process. Systematic drafting databank with important input and output data about provided cut will have an irreplaceable role. From statistical physical and analytical regularity evaluation of the relationship between input and output data, it is possible to proceed to the mathematical generalization of these regularities and derive an equation for prediction and project calculation of the concrete cuts. By that calculation it could be theoretical based technology factors selection that

will be optimal for the given machined material on required quality, the performance parameters and the total machining economy. We are currently solving the problems of quantification of the cutting process prediction, stress and strain state in the machined material and their influence on development of geometrical surface parameters. In our opinion, we have achieved some remarkable results in the field calculation of static and tensiometric properties of a workpiece, in describing the development of the stress and strain state in the elastic and plastic zone of the material being stressed, as well as in describing the hydrodynamics of the disintegration process using the AWJ tool.

ACKNOWLEDGMENT

The authors would like to acknowledge the support of IGS-HGF VŠB TUO-2005-516/ grant and project VEGA 1/1075/04, VEGA 1/1095/04, VEGA 1/2209/05, and KONTAKT ČR IČ 119, KONTAKT SR IČ 88.

REFERENCES

- [1] Bumbálek, B., Obvody, V., Oštádal, B.: Surface roughness. Praha, SNTL 1989. (in Czech)
- [2] Brezina, I.: Surface roughness. Fine mechanics and optics, No. 7, 1991. (in Czech)
- [3] Pernikář, J., Tykal, M., Vačkář, J.: Metrology and quality. Brno, CERM 2001. (in Czech)
- [4] Vašek, J., Martinec, P., Foldyna, J., Sitek, L., Šćučka, J.: Abrasives for AWJ cutting. Academy of Sciences, Ostrava, 2002.
- [5] Sigmund, M., Brychta, J., Čep, R.: Quality control at high speed machining. Technological Engineering, 2005, roč. II., č. 1, pp. 20 – 21.
- [6] Krajný, Z.: Vodní lžíč v praxi WJM. (Waterjet in the WJM practice.) Mračko – Bratislava, 1998. (in Slovak)
- [7] Monka, P.: Theoretical relationships of the peak value profile, Manufacturing Engineering, 2-3, II. pp. 20-21, FVT TU v Košiciach, Prešov, ISSN 1335-7972, 2003.
- [8] Monka, P.: Computer Aided Design of Fixtures for NC Machine Tools, Buletin Scientific, Seria C, Volumul XIX, Baia Mare, Rumunsko, pp. 495 – 499, ISSN- 1224-3264, 2005.
- [9] Valiček, J., et al. Optical method for surface analyses and their utilization for abrasive liquid jet automation. In Proceedings of the 2001 WJTA American Waterjet Conference, M. Hashish (ed.), WJTA, Minneapolis, Minnesota, 2001, pp. 1 – 11.
- [10] Valiček, J., Držík, M., Ohlídal, M., Hlaváč, L.M.: Application of optical methods for analyses of surfaces made by abrasive liquid jet. In METAL 2001 – Proceedings of the 10th International Metallurgical and Materials Conference, TANGER s.r.o., Ostrava, 2001, paper 104, pp. 1 – 7.
- [11] Valiček, J., et al. Utilization of the optical methods for analyses of cutting edges. BHR Group, 2004, p. 487 – 501
- [12] Hashish, M.: Modeling Study of Metal Cutting with Abrasive Waterjets. Trans. of the ASME, Journal of Eng. Mat&Tech, Vol. 106, No. 1, 1984.
- [13] Hashish, M.: Pressure Effect in Abrasive – Waterjet (AWJ) Machining. Trans. of the ASME, Journal of Eng. Mat&Tech., Vol. 111, No. 7, 1989.
- [14] Guo, N. S.: Schneidprozess und Schnittqualität beim Wasserabrasivstrahl – schneiden. VDI Verlag, 1994.
- [15] Hloch, S.: Evaluation of abrasive waterjet factors influencing the surface quality. In: Transactions of the Universities of Košice. No. 2 (2005), pp. 12-21, ISSN 1335-2334.
- [16] Hloch, S., Gombáš, M.: Drsnosť povrchu nehrdzavejúcej ocele pri delení vysokorychlosťnym hydroabrazívnym prúdom. (Roughness of stainless steel surface in the process of cutting with abrasive waterjet.) In: MM Spectrum. No. 7.8 (2006), pp. 48-50, ISSN 1212-2572. (in Slovak)
- [17] Hloch, S. et al.: Acoustic environment evaluation of manufacturing system with abrasive waterjet technology. In: ICMPM 2005: Advances in materials, product design & manufacturing systems: Proceedings of the international conference: 12 - 14 December 2005. India: Bannari Amman Institute of Technology, 2005. p. 568-575.

- [18] GOMBÁR, M. Využitie MATLABU pri tvorbe štatistického modelu drsnosti obrobeného povrchu . Manufacturing Engineering, 2006, roč. V, č.1, s. 14 -17,69 , ISSN 1335-7972.

On Length-Preserving Symmetric Cryptography

Zheng Jianwu, Liu Hui, and Liu Mingsheng

Department of Information Engineering,
Shijiazhuang Railway Institute, Hebei 050043, China.
{zhengjw, liuhui, liums}@sjzri.edu.cn

Abstract—This paper focuses on the length-preserving symmetric cryptography, with which people can encrypt messages of variable length (especially arbitrary length) to get ciphertext of length identical to that of plaintext being encrypted. Two confidentiality modes being able to achieve length-preserving encryption, i.e., OFB mode and CTR mode, are analyzed in terms of obstacles to guaranteeing message privacy. Furthermore, a new mode of operation, CBC-LP, is proposed for both achieving length-preserving encryption and exploiting advantages of implementing CBC mode over other confidentiality modes, such as OFB, CTR modes and so on.

I. INTRODUCTION

Symmetric cryptography is mathematical techniques of changing binary representation of the message for preventing message privacy from being comprised (loosely speaking, main goal of implementing symmetric cryptography), under control of the secret key possessed by legitimate parties. Symmetric cryptography is both widely utilized in designing connection-oriented security protocols, for example SSL/TLS [1] and IPSec [2], and heavily leveraged for providing application-oriented security services, as those provided by RADIUS [3], WS-Security [4] and so on.

A. What is the Length-Preserving Symmetric Cryptography

DES [5] and AES (the replacement of the former) [6] are two important underlying sets of mathematical techniques, also cryptographic algorithms, for guaranteeing message privacy, however, when talking about the symmetric cryptography, we in reality mention the modes of operation, according to which the underlying cryptographic algorithms are invoked during cryptographic operation. Moreover, these modes of operation (or confidentiality modes, named after being able to guarantee message privacy) are classified into two classes. One is the class of modes that can only manipulate messages of fixed length (block size) and its multiple, and the other is the class of modes that can manipulate messages of variable length.

Inspired by the two definitions of functions given by Goldreich in [7], i.e. length-regular function and length-preserving function, we name the latter class of confidentiality modes above length-preserving symmetric cryptography. Here, we repeat the definitions of length-regular and length-preserving functions as follows.

Length Regular Function: A function f is *Length-Regular* if for every $x, y \in \{0,1\}^*$ and $|x|=|y|$, then $|f(x)|=|f(y)|$.

Length-Preserving Function: A function f is *Length-Preserving* if for every $x \in \{0,1\}^*$, it holds that $|f(x)|=|x|$.

B. Why is the Length-Preserving Symmetric Cryptography

1) Inconvenience of Implementing Non-Length-Preserving Symmetric Cryptography

- 1) Extra operation should be executed for padding the message being encrypted to a length of block size or multiple of block size.
- 2) Extra bits are needed for indicating the number of bits been padded to expand the message. Alternatively, specific padding mechanism should be negotiated and implemented, for example, every message is padded with “100…0”, delimiting by “10” followed by all zero bits.
- 3) Extra computational resources are required, including time, memory, bandwidth and so forth, during cryptographic operation, transmission, and disposition.

2) Incapability of Non-Length-Preserving Symmetric Cryptography

In some circumstances, non-length-preserving symmetric cryptography is incapable of accomplishing security tasks facing the information infrastructures. We introduce two examples here for demonstrating the need for length-preserving symmetric cryptography.

Smart Card Application: The smart card is being widely used because of its intrinsic security characteristics. How to securely transmit APDU (Application Protocol Data Unit) messages is the focus of achieving secure smart card application, and a command APDU message is expressed as (please refer to [8] for more detail)

$$[CLA][INS][P_1][P_2][L_c][IDATA][L_e].$$

In the APDU message, the core part is the message body, *IDATA*, which carries transaction information valuable or sensitive, and is of variable length. In order to achieve privacy of *IDATA*, it is therefore needed to leverage length-preserving symmetric cryptography.

Web Services: Web services are hot topics these days, and are heavily leveraged by enterprises to create service-oriented information infrastructures in order to meet changing market and reduce the cost of developing and deploying the needed infrastructures.

As with the smart card application above, how to securely exchange SOAP (Simple Object Access Protocol) message is the focus of securing web services (please refer to [4] for more detail). SOAP message is essentially qualified XML 1.0 document, and the code segment below illustrates a SOAP message carrying account information.

```
<?xml version='1.0'?>
<PaymentInfo xmlns='http://example.org/paymentv2'>
  <Name>John Smith</Name>
  <CreditCard Limit='5,000' Currency='USD'>
    <Number>4019 2445 0277 5567</Number>
    <Issuer>Example Bank</Issuer>
    <Expiration>04/02</Expiration>
  </CreditCard>
</PaymentInfo>
```

The card number is the most important information, and therefore it should be encrypted prior to transmission. Moreover, it is required that the number of digits of the encrypted information should be identical to that of the card number in plaintext form for ease of validity verification of input and so forth, so a length-preserving symmetric cipher is also needed.

In the sequel, we pay main attention to the following things.

- 1) Some confidentiality modes that can accomplish length-preserving cryptographic operations are analyzed and compared.
- 2) A new length-preserving symmetric confidentiality mode of operation is proposed, which is based on the CBC mode.

Some symbols are used in the following discussion, please refer to the Appendix of this paper for the detail explanation.

II. LENGTH-PRESERVING SYMMETRIC CIPHERS: OFB MODE AND CTR MODE

As detailed in NIST Special Publication 800 series, in particular in 800-38A [9], there are two confidentiality modes that can accomplish length-preserving cryptographic operation. They are analyzed respectively in this section as follows.

Because it is trivial to select DES, or AES as underlying cryptographic algorithm, we will therefore proceed without specifying any underlying cryptographic algorithm.

A. Introduction to OFB Mode and CTR Mode

1) The Output Feedback Mode (OFB Mode)

The OFB mode features the iteration of the forward cipher operation ($\text{CIPH}_K(\cdot)$) on an IV to generate a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The OFB mode is defined as follows.

OFB Encryption:

$$\begin{aligned} I_1 &= IV; \\ I_j &= O_{j-1} \quad \text{for } j=2,\dots,n; \\ O_j &= \text{CIPH}_K(I_j) \quad \text{for } j=1,2,\dots,n; \\ C_j &= P_j \oplus O_j \quad \text{for } j=1,2,\dots,n-1; \\ C_n^* &= P_n^* \oplus \text{MSB}_u(O_n). \end{aligned}$$

OFB Decryption:

$$\begin{aligned} I_1 &= IV; \\ I_j &= O_{j-1} \quad \text{for } j=2,\dots,n; \\ O_j &= \text{CIPH}_K(I_j) \quad \text{for } j=1,2,\dots,n; \\ P_j &= C_j \oplus O_j \quad \text{for } j=1,2,\dots,n-1; \\ P_n^* &= C_n^* \oplus \text{MSB}_u(O_n). \end{aligned}$$

2) The Counter Mode (CTR Mode)

The CTR mode features the application of the forward cipher operation to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The counters are denoted T_1, T_2, \dots , and T_n respectively. The CTR mode is defined as follows.

CTR Encryption:

$$\begin{aligned} O_j &= \text{CIPH}_K(T_j) \quad \text{for } j=1,2,\dots,n; \\ C_j &= P_j \oplus O_j \quad \text{for } j=1,2,\dots,n-1; \\ C_n^* &= P_n^* \oplus \text{MSB}_u(O_n). \end{aligned}$$

CTR Decryption:

$$\begin{aligned} O_j &= \text{CIPH}_K(T_j) \quad \text{for } j=1,2,\dots,n; \\ P_j &= C_j \oplus O_j \quad \text{for } j=1,2,\dots,n-1; \\ P_n^* &= C_n^* \oplus \text{MSB}_u(O_n). \end{aligned}$$

B. Analysis to OFB Mode and CTR Mode

Although OFB mode and CTR mode can be implemented for achieving length-preserving encryption, as mentioned above, some security requirements related to them should be

kept in mind, and should be satisfied when implementing these modes. If you are incapable of dealing with the burden loaded by these modes, it is the best not to leverage these confidentiality modes for achieving length-preserving encryption.

1) OFB Mode

As mentioned in Section 1, the initialization vector is consecutively encrypted to generate output block O_j (for $1 \leq j \leq n$) that is exclusive-ORed with corresponding plaintext block P_j (for $1 \leq j \leq n$), also as shown in Fig. 1, it is therefore required that a unique IV should be utilized for encrypting every message if the identical secret key is used when calling the forward cipher function; otherwise, the confidentiality of those messages may be compromised.

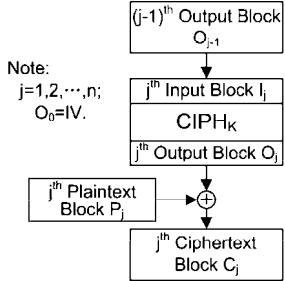


Figure 1. OFB Mode (Encryption)

Furthermore, Confidentiality may similarly be compromised if any of the input blocks to the forward cipher function for the encryption of a message is designated as the IV for the encryption of another message under the given key.

Specifically, the OFB mode requires that the IV is a nonce, i.e., the IV must be unique for each execution of the mode under the given key. This length-preserving symmetric cipher heavily depends on the uniqueness of the initialization vector, which in turn limits its flexibility and usability.

2) CTR Mode

Actually, as far as the algorithmic steps of the CTR mode are concerned, it is an elegant length-preserving symmetric cipher, as shown in the Fig. 2, moreover, in both CTR encryption and CTR decryption, every block can be manipulated independently from the other blocks. However, the sequence of counters must have the property that each block of the sequence is different from every other block, which may be the main obstacle to implementing this length-preserving symmetric cipher. This condition is not restricted to a single message, across all of the messages that are encrypted under the identical given key, all of the counters must be distinct.

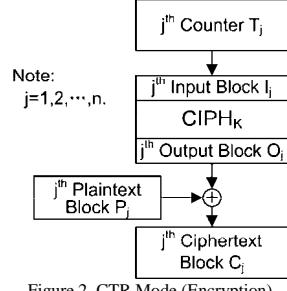


Figure 2. CTR Mode (Encryption)

As with the OFB mode, it is somewhat cumbersome to implement the CTR mode with satisfactorily respective to the requirement that a unique counter block for each plaintext block that is ever encrypted under a given key, across all messages.

III. CBC-BASED LENGTH-PRESERVING SYMMETRIC CIPHER

This section first introduces the CBC mode of operation, which can only manipulate messages of length being multiple of a block size, then a new mode of operation, based on the CBC mode, is proposed for achieving length-preserving encryption.

A. CBC Mode

The Cipher Block Chaining (CBC) mode features the combining ("chaining") of the plaintext blocks with the previous ciphertext blocks. Namely, in CBC encryption, each successive plaintext block (except the first) is exclusive-ORed with the previous output (ciphertext) block to produce the new input block, and the forward cipher function is applied to each input block to produce the ciphertext block; in CBC decryption, to recover any plaintext block (except the first), the inverse cipher function is applied to the corresponding ciphertext block, and the resulting block is exclusive-ORed with the previous ciphertext block. The CBC mode is defined as follows:

CBC Encryption:

$$\begin{aligned}
 C_0 &= IV; \\
 I_j &= C_{j-1} \oplus P_j \\
 &\quad \text{for } j=1,2,\dots,n. \\
 O_j &= CIPH_K(I_j) \\
 &\quad \text{for } j=1,2,\dots,n. \\
 C_j &= O_j \\
 &\quad \text{for } j=1,2,\dots,n.
 \end{aligned}$$

CBC Decryption:

$$\begin{aligned}
C_0 &= IV; \\
I_j &= C_j \\
&\quad \text{for } j=1,2,\dots,n. \\
O_j &= \text{CIPH}_K^{-1}(I_j) \\
&\quad \text{for } j=1,2,\dots,n. \\
P_j &= O_j \oplus C_{j-1} \\
&\quad \text{for } j=1,2,\dots,n.
\end{aligned}$$

where, $\text{CIPH}_K(\cdot)$ and $\text{CIPH}_K^{-1}(\cdot)$ are forward cipher function (encryption function) and inverse cipher function (decryption function) respectively, parameterized with secret key K . CBC encryption and CBC decryption are also depicted in Fig. 3.

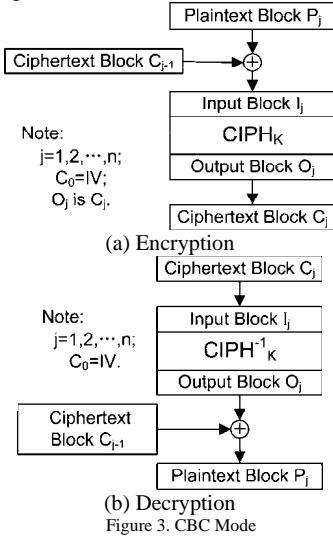


Figure 3. CBC Mode

Factors account for the widely use of the CBC mode are as follows.

- 1) Both encryption steps and decryption steps of CBC mode are straightforward;
- 2) Although the CBC mode requires an initialization vector, i.e. IV , it need not be secret. Moreover, the CBC mode is free from the dilemma plagued the OFB mode and CTR mode. Specifically, uniqueness of the IV and counter blocks, used in OFB mode and CTR mode respectively, is required to be guaranteed for ensuring data confidentiality without being compromised, but in CBC mode, it needn't to take the burden above into account.

However, the (standard) CBC mode is incapable of manipulating messages of arbitrary length, specifically, it is unable to encrypt message, whose length is not of some multiple of block size without padding the message. In the

sequel, the CBC mode is modified and turned to a length-preserving confidentiality mode.

B. CBC-LP Mode

For achieving length-preserving encryption, as accomplished by OFB mode and CTR mode, and for exploiting advantages of CBC mode detailed in the previous subsection, a CBC-Based length-preserving confidentiality mode is proposed, denoted CBC-LP mode. The CBC-LP mode is defined as follows:

Assuming that the plaintext string P is of arbitrary length, it is first divided into blocks as follows.

$$P = P_1 | P_2 | \dots | P_{n-1} | P_n^*.$$

The last block of the plaintext, P_n^* , may be a partial block, which consists of u ($0 \leq u \leq b$) bits. If u is equal to b , the number of bits of the plaintext P is multiple of the block size; therefore, it is no need to implement CBC-LP cipher for encryption, and the CBC-mode would accomplish the task.

CBC-LP Encryption:

$$\begin{aligned}
C_0 &= IV; \\
I_j &= C_{j-1} \oplus P_j \quad \text{for } j=1,\dots,n-1. \\
I_n &= C_{n-1} \oplus \left(P_n^* \left| \underbrace{00\dots0}_{(b-u) \text{ Zero bits}} \right. \right) \quad (\text{Padding}). \\
O_j &= \text{CIPH}_K(I_j) \quad \text{for } j=1,\dots,n. \\
C_j &= O_j \quad \text{for } j=1,\dots,n.
\end{aligned}$$

The most important step is to calculate the n^{th} input block, which is generated by exclusive-ORing $(n-1)^{\text{th}}$ ciphertext block and the last plaintext block being expanded to a complete block of block size with all zero binary bits. After accomplishing operations above, the $(b-u)$ least significant bits of the penultimate block, C_{n-1} (i.e. $(n-1)^{\text{th}}$ ciphertext block), are truncated (discarded), and C_{n-1}^* is generated, which consists of u bits.

$$C_{n-1}^* = \text{MSB}_u(C_{n-1}),$$

and the ciphertext string is made up of $C_1, C_2, \dots, C_{n-2}, C_{n-1}^*,$ and C_n as follows.

$$C = C_1 | C_2 | \dots | C_{n-2} | C_{n-1}^* | C_n.$$

It is clear that the ciphertext string is of length identical to that of the plaintext string, despite of whether the number of bits of the plaintext is multiple of the block size or not.

CBC-LP Decryption: For recovering the plaintext from the ciphertext of arbitrary length, C , it is to first divide the cipher string into different ciphertext block, and it is required that the partial block should be just prior to the last block of a

block size, i.e. the penultimate block should be the partial block, C_{n-1}^* . After partitioning the ciphertext string, it is straightforward for us to decrypt the ciphertext blocks, C_1 , C_2 , ..., and C_{n-2} according to the decryption steps below, i.e. CBC-Decryption.

$$\begin{aligned} C_0 &= IV; \\ I_j &= C_j \quad \text{for } j=1, \dots, n-2. \\ O_j &= \text{CIPH}_K^{-1}(I_j) \quad \text{for } j=1, \dots, n-2. \\ P_j &= O_j \oplus C_{j-1} \quad \text{for } j=1, \dots, n-2. \end{aligned}$$

Following steps below to recover P_{n-1} and P_n^* from C_{n-1}^* and C_n . The C_{n-1} is first calculated as,

$$C_{n-1} = C_{n-1}^* \left| \text{LSB}_{b-u} \left(\left(C_{n-1}^* \left| \underbrace{00 \dots 0}_{(b-u) \text{ zero bits}} \right. \right) \oplus \text{CIPH}_K^{-1}(C_n) \right) \right.$$

Then P_{n-1} and P_n^* are recovered as,

$$\begin{aligned} I_{n-1} &= C_{n-1} \\ O_{n-1} &= \text{CIPH}_K^{-1}(I_{n-1}) \\ P_{n-1} &= O_{n-1} \oplus C_{n-2} \\ I_n &= C_n \\ O_n &= \text{CIPH}_K^{-1}(I_n) \\ P_n^* &= \text{MSB}_u(C_{n-1} \oplus O_n) \end{aligned}$$

Namely, following the decryption steps above, the plaintext P can be recovered.

C. Underlying Reason for CBC-LP to Achieve Length-Preserving Encryption

Key idea of discarding $(b-u)$ least significant bits of the penultimate cipher block, C_{n-1} , while guaranteeing successful decryption, is that bits being truncated can be restored with the use of the ciphertext bits being kept, i.e. they are redundant.

In CBC-LP encryption, the last block of plaintext P_n^* of length u , which may be partial block, is padded with $(b-u)$ zero bits to form a complete block P_n , expressed as follows.

$$P_n = P_n^* \left| \underbrace{00 \dots 00}_{(b-u) \text{ zero bits}} \right. \quad \begin{array}{c} b \text{ bits} \\ \hline u \text{ bits} \end{array}$$

P_n is encrypted and C_n is calculated as follows.

$$C_n = \text{CIPH}_K(C_{n-1} \oplus P_n).$$

With knowledge of value of bits being padded to P_n^* , the bits being truncated from the penultimate block of ciphertext C_{n-1} can be restored as follows.

- 1) Call reverse cipher function to decrypt C_n as

$$\begin{aligned} \text{CIPH}_K^{-1}(C_n) &= \text{CIPH}_K^{-1}(\text{CIPH}_K(C_{n-1} \oplus P_n)) \\ &= C_{n-1} \oplus P_n. \end{aligned}$$

- 2) Exclusive-OR both sides of the equality above with P_n , the least $(b-u)$ significant bits of C_{n-1} can be calculated.

At this time, only the least $(b-u)$ significant bits (i.e. padding bits) of the last plaintext block, P_n , are known, and the most u significant bits of P_n haven been recovered. Therefore, these u most significant bits are denoted by “??...??” while exclusive-ORing with P_n .

$$\begin{aligned} C_{n-1} &= \text{CIPH}_K^{-1}(C_n) \oplus P_n \\ &= \text{CIPH}_K^{-1}(C_n) \oplus \left(\underbrace{\text{??} \dots \text{??}}_{u \text{ bits}} \left| \underbrace{00 \dots 00}_{(b-u) \text{ zero bits}} \right. \right). \end{aligned}$$

By the equation, the $(b-u)$ least significant bits of the penultimate block of ciphertext, C_{n-1} , which were discarded in CBC-LP encryption, can be restored by the recipient. In particular, those bits are the $(b-u)$ least significant bits of $\text{CIPH}_K^{-1}(C_n)$, given the padding bits are all zero bits. The penultimate block of ciphertext is formed as

$$C_{n-1} = C_{n-1}^* \left| \text{LSB}_{b-u} \left(\text{CIPH}_K^{-1}(C_n) \right) \oplus \underbrace{00 \dots 00}_{(b-u) \text{ zero bits}} \right.$$

Then all ciphertext blocks are at the recipient hand, and he can therefore recover all plaintext blocks. All plaintext blocks are concatenated as $P_1 | P_2 | \dots | P_n$, and the $(b-u)$ least significant bits should be discarded after concatenating all these plaintext blocks (equivalently, the $(b-u)$ least significant bits should be truncated from the last plaintext block before concatenating all the plaintext blocks), consequently, the plaintext P of variable length is ultimately recovered.

D. Capability Limitation of the CBC-LP Mode

Although the CBC-LP mode is introduced as length-preserving confidentiality mode, to the best of our work, it is feasible and applicable only for messages whose length is larger than or at least a block size specified by the underlying cryptographic algorithms, e.g., DES, AES, etc.. However, the CBC-LP is incapable of dealing with messages of length less than a block size, such as eight bytes of DES, sixteen bytes of AES and so on.

E. Applying the CBC-LP Mode

In this section, we just exemplify that the CBC-LP can be utilized for ease of implementing security protocols, which leverage block ciphers for encryption.

For XML Encryption: Section 5.2 of the “XML Encryption Syntax and Processing” [10] specification explicitly specifies how to manipulate messages of arbitrary length as follows.

“...Since the data being encrypted is an arbitrary number of octets, it may not be a multiple of the block size. This is solved by padding the plain text up to the block size before encryption and unpadding after decryption. The padding algorithm is to calculate the smallest non-zero number of octets, say N , that must be suffixed to the plain text to bring it up to a multiple of the block size....”

If the CBC-LP is utilized, the XML Encryption specification needn’t to take the length of the message into account, it can mainly focus on how to represent the plaintext and ciphertext in the tree structure of a XML document.

For IKE: IKE [11] (The Internet Key Exchange) is a dominant protocol for authentication and authenticated confidential data exchange over Internet (e.g. implemented for ISAKMP [12] framework and IPsec [2].). In section 5.3 of IKE specification, we find the paragraph below.

“... Encrypted payloads are padded up to the nearest block size. All padding bytes, except for the last one, contain 0x00. The last byte of the padding contains the number of the padding bytes used, excluding the last one. Note that this means there will always be padding.”

As with implementing CBC-LP in XML Encryption, the CBC-LP is also preferable to modes of operation, which are restricted to some fixed block size b , or to some multiple of a block size.

For Others: It is possible for us to enumerate a lot as above, where CBC-LP will find its position.

IV. CONCLUSION

In addition to ensuring flexibility and convenience, length-preserving ciphers are needed for guaranteeing data privacy in some circumstances, where non-length-preserving symmetric modes are infeasible and inapplicable to be implemented.

CBC-LP mode is proposed as a length-preserving confidentiality mode of operation in this paper, which can

both exploit the advantages of the CBC mode and achieve length-preserving encryption.

APPENDIX: SYMBOLS

This section is taken from Section 4.2 of [9] with modifications.

A. Variables

b , u	The block size, and size of the partial plaintext or ciphertext block, in bits.
n , j	The number of data blocks (or segments), and the index to a sequence of blocks ordered from left to right.
I_j , O_j	The j^{th} input block, output block, plaintext block, and ciphertext block.
P_j , C_j	
K , IV , T_j	The secret key, initialization vector, and the j^{th} counter block.
P_n^* , c_n^*	The block of the plaintext and ciphertext, which may be a partial block.

B. Operations and Functions

$X Y$	The concatenation of two bit strings X and Y .
$X \oplus Y$	The bitwise exclusive-OR of two bit strings X and Y of the same length.
$\text{CIPH}_K(X)$,	The forward cipher function and inverse cipher function of the block cipher algorithm under the key K applied to the data block X .
$\text{CIPH}_K^{-1}(X)$	
$\text{LSB}_m(X)$, $\text{MSB}_m(X)$	The bit string consisting of the m least significant bits and the bit string consisting of the m most significant bits of the bit string X .

REFERENCES

- [1] Netscape, SSL 3.0 specification, <http://wp.netscape.com/eng/ssl3/>
- [2] IETF, IP Security, RFC 2401-2412, <http://www.ietf.org/rfc>
- [3] RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000. Available at: <http://www.ietf.org/rfc/rfc2865.txt>
- [4] WS-Security: SOAP Message Security 1.0 (WS-Security 1.0), March 2004. Available at: <http://docs.oasisopen.org/wss/2004/01/>
- [5] FIPS Publication 46-3. Data Encryption Standard (DES). U.S. Doc/NIST, October 25, 1999.
- [6] FIPS Publication 197. Advanced Encryption Standard (AES). U.S. Doc/NIST, November 26, 2001.
- [7] Oded Goldreich, Foundations of Cryptography – Basic Tools, Cambridge University Press, 2001, P.39.
- [8] ISO/IEC 7816, Identification Cards-Integrated circuit(s) cards with contacts, International Organization for Standardization.
- [9] NIST Special Publication 800-38A. Recommendation for Block Cipher Modes of Operation: Methods and Techniques. U.S. Doc/NIST, December, 2001.
- [10] XML Encryption Syntax and Processing, December 2002. <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>
- [11] RFC 2409. The Internet Key Exchange (IKE). November 1998.
- [12] RFC 2408. Internet Security Association and Key Management Protocol (ISAKMP). November 1998.

Revocable Proxy Signature Scheme with Efficient Multiple Delegations to the Same Proxy Signer

Ji-Seon Lee, Jik Hyun Chang
Dept. Computer Science, Sogang University,
1 Sinsu-dong, Mapo-gu, Seoul, Korea

Abstract- In this paper, we propose a revocable proxy signature scheme which allows the original signer to revoke proxy delegations whenever necessary. In the proposed scheme, once the original signer revokes the proxy delegations, he can also generate a proxy signature which is indistinguishable from the proxy signatures generated by the proxy signer. This confirms to the verifier that the proxy signer does not have any authority to sign a message on behalf of the original signer anymore. In addition to this, in the proposed scheme, after the original signer revokes the delegations, he can delegate the signing capability more efficiently than other schemes if the original signer wants to delegate the signing capability to the same proxy signer again.

I . INTRODUCTION

Digital signature schemes are used to provide security services such as user authentication, data integrity and non-repudiations. Traditionally, the signer uses his secret key to sign messages by using some signature schemes. However, the signer may not be able to sign messages himself. For example, there are times when the signer could be away from the workplace. Therefore, the signer needs a proxy signer to sign messages in his behalf. In 1996, Mambo, Usuda, and Okamoto [7,8] first introduced the concept of proxy signature. Since then a number of proxy signature schemes have been proposed.

There are four types of proxy delegation: full delegation, partial delegation, delegation by warrant, and partial delegation with warrant. In full delegation schemes, the proxy signer is given the private key of the original signer. The main weakness of this scheme is that the proxy signature is indistinguishable from the original signer's signature. In partial delegation schemes [4,7,8], the original signer generates a proxy delegation key and delivers it to the proxy signer. The proxy signer can then generate a proxy signature key with this proxy delegation key and his secret key. However, since the partial delegation does not restrict the proxy signer's signing capability, the proxy signer can abuse his delegated rights. For the delegation by warrant scheme [3,10], a proxy warrant is given to the proxy signer to generate proxy signatures. The proxy warrant usually contains the identity of the proxy signer, the period of delegation, and other possible restrictions on the signing capability delegated to the proxy signer. The partial delegation with warrant scheme combines the benefit of the delegation by warrant and partial delegation schemes. Most work on proxy signature schemes has focused on partial delegation with warrant.

If the original signer is available to generate a signature or the proxy signer abuses his delegated rights, the original signer needs to revoke the proxy signer's signing capability. Sun [10] proposed a timestamped proxy signature scheme and claimed that the revocation problem can be solved by using a timestamp. However, Lu and Huang [5] showed that Sun's scheme is insecure and they have proposed a timestamping proxy signature scheme. Recently, several proxy signature schemes with revocation mechanism were proposed [1,6,9]. In all of these schemes, it can be verified whether a proxy signature was generated during the valid delegation period or not. These schemes also allow early termination of delegations if the original signer wants to revoke the proxy delegation before the delegation period expires. The downside is that in all of these schemes, if the original signer needs to delegate the signing capability to the same proxy signer again, the whole procedure should be processed again.

Our Contribution: In this paper, we present a new revocable proxy signature scheme which allows the original signer to revoke proxy delegations whenever necessary. To accomplish this purpose, we solve the revocation problem using designated verifier signature scheme. In our scheme, if the original signer Alice wants to revoke her proxy delegation, she gets trapdoor information from a trusted server called RS to make her possible to simulate a proxy signature indistinguishable from the signatures generated by the proxy signer. Therefore, after the revocation, the signatures generated by the proxy signer are meaningless. In our scheme, we split the message warrant into two parts. In this way, we make our scheme efficient when the original signer needs to delegate the signing capability to the same proxy signer again after the revocation. We believe that it is usual situation that the original signer delegates signing capability on similar kinds of messages to the same proxy signer multiple times in the workplace.

The rest of this paper is organized as follows. In section 2, we outlines the notations used throughout this paper, the basic idea of our scheme, designated verifier signature scheme used to construct our scheme, and the security requirements of the proposed scheme. In section 3, we propose a revocable proxy signature scheme and discuss its security properties in section 4. Finally, we make a conclusion in section 5.

II . PRELIMINARIES

A. Notations

- p, q : large primes such that $q \mid p - 1$
- g : a generator of a multiplicative subgroup of \mathbb{Z}_p^* of order q
- $H(\cdot)$: a collision resistant one-way hash function mapping $H : \{0,1\}^* \rightarrow \mathbb{Z}_q$
- m : message to be signed by the proxy signer
- m_w : message warrant composed of IDs of the original signer and the proxy signer, and other information on the proxy delegation except the delegation period
- m_{wp} : the warrant for the proxy delegation period related with m_w
- (x_A, y_A) : the key pair of the original signer (Alice)
- (x_B, y_B) : the key pair of the proxy signer (Bob)
- (x_T, y_T) : the key pair of the timestamp server (TS)
- (x_{rk}, y_{rk}) : the revocation key pair generated by the revocation key generation server (RS)

B. Basic Idea

The proposed scheme consists of a verifier and four participants – the original signer, the proxy signer, the revocation key generation server RS, and the timestamp server TS. The verifier can be anyone. RS generates a revocation key pair (x_{rk}, y_{rk}) for the original signer and maintains a bulletin board where information about the proxy delegation and revocation are posted. This bulletin board is accessible to anyone with a read-only permission. Only RS can write on the bulletin board. TS is responsible for issuing three timestamps – t_{begin} , t_{sign} , or t_{end} . The timestamp t_{begin} is issued to RS to record the time when the proxy delegation begins and t_{end} to record the revocation time of the proxy delegation. The timestamp t_{sign} is issued to the proxy signer to record the exact time of the proxy signature generation. Usually the message warrant is composed of the IDs of the original signer and the proxy signer, proxy delegation period, and some other information related to the message. In our scheme, we split the message warrant into two parts – m_w , m_{wp} . In our scheme, m_w is called the message warrant and m_{wp} is called the warrant for the proxy delegation period. m_w is composed of the IDs of the original signer and the proxy signer, and other information on the proxy delegation except for the proxy delegation period. m_{wp} only contains the valid proxy delegation period.

If Alice wants to delegate the signing capability to Bob, Alice sends (m_w, m_{wp}) to RS to request the revocation key pair. RS gets t_{begin} from TS and generates a revocation key pair (x_{rk}, y_{rk}) . RS then posts $(m_w, m_{wp}, y_{rk}, t_{begin})$ on the bulletin board and sends it to Alice and Bob. Alice creates a partial proxy delegation key (m_w, r_A, s_A) and delivers it to

Bob. Bob gets t_{sign} from TS and generates a proxy signature with the partial proxy delegation key, public revocation key y_{rk} , his own secret key, and t_{sign} . Later, if the proxy delegation period specified in m_{wp} expires or Alice wants to revoke the proxy delegation before m_{wp} expires, RS gets t_{end} , posts it on the bulletin board, and sends the corresponding secret key x_{rk} to Alice. Thereafter, Alice can generate a proxy signature which is indistinguishable from the signatures generated by Bob using x_{rk} . Therefore, the signatures generated by Bob after t_{end} is useless and anyone will know the exact times when the proxy delegation period begins and ends.

After the revocation of the proxy delegation, if Alice wants to delegate the proxy capability to Bob again with the same message warrant m_w , she does not have to generate a new partial proxy delegation key (m_w, r_A, s_A) . Whenever Alice wants to delegate her signing capability to the same proxy signer again, she sends m_w and new m_{wp} to RS. RS then generates a new revocation key pair and posts new y_{rk} and new t_{begin} on the bulletin board. Bob can use the partial proxy delegation key previously received from Alice. We believe that in the workplace, it happens often that one delegates the signing capability on similar kinds of messages to the same proxy signer several times in the workplace. In such situations, our scheme would be advantageous than previously proposed revocable proxy signature schemes.

C. Designated Verifier Signature Scheme

In our scheme, the way of simulating proxy signatures by Alice is an important concern to success the revocation. To accomplish this, we apply designated verifier signature scheme proposed by Jakobsson, Sako, and Impagliazzo [2]. In their scheme, a designated verifier himself can efficiently simulate signatures indistinguishable from the signer's signatures. Since the public keys of the signer and the designated verifier are both included in the verification step, anyone can verify the signature. However, unlike ordinary digital signature schemes, no one can be convinced that who the real signer is, except the signer and the designated verifier.

In our scheme, if the original signer Alice can get x_{rk} , she can simulate the proxy signature which is indistinguishable from the signatures generated by Bob. Since Alice cannot simulate a signature without x_{rk} , x_{rk} can be viewed as a trapdoor for Alice to simulate a proxy signature for any messages. x_{rk} is generated by RS and kept secret until the revocation. If the revocation occurs, x_{rk} is revealed only to Alice.

D. Security Requirements

The security requirements for proxy signature are first specified in [8,9], and later enhanced by [4]. We discuss the

security requirements of the proposed scheme based on [4], but with some additions on those related to the revocation functionality.

(i) Verifiability: From the proxy signature, a verifier can be convinced of the original signer's agreement on the signed message.

(ii) Strong identifiability: Anyone can determine the identities of the corresponding proxy signer from a proxy signature.

(iii) Strong unforgeability: Only the designated proxy signer can create a valid proxy signature on behalf of the original signer. In other words, the original signer and other third parties who are not designated as proxy signers cannot create a valid proxy signature before revocation.

(iv) Strong undeniability: Once a proxy signer creates a valid proxy signature on behalf of an original signer, he cannot repudiate the signature creation against anyone else.

(v) Prevention of misuse: The proxy signer cannot use the proxy secret key for purposes other than generating valid proxy signatures. In case of misuse, the responsibility of the proxy signer should be determined explicitly.

(vi) Revocability of the proxy delegation: Once the secret revocation key is disclosed to the original signer, she can generate a signature which is indistinguishable from the signature generated by the proxy signer. This confirms the verifier that the proxy signer does not have any authority to sign a message on behalf of the original signer anymore.

(vii) Efficient multiple proxy delegation: After the revocation, if the original signer wants to delegate the signing capability to the same proxy signer with the same message warrant again, the proxy signer can reuse the proxy signature generation key.

III. PROPOSED SCHEME

Our scheme is based on the discrete logarithm problem and uses partial delegation with warrant scheme. Our revocable proxy signature scheme is as follows:

Phase 1. Revocation Key Pair Generation

1. The original signer Alice sends m_w and m_{wp} to the proxy signer Bob and RS.
2. RS generates a key pair (x_{rk}, y_{rk}) such that $x_{rk} \in \mathbb{Z}_q^*$ and $y_{rk} = g^{x_{rk}} \mod p$.
3. RS requests the timestamp t_{begin} to TS for the record of the time when the revocation key pair is generated. This means that the proxy delegation begins.
4. RS posts $(m_w, m_{wp}, y_{rk}, t_{begin})$ on the bulletin board accessible by anyone and sends $(m_w, m_{wp}, y_{rk}, t_{begin})$ to Alice and Bob.
5. Alice and Bob will check that $(m_w, m_{wp}, y_{rk}, t_{begin})$ from RS is the same as the information on the bulletin board.

Phase 2. Proxy Key Generation

1. Alice chooses a random number $k_A \in \mathbb{Z}_q^*$ and computes the partial proxy delegation key (m_w, r_A, s_A) as follows.

$$r_A = g^{k_A} \mod p$$

$$s_A = x_A H(m_w, r_A) + k_A \mod q$$

Alice sends (m_w, r_A, s_A) to Bob in a secure manner.

2. To confirm the validity of (m_w, r_A, s_A) , Bob verifies if the following equation holds:

$$g^{s_A} = y_A H(m_w, r_A) r_A \mod p.$$

3. If this holds, Bob computes the proxy signature generation key x_p as:

$$x_p = s_A + x_B H(m_w, r_A) \mod q.$$

The corresponding proxy signature verification key is then

$$y_p = (y_A y_B)^{H(m_w, r_A)} r_A \mod p.$$

Phase 3. Proxy Signature Generation

Bob generates a proxy signature on the message m as follows:

1. Bob sends m and m_w to TS.
2. TS gets m_{wp} from the bulletin board and generates a timestamp t_{sign} .
3. TS selects a random number $k_T \in \mathbb{Z}_q^*$ and computes the following:

$$r_T = g^{k_T} \mod p$$

$$s_T = x_T H(m, m_w, m_{wp}, t_{sign}, r_T) + k_T \mod q.$$

TS sends (t_{sign}, r_T, s_T) to Bob.

3. Bob checks whether $g^{s_T} = y_T H(m, m_w, m_{wp}, t_{sign}, r_T) r_T \mod p$ holds or not.
4. If this holds, Bob selects three random numbers a, b, k from \mathbb{Z}_q^* .
5. Bob computes w and z as follows:

$$w = H(m, m_w, m_{wp}, g^a y_{rk}^b, g^k, t_{sign})$$

$$z = k - x_p (w + a) \mod q.$$

6. The proxy signature consists of the following:

$$(m, m_w, m_{wp}, t_{sign}, r_A, r_T, s_T, y_{rk}, a, b, w, z).$$

Phase 4. Proxy Signature Verification

The verifier checks the validity of t_{sign} , computes y_p , and checks the validity of w as follows:

$$g^{s_T} = y_T H(m, m_w, m_{wp}, t_{sign}, r_T) r_T \quad (1)$$

$$y_p = (y_A y_B)^{H(m_w, r_A)} r_A \mod p \quad (2)$$

$$w = H(m, m_w, m_{wp}, g^a y_{rk}^b, g^z y_p^{w+a}, t_{sign}). \quad (3)$$

Phase 5. Proxy Revocation

There are two cases when the proxy revocation could occur. One is when m_{wp} expires and the other is when Alice wants to revoke the proxy delegation before m_{wp} expires. In both cases, RS gets t_{end} and posts it on the bulletin board to notify that the revocation occurred. That is, $(m_w, m_{wp}, y_{rk}, t_{begin}, t_{end})$ is left on the bulletin board. RS also sends the secret revocation key x_{rk} to Alice. Once Alice gets the secret revocation key x_{rk} , she can generate a proxy signature on the message m , m_w , and m_{wp} just like Bob does in an indistinguishable way as follows:

1. Alice gets (t_{sign}, r_T, s_T) from TS.
2. Alice randomly selects $\alpha, \beta, z \in \mathbb{Z}_q^*$.
3. Alice computes w, a , and b in this order.

$$\begin{aligned} w &= H(m, m_w, m_{wp}, g^a, g^z y_p^\beta, t_{sign}) \\ a &= \beta - w \\ b &= x_{rk}^{-1}(\alpha - a) \bmod q \end{aligned}$$

4. The simulated proxy signature is:

$$(m, m_w, m_{wp}, t_{sign}, r_A, r_T, s_T, y_{rk}, a, b, w, z).$$

We can show that this transcript is valid. Equations (1) and (2) can be checked and computed easily. The validity of (3) is checked as follows:

$$\begin{aligned} w &= H(m, m_w, m_{wp}, g^a, g^z y_p^\beta, t_{sign}) \\ &= H(m, m_w, m_{wp}, g^{a+bx_{rk}}, g^z y_p^{(w+a)}, t_{sign}) \\ &= H(m, m_w, m_{wp}, g^a y_{rk}^b, g^z y_p^{(w+a)}, t_{sign}). \end{aligned}$$

Phase 6. Multiple Proxy Delegation to the Same Proxy Signer

Later, if Alice wants to delegate the signing capability to the same proxy signer Bob again with the same m_w and new m_{wp} , Alice sends the m_w and new m_{wp} to Bob and RS. That is, phase 1 for the revocation key pair generation is executed. Alice can skip phase 2 this time. That is, Bob can use the same proxy signature generation key x_p . In phase 3, Bob generates a proxy signature with x_p and newly generated public revocation key y_{rk} . Phase 4, phase 5, and phase 6 can be processed as before.

IV. ANALYSIS OF THE PROPOSED SCHEME

In this section, we analyze that the proposed scheme satisfies the security requirements of proxy signatures. The proposed scheme also provides a revocation mechanism.

(i) Verifiability: The proxy signature consists of $(m, m_w, m_{wp}, t_{sign}, r_A, r_T, s_T, y_{rk}, a, b, w, z)$ in the proposed scheme. From message warrant m_w , any verifier can determine the identity of the original signer and the proxy signer. That is, the verifier can be convinced of the original signer's agreement on the proxy signed message.

(ii) Strong identifiability: In our scheme, identity information of a proxy signer is included explicitly in the message warrant m_w . Thus, anyone can determine the identity of the proxy signer.

(iii) Strong unforgeability: We consider two attack scenarios as follows. First, the original signer would try to forge a proxy signature before he revokes the proxy delegation. Second, a malicious attacker would try to forge a proxy signature by eavesdropping (m_w, r_A, s_A) in phase 2. In both cases, the proxy secret key x_p is needed to generate the proxy signature generation and the secret key x_B of the proxy signer Bob is needed to get x_p . Since x_B is protected under the discrete logarithm assumption, the proposed scheme is unforgeable in both cases.

(iv) Strong Undeniability: No one can know the proxy signer's secret key due to the difficulty of the discrete logarithm problem, only the proxy signer knows his secret key. Therefore, once a proxy signer creates a valid proxy signature, he cannot repudiate it, because the proxy signature is created by using his private key x_B .

(v) Prevention of misuse: If the proxy signer uses the proxy key pair for other purposes, it is his responsibility because only he can generate the proxy signature with his secret key. Therefore, the scenario of proxy signer's misuse is impossible. Moreover, the original signer or the malicious attacker's misuse is also prevented, because they cannot compute for a valid proxy key pair.

We show that the proposed proxy signature scheme provides a multiple revocation mechanism.

(vi) Revocability of the proxy delegation: Once the original signer gets the revocation secret key x_{rk} and the timestamp t_{sign} , he can simulate the proxy signature indistinguishable from the signature generated by the proxy signer as many times as he wants.

(vii) Efficient multiple proxy delegation: After the revocation of the proxy delegation of the original signer, if the original signer needs to delegate the signing right to the same proxy signer with the same warrant m_w , the original signer would request the revocation key to RS again. Once RS generates a key pair and posts the public key of the pair with t_{begin} on the bulletin board, the proxy signer can generate a proxy signature without going through the proxy key generation step. That is, the proxy signer can use the same proxy signature generation key and the verification key. Therefore, it is efficient to

delegate the signing capability to the same proxy signer with the same message warrant.

V . CONCLUSIONS

In this paper, we propose a proxy signature with revocation mechanism using designated verifier signature scheme. In our scheme, it is possible to verify whether or not the proxy signature was generated during the valid delegation period. If the original signer wants to revoke the delegation rights of the proxy signer, the original signer has the ability to generate a proxy signature by himself with the help of the revocation key generation server. Therefore, the proxy signer's signature becomes meaningless. After the revocation, if the original signer wants to delegate the signing rights to the same proxy signer on the same message warrant m_w again, only RS needs to generate a new pair. And the same proxy signature generation/verification key can be used. Therefore, it is easy for our scheme to delegate to the same proxy signer with the same message warrant several times.

REFERENCES

- [1] M.L.Das, A.Saxena, and V.P.Gulati, "An efficient proxy signature scheme with revocation," *Int. Journal Informatica*, vol. 15, no. 4, pp.455-464, 2004.
- [2] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," *Advances in Cryptology - EUROCRYPT '96, volume 1070 of LNCS*, pp.143-154, 1996.
- [3] S. Kim, S. Park, and D. Won, "Proxy signatures, revisited," *Proceedings of International Conference on Information and Communications Security, volume 1334 of LNCS*, pp. 2223-232, 1997.
- [4] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its applications," *Proceedings of 2001 Symposium on Cryptography and Information Security (SCIS 2001)*, Japan. pp. 603-608, 2001.
- [5] E.J.-L. Lu and C.-J. Huang, " Cryptanalysis of a time-stamped proxy signature scheme," *Int. Journal of Computational and Numerical Analysis and Applications*, Vol.5, No.2, pp. 106-115, 2004.
- [6] E.J.-L. Lu., M.-S. Hwang, and C.-J. Huang, "A new proxy signature scheme with revocation," *Applied mathematics and Computation* 161, pp.799-806, 2005.
- [7] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for delegating signing operation," *Proceedings of 3rd ACM conference on Computer and Communications Security*, pp. 48-57. 1996.
- [8] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Trans. Fundament.*, Vol. E79-A, No. 9, pp.1338-1353, 1996.
- [9] S.-H. Seo, K.-A. Shim, and S.-H. Lee, "A mediated proxy signature scheme with fast revocation for electronic transactions," *TrustBus 2005, volume 3592 of LNCS*, pp. 216-225, 2005.
- [10] H.-M. Sun, " Design of Time-stamped proxy signatures with traceable receivers," *IEE Proc. Comp. Digital Techn.* 147 (6), pp. 462-466, 2000.

A Robust Method for Registration of Partially-Overlapped Range Images Using Genetic Algorithms

J. W. Branch¹, F. Prieto², and P. Boulanger³

¹ Escuela de Sistemas, Universidad Nacional de Colombia – Sede Medellín

² Departamento de Eléctrica, Electrónica y Computación, Universidad Nacional de Colombia – Sede Manizales

³ Department of Computing Science, University of Alberta – Canada

Abstract— *Registration is a fundamental stage in the 3-D reconstruction process. We consider the problem of Euclidean alignment of two arbitrarily-oriented, partially-overlapped surfaces represented by measured point sets contaminated by noise and outliers. Given two approximately aligned range images of a real object, it is possible to carry out the registration of those images using numerous algorithms such as ICP. Basically the task is to match two or more images taken at different times, from different sensors, or from different viewpoints. In this paper, we discuss a number of possible approaches to the registration problem and propose a new method based on the manual pre-alignment of the range images of arbitrarily-oriented surfaces followed by an automatic registration process using a novel genetic optimization algorithm in 3-D data registration. Results for real range data are presented with precision and robustness, combined with the generality of genetic algorithms. This procedure focuses on the problem of obtaining the best correspondence between points through a robust search method between partially overlapped images.*

Index Terms— *3-D reconstruction process, range images, registration*

I. INTRODUCTION

Reconstruction is the process whereby real objects are reproduced within computer memory. Physical characteristics such as dimension, volume, and shape are represented in digital form. The task of surface reconstruction of 3-D objects from range images covers several stages: acquisition, registration, integration, segmentation, and adjustment, which when they are combined, transform a set of partial images of the object into a complete 3-D model [1].

The misalignment that is unavoidably produced when two or more images have been taken from different views, and without any control of the relative positions of the sensor and the object, becomes the central problem of registration. The purpose of the registration process is to align these views in such a way that the object's shape is recovered with the highest precision.

During this process two situations become evident. First, it is not possible to determine which of the coordinate system points of one image matches with the correspondence points of another image. This is known as the matching problem, and is the most time-consuming stage during the execution of the algorithm. Second, a transformation is required in the

three-dimensional information of one of the images regarding its coordinate system and its relationship to the image that was chosen as its reference.

The objective here is to adjust both images using common information between them. Because of the inexact nature of the data and the uncertainness of the common surfaces, the procedure to calculate this transformation is iterative and is guided by the strategies and metrics that a particular algorithm uses. Due to this, the registration process is one of the slowest and most delicate stages in the process of 3-D reconstruction. The quality of the alignment process determines the quality of the model that will be obtained.

Since 1992, with the appearance of the ICP algorithm (Iterative Closest Point) [2], there are many variants which have appeared to mitigate the deficiencies of this method. This algorithm states a basic scheme for the obtention of the alignment, by minimizing a cost function based in the sum of the square of the distances between the points of the images; the basic procedures involves the features' identification, matching of corresponding features and the alignment of these correspondences by means of the evaluation of a metric for the error [2], [3]. This method is composed of two basic procedures: The first one is to find the correspondent points and the second one, to estimate iteratively the transformations for these points until satisfy a precision level.

Another approach for the registration of images consists in determining a set of correspondences through a process of points correspondence searching, instead of the classical approach, based in distance. The approach based in searching presents several advantages against the distance based method, for instance: It does not require a fine pre-alignment, the data set of the image to be registered has not to be a subset of the reference image and besides, because it does not perform a combinatory exploration, guided through a domain created from the neighbors which are located around the point on the image to be registered, what permits to obtain a better correspondence between data.

In a general way, the approach based in searching consists in finding a solution near to the global minimum in a reasonable time and a way to perform this searching is by means of genetic algorithms (GA).

The Genetic Algorithms are computational method based in the natural evolution, in which, a population of individuals which represent a possible solution is evolved through a

succession of cycles of selection, reproduction, mutation and replacement until finding the desired solution [4].

In this paper, we show a procedure based on a Genetic Algorithm for the registration of a pre-aligned image pair. This procedure focuses on the problem of obtaining the best match between points through a robust search method on images that are partially overlapped. This set of matches allows the calculation of transformation which precisely registers the images.

This paper is organized as follows: Section 2 presents a literature review. Section 3 describes the methodology used to do the registration of a pre-aligned image pair using a Genetic Algorithm. Section 4 presents realized experiments, and in Section 5, the conclusions of this work are presented.

II. ICP ALGORITHM (Iterative Closets Point).

A set of points is moved in a rigid way, in such a way they be aligned in the best possible way with the corresponding CAD model, through the following iterative procedure:

1. In the first iteration step, for every point of the image to be registered $X = (x_1; x_2; \dots; x_n)$, it is calculated the nearest point to the reference image $Y = (y_1; y_2; \dots; y_n)$, where every point x_i corresponds to the point y_i . This is the part of the algorithm which is more time consuming. As the first step result, it is obtained a sequence of the nearest points of the reference image corresponding with the sampled points on the image to be registered.
2. In the second step of every iteration, the rigid movement M is calculated in such a way that the transformed data points $M(x_i)$ be the nearest to its corresponding points y_i , where the target function to be minimized is:

$$\sum_{i=1}^n \|y_i - M(x_i)\|^2$$

This least squares problem can be solved explicitly. The translational part of M brings the mass center of X onto the mass center of Y . The rotational part of M can be obtained as the unitary eigenvector corresponding to the maximum eigenvalue of a symmetrical matrix 4×4 . The solution eigenvector is not more than the unitary quaternion of the rotational part of M .

3. In the third step, the positions of the data points are updated through $X_{new} = M(X_{old})$.

Now, the steps 1 and 2 are repeated, using the data of the updated points, while the change on the mean square error is kept under a pre-selected threshold. The ICP algorithm always converges monotonically at a local minimum, because of the value of the target function is always decremented in the steps 1 and 2. In a general way, the classical ICP can be seen in the algorithm 3.1.

```
Registration ICP()
begin
  while Error < EMAX do
    1. Sampling Images
    2. Matching Selection
    3. Matching Rejection
    4. Calculation of the Transformed
  end
end
```

Algorithm 3.1. Classical ICP.

III. MATCHING METHOD OF RANGE IMAGES USING A GENETIC ALGORITHM (ICP+GA)

The literature review about the problematic of registration reveals the numerous attempts to solve that problem. Among them, the ICP algorithm has an outstanding place, in spite of its serious limitations. Another approach to register to range images, is finding the geometrical transformation through a searching space, more than the searching based on correspondences of the methods based on ICP. In these case, the goal is finding a searching space of geometrical transformations, a solution which can be used to align precisely two views. A reasonable way to perform this searching is through the use of stochastic optimization techniques such as Genetic Algorithms. This approximation generally is considered to provide thick registration. However, several operators can be combined, such as heuristic local searching's, to obtain precise alignments during the convergence process.

The searching of precise alignments is a problem that can be approach from the view point of the optimization. The genetic algorithms are one of the recent tools that permit to find solutions by means of the searching in big spaces. The general principle of a genetic algorithm is to submit to a evolution process to a individuals population codified as chromosomes, which represent possible solutions of a searching problem. During the evolution, every individual is assigned with a fitness value obtained form a specifically defined function for the problem being solved. This function, called fitness function must be designed in such a way that favor to the most suitable as the solution of the problem. The assigned fitness to every individual is kept in mind to select the progenitors to participate in the reproduction process, which consists in interchange the genetic material contained in a couple of selected individuals to generate two new individuals or two new possible solutions of the problem, which, according to a mechanism of replacement, are incorporated into the population. The new descendent individuals are besides subjected to a mutation process, which consists in a random perturbation of its genetic material, with the objective of giving variability and to enrich the exploration of the possible solutions of the problem represented as chromosomes. Finally, after a determined number of fitness assignment, reproduction, mutation and replacement cycles, called generations, the best solution of the problem is chosen, that is to say, the individual with best fitness.

Brunnstrom and Stoddart [4] proposed a method that integrates the classical ICP method with a genetic algorithm to couple free form surfaces. Here an alignment is obtained with a genetic algorithm, which is later refined with the ICP. The main problem treated by Brunnstrom and Stoddart is to find a corresponding set of points between the two views. For it, dense samples are taken on both views and proceeding to perform the searching with a genetic algorithm that associates points between views, guided by the fitness function that goes counting the number of good correspondences using the invariants of translation and rotation, such as the relative orientation of the normal surfaces and the relative distance between points. In this thesis a chromosome represents a point assignation on both views.

Robertson and Fisher [5] proposed a parallel genetic algorithm which reduces the computational time, but its solution is not more accurate than the ones obtained with the first method. In this proposal, the individuals of a population are vectors formed by six parameters, which represent a transformation.

Silva *et al.* [6] proposed a method for the registration of range images, making two key contributions: The hybridization of a genetic algorithm with the heuristic optimization method of hill climbing, and a measurement of the performance of the interpretation of the surfaces different to the classical metric, based on the calculation of the mean square error between corresponding points on the two images after the registration. The performance measurement proposed in this work, consists in calculating the fraction of points that stay overlapped in the view A and in the view B after the registration. This method is specialized in searching the parameters of a transformation formed by six values, three parameters of rotation, and three parameters of translation.

Yamany *et al.* [7] used a genetic algorithm for registration of partially overlapped 2-D and 3-D data by minimizing the mean square error cost function. The method is made suitable for registration of partially Overlapped data sets by only considering the points such that $p_i \in S_1 \cup S_2$, where S_1 and S_2 are space bounding sets for the two data-sets. Unfortunately, the authors give very few details about their genetic algorithm, focusing on the Grid Closest Point transformation they use to find the nearest neighbor.

Salomon *et al.* [8] apply a so-called differential evolution algorithm to medical 3-D image registration. Differential evolution uses real-valued representation and operates directly on the parameter vector to be optimized.

A recent survey about usage of genetic algorithms for range data registration was presented by Chow *et al.* [9]. For handling partially overlapped data, the media of the remainders is used as an error metric. This improves the robustness, but turns un-applicable the method when the overlapping is under 50%. An advanced dynamic operator of mutation is introduced, what improves the registration error, and helps to avoid early convergence. A trying to improve the precision is done, using dynamic borders. When the genetic algorithm has converged, the searching space is reduced, and the genetic algorithm is applied again.

It is difficult to compare the different algorithms. Every researcher uses a different image base, which makes it very difficult to compare results due to the different metrics each employs.

Sometimes, the strategy to pre-align the images can guide the process to a convergence which obtains an erroneous solution. As well, the strategies that exhaustively explore the space correspondences and transformations are computationally expensive. Although a reject may be made of the erroneous couples, this is not an adequate parameter to guarantee an adequate adjustment. Evaluation of the accuracy of the adjustment is another item that requires attention. It is the easiest way to compare the obtained model with another model, synthetic or real.

Another topic that aspects the performance of the method is the images' size. Modern scanners can offer elevated resolutions because the density of information of the images is

high. Because of this, many sub-scanning strategies are proposed to reduce the number of corresponding points to guide the registration, the uniform random scanning, and the uniform scanning of the normals [10]. An-other consideration in the registration problem are the rejection rules.

These are many strategies to clean the matches, discarding the ones that are incorrect. One of the main rules is the exclusion of points at the boundaries. Its application is inexpensive and excluded regions are not overlapped. The parametric method offers advantages related to convergence speed and minimization to reach superior levels of accuracy. Therefore, it must be considered that the combination of parametric minimization methods form an acceptable registration.

Genetic algorithms have been previously applied to the registration problem; however, the complexity of the space search has become a major challenge. A proposal to use genetic algorithms in the registration problem of two views of approximately aligned range images is presented and described. This proposal is based on searching a set of points that when taken as entrance to Horn's method [11], a very good transformation is obtained that allows the integration of images with a very small margin of error. The algorithm 3.2 shows a general diagram of the proposed method.

In the following paragraphs it will be explained in detail each one of the stages that compose the proposed method.

```

ICP+GA Registration()
begin
    1. Pre-alignment and obtention of the overlapping area
    2. Points sampling
    3. Sub-domain determination
    4. Matching optimization by means of GA
end

```

Algorithm 3.2. Proposed Method for the registration of range images partially overlapped using genetic algorithms (GA).

A. Pre-alignment and Obtaining of the Overlapped area

Generally, as initial stage of the registration process, a previous process is required, which permits to find a global solution for range image registration. That is due to the fact that different types of acquisition devices generate partial images of the objects within different coordinates system. The coordinates system are altered due to occlusion problem in regions which are difficult to scan, or in objects of big size, when it is necessary to move to acquisition device. The reference coordinates systems in every image can be altered in terms of translation, rotation or a combination of both, however, the scaled parameter generally is not altered between partial samples, and is not considered a problem of the registration.

Because is possible to find images whose coordinates system different significantly, the proposed method requires an initial pre-alignment of the images. Usually, the performed works in registration of range images do not consider explicitly a pre-alignment stage, that to say, it is assumed that the images are close enough, or that the initial position of the views does not affect the registration process. The pre-alignment of the views improves the convergence time of the method, and warranties to find an adequate solution for the registration of images. Without a pre-alignment process, the registration method could take an excessive time to find the solution, or they could

not find it. For example, the traditional registration method ICP, requires that the images be close enough to warranty the convergence. The problem of automatic pre-alignment is a research topic within registration, called thick registration, which tries to get the images close enough so that a fine registration method works rightly.

Once the image set has been pre-aligned, is possible to calculate a common area between two images (A y B). This area between the images is called overlapped area. The overlapped area consists in the set of pair points which have a distance lower than a threshold λ :

$$AB = \{(a_i b_l, a_k b_l, \dots, a_p b_q) / i, k, \dots, p \in I_A \wedge j, l, \dots, q \in I_B\}$$

where I_A , I_B are the set of indexes of points in each one of the images A y B respectively, a_i is the closest point to b_j , this is, $Dist(a_i, b_j) = Min(Dist(a_r, b_j))/r \in I_A$.

The overlapped areas are necessary in the process of registration due to this ones are taken as reference to perform a right alignment. That is to say, every registration method searches, in general, to match rightly the overlapped area of the images. The overlapped area constitute the most important reference parameter in the registration process, and the adequate matches are searched on, therefore, on pairs of view which does not exist overlapped area is not possible to perform a right registration of the images.

B. Points Sampling

Given two images of ranges A and B where A is the image model and B is the image to be registered, it is a random selected set of N points that belongs to the overlapped area in B and establishes, for each one of them, a subset of points or sub-domain in A . The sub-domains contain m points near the closest point in A for each point in B . This approach of sub-domains reduces the space search and betters the global efficiency of the algorithm. The establishment of the domains has a critical computational step; that is, searching the closest point in A to each one of the points of the selected sample in B . Because this implies both calculating and comparing the distances to all the points which make up the overlapped area in A . Such a search is improved by implementing a K-d tree structure.

C. Sub-domain Determination

The division of the searching space into sub-domains, reduces the computational cost to find the right matching point of a selected point on the reference image. However, is not possible to warranty that inside the searching space of every sub-domains such point exists.

The probability of existence of a solution within every domain augments in relationship with the size of this. Thus, if every sub-domain has the size of the available points cloud, the probability to find the solution is 100% (See Figure 1).

The sub-domains are formed by the set of points P_i , in such a way that for every sample, $i \in B$, $P_i = (a_i, a_j, \dots, a_k) / i, j, \dots, k \in I_A$ and constitute a set of near points, circularly symmetric, this is, $Dist(\{a_i, a_j, \dots, a_k\}, b_i) < \beta$, where β is the neighborhood radius, and I_A is the index of the points on the image.

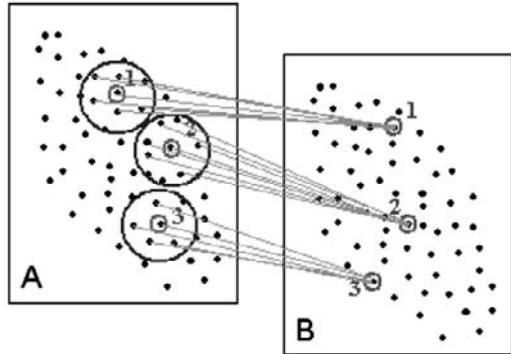


Fig. 1. Sub-domains determination.

D. Matching Optimization by Means of GA

The genetic algorithms constitute an adequate tool to solve the optimization problem due to its implicit parallelism in the searching, its ability to find and keep multiple optimal in every generation of the evolution and its ability to optimize non derivable criteria. In general, the GA codify every possible solution in individuals by means of representation schema; for every individual, it is estimated a fitness function which suggests the level of quality of the implicit solution within the individual. For every generation, every individual is evolved by means of the application of genetic operators as crossing and mutation. As it was stated previously, given two range images A and B , where A is the reference image and B is the image to be registered, the searching of the best points on A which couple with a points sample selected on B , is done by a genetic algorithm, which is composed by three elements: the representation scheme, the fitness function and the configuration of the genetic operators.

Representation scheme. It is represented as a chromosome of size N , that is, to each one of the points of the selected samples in view B there is a corresponding gene of the chromosome. Each gene contains an index that identifies a point within the neighborhood corresponding to a point as defined in view A . Figure 2 illustrates this representation.

Image A →	12	25	78	1
Image B →	1	2	3		N

Fig. 2. Representation scheme of a chromosome.

Gene 1 corresponds to the first point of the sample, whereas gene 2 corresponds to the second point of the sample and subsequently to the N -th point of the sample taken in view B . For instance, in Figure 2 gene 1 contains value 12, which means that point 12 is found within the sub-domain corresponding to the first point of the sample in B . Twenty-five (25) is an index of a point-from-view A that belongs to a neighborhood of points close to point 2 of the sample taken in view B . Each point of the sample taken in view B has a defined neighborhood of points in view A from which the respective gene will take values.

Aptitude function. The aptitude function measures the average error between the points of the overlapped areas

originating in the registration of the views. Each individual can be seen as a set of points with their respective couples translated into a transformation by Horn's method. The transformation is applied to the two views and the average error of this registration is assigned as the aptitude of an individual. The more accurate the individual, the smaller the error:

$$\varepsilon = \sqrt{\frac{1}{N} \sum_{i=1}^N (P_i - R_i)^2}$$

Parameter P denotes each point in the overlapped area in view A obtained by applying each transformation. Parameter R is each point in the overlapped area in view B after applying the transformation.

Genetic operators. The proposal presented for a two-view registration applies a simple cross with only one cut point, in which the parents' genetic content is exchanged on each side of the cut point in order to generate two new (See Figure 3). In turn, the mutation operator varies the information of each gene according to the mutation probability, taking into account the defined neighborhoods for each point represented. That is, if gene i represents the i -th value of the sample taken in view B , and it has to be mutated, a respective point in the defined neighborhood is selected at random in view A , and it is changed by the former value.

The sampling of N points of view B , is only performed once during the whole of the genetic algorithm, what means that the genetic algorithm is specialized in the searching of points that get the best coupling with the selected sample. The pre alignment of the images permits to reduce the searching space for this procedure.

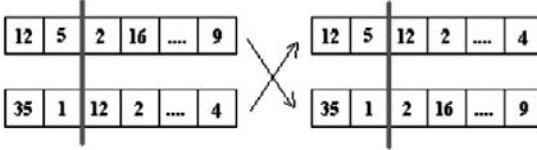


Fig. 3. Cross with a single cut point.

IV. EXPERIMENTS AND RESULTS

The procedure of optimization of the matching by means of GA, is validated with a set of tests, to demonstrate the effectiveness of the proposed method (ICP+GA), which correspond to: Analysis of the convergence of the error and the time, front to the methods ICP and ICP+N. Finally, it is demonstrated the robustness of the proposed method, with respect to the initial alignment of a pair of range images, front to ICP and ICP+N, by means of one intensive experimental test.

Comparison of the error and time convergence. This experiment consists in measuring the convergence of error and time for the registration of range image pairs of a scanned real object which serves as reference for the registration process. The error convergence test was executed fixing the error threshold at 1×10^{-3} y 1×10^{-6} and running the method iteratively until it converges. The results show that as for all the tests, the proposed method converges in less number of iterations (see Tables 1 y 2).

Table 2. Convergence for 1×10^{-3} .

Test	Iterations			Time (seconds)		
	ICP	ICP+N	ICP+GA	ICP	ICP+N	ICP+GA
Test 1	13	12	9	3.125	7.327	180.325
Test 2	17	15	11	6.325	15.327	235.235
Test 3	17	15	11	5.325	13.254	210.254

Table 3. Convergence for 1×10^{-6} .

Test	Iterations			Time (seconds)		
	ICP	ICP+N	ICP+GA	ICP	ICP+N	ICP+GA
Test 1	15	14	13	5.125	7.327	235.658
Test 2	21	15	13	8.251	19.325	220.325
Test 3	18	16	13	6.016	18.327	345.658

Analysis of the robustness of the method proposed with respect to the initial alignment. The test consists in the average of a set of 30 registrations of pairs of range images with different initial alignments. For each pair of images, the image to register is rotated each 5° , from 10° to 70° (see Figure 4). The images were registered with methods ICP, ICP+N and ICP+GA, and it were calculated the averages of these results for each angle.

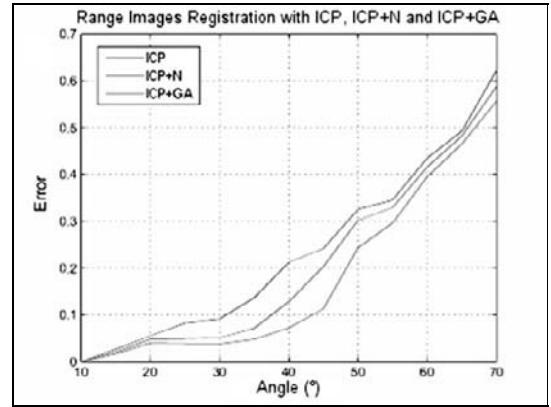


Fig. 4. Errors average of Registration with ICP, ICP+N and ICP+GA.

Figure 5 shows the difference of the errors average of the method ICP+GA with respect to methods ICP and ICP+N. the robustness of the method ICP+GA, it can be seen in the interval 20° to 55° , since this is able to generate registries with higher levels of precision. With reference to method ICP, the ICP+GA obtains the maximum difference in the improvement of the error in angles near 40° . On the other hand, with respect to method ICP+N, the maximum difference is in the angles near 45° . The difference from these angles, begins to decrease until 55° , from which, the errors obtained by the three methods are similar.

The analysis of the test of the differences of errors average made in this experiment, to demonstrate the robustness of the method proposed for registration of partially-overlapped range images using genetic algorithms, is validated statistically by means of the method of the confidence region.

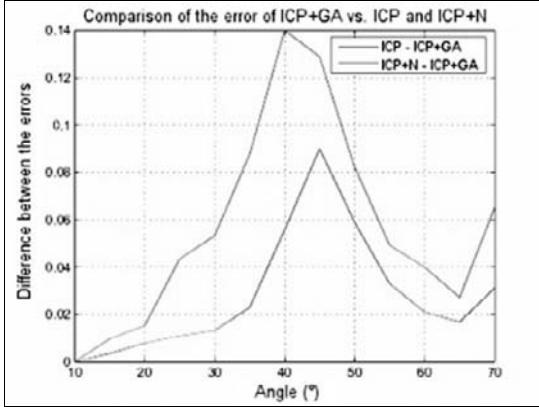


Fig. 5. Difference of the errors average of ICP+GA vs ICP and ICP+N.

Complete registration. The registration process is carried out registering each one of the images with the fusion of the previously registered images. The Figure 6 shows the sequence of the registration process that one obtains for each image of the object mask. Finally the registered object is shown in the Figure 6(f).

In all the cases a smaller registration error was obtained with the model GA (Error average = 0.1011), front to the ICP (Error average = 0.1196) and the ICP+N (Error average = 0.1104).

However, the differences of time between the ICP and ICP+N and the ICP+GA, it is significant for these tests in those that the images contain 35000 points on the average. The ICP and ICP+N methods, took on the average 1.5 minutes, to register each pair of views, while, the method ICP+GA, takes on the average 7 minutes for each pair of views.

V. CONCLUSIONS AND FUTURE WORK

A semi-automatic method has been proposed for the registration of multiple view range images with low overlap that is capable of finding an adequate registration without needing a fine preliminary pre-alignment of the images. This method is based on a genetic algorithm to perform a query of the best correspondence between a set of sample points, starting from an approach based on sub-domains that reduces the space search of the genetic algorithm which implies global algorithm efficiency.

The results obtained by means of the different made experiments, showed that the proposed method, converges to one better solution than methods ICP and ICP+N. The proposed method is more robust than ICP and ICP+N, with respect to the error, when the images to register have an initial alignment with rotation angles among 20° and 55°, which allows to register images without pre-alignment detailed. However, the proposed method uses more computational time in finding the solution.

For future work, the exploration of a parallel version to reduce the computational cost of the proposed method is suggested.

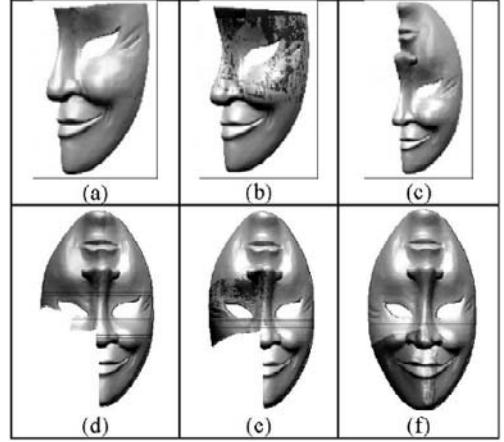


Fig. 6. Registration of the Mask with the ICP+GA method.

REFERENCES

- [1] A. Myers, "Introductory literature review surface reconstruction from three dimensional range data". Technical report, The University of Adelaide, Department of Computer Science, 1999.
- [2] P. J. Besl and N.D. McKay, A method for registration of 3-d shapes. *IEEE Trans. Pattern Anal. Mach. Intell.*, 14(2):239-256, 1992.
- [3] Y. Chen, Object modeling by registration of multiple range images. *Image and Vision Computing*, 10, 1992.
- [4] K. Brunnstrom, Genetic algorithms for freeform surface matching. Technical report, 1996.
- [5] C. Robertson and R. Fisher, Parallel evolutionary registration of range data. *Computer Vision and Image Understanding*, pages 39-50, 2002.
- [6] L. Silva, O. Bellon and K. Boyer, Precision range image registration using a robust surface interpenetration measure and enhanced genetic algorithms. *IEEE Trans. Pattern Anal. Mach. Intell.*, 27(5):762-776, 2005.
- [7] S. Yamany, New genetic-based technique for matching 3-D curves and surfaces. *Pattern Recognition*, 32(10):1817-1820, 1999.
- [8] M. Salomon, G. Perrin and F. Heitz, Differential evolution for medical image registration, pages 201-207, 2001.
- [9] C. Chow, H. Tsui and T. Lee, Surface registration using a dynamic genetic algorithm. *Pattern Recognition*, 37(1):105-117, 2004.
- [10] S. Rusinkiewicz, Real-time acquisition and rendering of large 3-D models. PhD thesis, Stanford University, 2001.
- [11] B. Horn, Closed-form solution of orientation using unit quaternions. *Journal of Optical Society of America*, 4, 1987.

Lips Movement Segmentation and Features Extraction in Real Time

Juan Bernardo Gómez¹, Flavio Prieto¹ and Tanneguy Redarce²

¹Universidad Nacional de Colombia sede Manizales,
Carrera 27 N 64-60, Manizales, Caldas, Colombia
{jbgomez,faprietoo}@unal.edu.co

²Laboratoire d'Automatique Industrielle,
INSA de Lyon, Antoine de SAINT-EXUPERY,
25 avenue Jean Capelle, 69621 Villeurbanne Cedex
tanneguy.redarce@insa-lyon.fr

Abstract- In this paper a new method for lips segmentation in facial video sequences is presented. The method uses a mixture of different color space representations that enhances the mouth area compared to the rest of the skin. It also uses an elliptical clipping condition which delimits the region of interest. The selection of the mouth area is dependent from both the current frame properties and past characterizations. The aim of the segmentation process is to provide a small yet sufficient set of characteristics that can be used in robot control and manipulation. The results show that in most cases accurate landmarks can be obtained using our algorithm.

I. INTRODUCTION

Traditional surgery in laparoscopy requires the aid of a person to manipulate the endoscope according to the instructions of the surgeon. This technique of operation is not optimal because the laparoscope moves constantly, due to the tremors of the hand of the operator. The orders of the surgeon can be interpreted badly by the operator and, therefore, badly executed. This problem can be solved by developing a Laparoscopy Positioning System for a Robot Arm (LPSRA). That is a robot arm controlled directly by the surgeon who manipulates the laparoscope [1]. Using a high level surgeon-robot interface, the surgeon can control the laparoscope by the means of a joystick, the voice, or movements of the head.

The LPSRA that uses an interface based on joystick or pedal, require using the hand or the foot of the surgeon in order to control the camera. These types of interface are not of easy use, because the surgeon has already occupied his hands and feet to control a great variety of surgical tools. Some works tried to use the voice to develop a LPSRA [2], these systems have as disadvantage the background noise, which can be interpreted by the robot like orders. Therefore, it seems that

the best way to control a LPSRA is by using face gestures. The FAce MOUsE system [3], is an interface based on the movements of the face, in which a normal camera observes the head of the surgeon, who controls the laparoscope position and direction with intentional head movements. This way, the surgeon can control a LPSRA by head movements, without a special device. Nevertheless, it seems more natural to control the movement of a robot only with lip movements.

The laparoscope movements of are restricted to four degrees of freedom (DF). The first two DF are movements of perpendicular inclination (pan and tilt) around the point of insertion where the laparoscope is introduced. The third DF is the zoom of the images. The last DF is the laparoscope rotation. This one is always avoided during the surgical operation because the observation of these rotated images demand and additional mental effort [4], so the LPSRA only requires three DF. The normal lips movements allow reproducing these three DF. Of course, the surgeon lips must be visible by the camera.

The operation console of the Surgical System DaVinci is usually located to 3 meters far from the patient. In this console the surgeon does not require mouth covers and therefore he can use his lips to control the laparoscope camera. This control is made by a camera that follows the movement of the surgeon lips. So, the laparoscope movement could be modeled by a state machine, whose inputs are defined by the position lips.

As a first stage for the development of a LPSRA, we present in this paper a lips movement segmentation and features extraction algorithm which works in real time. In last years, the analysis of lips images has received much attention [5, 6]. Specially, because of the visual information allows improving the language recognition.

This paper is organized as follows. Section II introduces several techniques of lips segmentation and tracking. Section III describes our method of segmentation and its different stages. The algorithms for landmarks extraction and features extraction are described in the Sections IV, V respectively. The analysis and results are shown in the Section VI. Finally, the conclusions are presented in the Section VII.

II. RELATED WORK

One way of approaching the lip segmentation problem is finding an appropriate color space transformation that enhances the difference between the lips area and the skin area. In this domain, several works have been developed. In [7] it is stated that, since the red component is the predominant in face area in RGB color space, the separation between the skin and the lips is easier to see in the relation between the G and B components. In [8] it is presented a new set of composed non-linear transformations in the YCbCr color space. They show that the non-linear transformation is able to improve significantly the contrast between the mouth area and the rest of the face. In [9] the authors define a new transformation based on RGB color space which they call the chromatic curve map. That transformation enhances the difference between lips and skin, and allows robust lips detection under non uniform lighting conditions and without any particular make-up. The transformation relies in the fact that the amount of green in the skin area compared to the blue component is greater than in the lips area. In [10] the authors presented a system for automatic lip reading and synthetic reproduction of gestures and audio. In that work they utilized a novel logarithmic HSV color space transformation, and a spatiotemporal neighborhood analysis in order to properly segment the lips area in the video sequence. In [11] the author stated that there are predictable thresholds in HSV space that properly segments the skin and the mouth areas.

In [12] the authors proposed a new method of fuzzy lip segmentation based in a multi-background and one object scheme. They use a dual distance function which has a Euclidean part and an elliptical part. They presented a cost function that is derived from the FCM (fuzzy clustering method) algorithm. However, their method is focused in achieving high detection accuracy rather than reducing computational cost. Another work that uses FCM is the one presented in [13]. In that paper they use a FCM segmentator based in a representation in CIELAB and CIELUV color spaces. An iterative parameter estimation for the membership functions of the FCM process it used, and they show a good convergence in as low as three iterations. In [14] a new region-based lip contour extraction algorithm that combines the merits of the point-based model and the parametric model is presented. Given a robust probability map of the color lip

image generated by a fuzzy clustering method that incorporates shape constraints, a region-based cost function that maximizes the joint probability of the lip and non-lip region is established.

In [15] the authors proposed a method based on a statistical model of shape with local appearance gaussian descriptors. They show that, in some cases the response of the local descriptors can be predicted from the shape. This prediction is achieved by a non-linear neural network.

II. LIPS SEGMENTATION

The first stage in the characteristics extraction process from video face images is the lips segmentation. This process is illustrated in Figure 1. It consists fundamentally of four stages. The first one is a pre-processing stage, in which we use a linear low-pass filter for noise reduction in the original RGB color space. On the second stage, the mouth map is extracted by using some transformations and combinations in many color spaces, in order to emphasize the intensity of the lips. On a third one, an extraction of landmarks from the region of the segmented lips is done. Finally, using the landmarks some metrics of the mouth are computed. Those metrics are used to perform the mouth characterization.

A. Extraction of the mouth map.

In this stage the combination of three different components of color is used in order to emphasize the color information of the lips. The first component used is the green component of the RGB color space. Since images have skin and lips information, the green component is a discriminate characteristic between them. In order to stabilize the results in the whole video sequence, a dynamic expansion of the green component is performed prior to the component threshold operation.

The next component is the result of the map mouth presented in [8]. The mouth region has a greater value of red chromaticity (C_r) than of blue chromaticity (C_b) obtained by using the (YC_bC_r) color space. The value of the chromaticity of the (C_r) component is increased by using its square value. On the other hand, the region of the mouth has a low answer to the relation (C_r/C_b). The expression that governs the component of the mouth is described in the Equation (1)

$$f(C_b, C_r) = C_r^2 \left(C_r^2 - \eta \frac{C_r}{C_b} \right)^2 \quad (1)$$

Where, C_r^2 y C_r/C_b are standardized in the range of [0,255], and η is the relation of the average C_r^2 and C_r/C_b . When the component is computed it is standardizes in the range of [0,255]

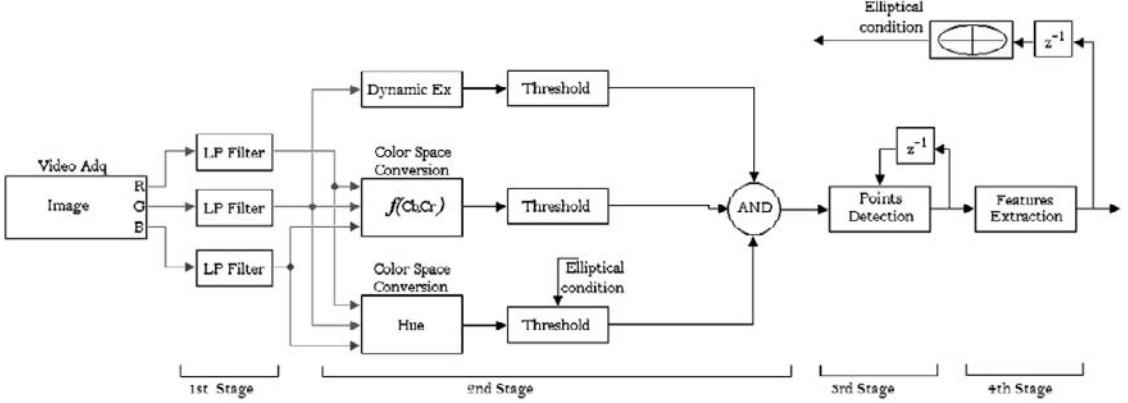


Figure 1. Lips Segmentation Process

The third parameter used is the hue (H) component of the HSV color space, which is an angular color component. Due that the red tone is centered in 0° and 360° , it must be rotated by 120° in order to avoid a double-side threshold operation.

B. Thresholding

For the first component used, an adaptive threshold based on the statistical information of average ($\mu_{g\exp}$) and variance ($\sigma_{g\exp}$) of the image is applied. The dynamic range of the threshold is defined as $\mu_{g\exp} - 1.5\sigma_{g\exp} \leq mouth \leq \mu_{g\exp} - 1.7\sigma_{g\exp}$. Along with the chromaticity component, it also used a variable threshold which depends only of the mean value ($\mu_{f(C_r,C_b)}$). The dynamic range of the threshold is defined as $mouth \leq \mu_{f(C_b,C_r)}$. Finally, the used thresholds are the values defined by [11], where the hue of the lips ranges from 60 to 90.

In the threshold operation process an elliptical condition is applied, which clips the interest region and restricts the search of the mouth for the next iterations, and reduces the level of noise in the binary image. The parts of the image outside the elliptical region are rejected. The description of the selection algorithm is done in the Section V.

IV. LANDMARKS EXTRACTION

For characterization of the mouth an algorithm that makes the search of four landmarks was implemented: the two horizontal corners of the mouth (left and right) and the two vertical corners of the mouth (superior and inferior), as shown in Figure 2.

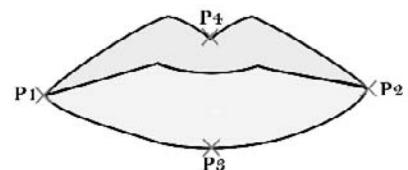


Figure 2. Corners of the Mouth (Landmarks)

The computation of the points is made within the box that surrounds the mouth. This box is found by accumulating the white pixels in each one of the axes (X and Y) on each frame starting from the boundaries. In each case, the selection is made by setting a sum threshold in which the first occurrence is taken into account as a reference row or column. At the end, the references are biased in a proportional way to the vertical and horizontal ranges, in order to cover the whole area of the mouth.

The computation of the box is made in the first iteration. In next iterations the search of the points is done in the neighborhoods of the points found in the previous iteration and having been fulfilled the ellipse condition (Section V). The points search is made by using the information of the best straight line than characterizes the mouth. The slope and cut parameters of the straight line are computed by doing a linear regression with all the points that form the segmented area of the mouth. Nevertheless, the slope value weighed with the obtained one using the resulting slope between the points

P_1, P_2 with a contraction value of 40%. Once we have performed the new main axis calculation, a perpendicular axis that passes through the midpoint between P_1 and P_2 is computed. In the next step the points are computed in a conventional way and it is verified its proximity with the points P_1 and P_2 with the horizontal straight line and of

P_3 and P_4 with the vertical straight line, respectively. When the distance of some of the points surpasses a threshold, the point is projected on its respective straight line and it is moved on it until the cut with the mouth.

V. FEATURE EXTRACTION

By using the computed landmarks the features extraction of the lips is performed. The selected features are: the distance between horizontal corners of the mouth P_1, P_2 , the distance between vertical corners of the mouth P_3, P_4 , and the rotation of the mouth. The ellipse that surrounds the mouth is also computed (Figure 3.).

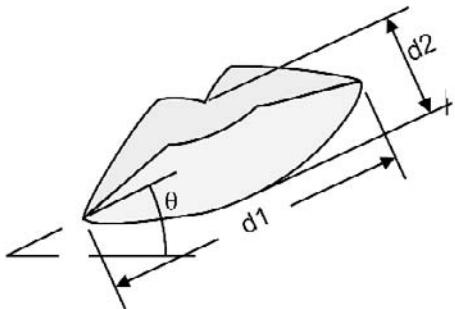


Figure 3. Feature extraction

The ellipse is composed by the center (pCM) two normal vectors (\vec{u}, \vec{v}) and the distances in each one of the axes (r_1, r_2), as shown in Figure 4.

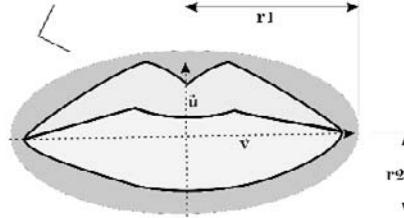


Figure 4. Geometrical description of the elliptical condition

In each one of the computed values the points of the previous iteration are used. The center of the ellipse is computed as the center of mass of the mouth in the current iteration. The normal vectors and the distances of each axis use the landmarks P_1 and P_2 as is shows by the Equation (2) and by the Equation (3).

$$\vec{u} = \frac{\vec{p}_2 - \vec{p}_1}{\|\vec{p}_2 - \vec{p}_1\|} \quad \vec{v} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \vec{u} \quad (2)$$

$$\begin{cases} r_1 = 1.2 \times \max(\|p_1 - pCM\|, \|p_2 - pCM\|) \\ r_2 = 1.2 \times \min(\max(\|p_4 - pCM\|, \|p_3 - pCM\|), r_1) \end{cases} \quad (3)$$

The computed values are used to determine the region of interest (ROI), which is defined by the Equation 4.

$$r^2 < ROI = u^2 + (\gamma v)^2 \quad (4)$$

The elliptical relation (γ) defines the shape of the ellipse, and a bidimensional transformation matrix translates from the image coordinates (x and y) to the ellipse coordinates (u and v). That transformation sets up the appropriate rotation and translation such that the center of the ellipse is located in ($u=0, v=0$), which corresponds to the center of mass of the mouth area in the previous iteration, and the main axis of the ellipse has the same slope as the main axis of the mouth of the current iteration.

VI. IMPLEMENTATION AND RESULTS

The algorithms were implemented in C++ using the MinGW compiler. The system is a Dell Precision 380 with a 3.2GHz Pentium 4 processor and 1 GB of RAM memory, running Microsoft Windows XP Professional. The DAQ system is composed by a SONY teleconference video camera with automatic bright and contrast compensation, and a NI IMAQ 1411 video capture card. Most of the algorithms were

simplified and implemented using integer mathematics, in order to achieve higher performance ratings using mainstream hardware.

The illumination was set up using a ceiling semi-diffuse white light and two white spotlights at both sides of the face. The camera was located in front of the face, slightly over the superior line of the head. The acquisition frame size was clipped to 300x300 pixels, covering most of the mouth area in all cases.

Four video sequences were taken from different subjects, each one having more than 900 frames. Those sequences were analysed using the proposed lip segmentation algorithm and feature extraction. The figure 5 shows examples of segmentation results for each subject. The best results were obtained for the pale skinned, non-bearded subject. The elliptical filter reduces the noise problem that was introduced by the hue component, but in some cases it turned the system unstable and lost the mouth with ease. That instability arises because of the expansion – compression conditions used to adapt the ellipse over the time, and the noise that appears near the mouth area. The first two subjects show segmentation problems in the upper lip.



Figure 5. Segmentation examples

Some lip points extraction results are shown in Figure 6. It is shown that accurate landmarks extraction can be obtained using our algorithm in most cases.

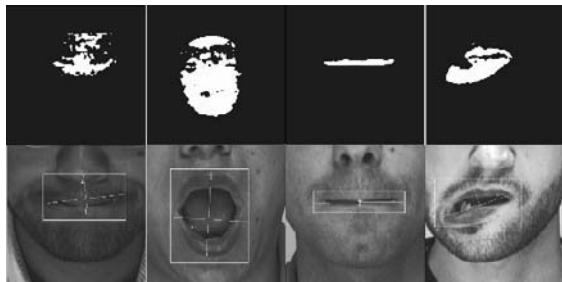


Figure 6. Features extraction of different mouth gestures

The following table shows the different metrics of the mouth (see Figure 6.)

Figure	Vertical distance [pix]	Horizontal distance [pix]	Rotation Angle [deg]
1	22.02	124.04	181.28
2	165.25	120.20	183.34
3	6	149.05	178.85
4	68.01	145.88	165.26

Table 1. Features used for the gesture estimation.

VII. CONCLUSIONS

The algorithm outperforms giving a good balance of speed and accuracy for real-time video applications. Given that several processes depend on the size of the ROI for the computational cost calculation, the speed of the whole system working from a pre-recorded sequence can be as low as 30 fps, or as high as 60 fps. For on-line video acquisition the frame rate is kept at 25 fps in conformance with the approved frame rate for PAL standards. However, if higher frame rates are needed, some of the image processing algorithms can be optimized in a parallel scheme using GPU-based implementation using fixed-point mathematics.

Due to the acquisition camera was set-up to make brightness and contrast auto-compensation, it made difficult to obtain constant results over different illumination conditions. It is object of study to generate a robust algorithm which can eliminate the strong dependency that exists between the lips detection and the illumination and the sensor parameters and dynamical response to light. Experimental results shown that, for images with low levels of contrast, the auto-compensation algorithms disables the rest of the process to perform in a good manner.

One of the main sources of noise is the presence of shadows near the mouth area. Those shadows appear below the nostrils and in some special cases depending on the gesture. The elliptical condition helps out eliminating most of the noise in sparse areas, but noise near the mouth area is still present in the final segmentation.

ACKNOWLEDGES

This work has been supported by the ECOS Franco-Colombiano (ECOS- Nord/COLCIENCIAS/ICFES/ICETEX) program. We would like to thank to the Universidad Nacional de Colombia Sede Manizales and to the LAI-INSA de Lyon.

REFERENCES

- [1] J. M. Sackier and Y. Wang, "Robotically assisted laparoscopic surgery from concept to development," *Surgical Endoscopy*, vol. 8, no. 1, pp. 63–66, Jan. 1994.
- [2] V. F. Murioz, C. Vara-Thorbeck, J. G. DeGabriel, J. F. Lozano, E. Sanchez-Badajoz, A. Garcia-Cerezo, R. Toscano, and A. Jimenez-Garrido, "A medical robotic assistant for minimally invasive surgery," in Proc. IEEE Int. Conf. Robotics and Automation, San Francisco, CA, Apr. 2000, pp. 2901–2906.
- [3] A. Nishikawa, T. Hosoi, K. Koara, D. Negoro, A. Hikita, S. Asano, H. Kakutani, F. Miyazaki, M. Sekimoto, M. Yasui, Y. Miyake, S. Takiguchi, and M. Monden, "Face Mouse: A Novel human-machine interface for controlling the position of a laparoscope," *IEEE Trans. On Robotics and Automation*, vol. 19, no. 5, pp. 825–841, Oct. 2003.
- [4] A. Casals, J. Amat, and E. Laporte, "Automatic guidance of an assistant robot in laparoscopic surgery," in Proc. IEEE Int. Conf. Robotics and Automation, Minneapolis, MN, Apr. 1996, pp. 895–900.
- [5] S. Leung, S. Wang and W. Lau, "Lip Image Segmentation Using Fuzzy Clustering Incorporating an Elliptic Shape Function", *IEEE Transactions on Image Processing*. Volume: 13 , Issue: 1 , Jan. 2004. Pages: 51 – 62.
- [6] A. Liew, S. Hung Leung and W. Hong Lau. "Segmentation color lip images by spatial fuzzy clustering". *IEEE Transactions on Fuzzy Systems*. Volume: 11 , Issue: 4 , Aug. 2003. Pages: 542 – 549.
- [7] Lewis and David M.W. Powers. Lip Feature Extraction Using Red Exclusion. Trent W. Pan-Sydney Workshop on Visual Information Processing, 2001.
- [8] Rein-Lien Hsu, Mohamed Abdel-Mottaleb, Anil K. Jain. Face Detection in Color Images. *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 24, no. 5, pp. 696–706, May 2002.
- [9] N. Eveno , A. Caplier, P.-Y. Coulon. A New Color Transformation For Lips Segmentation. *IEEE Fourth Workshop on Multimedia Signal Processing*, 2001.
- [10] M.Liévin, P.Delmas, P.Y. Coulon, F. Luthon and V. Fristot. Automatic Lip Tracking: Bayesian Segmentation and Active Contours in a Cooperative Scheme. In Proceeding ICMCS, 1999.
- [11] Martina Eckert. Ph.D. Thesis. Compensación de movimiento avanzada para codificación de vídeo.. Universidad Politécnica de Madrid, Marzo 2003.
- [12] S.L.Wang, W.H. Lau, S.H. Leung, A.W.C. Liew. Lip Segmentation With The Presence of Beards. In Proceeding of the IEEE International Conference on Acoustics, Speech and Signal Processing, 2004.
- [13] Ivana Arsic, Roger Vilagut and Jean-Philippe Thiran. Automatic Extraction of Geometric Lip Features With Application to Multi-Modal Speaker Identification. In Proceeding of the IEEE International Conference on Multimedia and Expo (ICME) 2006.
- [14] S.L.Wang,W.H. Lau, S.H. Leung. Automatic lip contour extraction from color images, *Pattern Recognition*, vol. 37, No. 12, pp. 2375–2387. 2004.
- [15] Pierre Gacon, Pierre-Yves Coulon, Gérard Bailly. Non-Linear Active Model For Mouth Inner And Outer Contours Detection. In Proceeding of the 13th European Signal Processing Conference. September, 2005.

DROPLET ACCELERATION IN THE ARC

J. Hu

Department of Mechanical Engineering,
University of Bridgeport,
Bridgeport, CT 06604, USA

H.L. Tsai

Department of Mechanical and Aerospace Engineering,
University of Missouri-Rolla,
Rolla, MO 65409

ABSTRACT

This paper simulates the acceleration of the droplet in the arc during gas metal arc welding process. After a droplet is detached from the electrode, it is accelerated in the high temperature and high velocity arc to the workpiece. The droplet is subjected to several forces, such as the arc plasma shear stress, arc pressure force, surface tension force, gravity force, and electromagnetic force. A comprehensive model is used to simulate the changes of droplet shape, temperature, and velocity during the acceleration in the arc. The transient interaction of droplet and arc plasma is through coupled boundary conditions, thus, no assumptions are needed to simulate the droplet acceleration. The simulated results were compared with the published experimental data and an agreement was found.

I. INTRODUCTION

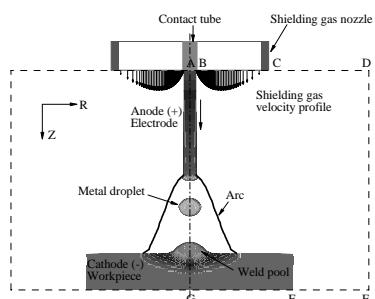


Fig. 1. A schematic representation of a GMAW system including the electrode, the arc, and the weld pool (not to scale).

Gas metal arc welding (GMAW) is an arc welding process that uses a plasma arc between a continuous, consumable filler-metal electrode and the weld pool, as shown in Fig. 1. The high temperature plasma arc melts the electrode and forms a droplet at the electrode tip. After a droplet is detached from the electrode, it is heated up and accelerated in the high temperature and high velocity arc. The accelerated high temperature droplet impinges onto the workpiece and a weld pool forms under the influences of the arc plasma and the periodical impingement of droplets. The influence of droplet impingement on the weld pool varies with the droplet temperature and size, the impingement frequency, and the impingement velocity. The transport of droplets into the weld pool is found largely responsible for the finger penetration commonly observed in the fusion zone [1]. A better understanding of the metal transfer process is

important for improvements in the quality and productivity of welding.

Many researchers [2-8] have investigated the droplet impingement and weld pool dynamics. In their models, the droplet is often assumed to be spherical; the droplet size, temperature and impingement frequency are set to be a constant, the droplet acceleration is either not calculated [2-3] or calculated by applying a plasma drag force [4-7]. Tsao et al. directly assumed the droplet impingement velocity [2] in their model, thus, the droplet acceleration was not calculated. Fan and Kovacevic [3] calculated the droplet impingement velocity, but the droplet acceleration is not calculated, which was set to an experimentally measured value. Fan and Kovacevic [4,5] and Wang and Tsai [6,7] calculated the droplet acceleration by applying an arc plasma drag force on the droplet. As the arc model is not included, the acceleration of the droplet is calculated by applying an arc plasma drag force on the droplet.

The arc plasma drag force F_d is calculated from an empirical formation [8] for a sphere immersed in a fluid stream of uniform velocity by

$$F_d = \frac{\pi}{2} V_{eff}^2 \rho_p R_d^2 C_d \quad (1)$$

where V_{eff} is the mean effective arc plasma axial velocity, which is taken as half of the arc plasma axial velocity, ρ_p is the arc plasma density, R_d is the droplet radius, C_d is the drag coefficient. The drag coefficient C_d depends on the Reynolds number and can be calculated from empirical formulas. Assuming the droplet have a spherical shape and is accelerated to the workpiece with a constant acceleration, the droplet acceleration due to the plasma drag force can be calculated as,

$$a = \frac{3}{8} \frac{V_{eff}^2 \rho_p C_d}{R_d \rho_m} \quad (2)$$

where a is the acceleration of droplet due to plasma drag force, ρ_m is the droplet density.

To calculate the plasma drag force exerted on the droplet using these formulations [4-8], it is required to assume the droplet has a spherical shape and is accelerated to the workpiece with a constant acceleration. The physical properties of the arc plasma, the drag coefficient, and the plasma velocity also have to be assumed. Given the range of temperature found in a welding arc, the appropriate value of the arc plasma properties is difficult to determine. There is also much uncertainty in the drag coefficient and the plasma

flow velocity changes dramatically during the welding process. Furthermore, the shape of the droplet changes along the way as it is transported to the workpiece [9]. An effective method is needed to simulate droplet acceleration without assuming the droplet shape, the plasma properties, the drag coefficient, and the plasma velocity.

To accurately model the acceleration of droplet in the arc, the transient interaction of the droplet with the arc has to be considered. In this paper, a comprehensive model [10-11] is used to simulate the gas metal arc welding as an integrated system which includes both the metal domain and the arc domain. The electrode melting, droplet formation and transfer in the arc, droplet impingement onto the workpiece and weld pool dynamics are simulated in the metal domain. The heat transfer and fluid flow in the arc plasma and its surrounding gas environment are simulated in the arc domain. The transient interaction of the gas domain and metal domain are coupled through the energy, momentum, and current boundary conditions at each time step. The changes of droplet shape and temperature during droplet growth when it is still attached to the electrode and during the acceleration in the arc are modeled by simulating the fluid flow and heat transfer inside the droplet. The heat exchange between the arc and droplet and the momentum transfer from the arc to the droplet are obtained directly from the arc plasma calculation at each time step. Thus, no assumptions of the arc plasma temperature, properties and velocity and the drag coefficient, and droplet size and droplet shape are needed.

The direct and accurate measurement of droplet velocity and acceleration is difficult to conduct due to the complicated welding process of high speed and high temperature arc plasma. Jones et al. [12] have taken video images of droplets from the moment they were detached to the time they contacted the workpiece. Taken from the video images, the center positions of the droplets were then drawn with time as the flight trajectories. It was found that the flight trajectories could be fitted with quadratic curves within error limits. The first derivatives of these fitted curves were taken as the droplet velocities and the second derivatives were taken as the droplet accelerations. The simulated results are then compared with the published experimental data [12] and a reasonable agreement is found.

II. MATHEMATICAL MODELS

Figure 1 is a schematic representation of a two-dimensional axisymmetric GMAW system, with the computational domain marked by ABCDEFGA. There are three phases inside the computational domain: a solid phase, a liquid phase and a gas phase. The solid phase includes the unmelted electrode and part of the workpiece, while the liquid phase includes the melted electrode, falling droplet, and the weld pool on the workpiece. The gas phase includes the partially ionized arc plasma and shielding gas. Between the liquid zone and solid zone, there is a small zone called mushy zone where the solid and liquid metal coexist. A

continuum formulation [13] was used to handle the metal domain consisting of the solid phase, liquid phase and mushy zone. Latent heat during melting and solidification was considered using the enthalpy method. As the properties of gas are far different from those of metal, two computational domains are used for computational robustness and efficiency. One computational domain is used to calculate the heat transfer and fluid flow in the gas phase and another is used for metal, which includes both solid phase and liquid phase. The heat transfer and fluid flow in both computational domains are coupled with the electromagnetic field.

The differential equations governing the conservation of mass, momentum, and energy based on the continuum formulation given by Chiang and Tsai [13] are employed in the present study, and the current continuity equation is used to calculate the current density distribution. The equations are given below:

Mass continuity

$$\nabla \cdot (\rho \mathbf{V}) = 0 \quad (3)$$

Momentum

$$\begin{aligned} \frac{\partial}{\partial t}(\rho u) + \nabla \cdot (\rho \mathbf{V} u) &= \nabla \cdot \left(\mu_l \frac{\rho}{\rho_l} \nabla u \right) - \frac{\partial p}{\partial r} - \frac{\mu_l \rho}{K \rho_l} (u - u_s) \\ &- \frac{C \rho^2}{K^{1/2} \rho_l} |u - u_s| (u - u_s) - \nabla \cdot (\rho f_s f_l V_r u_r) - J_z \times B_\theta \end{aligned} \quad (4)$$

$$\begin{aligned} \frac{\partial}{\partial t}(\rho v) + \nabla \cdot (\rho \mathbf{V} v) &= \nabla \cdot \left(\mu_l \frac{\rho}{\rho_l} \nabla v \right) - \frac{\partial p}{\partial z} - \frac{\mu_l \rho}{K \rho_l} (v - v_s) \\ &- \frac{C \rho^2}{K^{1/2} \rho_l} |v - v_s| (v - v_s) - \nabla \cdot (\rho f_s f_l V_r v_r) + \rho g \beta_T (T - T_0) + J_r \times B_\theta \end{aligned} \quad (5)$$

Energy

$$\begin{aligned} \frac{\partial}{\partial t}(\rho h) + \nabla \cdot (\rho \mathbf{V} h) &= \nabla \cdot \left(\frac{k}{c_s} \nabla h \right) + \nabla \cdot \left(\frac{k}{c_s} \nabla (h_s - h) \right) - \nabla \cdot \\ &(\rho (\mathbf{V} - \mathbf{V}_s)(h_l - h)) - \Delta H \frac{\partial f_l}{\partial t} + \frac{J_r^2 + J_z^2}{\sigma_e} - S_R + \frac{5k_b}{e} \left(\frac{j_r}{c_s} \frac{\partial h}{\partial r} + \frac{j_z}{c_s} \frac{\partial h}{\partial z} \right) \end{aligned} \quad (6)$$

Current continuity

$$\nabla^2 \phi = \frac{1}{r} \frac{\partial}{\partial r} \left(r \frac{\partial \phi}{\partial r} \right) + \frac{\partial^2 \phi}{\partial z^2} = 0 \quad (7)$$

Ohm's law

$$J_r = -\sigma_e \frac{\partial \phi}{\partial r}, \quad J_z = -\sigma_e \frac{\partial \phi}{\partial z} \quad (8)$$

Maxwell's equation

$$B_\theta = \frac{\mu_0}{r} \int_0^r J_z r dr \quad (9)$$

In Eqs. (3)-(6), u and v are the velocities in the r and z directions, respectively. $\mathbf{V}_r = \mathbf{V}_l - \mathbf{V}_s$ is the relative velocity vector between the liquid phase and the solid phase in the mushy zone. The subscripts s and l refer to the solid and liquid phases, respectively, and the subscript 0 represents the initial condition. p is the pressure; T is the temperature; h is the enthalpy; ϕ is the electrical potential; ρ is the density; μ is the viscosity; k is the thermal conductivity; g is the gravitational acceleration; β_T is the thermal expansion

coefficient; c is the specific heat; σ_e is the electrical conductivity; J , and J_z are current densities, in the respective r and z directions; B_θ is the self-induced electromagnetic field; S_r is the radiation heat loss; μ_0 is the magnetic permeability; k_b is the Stefan-Boltzmann constant; and e is the electronic charge.

The third and fourth terms on the right-hand side of Eqs. (4) and (5) represent the respective first- and second-order drag forces for the flow in the mushy zone. The fifth term on the right-hand side of Eqs. (4) and (5) represents an interaction between the solid and the liquid phases. The second term on the right-hand side of Eq. (6) represents the net Fourier diffusion flux. While the third term represents the energy flux associated with the relative phase motion, and the forth term is used to consider the latent heat of fusion. All the terms mentioned in this paragraph are zero, except in the mushy zone. When Eqs. (4)-(6) are used to calculate the arc plasma, these terms associated with the mushy zone are set to zero and all the thermal physical properties are replaced by those of the arc plasma.

The second-to-last term on the right-hand side of Eq. (5) is the thermal expansion term. The last term of Eq. (4) and Eq. (5) is the electromagnetic force term. The last three terms in Eq. (6) are Ohmic heating, radiation loss, and electron enthalpy flow, respectively.

The coupling of the metal domain and the arc domain are through boundary conditions. For the arc domain, the metal domain was treated as inner obstacles, while the arc plasma temperature, velocity, and pressure distributions were calculated. For the metal domain, a volume-of-fluid (VOF) method [13] was used to handle the free surfaces for the droplet and the surface of the weld pool. Additional body force source terms are added to the momentum transport equations at the metal free surface to consider the effects of surface tension, Marangoni shear stress, arc plasma shear stress and arc pressure. Additional source terms [10] are added to the energy equation for the special treatment of heat transfer near the anode sheath and the cathode sheath.

At the metal surface, surface tension pressure normal to the free surface can be expressed as [15]

$$p_s = \gamma \kappa \quad (10)$$

where γ is the surface tension coefficient and κ is the free surface curvature given by

$$\kappa = -\left[\nabla \cdot \left(\frac{\vec{n}}{|\vec{n}|} \right) \right] = \frac{1}{|\vec{n}|} \left[\left(\frac{\vec{n}}{|\vec{n}|} \cdot \nabla \right) |\vec{n}| - (\nabla \cdot \vec{n}) \right] \quad (11)$$

where \vec{n} is a vector normal to the local free surface which equals the gradient of the VOF function

$$\vec{n} = \nabla F \quad (12)$$

The temperature-dependent Marangoni shear stress at the free surface in a direction tangential to the local free surface is given by [4]

$$\tau_{Ms} = \frac{\partial \gamma}{\partial T} \frac{\partial T}{\partial \vec{s}} \quad (13)$$

where \vec{s} is a vector tangential to the local free surface.

The arc plasma shear stress is calculated at the free surface from the velocities of arc plasma cells immediately adjacent the metal cells

$$\tau_{ps} = \mu \frac{\partial V}{\partial \vec{s}} \quad (14)$$

where μ is the viscosity of arc plasma.

The arc pressure at the metal surface is obtained from the computational result in the arc region. The surface forces are included by adding source terms to the momentum equations according to the CSF (continuum surface force) model [15,16]. Using F of the VOF function as the characteristic function, the surface tension pressure, Marangoni shear stress, arc plasma shear stress, and arc pressure are all transformed to the localized body forces and added to the momentum transport equations as source terms at the boundary cells.

Only half of the entire physical domain is calculated due to the cylindrical symmetry along the centerline AG. The wire feed rate is incorporated through a boundary condition on axial velocity along AB. The imposed shielding gas flow is set through a boundary condition on axial velocity along BC. A constant mass flow boundary condition is used for the open boundaries CD and DE. The temperature boundaries along AD, DE, and EG are determined by the ambient condition, which is set as room temperature. Uniform current density is specified along AB. The voltage is set to zero at the bottom of the workpiece FG.

The current distribution is greatly influenced by the temperature in the arc column and the shape of the metal domain, but it is only slightly influenced by the temperature distribution in the metal domain as the electrical conductivity of metal varies slightly with temperature. Therefore, the current continuity equation and its associated boundary conditions are solved in the entire domain, while other primary variables, including p , u , v , and T , are calculated separately in the metal domain and the arc domain. The current continuity equation is iterated with the transport equations in the arc domain to obtain the current density distribution for both the arc domain and the metal domain. Iterations are required to assure convergence of each domain and then the boundary conditions are calculated from each domain for the coupling between the two domains.

For the metal domain, the method developed by Torrey et al. [14] was used to solve p , u , v , and T . This method is Eulerian and allows for an arbitrary number of segments of free surface with any reasonable shape. The basic procedure for advancing the solution through one time step, Δt , consists of three steps. First, at the beginning of the time step, explicit approximations to the momentum equations (4) and (5) are used to find provisional values of the new time velocities. Second, an iterative procedure is used to solve for the advanced time pressure and velocity fields that satisfy Eq. (3) to within a convergence criterion at the new time. Third, the energy equation is solved.

For the arc plasma domain, a fully implicit formulation is used for the time-dependent terms, and the combined convection/diffusion coefficients are evaluated using an

upwind scheme. The SIMPLE algorithm [17] is applied to solve the momentum and continuity equations to obtain the velocity field. At each time step, the current continuity equation is solved first, based on the updated parameters. Current density and electromagnetic force are then calculated for the momentum and energy equations. The momentum equations and the continuity equation are then solved in the iteration process to obtain the new pressure and velocity. With the new pressure and velocity distributions, the energy equation is solved to get the new temperature distribution. Next, the temperature-dependent parameters are updated, and the program goes back to the first step to calculate the current continuity equation. This process is repeated for each time step until the convergence criteria are satisfied.

III. RESULTS AND DISCUSSION

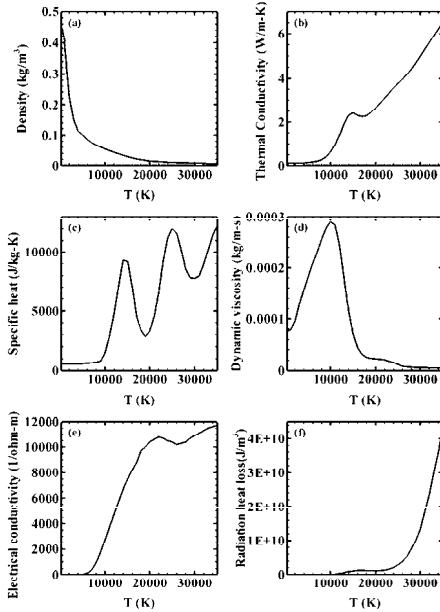


Fig. 2. Temperature-dependant material properties of argon and the volume radiation heat loss taken from [8].

The electrode is mild steel with a 0.16 cm diameter. The workpiece is also a mild steel disk with a 3 cm diameter and a 0.5 cm thickness. The shielding gas is argon and flows out of a 1.91 cm gas nozzle at a rate of 24 l/min. The contact tube is set flush with the bottom of the gas nozzle and is 2.54 cm above the workpiece. The initial arc length is set as 0.8 cm. Temperature-dependant material properties of argon and the volume radiation heat loss are taken from [8] and drawn in Fig. 2. The thermophysical properties of the solid and liquid mild steel are taken from [4] and listed in Table 1. Five current levels in the range of 200 A to 280 A, with 20 A increases, are chosen to study the droplet acceleration at different current levels. For each of the five current levels, the temperature, velocity, arc pressure, and current density

distributions are obtained by solving Eqs. (2)-(9), but only a full set of data is drawn for the current level of 220 A in Figs. 3-8.

Table 1. Thermophysical properties of mild steel and other parameters.

Nomenclature	Symbol	Value (unit)
Specific heat of solid phase	c_s	700 (J kg⁻¹ K⁻¹)
Specific heat of liquid phase	c_l	780 (J kg⁻¹ K⁻¹)
Thermal conductivity of solid phase	k_s	22 (W m⁻¹ K⁻¹)
Thermal conductivity of liquid phase	k_l	22 (W m⁻¹ K⁻¹)
Density of solid phase	ρ_s	7200 (kg m⁻³)
Density of liquid phase	ρ_l	7200 (kg m⁻³)
Thermal expansion coefficient	β_T	4.95×10^{-5} (K⁻¹)
Radiation emissivity	ϵ	0.4
Dynamic viscosity	μ	0.006 (kg m⁻¹ s⁻¹)
Latent heat of fusion	H	2.47×10^5 (J kg⁻¹)
Latent heat of vaporization	H_{ev}	7.34×10^6 (J kg⁻¹)
Solidus temperature	T_s	1750 (K)
Liquidus temperature	T_l	1800 (K)
Vaporization temperature	T_{ev}	3080 (K)
Ambient temperature	T_∞	300 (K)
Surface tension coefficient	γ	1.2 (N m⁻¹)
Surface tension temperature gradient	$\partial\gamma/\partial T$	10^{-4} (N m⁻¹ K⁻¹)
Electrical conductivity	σ_e	7.7×10^5 ($\Omega^{-1} m^{-1}$)
Magnetic permeability	μ_0	1.26×10^{-6} (H m⁻¹)
Work function	ϕ_w	4.3 V
Argon ionization energy	V_i	15.76 (V)

Figures 3-8 show a sequence of the first droplet formation, detachment and transfer in the arc. The temperature and velocity distributions in the meal domain are shown in Figs. 3 and 4, respectively. The arc plasma temperature, velocity, and pressure distributions are shown in Figs. 5-7 and the current density distributions are drawn in Fig. 8.

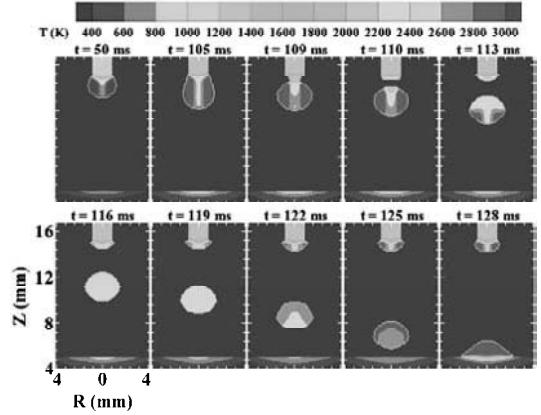


Fig. 3. Temperature distributions in the metal domain for $I = 220$ A.

After the droplet is detached, the temperature distribution in the droplet becomes more uniform through the mixing of fluid flow inside the droplet at the beginning of the separation. The detached droplet is then heated by the surrounding high temperature arc. The detached droplet is also subjected to the electromagnetic force, gravity, arc

pressure, plasma shear stress, and surface tension. At the balance of these forces, the droplet is accelerated to the workpiece. These forces are also responsible for the changes of the droplet shape during the flight in the arc.

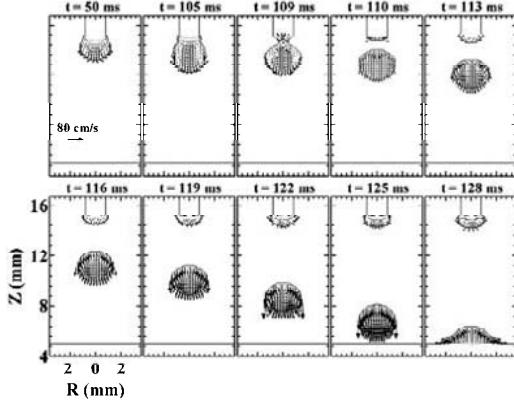


Fig. 4. Velocity distributions in the metal domain for $I = 220$ A.

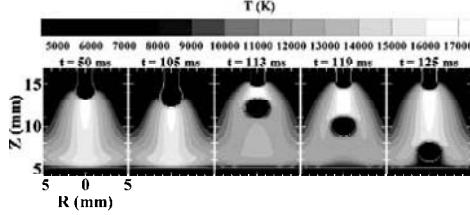


Fig. 5. Arc plasma temperature distributions for $I = 220$ A.

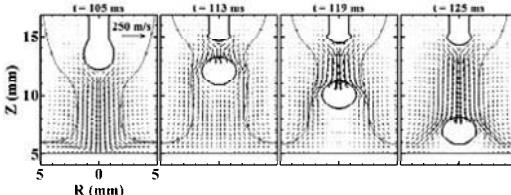


Fig. 6. Arc plasma velocity distributions for $I = 220$ A.

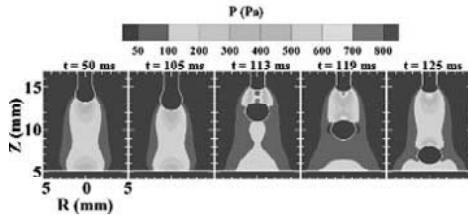


Fig. 7. Arc pressure distributions for $I = 220$ A.

As shown in Fig. 7, there are two high pressure regions before the droplet is detached. One is underneath the droplet, and the other is near the electrode. The high pressure underneath the droplet is caused by the pinch effect of the electromagnetic force, which draws arc plasma flow

underneath the droplet. The pressure increase near the workpiece is due to the stagnation of the plasma flow impinging onto the workpiece. After the droplet is detached from the electrode, new arc plasma is struck between the electrode tip and the top surface of the detached droplet. There are two new high pressure regions, with one under the electrode tip and the other at the top surface of the droplet. The arc pressure difference between the top and bottom surfaces of the detached droplet propels the droplet down to the workpiece. The effect of the plasma shear stress is also remarkable in bringing down the detached droplet. From the plasma velocity distributions in Fig. 6, it can be seen that the plasma flow around the detached droplet is significant.

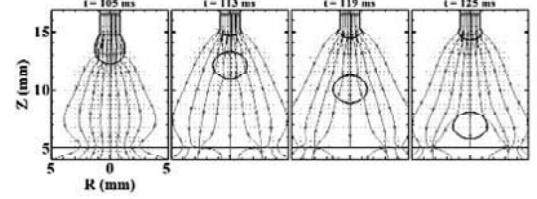


Fig. 8. Current density distributions for $I = 220$ A.

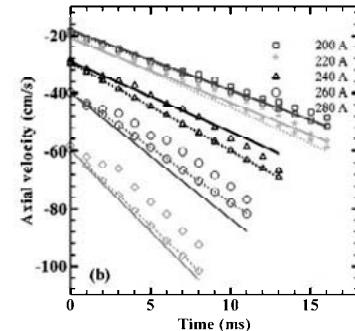
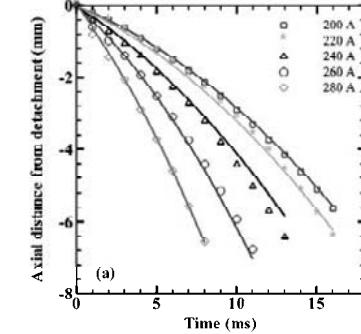


Fig. 9. Computational droplet positions and axial velocities compared with the experimental results at different currents. (a) Droplet flight trajectories; (b) Axial droplet velocities. In (a), the symbols are the droplet center positions from the computational results and the solid line is the fitted curve of the droplet trajectories from the experimental results of Jones et al. [12]. In (b), the symbols are the axial velocities at the droplet center from the computational results; the dashed lie is the axial velocities calculated by taking the first derivative of the computational trajectories; and the solid line

is the velocities calculated by taking the first derivatives of the experimental trajectories.

The arc pressure is high at the top surface of the detached droplet. The high arc pressure does not flatten the droplet, because of the effect of surface tension, which tries to maintain a round droplet shape. The oscillation of droplet shape from oblate to prolate is mainly the work of surface tension. However, the electromagnetic force also helps the droplet to resist being flattened to oblate by the arc pressure. From the current streamlines drawn in Figs. 8, it can be seen that current flows around the detached droplet. Except at the place where the droplet is close to the electrode tip, only a small amount of current flows through the detached droplet. When the droplet moves farther away from the electrode tip, less current flows through it and the electromagnetic force in the droplet also becomes smaller. As can be seen in Figs. 5-7, the detached droplets have a more flattened shape near the workpiece than when they are near the electrode tip.

The droplet center positions from the computational results are compared with the fitted curves of the flight trajectories of Jones et al. [12] in Fig. 9(a). The solid lines are the fitted curves of the droplet trajectories from Jones et al. [12] and the symbols are the center positions of droplets from the computation. As can be seen, the calculated droplet center positions match the fitted curve well, except at some points near the electrode tip. The computational results show the droplets have a bigger acceleration at the early stage of the flight when they are near the electrode tip. While this bigger acceleration could not be shown in the fitted curve, as a constant acceleration was assumed, it was shown in the original flight trajectories made from the video images [12]. The bigger acceleration can also be explained by the computational results. From Figs. 6-7, it can be seen that the plasma flow between the electrode tip and the droplet is stronger and the arc pressure at the top surface of the droplet is higher when the distances between them are shorter. From the axial velocity distributions at the droplet center, which is drawn in Fig. 9(b) with only symbols, the trend of higher acceleration at the early stage is more obvious. The droplet velocities calculated by taking the first derivatives from both the fitted curves of the experimental and computational trajectories are drawn in Fig. 9(b). The droplet velocities calculated from the experimental trajectories are drawn with a solid line for each current level. The droplet velocities calculated from the computational trajectories are drawn with a dotted line and the symbol for each current level. The droplet velocities calculated from the trajectories match well for each current level. However, the velocities at the droplet center from the computational results do not fit well with them, especially at higher current levels. This is because the acceleration of the droplet is higher at the early stage. The droplet size, frequency and acceleration at different current levels are summarized in Table 2 with the corresponding experimental results.

IV. CONCLUSION

A comprehensive model has been used to study the acceleration of the detached droplet in the arc during a gas metal arc welding process. After a droplet is detached from the electrode, it is further heated by the high temperature arc during the acceleration in the arc. The shape of the detached droplet changes in the arc at the balance of electromagnetic force, arc pressure, plasma shear stress, and surface tension. More flattened droplets were found near the workpiece than near the electrode tip, due to the smaller electromagnetic force acted on the droplet further away from the electrode tip. The detached droplet is accelerated to the workpiece by the pressure difference at its top and bottom surfaces and the plasma shear stress as plasma flows pass around the droplet. The acceleration of the detached droplets was higher at the early stage of the flight and was near constant at the later stage. The calculated droplet flight trajectory and droplet velocities are compared with the experimental results and a good agreement was found.

Table 2. Comparison of the droplet size, frequency, and acceleration at different current levels.

Current (A)	Wire feed rate (cm/s)	Droplet radius (mm)	Droplet frequency (Hz)	Droplet acceleration (m/s ²)
200	4.0 (3.8)	1.49 (1.47)	5.5 (5.0)	20.6 (21.0)
220	4.5 (4.3)	1.32 (1.34)	9.2 (8.8)	25.0 (22.4)
240	5.0 (4.8)	1.13 (1.17)	16.8 (13.8)	30.4 (24.5)
260	5.5 (5.3)	0.95 (0.97)	31.5 (23.8)	38.0 (43.8)
280	6.0 (5.8)	0.82 (0.81)	65.0 (59.0)	52.4 (55.8)

Note: The experimental results shown in the parentheses are from Jones et al. [12]. The experiment was continuous constant current welding for 1.6 mm mild steel electrode shielded by Ar-2% O₂. The shielding gas flow rate was 24 l/min and the inner diameter of the nozzle was 19.1 mm. The contacted tube was mounted flush with the bottom of the gas nozzle and was 25.4 mm above the workpiece.

REFERENCES

- [1] C.H. Kim, W. Zhang, and T. DebRoy, "Modeling of Temperature Field and Solidified Surface Profile during Gas-Metal Arc Fillet Welding," *J. Appl. Phys.*, 94, 2003, pp. 2667-2679.
- [2] Z. Cao, Z. Yang and X.L. Chen, "Three-Dimensional Simulation of Transient GMA Weld Pool with Free Surface," *Welding J.*, 2004, pp. 169-176.
- [3] H.G. Fan, and R. Kovacevic, "Dynamic Analysis of Globular Metal Transfer in Gas Metal Arc Welding - A Comparison of Numerical and Experimental Results," *J. Phys. D: Appl. Phys.* 31, 1998, pp. 2929-2941.
- [4] H.G. Fan, and R. Kovacevic, "Droplet Formation, Detachment, and Impingement on the Molten Pool in Gas Metal Arc Welding," *Metall. Trans.* 30B, 1999, pp. 791-801.
- [5] H.G. Fan, and R. Kovacevic, "A Unified Model of Transport Phenomena in Gas Metal Arc Welding including Electrode, Arc Plasma and Molten Pool," *J. Phys. D: Appl. Phys.* 37, 2004, pp. 2531-2544.
- [6] Y. Wang and H.L. Tsai, "Impingement of Filler Droplets and Weld Pool Dynamics during Gas Metal Arc Welding Process," *Int. J. Heat and Mass Transfer* 44, 2001, pp. 2067-2080.
- [7] Y. Wang and H.L. Tsai, "Effects of Surface Active Elements on Weld Pool Fluid Flow and Weld Penetration in Gas Metal Arc Welding," *Metall. Trans.* 32B, 2001, pp. 501-515.
- [8] J.F. Lancaster, *The Physics of Welding*, Oxford Pergamon, 2nd Edition, 1986, pp. 265-267.
- [9] S. Subramanian, D.R. White, D.J. Scholl, and W.H. Weber, "In Situ Optical Measurement of Liquid Drop Surface Tension in Gas Metal Arc Welding," *J. Phys. D: Appl. Phys.*, 31, 1998, pp. 1963-1967.
- [10] J. Hu and H.L. Tsai, "Heat and Mass Transfer in Gas Metal Arc Welding, Part I: the Arc," *Int. J. Heat Mass Transfer*, 2006, in press.
- [11] J. Hu and H.L. Tsai, "Heat and Mass Transfer in Gas Metal Arc Welding, Part II: the Metal", *Int. J. Heat Mass Transfer*, 2006, in press
- [12] L.A. Jones, T.W. Eagar and J.H. Lang, "A Dynamic Model of Drops Detaching from a Gas Metal Arc Welding Electrode," *J. Phys. D: Appl. Phys.* 31, 1998, pp. 107-123.
- [13] K.C. Chiang and H.L. Tsai, "Shrinkage induced fluid flow and domain change in two-dimensional alloy solidification", *Int. J. Heat and Mass Transfer*, 35, 1992, pp. 1763-1770.
- [14] M.D. Torrey, L.D. Cleatum, R.C. Mjolsness, and C.W. Hirt, "NASA-VOF2D: A Computer Program for Incompressible Flows with Free Surfaces," LA-10612-MS, Los Alamos National Laboratory, 1985.
- [15] J.U. Brackbill, D.B. Kothe, and C. Zemach, "A Continuum Method for Modeling Surface Tension," *J. of Computational Physics*, 100, 1992, pp. 335-354.

- [16] A. Celic, and G.G. Zilliac, "Computational Study of Surface Tension and Wall Adhesion Effects on an Oil Film Flow underneath an Air Boundary Layer," Nasa Ames Research Center, 1997.
- [17] Patankar, S.V., "Numerical Heat Transfer and Fluid Flow", New York: McGraw-Hill, 1980.

A Comparison of Methods for Estimating the Tail Index of Heavy-tailed Internet Traffic

Karim Mohammed Rezaul

Centre for Applied Internet Research
(CAIR)

University of Wales, NEWI

Plas Coch Campus, Wrexham, UK
morekba786@yahoo.co.uk

Vic Grout

Centre for Applied Internet Research
(CAIR)

University of Wales, NEWI

Plas Coch Campus, Wrexham, UK
v.grout@newi.ac.uk

Abstract- Many researchers have discussed the effects of heavy-tailedness in network traffic patterns and shown that Internet traffic flows exhibit characteristics of self-similarity that can be explained by the heavy-tailedness of the various distributions involved. Self-similarity and heavy-tailedness are of great importance for network capacity planning purposes in which researchers are interested in developing analytical methods for analysing traffic characteristics. Designers of computing and telecommunication systems are increasingly interested in employing heavy-tailed distributions to generate workloads for use in simulation although simulations employing such workloads may show unusual characteristics. In this paper, we describe some of the most useful mechanisms for estimating the tail index, particularly for distributions having the power law observed in different contexts in the Internet.

I. INTRODUCTION

In the Internet, heavy-tailed distributions have been observed in the context of traffic characterization. It has been observed that the Ethernet traffic is characterized by the self-similar properties [1] and WAN traffic also exhibits self-similar properties [2] specifically when it is associated with WWW transfers [3]. The condition of self-similarity is that the autocorrelation function (ACF) of time-series declines like a power-law, leading to positive correlations among widely separated observations [4].

When the sizes of files transferred from a web-server, the distribution is heavy-tailed to a good degree of accuracy meaning that there are a large number of small files transferred but the number of very large files transferred remains significant. The superpositions of samples from heavy-tailed distributions aggregate to form long-range dependent time series. It is necessary to model the heavy-tail traffic so that networks can be provisioned based on accurate assumptions of the traffic that they carry. Heavy-tail distribution can characterise the Internet traffic more accurately as a number of multiplexed sources (e.g. video, audio, web requests, email, chat, game, etc.) exhibit the properties of selfsimilarity and LRD.

In most cases the tail index (α) is measured by the so-called Hill estimator which has been used widely in the applied finance and Economics [5, 6], insurance [7] and telecommunications [1, 6, 8, 9, 10,] literatures. The distributions having infinite variances are called heavy-tailed and the weight of their tails is determined by the parameter $\alpha < 2$ [9]. The properties of heavy-tailed distributions are qualitatively different to commonly used memoryless distributions such as the exponential, normal or Poisson distributions. The research [2] concludes that such exponentiality assumptions mislead to explore the presence

of heavy-tailed distributions. The heavy-tailed distributions are ubiquitous in the Internet. Paxson [11] observed that wide variability in path characteristics such as losses, round-trip times and bandwidth and high variability is one of the landmarks of heavy-tailed distributions. The distribution of burst sizes, for both ftp and HTTP transfers appears to be heavy-tailed [12] and there is little evidence that interarrival times and transfer times are long-tailed. It is evident [1, 13] that the characteristic of the service process (provided by the Web servers, routers etc.) in Internet-related systems is heavy-tailed which affects the complexity of such systems.

The paper is organised as follows. Section II defines the self-similarity and long-range dependence. Section III describes the methods used for estimating tail index in Internet traffic. Finally the results are presented in section IV.

II. SELF-SIMILARITY AND LONG-RANGE DEPENDENCE

A phenomenon that is self-similar looks the same or behaves the same when viewed at different degrees of magnification or different scales on a dimension and bursty over all time scales. Self-similarity is the property of a series of data points to retain a pattern or appearance regardless of the level of granularity used and is the result of long-range dependence in the data series. Several studies [1, 2, 3, 4, 14] have shown that network traffic often shows self-similarity meaning that network traffic shows remarkable bursts at a wide range of time scales. One of the observations [1] showed that the Ethernet LAN traffic is statistically self-similar and Hurst parameter, H is used to measure the burstiness of the traffic. The traffic burstiness (i.e. large variation of traffic bit rate) occurs due to heavy-tailed traffic. If a self-similar process is bursty at a wide range of time scales, it may exhibit long-range dependence (LRD) and the parameter H lies between 0.5 and 1. Note that LRD does not imply self-similar but the process is both LRD and self-similar for $0.5 < H < 1$.

Long-range-dependence means that all the values at any time are correlated in a positive and non-negligible way with values at all future instants. For a continuous time process $Y = \{Y(t), t \geq 0\}$ is self-similar if it satisfies the following condition [14]: $y(t) = a^{-H} y(a t)$, $\forall a > 0$, and $0 < H < 1$ where H is the index of self-similarity, called Hurst parameter and the equality is in the sense of finite-dimensional distributions. The stationary process X is said to be a LRD process if its ACF (ρ_k) is non-summable [15] meaning that $\sum_{k=-\infty}^{\infty} \rho_k = \infty$

III. METHODS FOR ESTIMATING THE TAIL INDEX

In this section various methods for estimating tail index are described which are used in telecommunication network traffic. The principle for detecting the heavy tailed traffic is that the tail of the distribution decays much more slowly than exponential [16]. In general the Pareto model is widely used as it follows heavy tail distribution. The cumulative distribution for Pareto is

$$F(x) = P[X \leq x] = 1 - \left(\frac{\beta}{x}\right)^{\alpha}$$

where β represents the smallest (positive constant) possible value of the random variable and α the shape parameter indicating tail index. Suppose for a random sample X_1, \dots, X_n from a distribution F satisfying

$$\bar{F}(x) = P[X > x] = 1 - F(x) = \left(\frac{\beta}{x}\right)^{\alpha}$$

$$= \beta^{\alpha} x^{-\alpha} \approx x^{-\alpha} L(x); x \rightarrow \infty, \alpha > 0$$

where L is a slowly varying function satisfying

$$\lim_{t \rightarrow \infty} \frac{L(tx)}{L(t)} = 1$$

A random variable X follows a heavy tailed distribution [4, 6] if $P[X > x] \sim Cx^{-\alpha}$, as $x \rightarrow \infty$, $0 < \alpha < 2$. (1)

The complementary cdf (ccdf) $\bar{F}(x) = 1 - F(x) = P[X > x]$, where α represents the tail index ; $0 < \alpha < 2$. The presence of heavy-tailed distributions in observed data can be explored by equation (1) as follows:

$$\lim_{x \rightarrow \infty} \frac{d \log \bar{F}(x)}{d \log(x)} = -\alpha \quad (2)$$

which appears to be a straight line on log-log axes with slope $-\alpha$ for large x .

A number of log-log complementary distribution (LLCD) plots have been illustrated in [9] to estimate the tail weight. These are plots of the ccdf on log-log axes. Having plotted in this way, heavy-tailed distributions have the property that follows the equation (2). The random variable X has infinite mean when $\alpha \leq 1$, finite mean but infinite variance when $1 \leq \alpha \leq 2$ and finite mean and variance when $2 < \alpha$ [17]. For the traffic rate process X , the autocorrelation function satisfies [18]

$$r(k) \approx ck^{2H-2}; \text{ as } k \rightarrow \infty, 0.5 < H < 1 \quad (3)$$

where the Hurst parameter H measures the degree of long-range dependence in X in terms of tail-index α in (1) and H is given by $H = (3 - \alpha)/2$.

A basic statistical calibration problem is to estimate the shape parameter α which is the negative of the index of regular variation. A popular method to estimate α is called the Hill estimator, developed by B. M. Hill [19]. Suppose X_1, \dots, X_n are random variables (e.g. web file size) from a distribution F and $X_1 > X_2 > \dots > X_n$ be the order statistics. The Hill estimator of α is

$$\hat{\alpha} = \left\{ \frac{1}{k} \sum_{i=1}^k \log \frac{X_i}{X_{k+1}} \right\}^{-1} \quad (4)$$

where k is the number of upper order statistics used in the estimation. Hill plot can be defined as $\{(k, \hat{\alpha}), 1 \leq k \leq n-1\}$

and then the index can be found from a stable region in the graph.

The Hill estimator is the most favourable technique [10] to detect the heavy tailedness of the traffic when the underlying distribution is close to Pareto. The plot sometimes might exhibit excessive bias while the distribution is far from Pareto. In fact, the Hill estimator is designed for the Pareto distribution. Hill plot is not always informative and the alternative estimators described in the literatures are alternative Hill plot abbreviated as AltHill, SmooHill for smoothing Hill plot [10], qq estimator [10, 20] and De Haan's moment estimator [21]. The dynamic qq – estimator [10] is given by

$$\hat{\alpha}_{k,n}^{-1} = \frac{\frac{1}{k} \sum_{i=1}^k \left(-\log \left(\frac{i}{k+1} \right) \right) \log \left(\frac{X_{(i)}}{X_{(k+1)}} \right) - \frac{1}{k} \sum_{i=1}^k \left(-\log \left(\frac{i}{k+1} \right) \right) H_{k,n}}{\frac{1}{k} \sum_{i=1}^k \left(-\log \left(\frac{i}{k+1} \right) \right)^2 - \left(\frac{1}{k} \sum_{i=1}^k \left(-\log \left(\frac{i}{k+1} \right) \right) \right)^2}$$

$$\text{where } H_{k,n} = \frac{1}{k} \sum_{i=1}^k \log \frac{X_{(i)}}{X_{(k+1)}} \quad (5)$$

The dynamic qq-plot can be obtained by plotting $\{(k, 1/\hat{\alpha}_{k,n}^{-1}), 1 \leq k \leq n\}$ which is similar to the Hill plot.

The moment estimator is defined as

$$H_{k,n}^{(r)} = \frac{1}{k} \sum_{i=1}^k \left(\log \frac{X_{(i)}}{X_{(k+1)}} \right)^r \quad (6)$$

where $H_{k,n}^{(1)}$ is the Hill estimator and $X_1 > X_2 > \dots > X_n$ be the order statistics from a random sample size of n . Define for $r = 1, 2$ and then

$$\hat{\gamma}_n = H_{k,n}^{(1)} + 1 - \frac{1/2}{1 - (H_{k,n}^{(1)})^2 / H_{k,n}^{(2)}} \quad (7)$$

Then the moment is estimated by plotting $\{k, \hat{\gamma}_n\}$.

In addition the modified qq plot [7, 16] can be illustrated which is obtained from the following equation by choosing and fixing k .

$$\left\{ \left(\log \left(\frac{X_j}{m} \right); -\log \left(\frac{j}{k+1} \right) \right); \quad 1 \leq j \leq k \right\} \quad (8)$$

where m represents a higher order statistics of a distribution for the samples X_1, \dots, X_n , i.e., $m = X_1 \geq X_2 \geq \dots \geq X_k$ be the order statistics of a distribution. If the data follow approximately Pareto, the plot will look like a straight line with slope α . A least squares line can be fitted through the points with small deviation while computing the slope.

A graphical procedure is introduced in [22], called the Sum plot which suggests a proper value for k by using the well-known Hill estimator. The sum plot is given by

$$S_k = \alpha^{-1} [k \log(k+1) - \sum_{i=1}^k \log i] \quad (9)$$

$$\text{where } \hat{\alpha}^{-1} = \frac{k}{k-1} H_{k,n} - \frac{1}{k-1} \log X^{(1)} \quad (10)$$

$H_{k,n}$ can be found from equation (5). The graph will look

like a straight line when plotting S_k against k and then the slope is estimated from the least squares line.

IV. RESULTS AND DISCUSSION

In this research, we have analysed six different traffic traces, each of sample length (N) 10000. The traces used in the analysis are EPA, NASA-Jul95, NASA-Aug95, ClarkNet, Saskatchewan and Calgary, all publicly available in [23].

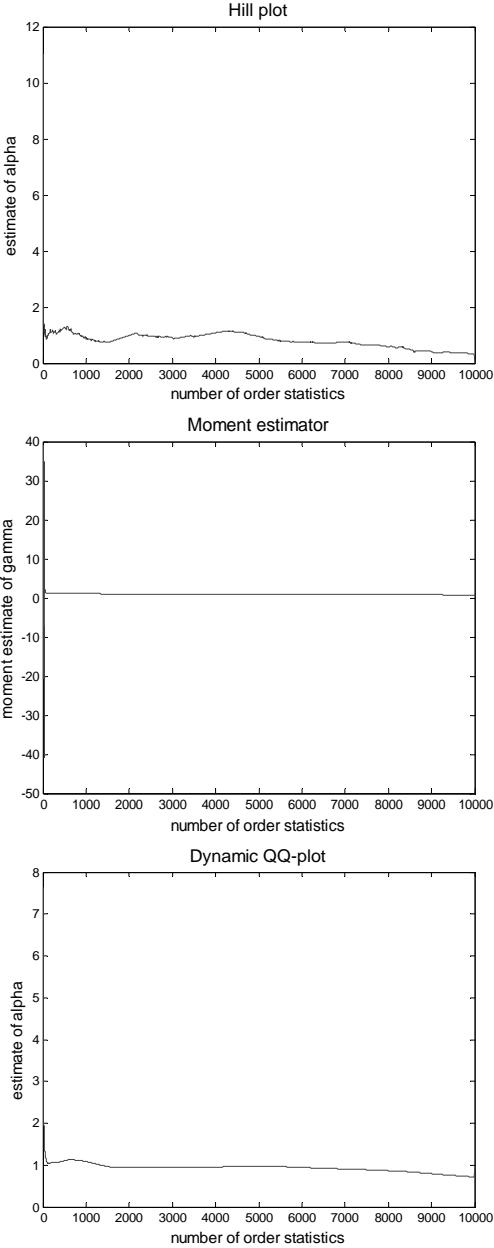


Fig. 1. Estimation of tail index by Hill plot, Dehaan's moment estimator and dynamic-qq plot (EPA-htp traffic)

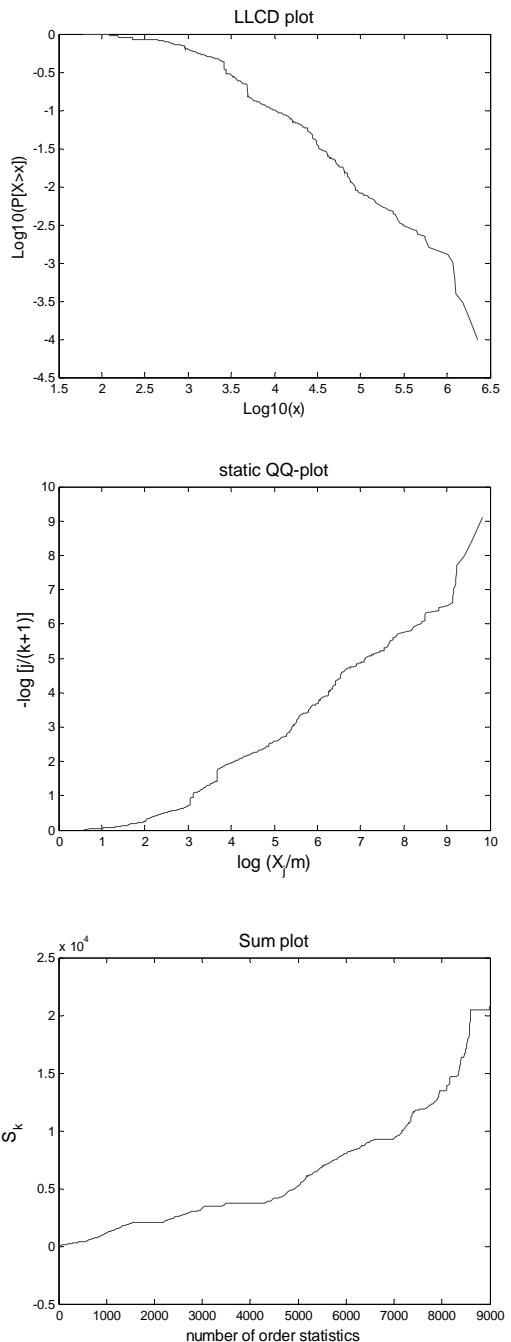


Fig. 2. Estimation of tail index by LLCD plot, static-qq plot and Sum plot (EPA-htp traffic)

The tail index α from these traffic traces is estimated by several methods. Figures 1 and 2 provide a graphical representation of EPA traffic. Results from other estimates are presented in Table I. An instability of the graph in some region has been observed for NASA-Jul95, NASA-Aug95, ClarkNet and Calgary traffic when plotting the moment

estimate of gamma. Clearly the moment estimator is not so informative for these traffic traces. The Dynamic qq (dyn-qq) plot was also a bit unstable for NASA-Jul95, NASA-Aug95 and Saskatchewan traffic.

Here a number of order statistics, $k=9000$ have been chosen for the Static qq (stat-qq) and Sum plots. In most traffic cases, α was found to be less than 2, i.e., there is an infinite variance observed in the traces, which implies the existence of heavy-tailedness in the data traffic. The Sum plot yields an index greater than 2 (i.e., $\alpha > 2$) for NASA-Jul95, NASA-Aug95 and ClarkNet. In particular Hill plot, Static qq plot and LLCD plot are in good agreement as they provide close results to each other as shown in Table I.

Table I. Estimation of tail index for various http traffic by different methods.

Web File	N	Tail index for various methods					
		Hill	moment	dyn-qq	stat-qq	Sum plot	LLCD
EPA	10000	0.764	0.92	0.94	0.74	1.88	0.802
NASA-Jul95	10000	0.583	0.79	1.08	0.57	2.57	0.601
NASA-Aug95	10000	0.619	0.76	0.99	0.60	2.39	0.703
ClarkNet	10000	0.788	1.28	1.11	0.73	2.04	0.810
Saskatchewan	10000	0.830	1.07	1.02	0.82	1.71	0.816
Calgary	10000	0.697	0.80	0.89	0.70	1.76	0.713

V. CONCLUSION

The performance of several estimators of the tail index for heavy-tailed Internet traffic have been studied in this research. In most cases, the moment estimator, dynamic qq plot and sum plot are unable to provide an acceptable measured index because of an unstable region observed in the graph. Hill plot, static qq plot and LLCD plot show a good level of agreement when estimating the index from graphs. Our results show that there are infinite variances (i.e. $\alpha < 2$) observed in the traffic which is indicative of the existence of heavy-tailedness in Internet traffic.

REFERENCES

- [1] W.E. Leland, M.S. Taqqu, W. Willinger, and D.V. Wilson, On the Self-Similar Nature of Ethernet Traffic (Extended Version), *IEEE/ACM Transactions on Networking*, February 1994, pp.1-15,
- [2] V. Paxson and S. Floyd., Wide Area Traffic: The Failure of Poisson Modeling, *IEEE/ACM Transactions on Networking*, June 1995, pp.236-244.
- [3] M. Crovella and A. Bestavros, "Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes", *IEEE/ACM Transactions on Networking*, December 1997, pp.835-846.
- [4] Mark E. Crovella and Lester Lipsky, "Long-Lasting Transient Conditions in Simulations with Heavy-Tailed Workloads", In *Proceedings of the 1997 Winter Simulation Conference*, 1997. pp.1005-1012.
- [5] Jansen, D. and de Vries, C., "On the frequency of large stock returns: putting booms and busts into perspective", *Review of Economics and Statistics*, 1991, 73, pp. 18-24.
- [6] Mark E. Crovella, Murad S. Taqqu and Azer Bestavros Heavy-Tailed Probability Distributions in the World Wide Web, In: Robert J. Adler, Raisa E. Feldman, Murad S. Taqqu (eds.), *A Practical Guide To Heavy Tails*, 1998, 1, pp.3-26.
- [7] P. Embrechts, C. Kluppelberg and T. Mikosh, *Modeling Extremal Events for Insurance and Finance*, Springer-Verlag, Berlin Heidelberg, 1997.
- [8] Dacorogna, M. M., M'ller, U. A. and Pictet, O. V., "Heavy-tails in high-frequency financial data", In *A Practical Guide to Heavy Tails: Statistical Techniques and Applications*, 1998, pp.55-77, Birkhauser
- [9] Mark E. Crovella and Azer Bestavros, "Explaining World Wide Web Traffic Self-Similarity", October 12, 1995, Boston University, Technical Report TR-95-015.
- [10] Resnick S. I. , "Heavy Tail Modeling and Teletraffic data". *The Annals of Statistics*, 1997, vol.25, No.5, pp. 1805-1849.
- [11] Vern Paxson, End-to-End Internet Packet Dynamics, *IEEE/ACM Transactions on Networking*, June 1999, Vol.7, No.3, pp. 277-292.
- [12] Allen B. Downey, "Evidence for Long-tailed Distributions in the Internet", *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, San Francisco, California, USA, 2001, pp. 229 – 241.
- [13] M. Arlitt and T. Jin, "Workload Characterization of the 1998 World Cup Web site", Technical Report, Hewlett-Packard Laboratories, September 1999.
- [14] Walter Willinger, Vern Paxson, and Murad Taqqu, "Self-similarity and Heavy Tails: Structural Modeling of Network Traffic", In *A Practical Guide to Heavy Tails: Statistical Techniques and Applications*, Adler, R., Feldman, R., and Taqqu, M.S., (editors), Birkhauser, 1998.
- [15] Cox D., Long-Range Dependence: Review. H. A. David and H. T. David (eds.), *In Statistics: An Appraisal*, Iowa State Statistical Library, The Iowa State University Press, 1984, pp.55-74.
- [16] Trang Dang D., Sandor M. and Vidacs A., "Investigation of Fractal properties in Data traffic", *Journal on communications*, 1999, XLIX: 12-18.
- [17] Judith L. Jenkins and Jonathan L. Wang, "From the Network Measurement Collection to Traffic Performance Modeling: Challenges and Lessons Learned", *Journal of Brazilian Computer Society*, vol. 5, No. 3, 1999.
- [18] R. H. Riedi and W. Willinger, "Towards an Improved understanding of Network Traffic Dynamics", *Self-similar Network Traffic and Performance Evaluation*, Wiley, 2000, Chapter20, Eds. Park and Willinger, pp. 507-530.
- [19] Hill B.M., "A simple approach to inference about the tail of a distribution", *The Annals of Statistics*, 1975, vol. 3, 1163-1174.
- [20] Kratz M. and Resnick S., "The qq Estimator and Heavy tails". *Stochastic Models*, 1996, 12, pp. 699-724.
- [21] Dekkers A., Einmahl J. and De Haan, L., "A Moment Estimator for the Index of an Extreme Value Distribution", *The Annals of Statistics*, 1989, vol. 17, pp. 1833-1855.
- [22] Bruno C. Sousa, "A Contribution to the Estimation of the Tail index of Heavy-tailed Distributions", PhD thesis, The University of Michigan, 2002.
- [23] Internet traffic archive: <http://ita.ee.lbl.gov/html/traces.html>

IEC61499 Execution Model Semantics

Kleanthis Thramboulidis, George Doukas
Electrical & Computer Engineering
University of Patras
26500, Patras, Greece
{thrambo,gdoukas}@ece.upatras.gr

Abstract- The International Electro-technical Commission (IEC) has adopted the function block (FB) concept to define the IEC 61499 standard for the development of the next generation distributed control applications. However, even though many researchers are working last years to exploit this standard in factory automation a lot of issues are still open. Except from the open issues in the design phase a lot of execution semantics are still undefined making the development of execution environments a difficult task. In this paper the semantics of the execution of the IEC 61499 Function Block model are examined, possible alternatives are investigated and existing implementations are discussed.

Index terms—IEC 61499, Function Block, Factory Automation, IEC61499 execution environment, execution model semantics, distributed control applications.

I. INTRODUCTION

The Function Block (FB) is a well-known and widely used by control engineers construct. It was first introduced by the IEC1131 standard on programming languages for programmable logic controllers, and was later extended by the IEC's 61499 standard [1] to share many of the well defined and already widely acknowledged benefits of object technology. The IEC61499 describes a methodology that utilizes the FB as the main building block and defines the way that FBs can be used to define robust, re-usable software components that constitute complex distributed control systems (DCSs). Complete control applications, can be defined by one or more FB Networks (FBNs) that specify event and data flow among function block or subapplication instances. The event flow determines the scheduling and execution of the operations specified by each function block's algorithm(s).

The standard mentions that “standards, components and systems complying with this part of IEC 61499 may utilize alternative means for scheduling of execution.” From this statement it is clear that some issues have been intentionally open to be defined later by developers. However, in our attempt during last years to develop prototype implementations of execution environments [2][3][4][5] we have confronted a lot of open issues that can result in implementations that will give quite different behaviour for the same FBN. This problem is also recognized by other research groups working towards the implementation of IEC61499 execution environments [6][7][8][9]. This means that a lot of execution semantics have to be further defined by

the standard to avoid the existence of many different execution platforms with different behaviours.

In this paper, the execution semantics of the function block model as presented in the IEC61499 are examined. Open issues are highlighted and discussed and alternative solutions are proposed to address these problems. The execution semantics of the FB instance are first examined, followed by an in depth discussion of the FBN execution semantics. Alternatives are discussed and already existing implementations of these alternatives in today's execution environments are presented.

The remainder of the paper is organized as follows. In the next section a brief introduction to the FB model is given. In section 3, the execution semantics of the FB instance are examined. The execution semantics of FB network are examined in section 4. Section 5 deals with the implementation of the interface of the FBN to the mechanical process, and finally the paper is concluded in the last section.

II. THE IEC 61499 FUNCTION BLOCK MODEL

The FB, the basic construct of IEC61499, consists of a head and a body, as shown in figure 1(a). The head is connected to the event flows and the body to the data flows, while the functionality of the function block is provided by means of algorithms, which process inputs and internal data and generate output data. The sequencing of algorithm invocations is defined in the FB type specification using a variant of statecharts called Execution Control Chart (ECC). An ECC consists of EC states, EC transitions and EC actions, as shown in fig. 1(b). An EC state may have zero or more associated EC actions, except from the initial state that shall have no associated EC actions. An EC action may have an associated algorithm and an event that will be issued after the execution of the algorithm. EC transitions are directed links that represent the transition of the FB instance from one state to another. An EC transition has an associated Boolean expression that may contain event inputs, data inputs, and internal variables. As soon as this expression becomes true the EC transition fires.

FB instances are interconnected to form FBNs, as shown in fig. 2. A FBN may be executed on a single device but it is usually executed on a network of interconnected devices. A device may contain zero or more resources, where a resource is considered [1] to be “a *functional unit*, contained in a *device* which has independent control of its operation and may be created, configured, parameterized, started-up, deleted, etc., without affecting other resources within a *device*.” The use of the term “resource” taken into account the

resource model that is given in [1] is too restrictive and misleading if we consider the meaning of the term in computer engineering according to which a resource is a more general concept that abstractly describes a run-time entity that offers one or more services. Except from the fact that the use of the “IEC61499 resource” is restrictive and misleading, specific arguments for its use are not given. Even more, questions are still open on the semantics and usability of the resource concept and on its realization with real-world artifacts. A special kind of resource may be used to act as container of FB instances, as is the case in the RTAI-AXE execution environment, but this is an implementation issue that should not be defined by a standard that claims that defines an implementation independent specification. This is the reason for not dealing with the IEC61499 resource in the rest of this paper.

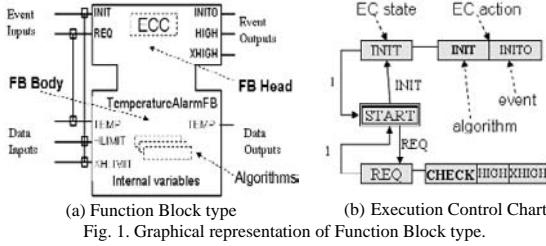


Fig. 1. Graphical representation of Function Block type.

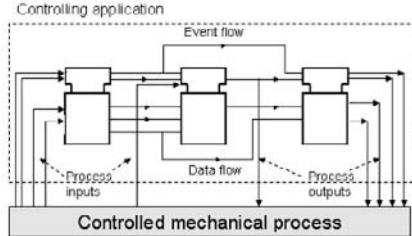


Fig. 2. The control application as a network of interconnected FB instances.

III. FB INSTANCE EXECUTION SEMANTICS

Two main kinds of FB types are proposed by the standard, the basic FB type and the composite FB type. The basic function block type utilizes the ECC to control the execution of its algorithms. The composite function block type is composed of a network of interconnected FB instances and has no ECC, so its execution semantics are quite different from those of the basic FB type. The following subsections address these two kinds of FB type and the event processing policy.

A. Basic Function Block execution semantics

According to [1] the execution of algorithms in basic FB instance is “coordinated by the execution control portion (FB head) of the FB instance in response to events to its event inputs.” A brief description of the timing characteristics of this process is presented in fig. 3. t₂ is the time that the event arrives at the event input of the FB instance and the ECC starts its execution. It is assumed that at a previous time t₁,

the required by the FB instance data, to process this event were made available. At t₃ the execution control function notifies the scheduling function to schedule an algorithm for execution. At t₄ the execution begins and at t₅ the algorithm derives the output data that are associated with the WITH qualifier to the output event of the corresponding EC action (see fig.1). At t₆ the scheduling function is notified that the algorithm execution has ended. The scheduling function invokes at t₇ the execution control function, which signals at t₈ the event that is defined by the corresponding EC action.

The standard assumes the existence of a scheduling function to the associated 61499 resource. However, this assumption except from the fact that implies a big overhead for devices with resource constraints such as IEC-compliant sensors and actuators where a scheduler is not required, it is not actually required, even for devices with no restrictions on resources, since the thread that executes the ECC can also execute the algorithms of the corresponding EC actions. This thread can be either the thread of the FB instance in the case of an active FB instance (FB instance with its own thread of execution) or the thread of the FB container [4] in which the FB instance was injected, as explained in the next section.

In the case of assigning the same thread for the execution of the ECC and algorithms, that is the case of our execution environments[3][4][5], it is clear that the ECC cannot react during the execution of algorithms to the events that occur at the FB instance’s event inputs. However, this is not possible even for the case of having two threads, one for the ECC and one for algorithms as is the case with the standard, since according to [1] “all operations performed from an occurrence of transition t₁ to an occurrence of t₂ (see fig. 4) shall be implemented as a critical region with a lock on the function block instance.”

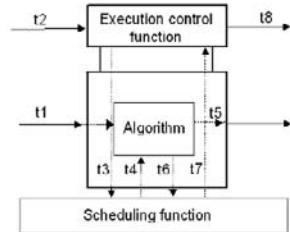


Fig. 3. Execution model of Basic Function Block [1]

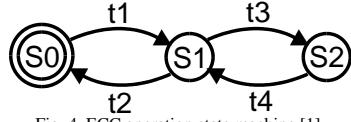


Fig. 4. ECC operation state machine [1].

To further examine this problem, the operation state machine of the ECC presented in fig.4 is used. S₀ represents the idle state, S₁ represents the state of evaluating transitions and S₂ the state of performing the actions. Based on this state machine the following two scenarios are considered:

1. the event has to be consumed by the FB instance before the occurrence of the next event to its event inputs. That is, the transition t₂ should occur before the arrival of the

- next event,
2. the event may occur when the FB instance is in states S1 or S2.

To satisfy the requirement of the first scenario the FBN should be scheduled in such a way that the execution of the FB instance will be terminated before its deadline that should be before the appearance of the next event. For the second scenario, if the loss of the event is permitted by the nature of the application, the event is simply ignored, either wise the event is stored so as to be consumed immediately after the transition t2 to the S0 state. All the above alternatives can be supported by the execution environment given the appropriate notation at the design level. For example the control engineer should define, at design time, for each event the following properties: ‘event loss permitted’ and ‘event consumption before next event’. The latter property will be utilized during schedulability analysis of the FBN to define the deadline of the corresponding FB instance that has to be met by the scheduler.

The solution proposed above and implemented in the context of RTAI and RTSJ-AXE execution environments can also implement the proposed by the standard behavior, if there is a need for such a behavior. After the execution of the ECC the corresponding thread should issue a yield command to the operating system that will result to the rescheduling of this thread, which of course in this time will execute the algorithms of the associated EC actions. If a different priority for the algorithm execution is required the proper update of the thread’s priority is required before the yield operation.

A different approach is proposed in [8] where two threads are used for the execution of FB instance: a) the “event executing” thread, which handles incoming events and execute the ECC, and b) the “algorithm executing” thread, which executes the activated algorithms. This approach was adopted, according to the authors, to allow the acceptance of events by the FB instances during algorithm execution. However, this doesn’t really make any sense if we consider the constraint imposed by the FB model according to which the new incoming event(s) should not trigger an ECC transition before the currently executing FB algorithm/action finishes. The only advantage of this approach i.e., the ability to execute FB algorithms and ECC with deferent priorities can be also obtained in the case of one thread as it was already stated.

B. Composite Function Block execution semantics

As defined in [1] the composite FB type has event input and output, as well as data input and output variables. The WITH qualifier is also supported by the composite FB type. This definition means that the composite FB type could not be considered only as a design time artefact but an implementation-time construct should be defined for the proper implementation of the composite FB instance. This construct may have its own thread of execution if the FB instance is defined at design time as active, or it can be executed by the thread of the FB container (a concept described in the next section) in which the FB instance will be assigned, if defined as passive. Since there is no ECC for the

composite FB type the ECC of the receiver constituent component FB instance will be executed. The remaining execution semantics of the composite FB instance will be the same as those of the FB network diagram execution semantics, which will be examined in the next section.

C. Event processing policy

The standard does not define the event-processing policy not even the clear-event policy, while an unreliable transition evaluation order is defined. To avoid the unpredictable behaviour of the FB-network diagram, the event-processing policy should be defined at the design phase so as the control engineer is aware of the corresponding execution semantics of its design. We consider three alternatives that can be supported by FB-based run-time environments for the processing of input events.

- a) events are processed on a first come order. This is implemented by a traditional FIFO event queue.
- b) events are processed on a priority based order. This can also be implemented by priority queues.
- c) All pending input events are candidates for processing at the time the thread of the FB inserts the running state.

The standard defines that the evaluation order of transitions is defined by the order in which they are declared in the textual FB specification. However, this results in a non deterministic execution, since the control engineer is working with the graphical notation during the ECC construction and editing time and there is no way to define the transition declaration order in textual specification. To address this problem we propose the use of the “evaluation-order priority” property for the transition. This priority has to be defined at the design level. A default priority that leads to a non deterministic evaluation order is also supported.

Regarding the clear event policy an event is considered to be consumed by the system whether this event is used or not in a transition expression of the corresponding state. The event is considered to be consumed in both cases either the transition fires or not. An exception will be supported for the events that are marked as ‘persistent’ in the design time. A persistent-event is cleared only when a transition has been fired by this event.

The assumption adopted by UML2.0 according to which an event may fire more than one transitions according to a guard condition is adopted. If all possibilities are not covered by the guard conditions and no transition is enabled, the event is simply cleared except from the case of a persistence event.

IV. FB NETWORK EXECUTION SEMANTICS

In this section an attempt is made to examine alternative means for implementing FBNs with more focus on scheduling the execution of the operations specified by algorithms of function blocks that constitute applications defined by FBNs.

A. Allocating FB instances to threads

One of the primary open issues for the implementation of the FBN is the allocation of FB instances to threads or processes. The following possible alternatives are considered for the allocation of FB instances to execution threads:

a) All passive FB instances of the FBN are assigned to one thread of execution

This sequential single-threaded approach that is proposed by some research groups [10][11] seems to be inefficient for complex FB networks, as is also depicted in [6][9], and should be avoided.

b) One thread per each FB

This approach, which is simple and straight-forward for devices that have to execute a small number of FB instances, was successfully adopted in the RTSJ-AXE package where the ECC class is defined to extend the RealtimeThread of the real time Java specification. An instance of the ECC class is assigned to each FB instance. However, as the number of FB instances of the FBN increases this approach may introduce a significant overhead since each thread has a cost in terms of device resources.

c) One thread may execute a subset of the FB instances of the FBN

This approach seems to be the most efficient and flexible for large FBNs and since it was successfully adopted in the RTAI-AXE and CCM-AXE packages is studied in more detail in the rest of this section.

B. Allocating a subset of the FBN to a thread

Two possible alternatives are considered in the allocation process of FB instances to system threads: a) allocation is done with the constraint that each FB instance is allowed to be executed by only one thread, b) more than one threads are allowed to execute (in different time instances) the same FB instance.

According to the first scenario the execution of a specific FB instance or a set of FB instances is assigned to a single specific thread. This scenario was first presented in [2] where a first implementation was also discussed by introducing the concept of FBC, which is a single-threaded active object. FB instances are injected into FB containers which handle the execution of those FB instances. The FBC accept input events and dispatch them to its injected FB instances enforcing their execution, i.e., the execution of ECC and corresponding algorithms. Generated output events are also handled by the FBC and are either routed to FBC's queue if the target FB instance belong to the same FBC, or to the Event Connection Manager (ECM) of the device [2]. This approach does not impose synchronization issues on the access of FBs. Each FBC is independent in both aspects of execution and (re)configuration and can communicate with other FBCs through simple communication mechanisms (ECM, DCM) responding to events without imposing complicated synchronization. This scenario was adopted for the prototype implementation of the RTAI Archimedes execution environment [4]. A quite similar implementation approach is proposed in [6] even though the concept of FBC is not explicitly used. However, the decision to implement the IEC61499 resource as a single thread process makes the resource quite similar to our FBC concept and the approach similar to the one described above.

An approach for allocating FB instances to threads with the possibility of an FB instance to be executed by more than one

threads is discussed in [16]. According to this a thread is statically assigned to an event-source and is allowed to execute the FB instances along the propagation path (event path) of the event into the FBN to the corresponding output event-sink (output IPP). To get a better utilization of threads and eventually OS resources than the one obtained in [16] a thread pool can be considered and a demand-led policy can be adopted in thread assignment without any static allocation of FB instances to the thread-pool threads. It should be mentioned that in both cases, FB instances should be considered as shared resources and should be protected from concurrent access by multiple threads, since they are not be reentrant. Mechanism of the OS such as priority inheritance and priority ceiling may be exploited in the case of hard real-time applications to resolve problems such as priority inversion that may occur when multiple threads are allowed to access the same FB instance. Moreover, dynamic priority schedulers may be needed, especially in the thread-pool case, as threads may need to alter their priority as they execute different FBs.

C. FB instance to thread allocation heuristics

The assignment of FB instances to FBCs or threads is not a trivial task for complex FBNs since multiple aspects and contradicting parameters such as OS resource economy and runtime efficiency should be taken into account. The following allocation heuristics can be used in this process.

- FB instances that are sequentially connected in the FBN without the need to be executed concurrently are allocated in the same FBC, as is the case for FBIs B and C in fig. 5a, A and B in fig.5b, and A, B, C, D and E in fig.6.
- For the case of event-path (EP) merging that is shown in fig. 5a two alternatives are possible. The FBIs of one event-path (A, B and C or D, B and C) are allocated in one FBC and the remaining FBIs of the other event path (D and A respectively) are allocated to another FBC. Alternatively the common FBIs of the event paths, i.e., B and C, are allocated to one FBC, and the remaining FBIs of each event-path are allocated to one FBC. An analogous process is followed for the case of event-path splitting. Table II presents the possible allocation scenarios, where the notation {A,B,C} denotes that the FB instances A, B and C are allocated to the same FBC or thread.

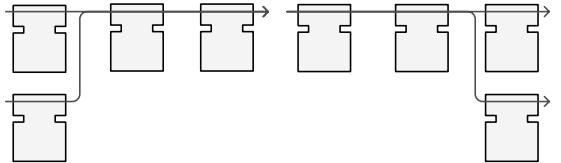


Fig. 5. FB instance allocation scenarios for event-path merging and splitting.

- More alternatives are possible for the case of event-path merging shown in fig. 6. FBIs of one EP can be allocated to one FBC, as for example {A, B, C, D and E} or {F, G, C, H and J} with the remaining FBIs of the other EP either

allocated to one FBC as for example {F, G, H and J} or to other two FBCs as for example {F, G} and {H, J}. A more distributed allocation can also be defined leading to 5 FBCs as shown in Table I.

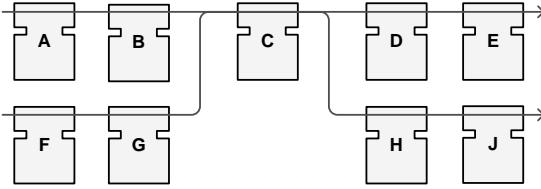


Fig. 6. FB instance allocation scenarios for event-path crossing.

Table I. FB instance-allocation scenarios

FB Network	Thread assignment scenarios		
	2 threads	3 threads	5 threads
EP merging	{A,B,C} {D}	{A} {B,C} {D}	-
EP splitting	{A,B,C} {D}	{A,B} {C} {D}	-
EP crossing	{A,B,C,D,E} {F,G,H,J}	{A,B,C,D,E} {F,G} {H,J}	{A,B} {C} {D,E} {F,G} {H,J}

It is clear that the 2-thread assignment scenarios constitute the most lightweight solutions in terms of OS resource requirements. Scenarios that result in bigger number of FBCs offer greater degree of flexibility and parallelism. For example lets consider the case where the FB instance B of fig. 5a has just been activated as a result of an event propagation through the event path D, B, C. In the case of a 2-thread solution ({A,B,C} {D}) the execution of FB instance B must be completed before an incoming event in the FB instance A can be processed, that is not a restriction in the case of a 3-thread solution such as the ({A} {B,C} {D}).

D. Implementing Event Connections

A first attempt to provide a flexible realization of event connections that would favor run time re-configurability is presented in [12]. The use of the Event Connection Manager was proposed to implement both inter and intra-device connections. Event connections between FBs that are allocated to the same FBC or thread are implemented locally through the use of the FBC event dispatcher and not through the ECM [2]. Specifically for the inter-device connections the use of SIFBs, a special kind of FB proposed by the standard, was disputed since it destroys the implementation independent design that the standard is supposed to ensure. An extended description of the proposed approach to obtain location transparency in FBNs is given in [13]. Regarding the implementation of intra-device connections, either using SIFBs or not, the following alternative implementations are considered:

- Using common function calls. This approach currently adopted by FBRT is inefficient as it imposes a sequential non-preemptable execution scheme.
- Using native signaling mechanisms of the underlying OS. This approach is very efficient but portability is lost.

- Using existing middleware's. This approach provides extra functionality, allows maximum portability, flexibility and favors reconfigurability. An advantage of this approach is also the centralized, single-point of event synchronization. This is an approach adopted in [2][4] where the ECM was implemented on top of a common middleware.

An alternative implementation that greatly simplifies the task of control engineer by hiding communication idiosyncrasies was proposed in [14] and considers the use of the IPCP.

E. Implementing Data Connections

Data overwriting is not an issue in the FBN so there is no need for buffering data values. A single storage location is reserved per each data for the most recent (valid) value to be stored and read when needed. The Data Connection Manager (DCM) concept first introduced in [12] and later implemented in [2][4], is a passive object that provides protected (on the concurrent access point of view) storage elements for FB instance data outputs and also provides the links required by consumers to these storage elements to realize data connections.

V. INTERFACING TO MECHANICAL PROCESS

According to the standard the process interface of a device “provides a mapping between the physical process and the resources. Information exchanged with the physical process is presented to the resource as data or events, or both.” The standard also proposes that this process mapping may be modeled by a special kind of service interface function blocks (SIFBs). SIFBs are adopted by most of the research groups to interact with the controlled process without any further examination of the process interface. However, SIFBs make the design model implementation-platform dependent, so its use should be avoided.

There are various alternatives differing in the level of abstraction offered by the mechanical process interface (MPI) that may even affect the application design. At the lower level the process interface could probably offer a minimum set of trivial I/O services, just like an I/O device driver does. In this case the MPI should implement a great deal of platform dependent I/O functionality including the transformation of data from a hardware specific representation to an IEC compliant representation and vice-versa. Moving to the next level of abstraction the MPI may offer more complex services simplifying the implementation MPIFBs and making them more platform-independent. On an even higher level of abstraction the MPI may offer direct mapping of process parameters to IEC compliant event/data inputs and outputs within the application’s FBN. This solution may require more configuration and initialization effort but makes the use of SIFBs unnecessary (obsolete), thus simplifying the application design and making it more implementation independent. The concept of Mechanical Process Terminator (MPT) and Mechanical Process Parameter (MPP) were defined in [14] to allow an implementation of this highly abstract process interface.

In a first implementation attempt of the Mechanical Process Interface we compromise the higher level of abstraction and move to the 2nd level of abstraction. MPI FBs should utilize services of MPI layer in order to access (read/write) the parameters of the controlled process. These parameters are represented as MPP instances, each of which encapsulates the implementation specific mechanism that enables interfacing with the acquisition card. The current implementation of MPI is based on the comedı acquisition driver [4], thus MPPs refer to comedı device acquisition channels. The MPI can be configured during start-up so that actual process parameters are mapped through appropriate acquisition channels to named MPPs. A MPI FB can then refer to a MPP by its name or the id that is assigned during MPI configuration and access it using a simple API. For instance, an algorithm of an analog output MPIFB can write a value to an analog process actuator that is mapped to the “AO1” MPP, with the following statement:

```
mpi->getMPPAnalogOutputByName( "AO1" ) ->write( value );
```

VI. PROTOTYPE IMPLEMENTATIONS

The FBRT [11] is the first execution environment for IEC61499 FB based control applications. The method invocation approach that is adopted for the implementation of event connections makes the environment not usable for real-time applications and imposes many restrictions to its use in real world applications. Performance measurements for this execution environment are not available.

The RTAI-AXE execution environment (<http://seg.ece.upatras.gr/mim/RTAI-AXEpackage.htm>) exploits real-time Linux to provide a real-time execution platform for FBNs. Its design favors run-time re-configurability. It is supported by automatic code generators that translate the XML based design specifications to C++ code. Performance measurements are presented in [4].

The RTSJ-AXE (<http://seg.ee.upatras.gr/mim/RTSJ-AXEpackage.htm>) exploits the real-time specification for Java to provide the first real-time java based implementation for FBNs. Automatic code generation from XML based design specs is supported by Archimedes ESS. Performance measurements are presented in [5].

IsaGraph [15], a well known commercially available toolset that supports the IEC61131 function block, includes in its latest version support for IEC61499. The proposed execution environment even though very restrictive provides the first commercially available tool. Performance measurements for this execution environment are not available.

The Fuber execution environment is under development at Chalmers University of Technology [8]. This environment is not currently described in a publicly available document. Performance measurements are not available.

Torero project (<http://www.uni-magdeburg.de/iaf/cvs/torero/>) describes an effort for an IEC 61499 compliant device but no detailed implementation specific publications are publicly available

VII. CONCLUSIONS

The IEC 61499 standard has many open issues regarding the execution of FB networks. This may result in incompatible execution environments that would not ensure the same behavior for control applications. It is clear that the standard should be extended to this direction possibly in the form of an execution profile that has to define a set of execution semantics that will warrant portability of control applications across different execution environments. This paper intends to provide a contribution to this direction by presenting and discussing alternative execution scenarios and surveying existing execution run-time environments.

REFERENCES

- [1] International Electro-technical Commission, (IEC), International Standard IEC61499, Function Blocks, Part 1 - Part 4, IEC Jan. 2005.
- [2] K.Thramboulidis, G. Doukas, A. Frantzis, “Towards an Implementation Model for FB-based Reconfigurable Distributed Control Applications”, 7th IEEE International Symposium on Object-oriented Real-time distributed Computing, May, 2004.
- [3] K. Thramboulidis, D. Perdikis, S. Kantas, “Model Driven Development of Distributed Control Applications”, The International Journal of Advanced Manufacturing Technology, Springer-Verlag, DOI 10.1007/s00170-006-0455-0
- [4] Doukas, G., K. Thramboulidis, “A Real-Time Linux Execution Environment for Function-Block Based Distributed Control Applications”, 3rd IEEE International Conference on Industrial Informatics, Perth, Australia, August 2005, (INDIN’05).
- [5] Thramboulidis, K., A. Zoupas, “Real-Time Java in Control and Automation: A Model Driven Development Approach”, 10th IEEE Inter. Conference on Emerging Technologies and Factory Automation, Catania, Italy, September 2005. (ETFA’05).
- [6] M. Colla, E. Carpanzano, A. Brusaferrri, “Applying the IEC-61499 Model to the Shoe Manufacturing Sector”, 11th IEEE Inter. Conf. on Emerging Technologies and Factory Automation, Sept. 20-22, 2006.
- [7] A. Zoitl, G. Grabmair, F. Auinger, C. Sunder, “Executing real-time constrained control applications modelled in IEC 61499 with respect to dynamic reconfiguration”, 3rd IEEE International Conference on Industrial Informatics, 2005. INDIN ’05, 10-12 Aug. 2005
- [8] G. Cengic, O. Ljungkrantz, K. Akesson, “Formal Modeling of Function Block Applications Running in IEC 61499 Execution Runtime”, 11th IEEE International Conference on Emerging Technologies and Factory Automation, September 20-22, 2006, Czech Republic.
- [9] L. Ferrarini, C. Veber, “Implementation approaches for the execution model of IEC 61499 applications”, 2nd IEEE International Conference on Industrial Informatics, (INDIN ’04). 24-26 June 2004.
- [10] J.L.M. Lastra, L. Godinho, A. Lobov, R. Tuokko, “An IEC 61499 application generator for scan-based industrial controllers”, 3rd IEEE Inter. Conf. on Industrial Informatics. INDIN ’05. 10-12 Aug. 2005
- [11] FBRT (Function Block Run-time Toolkit), Rockwell Automation, <http://www.holobloc.com>
- [12] K. Thramboulidis, C. Tranoris, “An Architecture for the Development of Function Block Oriented Engineering Support Systems”, IEEE Intern. Conference on Computational Intelligence in Robotics and Automation, Canada August 2001.
- [13] K. Thramboulidis, “A Model Based Approach to Address Inefficiencies of the IEC61499 Function Block Model”, 19th International Conference on Software & Systems Engineering and their Applications, Paris - December 5-7, 2006
- [14] K. Thramboulidis, “Development of Distributed Industrial Control Applications: The CORFU Framework”, 4th IEEE International Workshop on Factory Communication Systems, Västerås, Sweden. August 2002.
- [15] ICS Triplex IsaGRAF, Commercially Available IEC 61499 Software, <http://www.icstriplex.com/>
- [16] A. Zoitl, R. Smolic, C. Sunder, G. Grabmair, “Enhanced real-time execution of modular control software based on IEC 61499”, Proceedings 2006 IEEE International Conference on Robotics and Automation. ICRA 2006, May 15-19, 2006, Page(s):327 – 332.

Towards a Practical Differential Image Processing Approach of Change Detection

KP Lam, School of Computing and Mathematics, University of Keele, STAFFS ST5 5BG U.K.

Abstract—A Laplacian-based derivative estimator with built-in noise filtration and good localisation properties is constructed for detecting changes in an x-ray transmission image sequence. In addition to the demonstrable efficacy in identifying significant image intensity transitions that are associated with the underlying physical process of interest, the technique has the distinct advantage of being conceptually simple and mathematically robust. These latter properties allow the characteristics of the proposed detection methodology be studied analytically, and offer a considerable potential for real-time applications. The performance of the resulting detector is examined in terms of its robustness and accuracy of detection, qualitatively with data visualisations and quantitatively based on an established method.

I. INTRODUCTION

An effective solution for detecting specific changes in an image sequence represents the single most important computational requirement for such practical computer vision tasks as intruder detection, vehicle tracking and automated scene surveillance. Recently, a novel x-ray imaging technique capable of detecting the presence and/or absence of (object) elements via a succession of transmission images has been proposed and subsequently demonstrated [1,18]. The technique offers a significant potential for the non-destructive study of object internal structures by attributing image intensity differences to the characteristic k-edge absorptions of known elements. As with many change detection applications, the ability to automatically identify the relevant element/object of interest from a background of generally unknown element/object(s) poses a considerable challenge in visual information processing. Furthermore, the principal requirement to locate the specified change by means of the visual correlation of image characteristics via the side-by-side two dimensional (2-D) image sequence generated by the polychromatic x-ray source, significantly adds to this challenge the non-trivial problem of detecting changes in the presence of noise.

Traditionally, the identification of changes between successive grey-scale images has been based on the method of pixel-by-pixel and/or neighbourhood image differencing [6,15]. More advanced algorithms designed particularly to tackle the problem of noise adopt a predominately application dependent or adaptive processing approach which necessitates the use of additional attributes such as motion information or background illumination compensation methods relevant to the problems at hand [3,10]. In most cases, they work reasonably well when/where the intensity differences are sufficiently large; *i.e.* a respectable signal-to-noise ratio. From a signal

processing viewpoint, the differentiator method in identifying 'significant' grey level discontinuities is closely allied to the classical approach of 2-D edge detection/enhancement, most relevantly here the Laplacian-based methods. The latter are generic derivative operators frequently adopted in one and two dimensional cases to detect edges by locating regions of local extremities, where the computed first-order gradients are the largest in magnitude. Indeed, contemporary use of the operator for second derivative estimations in a number of two and higher dimensional medical imaging applications have been reported [5,16,19]. Analytically, the success of this information processing methodology rests on the mathematical principle that the differential image intensities which frequently are of interest are significant intensity transitions associated with 'boundaries' of considerable changes along the dimension of interest, including local extrema and inflections often attributable to the underlying physical process. Being a second derivative operator, however, the Laplacian has the undesirable effect of amplifying noise. One approach to address this problem is to reduce the high frequency noise component by using a larger filter mask/operator to estimate the required gradients. However, this approach has several practical limitations, and is largely heuristic in nature. The alternative approach, as exemplified by the classical *Laplacian of Gaussian* and *Canny's* edge detectors [4,11], incorporates signal smoothing as an integral part of the differential operator. In terms of algorithmic complexity, this latter approach generally requires considerably more iterative and/or adaptive processing. To preserve computational efficiency, this paper presents an efficient and relatively effective change detection methodology, which works by unifying the above approaches of derivative estimations via a parameterised Laplacian operator constructed in the frequency domain. On the one hand, the estimators constructed were incorporated with adequate smoothing to provide noise filtration, in addition to a similarly band-limiting functionality required by the detector as described in [4]. On the other hand, the established *flat-fielding* procedure commonly applied to 2-D image enhancement was adopted as part of the methodology to enhance its capability to detect changes. By relating the image intensity changes to the characteristic k-edge absorption of two distinct elements contained in different regions of interest specified (*a priori*) in the spatial plane, we show that the differential technique was so developed that its primary objective was to reliably determine, without loss of generality, the locations of such elements from the collated sequence of x-ray images.

II. TECHNICAL BACKGROUND

The element specific imaging technology previously shown in [1,4] contrasted the so called ‘soft’ and ‘hard’ x-ray images produced immediately before and after the discontinuity in the x-ray absorption spectrum of the selected element. In the simplest case where the detection of a single unknown element/object is desired, this would require extracting the relevant image slices from a 3-D volume set of x-ray transmission images which are collated to provide an identical view of a given sample at different x-ray source energies (expressed in terms of the acceleration voltages of the x-ray source, in keV). The latter provides uniformly sampled data over a predetermined range, covering the distinctive k-edge discontinuity in x-ray absorption by the specific element/object. Analytically, the resulting image sequence defines the ‘temporal’ evolution of the image intensities as a 1-D sequence of 2-D grey-scale images in the xy-plane, such that the temporal dimension (t) parallel to the z -axis can be related directly to the x-ray source energy (E) applied. Within the data set, an (ordered) set of voxels which are formed by joining collinear voxels parallel to t , represents a single batch of correlated samples as a 1-D time-encoded signal, $I(E)$, with regions of interest (ROIs) modelled as voxel groups. This enables the latter to be segmented and rendered via a gradient/normal calculation procedure closely allied to that employed in the standard technique of volume slicing, but avoiding the computationally expensive processes of re-sampling and multiplanar reformatting [8,21]. An example is given in Fig. 1, where it is clear that the 2-D region showing the neodymium (Nd, k-edge = 43.57keV) impregnated lens generates the highest number of large gradient responses at the 50keV image. Given the 5keV resolution of the x-ray source, these results suggest the presence of the element’s k-edge at the range of 40-50keV.

As with many edge detection methods that relate local gradient changes to discontinuities in image intensity, the problem of false/undesirable detections must be addressed. This

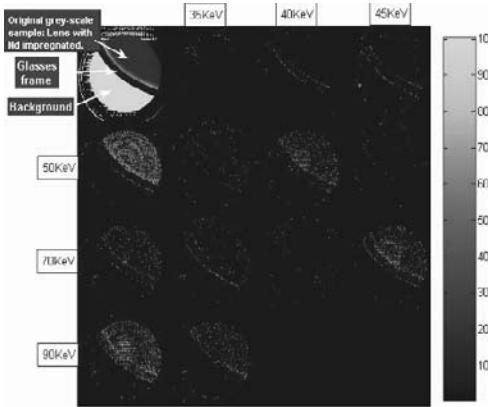


Fig. 1 The example image sample on the top left of the montage shows the neodymium impregnated lens from a pair of glass blower’s spectacle. The gradient changes can be observed to peak at the 50keV between the range accelerating voltages; shown from left to right and top to bottom.

is particularly evident in Fig. 1 where a noticeable response can be visualized at the 90keV image. The latter can be attributed in part to the complex characteristics of the general underlying model of image formation (in the xy -plane); *viz.*,

$$\mu(E) = aE^{-2.72} + b \quad (1)$$

$$I_n = \int_0^{E_0} \frac{12E^2(E_0 - E)e^{-\mu(E)d}}{(E_0)^4} dE$$

where I_n = image grey level, $\mu(E)$ = absorption coefficient, E_0 = input accelerating voltage, d = element’s thickness, a and b are empirical constants related to fluorescence and scattering respectively. In common with most practical visualization algorithms, however, the critical dependence on accurate gradient evaluations by the associated detector became apparent in the presence of the more realistic sample as shown in Fig. 2 [1,8]. From a signal analysis viewpoint, the identification of the individual element requires, on the one hand, the de-correlation of interfering signals which combine undesirably with the signal from the element(s) of interest. On the other hand, the inherent limitations of the x-ray source, particularly in terms of its polychromatic characteristics and maximum achievable (sampling) resolution (of 5keV), necessitate the use of more advanced techniques to maximize information extraction from the resulting imperfect data. To facilitate further analysis in light of these requirements, three ROIs are identified:

- **Region 1 (R1)** consists of the predominately large L-shaped area covered by the gold (Au) foil, excluding the region which overlaps with the three lead (Pb) wedges, 30, 24 and 18 μ m in thickness.
- **Region 2 (R2)** consists of the protruding part of the two lead wedges (12 μ m and 6 μ m in thickness) not covered by the gold foil.
- **Region 3 (R3)** consists of the three overlapped lead wedges which are excluded from **R1**.

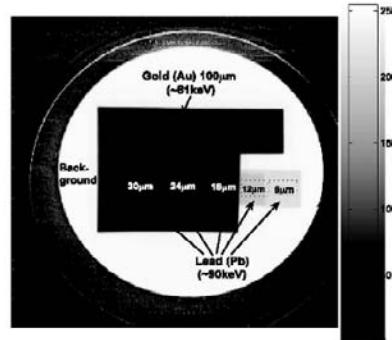


Fig. 2 Sample image (1008x1008) showing a gold foil and the partially overlapped 5-step set wedges of lead. The k-edge energy and thickness of the individual element are also included Note also the difference in k-edge absorption energies between Au and Pb is close to the Nyquist rate.

III. GRADIENT COMPUTATIONS

Gradient filtering forms an integral part of the standard volume visualization pipeline. The estimation of gradient is essential to the understanding of the (3-D) volume data as it provides vital information about the spatial cue and structure of the discrete data set [7, 21]. Computationally, the use of the second-order derivative ($\nabla^2 f(x, y) = \frac{\partial^2 f(x, y)}{\partial x \partial y}$) to locate the

2-D boundaries of discontinuities in the image intensity/luminance has long been established [20, 23]. The procedure is aided by the technique of edge sharpening primarily achieved through image convolution with a 2-D Laplacian kernel. For the 1-D sequence of $x[n]$, the standard Laplacian operator, $[1 - 2 1]$, reduces to become the second derivative estimation of $x[n]$. This second order derivative operator was applied to the collated 1-D image data sequences) as described in the preceding section, with the resulting response directly corresponded to a pixel-by-pixel comparison of the volume set within the selected regions of interest. The computed second derivatives provide the quantitative differential measurements of the grey level (I) discontinuities of the non-linear changes occur along a sample sequence.

Analytically, the detection of peak in the second derivatives, $\frac{d^2 I}{d^2 E}$, is a well documented method for identifying abrupt localised changes, provided that the image operators are expressed at a proper scale [9]. This method was further enhanced by adopting a similarly constructed edge sharpening procedure described in [16], whereby the standard Laplacian as obtained above can be used as a vehicle to estimate the localised change of intensity gradient, ∇_I , from the individual sample sequence of $I(E)$. In effect, the localization of 'significant' changes in $I(E)$ would be greatly facilitated if the change in ∇_I can be normalized against the grey-scale intensity. Such a procedure had previously been adopted to aid visual examinations of microstructure sub-movements via derivative plots [22], and, more recently, to improve the identification of principal components in chemometrics by means of derivatives ratio [13]. Mathematically, the analysis of $\frac{d\nabla_I}{dI}$ can be expressed as the ratio of the standard Laplaican, ∇_I^2 , and the first derivative, $\nabla_I = \frac{dI}{dE}$, by applying the *chain-rule* of continuous differentiation; namely,

$$\frac{d\nabla_I}{dI} = \frac{d\nabla_I}{dE} \frac{dE}{dI} = \frac{d^2 I}{dE^2} \quad (2)$$

In passing, this procedure is closely allied to the widely used 2-D image enhancement technique of *flat-fielding*, which emphasizes sharply localised features by diminishing slowly varying patterns superimposed on the data. This is supported in

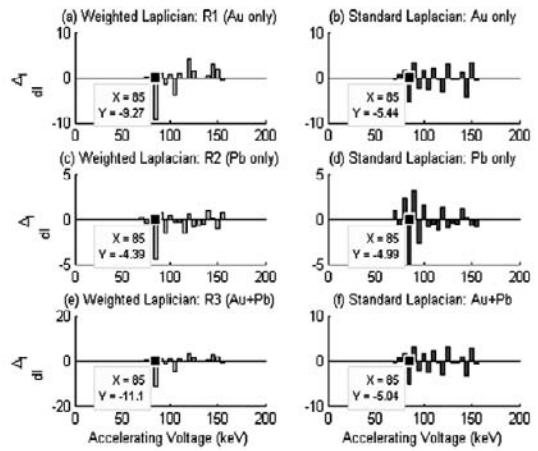


Fig. 3 Side-by-side comparisons of the results achieved with (2) and the standard Laplacian operator for the individual ROI, R1-R3. The relative magnitudes of response produced at 85keV (image) corresponding to the k-edge of gold (Au) are also included.

our case by the strong correlation ($\rho_{\mu\sigma}$) between the sample means (μ_i) and standard deviations (σ_i) of the individual ROI as defined earlier. The results obtained by applying (2) in each ROI are given in Fig. 3 alongside the corresponding responses achieved using the standard Laplacian operator. In terms of the capability to identify localised changes, the demonstrable improvement offered by the weighted Laplacian operator as defined in (2) is apparent. In particular, the large area covered by the gold (Au) foil in regions R1 and R3, had generated a definite response with significantly improved clarity at 85keV which closely matches the k-edge energy of Au. Similarly, the contrast in responses produced in these two regions and in R2 has also been enhanced by a factor of approximately two.

IV. SMOOTHED GRADIENT FILTERS

A closer examination of the results shown in Fig. 3 reveals several shortcomings of the weighted Laplacian approach as defined in (2). Firstly, in common with all second derivative operators, the approach had the undesirable effect of amplifying noise; when compared with the standard Laplacian, it generated a noticeably noisier response that, on average, amounted to a ~20% higher spread (in magnitude) in the ROIs. Secondly, a significant part of R2 had produced a detectably large response at 85keV, though its average strength is demonstrably lower than that produced by the standard Laplacian. Similarly, when the response produced at 95keV (which correspond to the k-edge energy of Pb) was examined in R1, a considerable part of the region was still visible, albeit at a noticeably reduced strength.

To address these problems, signal smoothing has been incorporated in our gradient filter design, as in classical edge detection algorithms [4,11]. To minimise computational complexity, in addition, a non-iterative approach of noise suppression was adopted, which works by modifying the

generalized *central difference* approximation algorithm most widely known to the volume visualization community. The algorithm provides an inexpensive but basic approximation of the ideal gradient estimator when extended to volume rendering (as 6-neighbour) alongside other traditional operators including Adaptive, Zucker-Hummel and Sobel for voxel shading and classification [2,7,14]. Mathematically, the algorithm in 1-D cases is equivalent to estimating the first derivative using a generalised difference equation, $x^1[n] = x[n+M] - x[n-M]$, of which the central difference approximator $[1 \ 0 \ -1]$ is simply a special case with $M = 1$. From a signal processing viewpoint, this has the smoothing effect in lowering the *cut-off* frequency of the resulting high-pass filter, albeit at the expense of small and fine details. Consequently, to optimise the filter length in respect of its low-pass filtering capability, a standard filter design technique has been used to specify the frequency characteristics of the (1^{st} -order) gradient operator from which the resulting Laplacian filter can be derived by digital convolution; noting that, in the limiting case when $[1 \ 0 \ -1]$ acts as a high pass filter, the frequency response of the *intermediate difference* operator, $[-1 \ 1]$, is practically a linear function with frequency comparable to that of the ideal derivative filter. In other words, the two-coefficient operator produces a ‘near’ ideal derivative under such conditions. These properties can be shown analytically by examining the normalized frequency response $|X^1(f)|$ of the generalised difference filter, as follows:

$$X^1(k) = \frac{\exp\left(-\frac{j2\pi kM}{N}\right) - \exp\left(-\frac{j2\pi k(-M)}{N}\right)}{2M} = \frac{j \sin\left(\frac{2\pi kM}{N}\right)}{M} \quad (3)$$

$$\therefore |X^1(f)| = \frac{\sin(2\pi fM)}{M}$$

where $M=1, 2, \dots$ represents the integer *skip* distance, N the number of signal samples, and $f = k/N$ represents the normalized frequency.. Thus $|X^1(f)|$ is zero at $f = n/2M$, where $n = \pm 1, 2, \dots$ representing discrete multiples of the sampling frequency f_s . When $n = 1$, it is clear that $|X^1(f)|$ approximates a true derivative only at the lower frequencies, approaching a maximum when $f = f_s/4$. Between $f_s/4$ and $f_s/2$, the magnitude $|X^1(f)|$ decreases monotonically from this maximum to zero, demonstrating the characteristic low-pass filtering effect. Moreover, increasing M , and consequently, the extent of the filter, has the expected effect of lowering the frequency range over which the filter acts as a derivative operator in addition to narrowing the low-pass filtering range.

This is because $|X^1(f)|$ repeats above $f = \frac{1}{2M} f_s$ by virtue of the half-wave symmetry of the sine function in $[0, 2\pi]$. In practice, M is kept small to minimise the computational requirements for the associated second order derivative operator (of length $2M-1$). This, in turns, simplifies the specification of the resulting cut-off frequency beyond which the derivative operator is acting as a low-pass filter to $x[n]$. Setting $M=1$ in the central difference equation, and using the two-coefficient (or near ‘ideal’) first-order derivative as a guide, a family of first-order derivative operators can be constructed in

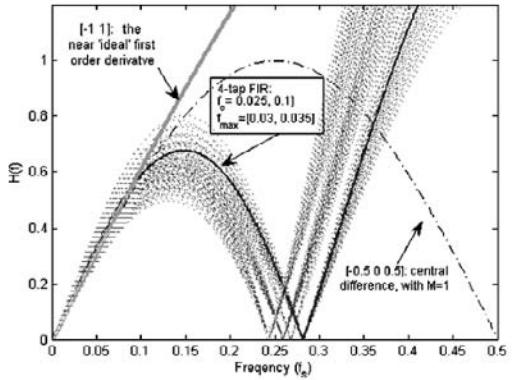


Fig. 4 Frequency response of the family of FIR filters constructed alongside the near ideal first derivative and central difference operators. The values of f_c and f_{\max} are normalized to the sampling frequency f_s .

the frequency domain using standard filter design procedures [12]. Fig. 4 shows the normalised frequency plots for the family in addition their specified parameters. The results are consistent with the frequency domain analysis originally proposed in [2].

In summary, the 4-tap *finite response filter* (FIR) approximates the ideal first derivative operator, operating linearly in the frequency domain as a differentiator within the normalised frequency range of $f \in [0, f_{\text{coff}}]$, where f_{coff} represents the specified *cut-off* frequency. Beyond f_{coff} , the response was rapidly reduced to zero within a predefined frequency range f_{doff} which was set to $0.2f_s$ given the relatively small value of M . An upper *stopband* beginning at a frequency $f = f_{\text{coff}} + f_{\text{doff}}$ was also specified, emphasizing the zero gain requirement at the highest frequency f_{\max} , and minimising the error response resulting in this band relative to the others. Given the mean values of f_{coff} and f_{\max} as shown in Fig. 4, the solid line traces the frequency response of the filter which has been selected from the family for subsequent analysis of the data set collated.

In addition to producing a smoothed second derivative estimate, the proposed differential operator is expected to improve on the relative ratios of the response obtained in the individual regions of R1-R3, particularly at $E=85\text{keV}$ and 95keV , where the characterising k-edge absorption of Au and Pb elements respectively are anticipated. This latter point is illustrated by the scatter plots presented in Fig. 5, noting that: firstly, the average responses produced at 85keV and 95keV in the two regions of R1 and R2 are now much closer, converging to a value of -1.6. Secondly, the clusters of response produced in these two regions are both distinct and reasonably well separated, with mean response vectors shown as $(-2.104, -1.451)$ and $(-1.231, -1.746)$ for R1 and R2 respectively. Thirdly, the ambiguity of response produced by the weighted Laplacian method as discussed at the beginning of this section is resolved, since the two clusters are now populated on the opposite side of the equality line $y=x$. More significantly, the average strength of response generated in R1 at $E = 85\text{keV}$ is considerably higher than that produced at $E = 95\text{keV}$. As expected, the reverse is true for R2.

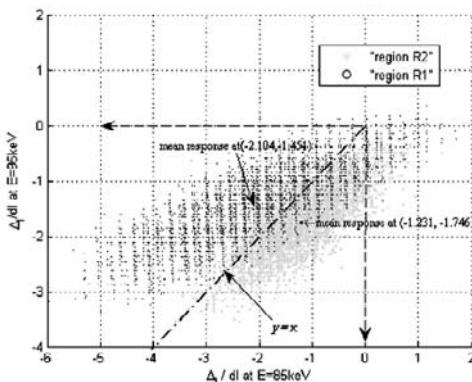


Fig. 5 Scatter plots of the individual response produced in regions R1 & R2 at E=85keV and 95keV. Conceptually, each point represents a two-component signal vector generated by the individual pixel from the respective ROIs.

V. PERFORMANCE AND DISCUSSIONS

The efficacy of the method proposed in section IV was examined using a quantitative procedure closely allied to established approach of [17]. Specifically, the quality of detection, ζ , was formulated in (4), as follows:

$$\zeta = \left(\frac{100}{I_N} \right) \sum_i^I \frac{1}{1 + \alpha d_i^2} \quad (4)$$

where $I_N = \max(I_I, I_A)$, I_I = number of expected changes, I_A = number of detected changes, α = scale factor to penalise offset position of changes, and d_i = distance of the detected change from its true position. The unit of d_i was scaled by a factor of 5, mirroring the 5keV resolution of the image data set. The parameter α was then set to 2, allowing a steep performance penalty ratio of just under 0.9, or equivalently, $\zeta = 11$, to be imposed when a total false detection occurs at $d = 2$. The latter corresponds to the 10keV separation of the k-edge energies of gold (at E= 85keV) and lead (at E = 95keV), expected to be detectable in the relevant ROIs previously defined. Without loss of generality, the calculation of ζ had been simplified by limiting the maximum detectable response to E = 105keV, thus giving a potential distance of error $d=0, \pm 1, \pm 2$ for gold, in light of the fact that ζ deteriorates as $\frac{1}{\alpha d^2}$ to practically zero for larger values of d .

To aid comparisons, individual values of ζ_R are computed, where $R = R1, R2$ and $R3$ corresponding to three ROIs. These results are presented in Figure 6 alongside some relevant statistics to facilitate the discussions below.

Fig. 6(A) shows the quality of detection ζ_{R1} over a range of thresholds that were universally applied to the selected ROIs. As expected, the performance of the detector improves as the magnitude of the threshold T is lowered, since the number of pixels having a response equal to or higher than $|T|$ within the region increases generally as a result. This latter characteristic

was shown in the same graph, where the percentages of pixel having a response $\geq |T|$ are separately plotted for 85keV and

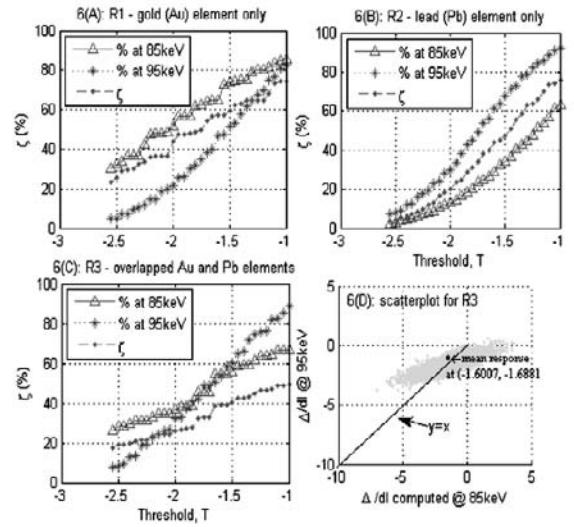


Fig. 6 Summary of results obtained in the individual region of interest – R1, R2, and R3. 6(D) further illustrates the results obtained in R3 with a similarly constructed scatter-plot as given in Fig. 5.

95keV. For region R1, the quality of detection ζ is expected to be limited by the rapid increase in responses generated at 95keV as $|T|$ decreases, corresponding to an increase in the number of false detections (of lead element) in the region. This can be understood by observing that the two response curves converged at high values of T, causing ζ , the quality of detection, to level off at a peak of just below 75% as T approaches -1 at the edge of the graph. Similarly, the graph of ζ_{R2} in Fig. 6(B) was shown to display comparable characteristics to that of ζ_{R1} , with two major differences. Firstly, as $|T|$ is raised, the quality of detection is bounded by the relatively low percentage of positive responses (expected at 95keV) and a similar number of false detections generated at 85keV, both are attributed to the lower average magnitude of responses produced in region R2 (see also Fig. 5). Secondly, the improvement in ζ_{R2} achieved by lowering $|T|$ reaches a plateau expected to level between the two response curves which, contrary to those obtained in R1, are expected to maintain a fixed gap as T increases beyond the value of -1. The latter is confirmed following a close examination of these two curves, where a significantly larger number of pixels had generated a positively signed response at 85keV than those produced at 95keV in this region. This is desirable, as it represents a reduction in number of potentially false detection at 85keV.

The quality measure for ζ_{R3} as displayed in Fig. 6(C) warrants a separate discussion. In particular, the relatively disappointing performance achievable by lowering $|T|$ is misleading. The apparently limiting performance of 50% is

primarily due to the parameter values selected in (4), which attribute an equal penalty for false detections at distance $d = \pm 2$, corresponding to the differences in the expected k-edge locations (85 and 95keV) of the two elements (Au and Pb) contained in this region. Consequently, ζ_{R3} is expected to approach a limiting value of $100 * (1+1/9)/2$, or 56%, as $|T|$ is lowered towards zero. These results are further evident in the existence of several intersections where the two response curves cross over as T increases in the interval [-2.0, -1.5]. The latter contains the mean response values of -1.60 and -1.68 obtained respectively at 85keV and 95keV. More significantly, these two means were extremely close in value (differed only by 5%), demonstrating an equal likelihood of detection at the two characteristic k-edge energies of Au and Pb elements in region R3. As in Fig. 5, the scatter plots displayed in Fig. 6(D) further illustrate this desirable property.

VI. CONCLUSIONS

Conventional algorithms for detecting changes in an image sequence approximate local derivatives with digital subtraction, which emphasizes high frequency features including false transitions due to noise. Consequently, additional post processing procedures are required to improve the quality of detection. Such a requirement is diminished if the differential strength of signal/image intensities can be suitably enhanced, thus simplifying the detection of intensity changes. This latter approach forms the basis of the change detection methodology presented in this paper. Traditionally developed for edge enhancement, the Laplacian-based derivative estimators were adapted here to enhance localised changes in intensity gradient, which can be extracted side-by-side from the spatially aligned sequence of x-ray images via a relatively straightforward volume slicing procedure. From a signal processing prospective, the Laplacian-based technique is amenable to specifications in the frequency domain by virtue of its mathematical relationships with first-order derivative and digital convolution, thus allowing noise suppression capability to be incorporated as an integral part of our design procedure. These characteristics have been shown both analytically and experimentally by means of a rigorously constructed real-world data set. Computationally, a principal novelty of the proposed detection methodology lies in its simplicity of design and uniformity of inexpensive operations. These properties are crucial to our on-going research in high performance and dependable image analyzer techniques capable of performing non-destructive testing by the element specific x-ray imaging technology. Effort is underway to adapt the techniques described for use as a coarse grained region of interest detector.

REFERENCES

- [1] JC Austin and KE Pitt et al, "Broad spectrum element-specific X-ray imaging," *NDT&E International*, 37, 2004, pp. 229—236.
- [2] MJ Bentum, BBA Lichtenbelt and T Malzbender, "Frequency analysis of gradient estimators in volume rendering," *IEEE Trans. Vis. Comp. Graphics*: 2(3), 1996, pp. 242-254
- [3] AG Bors and I Pitas, "Optical flow estimation and moving object segmentation based on median radial basis function network," *IEEE Trans. On Image Processing*. Vol.7, 1998, pp. 693-702.
- [4] J Canny, "A computational approach to edge detection," *IEEE Trans. Pattern Analysis and Machine Intelligence*, 8, 1986, pp. 679-714.
- [5] G Coppini, R Poli and G Valli, "Recovery of the 3-D shape of the left ventricle from echocardiographic images," *IEEE Trans. on Medical Imaging*, 14(2), 1995, 301-317.
- [6] JA Freer, BJ Beggs, HL Fernandez-Canque, F Chevrier and A Goryashko, "Automatic intruder detection incorporating intelligent scene monitoring with video surveillance," *Proc. European Conference on Security and Detection*, 1997, pp. 109-113.
- [7] D Hong, G Ning, T Zhao, M Zhang, and X Zheng, "Method of normal estimation based on approximation for visualization," *Journal of Electronic Imaging*, Vol 12(3), 2003, pp. 470-477.
- [8] KP Lam and JC Austin, "Visualising multidimensional signals from a dimension-dependent computational perspectives," *Procs IEEE Int'l Conf. Signal and Image. Processing*, in press
- [9] T Lindeberg, "Edge detection and ridge detection with automatic scale selection," *International Journal of Computer Vision*, 30(2), 1998, pp. 117-154.
- [10] A Makarov, "Comparison of background extraction based intrusion detection algorithms," *Procs Int'l Conf. on Image Processing*, Vol.1, 1996, pp. 521-524.
- [11] D Marr and E Hildreth, "Theory of edge detection," *Proc. the Royal Society of London, B207*, 1980, pp. 187-217.
- [12] MATLAB. Signal Processing Toolbox - User's Guide, The MathWorks, US, 2003-06.
- [13] AK Mithal and SA Douglas, "Differences in movement microstructure of the mouse and the finger-controlled isometric joystick," *Procs ACM/SIGCHI 96*. Available: <http://acm.org/sigchi/ch96/proceedings>
- [14] T Moller, R Machiraju, K. Mueller and R. Yagel, "Evaluation and design of filters using a Taylor series expansion," *IEEE Trans. Vis. Comp. Graphics*, 3(2): 1997, pp. 184-199.
- [15] E Oron, "Motion estimation and image difference for multi-object tracking," *IEEE Aerospace Conference Proceedings*, Vol. 4, 1999, pp. 401-409.
- [16] T-S Pan, MA King, DJ de Vries and M Ljungberg, "Segmentation of the body and lungs from Compton scatter and photopeak window data in SPECT: A Monte-Carlo investigation," *IEEE Trans. on Medical Imaging*, 15(1), 1996, pp. 13-24.
- [17] WK Pratt and IE Adbou, "Quantitative design and evaluation of enhancement/thresholding edge detectors," *Procs IEEE Vol 67-5 (May)* 1979, pp. 753-763.
- [18] JH Raistrick, "X-ray imaging in its element," *Materials World*, Vol. 9 (1), 2001, pp. 11-13.
- [19] BW Reutter, "Automated 2-D segmentation of respiratory-gated PET transmission images," *IEEE Trans. on Nuclear Science*, 44(6), 1997, pp. 2473-2476.
- [20] A Rosenfeld, M Thurston and Y Lee, "Edge and curve detection," *IEEE Trans. Computers*, C-21, 1972, pp. 677-715.
- [21] JC Russ, *The Image Processing Handbook*, Fourth Edition, CRC Press, 2002
- [22] T Syrovy and M Meloun, "Number of components using modified PCA cree plot in spectroscopy", *Procs. ChemStat 2004, International Conference on chemometrics*, 2004, pp 29-0. .
- [23] JS Weszka, RN Nagel and A Rosenfeld, " A threshold detection technique," *IEEE Trans. Computers*, C-23, 1974, pp. 1322-1326.

An ISP level Distributed Approach to Detect DDoS Attacks

Krishan Kumar, R C Joshi, and Kuldip Singh

Department of Electronics and Computer Engineering
Indian Institute of Technology Roorkee

kksaldec@iitr.ernet.in, joshifcc@iitr.ernet.in, kds56fec@iitr.ernet.in

Abstract— DDoS attacks are best detected near the victim's site as the maximum attack traffic converges at this point. In most of current solutions, monitoring and analysis of traffic for DDoS detection have been carried at a single link which connects victim to Internet Service Provider (ISP). However the mammoth volume generated by DDoS attacks pose the biggest challenge in terms of memory and computational overheads. These overheads make DDoS solution itself vulnerable against DDoS attacks. We propose to distribute these overheads amongst all Points of Presences (POPs) of the ISP using an ISP level traffic feature distribution based approach. Entropy of incoming flows is taken as metric for traffic feature distribution. Entropy calculated from traffic monitored at all POPs, and total number of packets seen by every POP are then sent to the coordinating POP for final computation of entropy by our proposed formula. Here it is compared with normal entropy already profiled for the network environment. Thresholds are very carefully chosen keeping in mind fluctuations in traffic. We use an ISP level topology and well known attack tools for simulations in ns-2.

Index Terms—Anomaly Detection, Distributed Denial-of-Service (DDoS), Entropy, False Positives, and False Negatives.

I. INTRODUCTION

Denial-of-Service (DoS) is an intentional attempt by attacker to compromise availability of a service to legitimate users [1]. Distributed Denial-of-Service attacks (DDoS) degrade or completely disrupt services to legitimate users by eating up communication, computational, and or memory resources of the target through sheer volume of packets. DDoS attacks are amplified form of DOS attacks where attackers direct hundreds or even thousands of compromised "zombie" hosts against a single target [2]. As per survey conducted by FBI/CSI in 2004 [4], these attacks are second most dreadful attacks in terms of revenue losses after information thefts.

The method in this paper concentrates on TCP low rate and high rate flooding attacks. Most of the public servers provide services through TCP [3], so protecting the TCP portion of the bandwidth is sufficient in protecting most of services. Most of existing solutions [5]-[7] use volume

based metrics (number of packets and byte count per unit time) to detect DDoS attacks. These suffer in the form of large number of false positives/negatives hence more collateral damage is incurred when attack is carried at slow rate or when volume per attack flow is not so high as compared to legitimate flows. The traffic is monitored and analyzed near the victim site only. The following fig. 1 suggests that DDoS attacks are best detected near the victim site as maximum attack traffic is available at this point for analysis.

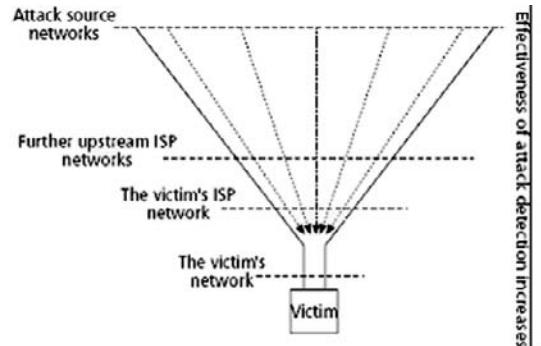


Fig. 1. Possible locations for DDoS attack detection [1]

Fig. 1 shows that the detection can be performed in four places on the paths between the victim and zombies. As depicted, a DDoS attack resembles a funnel in which attack packets are generated in a dispersed area, like the top of a funnel. The victim, like the narrow end of a funnel, receives all the attack packets generated. Thus, it is not difficult to see that detecting a DDoS attack is "relatively" easy at the victim network, because it can observe all the attack packets. In contrast, it is less likely for an individual source network, where attack sources (reflectors in case of indirect attacks) are located, to detect the attack unless a large number of attack sources are located in that network. In nutshell a scheme which can monitor all traffic destined to victim and analyze the same at single point gives best detection results. But in this case memory and computational overheads are also centered at single point which is itself vulnerability as far as huge volume of traffic generated by DDoS attack is concerned. So a technique, which can monitor and analyze traffic at distributed points but reflects as if the total traffic is monitored and analyzed at single point, is good for DDoS attack detection. So by applying this technique memory and computational overheads can be distributed from single point to multiple points.

Lakhina et al [10] observed that most of traffic anomalies despite their diversity share a common characteristic: they

induce a change in distributional aspects of packet header fields (i.e. source address, source port, destination address, and destination port etc called traffic features).

Our hypothesis to detect attacks also treats DDoS anomalies as events that disturb the distribution of traffic features. For example, a DoS attack, regardless of its volume, will cause the distribution of destination address to be concentrated on the victim address. Similarly, a scan for vulnerable port called network scan have a dispersed distribution for destination addresses, and a skewed distribution for destination ports that is concentrated on the vulnerable port being scanned.

The key question here is to decide which metric is to be used for measuring distribution of traffic features. We have chosen Entropy as a metric for this purpose because entropy captures in a single value the distributional changes in traffic features, and observing the time series of entropy on multiple features exposes unusual traffic behavior. Normally the focus for calculation of entropy is on four traffic features: source address (sometimes called source IP and denoted srcIP), destination address (or destination IP, denoted dstIP), source port (srcPort) and destination port (dstPort). This 4-tuple of 96 bytes called flow is chosen for calculation of entropy.

A metric that captures the degree of dispersal or concentration of a distribution is called sample entropy. We start with an empirical histogram $X = \{n_i, i = 1, \dots, N\}$ that feature i occurs n_i times in the sample. Let $S = \sum_{i=1}^N n_i$ be the total number of observations in the histogram. Then the sample entropy $H(X)$ is

$$H(X) = -\sum_{i=1}^N (p_i) \times \log_2(p_i) \quad (1)$$

$$\text{Where } p_i = n_i / S$$

The value of sample entropy lies in the range $0 - \log_2 N$. The metric takes on the value 0 when the distribution is maximally concentrated, *i.e.*, all observations are the same. Sample entropy takes on the value $\log_2 N$ when the distribution is maximally dispersed, *i.e.* $n_1 = n_2 = \dots = n_n$.

Sample entropy is a convenient summary statistic for a distribution's tendency to be concentrated or dispersed. Furthermore, entropy is not the only metric that captures a distribution's concentration or dispersal; however we have explored other metrics and find that entropy works well in practice.

We use GT-ITM [11], an ISP level topology generator and ns-2 [12] as test bed for simulations. We show that Entropy captures DDoS attack anomalies distinct from those captured in traffic volume.

Moreover we do not monitor traffic at single link instead it is done at all ingress points of the ISP. Entropy computed at these points is sent to the coordinator (a router responsible for analysis). The total entropy is computed using the proposed formula which is discussed in section III. Memory and computational overheads are thus distributed to protect our solution against high volume of packets generated by DDoS attacks.

The remainder of this paper is organized as follows. Section II discusses related work. In Section III detection

methodology with proof of proposed formula is explained. Section IV describes simulation experiments. Section V provides simulations results and discussion. Finally Section VI concludes our paper.

II. RELATED WORK

A commonly used detection approach is either signature-based or anomaly-based. Signature-based approach inspects the passing traffic and searches for matches against already-known malicious patterns. In practice, several signature-based detection systems such as Bro [13] and Snort [14] have been developed and deployed at firewalls or proxy servers. By contrast, an anomaly based detection system observes the normal network behavior and watches for any divergence from the normal profile. Most of DoS detection systems are anomaly based [5]-[9]. However, their normal traffic models are mainly based on flow rates. Due to the diversity of user behaviors and the emergence of new network applications, it is difficult to obtain a general and robust model for describing the normal traffic behaviors. As a result, legitimate traffic can be classified as attack traffic (false positive) and attacker traffic is classified as legitimate (false negative). To minimize the false positive/negative rate, a larger number of parameters are used to provide more accurate normal profiles. However, with the increase of the number of parameters, the computational overhead to detect attack increases. This becomes a bottleneck, especially for volume-oriented DDoS attacks that will be aggravated by the Computational overhead of the detection scheme. In [15], and [16] based on destination address, attack aggregate are found and then filtered using pushback technique. However in this case, collateral damage is more as legitimate traffic in that aggregate is also dropped.

Though schemes in [5]-[9], have been successful in isolating large traffic changes (such as bandwidth flooding attacks), but slow rate, isotropic attacks can not be detected and characterized because these attacks do not cause detectable disruptions in traffic volume. In contrast, we demonstrate the utility of a more sophisticated treatment of DDoS anomalies, as events that alter the distribution of traffic features. For low as well as high rate attacks, traffic distributions have appreciable deviation from normal to provide signs of DDoS attack.

III. DETECTION METHODOLOGY

The end systems or hosts (users PCs, PDAs, web Servers, and mail servers etc) in Internet connect to each other through a tiered hierarchy of Internet Service Providers (ISPs). Within an ISP's network, the points at which the ISP connect to other ISPs (whether below, above, or at the same level in the hierarchy) are known as points of presence (POPs). The interconnection of POPs of an ISP through high bandwidth links is called ISP backbone. In an ISP's network a POP is actually a group of connected core and access routers to which core routers of the same or other ISPs (private/public peer or NAT) and ISP's own customers and servers are connected respectively.

Whenever two ISP are directly connected to each other, they are said to be peer with each other. Though, complexity of POP's connecting router will vary depending upon whether other ISP router (normally core) or own customer domain (normally access) is attached.

For simulation purpose, we have simplified ISP level network with four cooperative ISP domains (1, 2, 3, and 4) where each domain has 10 POPs represented by single node each as shown in fig. 2. One customer domain is attached to each POP which consists of legitimate and attacking hosts. Two POPs in every ISP are attached to other ISPS. ISP domain 4 has additional POP for connecting to our protected server. Our aim in this paper is to detect DDoS attack in ISP domain 4.

The first step is to detect novel attacks. Detecting DDoS attacks involves first knowing normal behavior of our system and then to find deviations from that behavior. The normal profile or behavior is obtained using Entropy $H(X)$ as a parameter to measure traffic feature distributions. We build normal profile off line using traces collected for the network without attack whereas for detection, on line monitoring, analysis and comparison with normal profile is done under attack. The packets for each flow are collected in a time window off line from the trace collected for our network to be protected when no attack is launched. As in IPv4 packets, there is no flow ID header information, so we designate different flow IDs to a unique 4-tuple SourceIP, SourcePort, DestinationIP, DestinationPort encountered in incoming packet. The traffic destined to our server and not the complete traffic is collected from link trace through which POP is connected to the server. POP collects information in a time window and calculates Entropy $H(X)$. Consider a random process $\{X(t), t = j\Delta, j \in N\}$, where Δ a constant time interval is called time window, N is the set of positive integers, and for each $t, X(t)$ is a random variable. Here $X(t)$ represents the number of packet arrivals for a flow in $\{t - \Delta, t\}$. $X(t)$ As a whole represent our empirical histogram for computing entropy. It is found in our simulation without attack that Entropy $H(X)$ value varies within very narrow limits after slow start phase is over. This variation becomes narrower if we increase Δ i.e. monitoring period. We take average of $H(X)$ and designate that as normal Entropy $H_n(X)$. The basic idea is to remove small scale perturbations by averaging over slightly longer-intervals of time. However it is also desirable that the window duration should not exceed a limit as Internet traffic show large variations across different times of the day. By this way, normal profile of traffic in terms of Entropy $H_n(X)$ is obtained by our approach. To detect the attack, the entropy $H_c(X)$ is calculated in shorter time window Δ continuously in real time, whenever there is appreciable deviation from $H_n(X)$, attack is said to be detected.

We assume that the system is under attack at time t_a , which means that all attacking sources start emitting

packets from this time: the network is in normal state for time $t < t_a$ and turns into attacked state in time t_a . Let t_d denote our estimate on t_a .

At time t_d following event triggers

$$\begin{aligned} (H_c(X) > (H_n(X) + a \times d)) \cup \\ (H_c(X) < (H_n(X) - a \times d)) \end{aligned} \quad (2)$$

$attack = true$; // variable maintained by POP for triggering Characterization module

Here $a \in I$ where I is set of integers and d is deviation threshold. Tolerance factor a is a design parameter and d is absolute maximum deviation in Entropy $H(X)$ from average value $H_n(X)$ while profiling for network without attack.

Ideally computation of $H_c(X)$ should be done at the POP P_s where server is connected. As maximum attack traffic is available at this point after launch of the attack. However sheer volume of DDoS attack make this defense implausible because of large memory and computational overheads at single point. To address this problem, we distribute complexity of monitoring and computation of entropy from the victim's site to all the POPs from which traffic is arriving. Finally $H_c(X)$ is computed at the victim's site from the accumulated $H(X)$ from all POPs. This makes the process analogous to existing methods in which total traffic is monitored at the victim's site where all the attack traffic converges.

We propose a solution that calculates entropy at single POP from individual entropies at different POPs.

Let $\{P_1, P_2, \dots, P_n\}$ are POPs of our ISP domain and n is the number POPs. Let $\{N_1, N_2, \dots, N_k\}$ N_i is number of flows in P_i . Let $\{H_1, H_2, \dots, H_n\}$ H_i is frequency histograms associated with POP P_i in time window Δt where $H_i = \{X_{i1}, X_{i2}, \dots, X_{iN_i}\}$. Here X_{ij} represent number of packets for POP P_i and flow j . Let

$$\{S_1, S_2, \dots, S_n\} \text{ where } S_i = \sum_{j=1}^{N_i} X_{ij}.$$

Let E_i represent entropy for POP P_i . Entropy E_i computed at P_i with S_i is sent to P_s (POP connecting server to ISP 4) where final entropy E_f is calculated using "3".

$$\begin{aligned} 2^{-E_f} = & (2^{-E_1})^{S_1/S_f} \times (2^{-E_2})^{S_2/S_f} \times \dots \times (2^{-E_n})^{S_n/S_f} \\ & \times (S_1/S_f)^{(S_1/S_f)} \times (S_2/S_f)^{(S_2/S_f)} \times \dots \times (S_n/S_f)^{(S_n/S_f)} \end{aligned} \quad (3)$$

The proof for the same is given as follows:-

$$\begin{aligned} -E_1 &= (x_{11}/S_1) \log(x_{11}/S_1) + (x_{12}/S_1) \log(x_{12}/S_1) + \dots \\ &+ (x_{1N_1}/S_1) \log(x_{1N_1}/S_1) \\ -E_1 &= \log(x_{11}/S_1)^{(x_{11}/S_1)} + \log(x_{12}/S_1)^{(x_{12}/S_1)} + \dots \\ &+ \log(x_{1N_1}/S_1)^{(x_{1N_1}/S_1)} \\ -E_1 &= \log((x_{11}/S_1)^{(x_{11}/S_1)} \times (x_{12}/S_1)^{(x_{12}/S_1)} \times \dots \times (x_{1N_1}/S_1)^{(x_{1N_1}/S_1)}) \\ \Rightarrow -E_f &= \log((x_{i1}/S_i)^{(x_{i1}/S_i)} \times (x_{i2}/S_i)^{(x_{i2}/S_i)} \times \dots \times (x_{iN_i}/S_i)^{(x_{iN_i}/S_i)}) \end{aligned}$$

$$\begin{aligned}
2^{-E_i} &= (x_{i1} / S_i)^{(x_{i1} / S_i)} \times (x_{i2} / S_i)^{(x_{i2} / S_i)} \dots \times (x_{iN_i} / S_i)^{(x_{iN_i} / S_i)} \\
\text{Let } S_f &= \sum_{i=1}^n S_i \\
2^{-E_f} &= (x_{11} / S_f)^{(x_{11} / S_f)} \times (x_{12} / S_f)^{(x_{12} / S_f)} \dots \times (x_{1N_1} / S_f)^{(x_{1N_1} / S_f)} \\
&\times (x_{21} / S_f)^{(x_{21} / S_f)} \times (x_{22} / S_f)^{(x_{22} / S_f)} \dots \times (x_{2N_2} / S_f)^{(x_{2N_2} / S_f)} \\
&\vdots \\
&\times (x_{n1} / S_f)^{(x_{n1} / S_f)} \times (x_{n2} / S_f)^{(x_{n2} / S_f)} \dots \times (x_{nN_n} / S_f)^{(x_{nN_n} / S_f)} \\
2^{-E_f} &= ((x_{11} / S_f) \times (S_1 / S_1))^{((x_{11} / S_f) \times (S_1 / S_1))} \times ((x_{12} / S_f) \times (S_1 / S_1))^{((x_{12} / S_f) \times (S_1 / S_1))} \\
&\dots \times ((x_{1N_1} / S_f) \times (S_1 / S_1))^{((x_{1N_1} / S_f) \times (S_1 / S_1))} \\
&\times ((x_{21} / S_f) \times (S_2 / S_2))^{((x_{21} / S_f) \times (S_2 / S_2))} \times ((x_{22} / S_f) \times (S_2 / S_2))^{((x_{22} / S_f) \times (S_2 / S_2))} \dots \\
&\dots \times ((x_{2N_2} / S_f) \times (S_2 / S_2))^{((x_{2N_2} / S_f) \times (S_2 / S_2))} \\
&\vdots \\
&\times ((x_{n1} / S_f) \times (S_n / S_n))^{((x_{n1} / S_f) \times (S_n / S_n))} \times ((x_{n2} / S_f) \times (S_n / S_n))^{((x_{n2} / S_f) \times (S_n / S_n))} \dots \\
&\times ((x_{nN_n} / S_f) \times (S_n / S_n))^{((x_{nN_n} / S_f) \times (S_n / S_n))}
\end{aligned}$$

$$\text{Substitute } 2^{-E_i} = (x_{i1} / S_i)^{(x_{i1} / S_i)} \times (x_{i2} / S_i)^{(x_{i2} / S_i)} \dots$$

$$\dots \times (x_{iN_i} / S_i)^{(x_{iN_i} / S_i)} \quad \forall i = 1 \text{ to } n$$

$$\begin{aligned}
2^{-E_f} &= (2^{-E_1})^{S_1 / S_f} \times (2^{-E_2})^{S_2 / S_f} \times \dots \times (2^{-E_n})^{S_n / S_f} \\
&\times (S_1 / S_f)^{(S_1 / S_f)} \times (S_2 / S_f)^{(S_2 / S_f)} \times \dots \times (S_n / S_f)^{(S_n / S_f)} \quad (3)
\end{aligned}$$

At the cost of communication overhead, memory and computational overheads are distributed.

IV. SIMULATION EXPERIMENTS

Simulation is performed using ns2 [12] network simulator.

A. Topology

GT-ITM [11] topology generator is used to create our simulation topology. We have represented transit domain routers as POPs of the ISP and stub

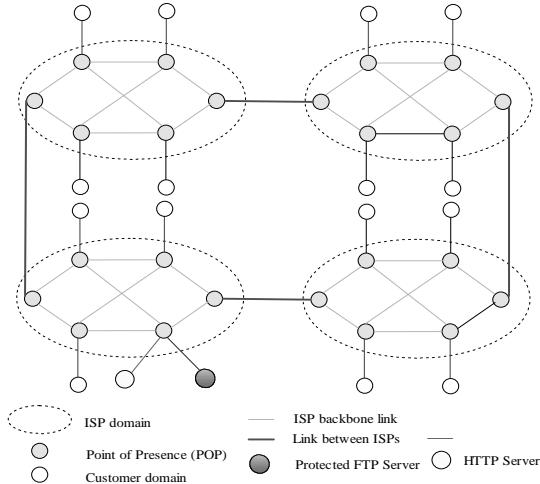


Fig. 2. A short scale simulation topology

Domains as customer domains attached to POPs as shown in fig.2. Following table 1 gives topology generator parameters.

TABLE 1
TOPOLOGY GENERATOR PARAMETERS

S.No.	Parameter	Value
1.	ISP domains	4
2.	No. of transit routers	12 (1 more in ISP 4 for connecting servers)
3.	Edge probability	.85
4.	Number of stub domains	10 / ISP
5.	Number of hosts	10 / stub domain
6.	Backbone link bandwidths	2.5Ghz
7.	Backbone link delays	0 seconds

There are four ISP domains with two peers each i.e. two other ISP domains are directly attached at POPs.

B. Basic parameters of simulation

Table 2 provides the basic parameters set for simulation.

TABLE 2
BASIC PARAMETERS OF SIMULATION

S.No	Parameter	Value
.	Simulation Time	60 seconds
2..	Number of legal sources	100 / ISP domain Total $4 * 100 = 400$
3.	No. of attackers	1-25 / ISP domain. Total = 1-100
4.	Access bandwidth for legitimate customers	1Mbps
5.	Bottleneck Bandwidth	310Mbps
6.	Mean attacker rate	0.1-1.0Mbps (low rate) 2.7-3.7Mbps (high rate)
7..	Attack duration	20-50 seconds

We varied attack rates as given in S.No.6 and computed entropy and goodput. Moreover for establishing a relationship between number of attackers and deviation observed in entropy we varied attackers from 20-100, keeping the total attack bandwidth 20Mbps. However this work is not contributed in this paper.

C. Traffic Parameters

TABLE 3
TRAFFIC PARAMETERS

S.No	Parameter	Value
1.	Traffic arrival process at legitimate clients	Poisson
2.	Traffic generator at attackers (mean)	Attack tools available at

	attack rate given in Table 2, S.No.6	www.nlanr.org
3.	Connection startup time	Random 1-8seconds
4.	Packet Size	1040bytes

All the legitimate TCP connections are not initiated at the same time as SYN backlog is also limited in size as shown in S.No.3.

D. Attack detection parameters

TABLE 4
ATTACK DETECTION PARAMETER

S.No .	Parameter	Value
1.	Window Size	.2 seconds
2.	Tolerance factor a for entropy deviation	3-10

Simulations are carried at different values of tolerance factor a for different attack strengths.

V. RESULTS AND DISCUSSION

Following aspects are discussed in this section:-

- A) Degradation of goodput with attack
- B) Threshold setting
- C) Detection of attack

A. Degradation of goodput with attack

The aim of any DDoS attack is to minimize legitimate traffic reaching at the server. Goodput is a measure of legitimate traffic reaching at server and is calculated as sum of bytes received per flow at server of all normal flows $\sum F_n$ divided by size of time window where F_n represent set of normal flows. Goodput at different attack rates are shown in fig. 3.

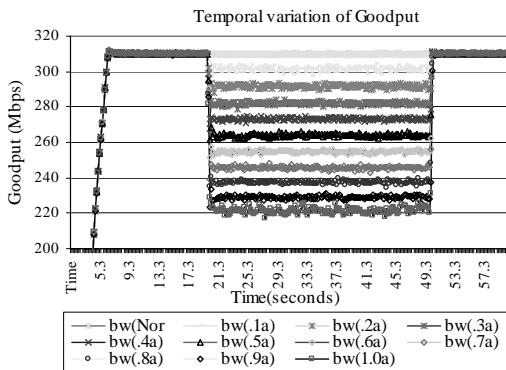


Fig. 3. Goodput at different attack strengths

Here attack is conducted at attack strengths ranging from 10Mbps (0.1Mbps mean attack rate per attacker) to 100Mbps (1.0Mbps mean attack rate per attacker) where bottleneck bandwidth is 310Mbps and number of attackers are 100. Clearly from fig. 3, we can say that as the attack starts at time 20 seconds, normal packet drops increases and hence goodput also decreases. Moreover at meek attack

rates, number of attack packet drops is almost negligible so they degrade to their full strength, however as attack strength increases number of legitimate as well as attack packet drops also increases. As for as high rate attacks are concerned, they almost bring the legitimate goodput to zero.

B. Threshold setting

We conducted simulation experiments for finding out threshold for entropy under normal condition as per simulation parameters given in previous section. The normal range of entropy by using frequency distribution of number of packets per flow ID (SourceIP, SourcePort, DestinationIP, and DestinationPort) in time windows of 0.2 seconds is shown in fig. 4. Simulation is also carried by taking longer window of 1.0 second. Deviations are still lesser as expected however average is almost same.

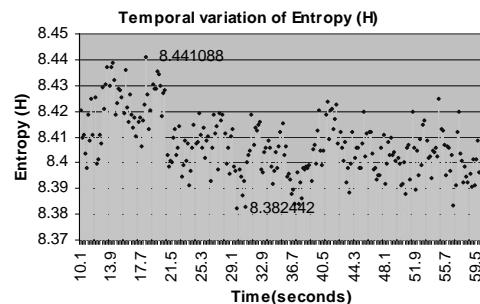


Fig. 4. Normal entropy range without attack

It is found that once the utilization of bottleneck link is 100% , entropy value also lies in small range as depicted in fig. 4. Our range is 8.382442 to 8.441088, whereas this varies depending upon network environment and type of application .The average is 8.407158, standard deviation is 0.012, and maximum absolute deviation from average is .03393 .Finalized simulation parameters are:-

Normal Entropy Value ($H_n(X)$):- 8.407158

Maximum absolute deviation from average (d):- 0.03393
We have bottleneck of 310Mbps but still on the higher side for better link utilization we assume to serve up to 400 legitimate clients with maximum 1Mbps (average 0.8Mbps) request bytes per client.

Though our work is simulation based, but on actual network for profiling purpose this kind of experiments can be conducted to find $H_n(X)$ and d .

C. Detection of attack

As soon as any event in “2” triggers, attack is said to have occurred. Fig. 5 shows entropy profile when our network is put under low rate attack. In this case attack is launched with 100 attackers with mean rate 0.3Mbps per attacker. Clearly in first time window after attack is launched at 20 seconds, there is jump in entropy value. The positive jump and persistent high value as compared to normal reflects that it is a low rate attack and the flows which are causing this anomaly have comparatively lesser frequency than

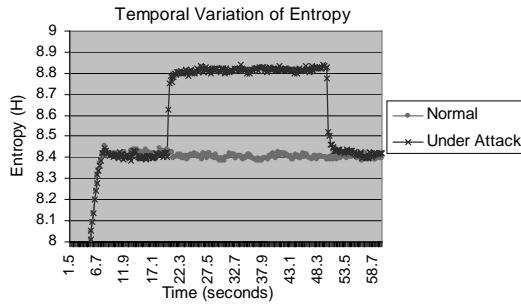


Fig. 5. Entropy for low rate DDoS attack

existing ones. We repeated the low rate attacks with 100 attackers ranging from mean rate 0.1-1.0Mbps per attacker; in all cases the trend was similar as shown in fig. 6, though deviation from normal value is different.

As the attack rate is very low, the traditional volume based techniques [5-7] are not able to distinguish between attack and normal condition, however fig. 7 clearly indicates the change in entropy justifying our claim of picking even a very meek rate attack.

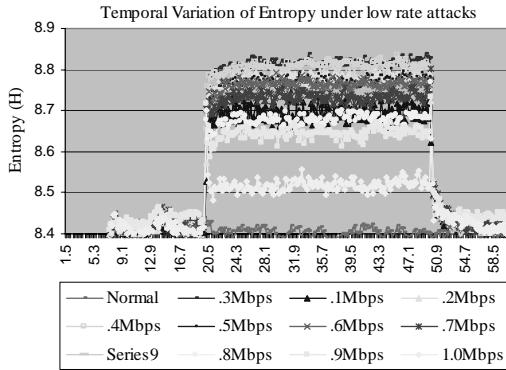


Fig. 6 Entropy at different attack strengths

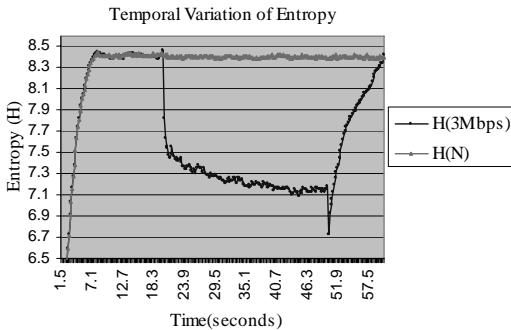


Fig. 7 Entropy for high rate DDoS attack

In case of high rate attacks, entropy value tends to be lower than normal. In our simulation using total attack strength of 300Mbps with 100 attackers, the Entropy variation is reflected in fig. 7.

However initially it can rise but with proper adjustment of window and start time, the same can also be lumped. In this case, the flows which have comparatively higher share of packets are reasons of anomaly. Similar trends exist for high rate attacks at different attack strengths with variation only in deviation from normal value.

VI. CONCLUSION

We presented a solution to detect both low rate degrading and high rate flooding DDoS attacks in ISP domain. It is found that traffic feature distributions are better measures as compared to volume to find signs of attack. Even very meek rate DDoS attacks are detected reliably in ISP domain. Memory and computational overheads are distributed amongst POPs responsible for any traffic destined to victim. Our proposed formula gives accurate values for final entropy value obtained from individual entropies at POPs of the ISP. In our future work we will do comparison of complexity analysis at single and distributed points.

REFERENCES

- [1] R.K.C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial," *IEEE Communication Magazine*, 2002.
- [2] J. Mirkovic, and P. Reiher, "A Taxonomy of DDoS Attack and DDoS defense Mechanisms," *ACM SIGCOMM Computer Communications Review*, Volume 34, Number 2, April 2004.
- [3] David Moore, Geoffrey M Voelker, and Stefan Savage, "Inferring Internet Denial-of-Service Activity," In Proceedings of 10th USENIX Security Symposium, Aug. 2001
- [4] Computer Crime Research Center. "2004 CSI/FBI Computer Crime and Security Survey," Available at: <http://www.crime-research.org/news/11.06.2004/423/>
- [5] T. M. Gil, and M. Poletto, "Multops: a data-structure for bandwidth attack detection," *Proceedings of the 10th USENIX Security Symposium*, 2001.
- [6] R. B. Blazek, H. Kim, B. Rozovskii, and A. Tartakovsky, "A novel approach to detection of denial-of-service attacks via adaptive sequential and batch sequential change-point detection methods," *Proceedings of IEEE Systems, Man and Cybernetics Information Assurance Workshop*, 2001.
- [7] Boldizsar Bencsath, and Istvan Vajda, "Protection against DDoS Attacks Based on Traffic Level Measurements," *Western Simulation MultiConference, San Diego, California, USA*, 2004.
- [8] C.M. Cheng, H.T. Kung, and K.S. Tan, "Use of spectral analysis in defense against DoS attacks," *Proceedings of IEEE GLOBECOM 2002*, pp. 2143-2148, 2002.
- [9] J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDoS at the source," *Proceedings of ICNP 2002, Paris, France*, pp. 312-321, 2002.
- [10] Anukool Lakhina, Mark Crovella, and Christophe Diot, "Mining Anomalies Using Traffic Feature Distributions," *ACM SIGCOMM*, 2005.
- [11] GT-ITM Traffic Generator Documentation and tool <http://www.cc.gatech.edu/fac/EllenLegura/graphs.html>
- [12] NS Documentation Available: <http://www.isi.edu/nsnam/ns>
- [13] V. Paxson, "Bro: A System for Detecting Network Intruders in Real-Time," *Computer Networks*, vol. 31, nos. 23-24, 1999.
- [14] M. Roesch, "Snort—Lightweight Intrusion Detection for Networks," *Proc. USENIX Systems Administration Conf. (LISA '99)*, Nov. 1999.
- [15] Y. Xu, and R. Guerin, "On the Robustness of Router-based Denial-of-Service Defense Systems," *ACM SIGCOMM*, 2005.
- [16] J. Ioannidis, and S. M. Bellovin, "Implementing Pushback: Router-Based Defense against DDoS Attacks," *IEEE INFOCOMM*, 2003.

PERFORMANCE ENHANCEMENT OF BLOWFISH ALGORITHM BY MODIFYING ITS FUNCTION

Modified Blowfish

PROF. KRISHNAMURTHY G.N, DR. V. RAMASWAMY and MRS. LEELA G.H

Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India

Abstract: There has been a tremendous enhancement in the field of cryptography, which tries to manipulate the plain text so that it becomes unreadable, less prone to hacker and crackers, and again obtain the plain text back by manipulating this unreadable text in some way.

In this regard, we have developed a secure algorithm which is a secret-key block cipher that enhances performance by modifying the function of the existing Blowfish[1], which would not only be a secure one, but also reduces total time taken for encryption and decryption.

This paper attempts to improve performance without violating memory requirements, Security and Simplicity of existing Blowfish algorithm. The proposed modification is only limited to the change in the implementation of the Function F of the Blowfish's Feistel network[1].

Because the change in the total time taken for encryption and decryption cannot be seen on software implementation, we have implemented VHDL application to show the differences in the delay.

Key words: Cryptography;Plain-text;Cipher-text;Encryption;Decryption;Secret-key;Feistel-network;P-array;S-box;Function.

DESCRIPTION OF THE ALGORITHM

Blowfish is a variable-length key[2], 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes.

Data encryption occurs via a 16-round Feistel network. Each round consists of a key-dependent permutation, and a key- and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

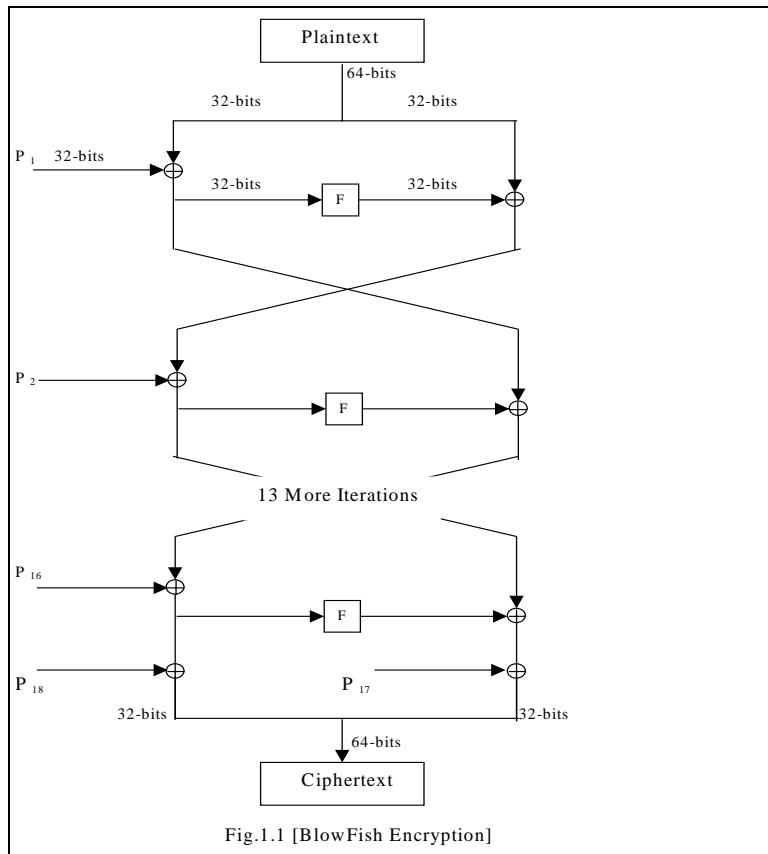


Fig.1.1 [BlowFish Encryption]

Subkeys:

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption.

1. The P-array consists of 18 32-bit subkeys: P1, P2,...,P18.

2. There are four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,..., S1,255;

S2,0, S2,1,..., S2,255;

S3,0, S3,1,..., S3,255;

S4,0, S4,1,..., S4,255.

Decryption for Blowfish is relatively straightforward. Ironically, decryption works in the same algorithmic direction as encryption beginning with the cipher text as input. However, as expected, the sub-keys are used in reverse order.

More complicated reversible function was decided one with modular multiplications and rotations. However these operations greatly increase the algorithm execution time. Since Function F is primary source of algorithm security, it was decided to save time complications for that function.

Function F is as follows:-

Divide X_L into four eight-bit quarters: a, b, c, and d

$$F(X_L) = ((S1,a + S2,b \bmod 2^{32}) \text{ XOR } S3,c) + S4,d \bmod 2^{32}$$

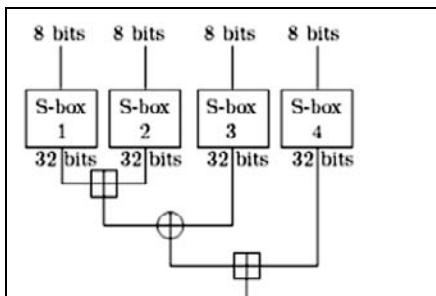


Figure 1.2. [Existing Blowfish Function F]

Without violating the security requirements, the Blowfish function F can be modified as follows:-

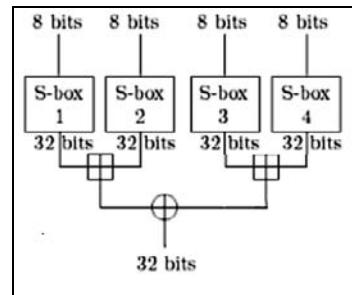


Figure 1.3. [Modified Blowfish Function F']

$$F'(X_L) = (S_{1,a} + S_{2,b} \bmod 2^{32}) \oplus (S_{3,c} + S_{4,d} \bmod 2^{32})$$

This modification supports the parallel evaluation of two addition operations ($S_{1,a} + S_{2,b} \bmod 2^{32}$) and ($S_{3,c} + S_{4,d} \bmod 2^{32}$) by using threads. The parallel evaluation reduces the time from two additions to time required for one addition. As the algorithm uses 16 iterations, this time is saved 16 times for every encryption/decryption. This is a considerable improvement. Also, as the security of Blowfish lies in the fact that it uses variable key, this modification does not make the algorithm vulnerable in any way so that cryptanalysis becomes easy. Also it does not violate any of the security issues discussed above for original Blowfish algorithm.

But true parallelism cannot be achieved on a uniprocessor system. So the effect of the modification can be seen only in multiprocessor system with at least two processors.

So this modified function can be best adopted for the hardware implementation of the algorithm. In the hardware implementation the of the function F' requires only two levels of computation, where as the original function F requires three levels of computation.

CONCLUSION

The improved modified algorithm has enhanced the performance over existing blowfish algorithm by reducing the number of clock cycles required for the execution of Blowfish function by 33% and hence reducing the overall execution time of the modified Blowfish algorithm by 14%. This is explained in detail in the Appendix along with sample waveforms.

This is possible because the modified Blowfish function F' executes both the summations in parallel, where as the existing function executes the sums in sequential fashion.

BIBLIOGRAPHY

i. (Journal Articles)

- [1] BRUCE SCHNEIER, "The Blowfish Encryption Algorithm." Dr.Dobb's Journal, April 1994.
- [2] BRUCE SCHNEIER, "Description of new variable-length key, 64-bit Block Cipher (Blowfish)." Workshop on Fast Software Encryption, December 1993; published by Springer-Verlag.

ii. (Books)

- 1. BRUCE SCHNEIER, Applied Cryptography, Protocols, Algorithms, and Source Code in C. New York:Wiley, 1996.

- 2. William Stallings, Cryptography and Network Security, Third Edition, Pearson Education, 2003

Appendix: SAMPLE WAVEFORMS:

The following Simulation diagram (Figure 1.4) shows the time required to execute the Function F of the existing Blowfish Function as marked by the 2 yellow lines. As per the result it is taking 55ps - 25ps = 30ps.

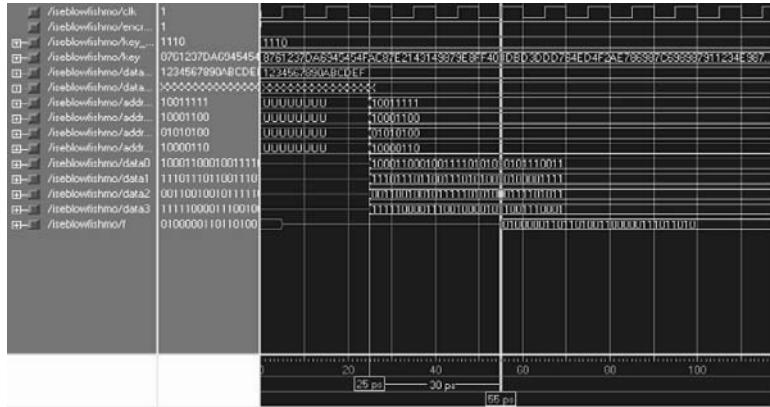


Figure 1.4. [Waveform for Existing Blowfish Function F]

The following Simulation diagram (Figure 1.5) shows the time required to execute the Function F of the modified Blowfish

Function as marked by the 2 yellow lines. As per the result it is taking 45ps - 25ps = 20ps.

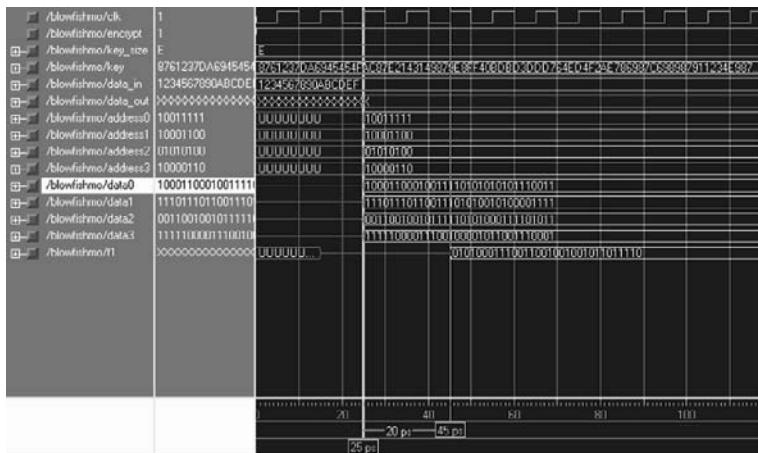


Figure 1.5. [Waveform for Modified Blowfish Function F']

So the ratio of time taken for modified to existing Blowfish Function=20/30=0.66, hence we have 33% improvement in the performance.

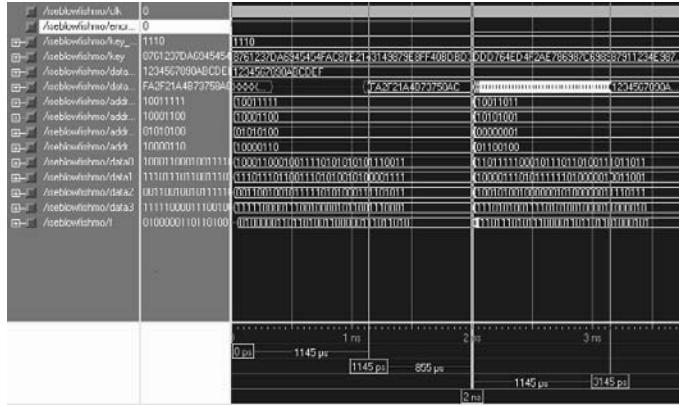


Figure 1.6 [Waveform for Existing Blowfish Algorithm]

The diagram (Figure 1.6) above shows the time taken to execute the existing Blowfish algorithm, where in the time required for encryption is shown between the first 2 yellow lines and the time taken for decryption is the time between last two yellow lines. As per the result shown above,

The time taken for encryption = $1145 - 0 = 1145$ ps.
The time taken for decryption = $3145 - 2000 = 1145$ ps(same as encryption).

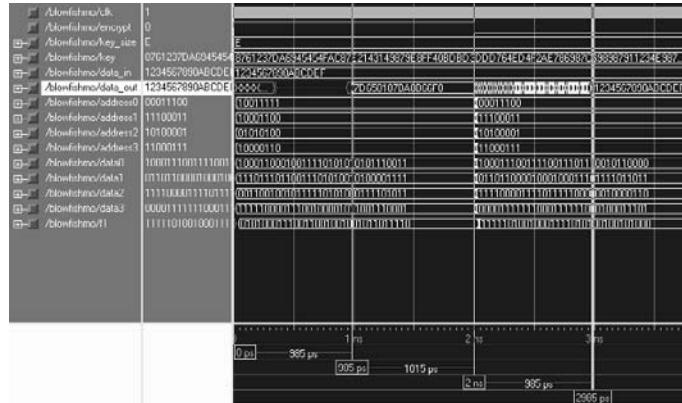


Figure 1.7 [Waveform for Modified Blowfish Algorithm]

The diagram (Figure 1.7) above shows the time taken to execute the existing Blowfish algorithm, where in the time required for encryption is shown between the first 2 yellow lines and the time taken for decryption is the time between last two yellow lines. As per the result shown above, The time taken for encryption = 985 – 0 = 985ps.

The time taken for decryption = $2985 - 2000 = 985\text{ps}$ (same as encryption).

So the ratio of time taken for modified to existing Blowfish algorithm=985/1145=0.86, hence we have 14% improvement in the over all performance.

A Clustering Algorithm Based on Geographical Sensor Position in Wireless Sensor Networks

Kyungjun Kim

Department of Radio Mobile Communication Engineering

Honam University

59-1 Seobong Gwangsan Gwangju, 506-714 Korea

Abstract - The lifetime of sensor nodes are severely constrained by the amount of available battery power. Sensor nodes should spend as little energy as possible receiving and transmitting data as wireless communications consume the significant amounts of battery power. For this reasons, an important requirements are energy consumption in nodes in order to extend the network lifetime. In this paper, we devise a fully centralized cluster formation algorithm. The goal is to have many child nodes at the sink in order to avoid bottleneck nodes near the sink and thus save energy. Our algorithm can reduce control traffic overhead by creating the dynamic cluster. We have evaluated the performance of our clustering algorithm through an analysis and a simulation. We compare our algorithm's performance to the best known centralized algorithm, and show that providing a good performance in terms of the life time.

I. INTRODUCTION

Wireless sensor networks have been identified as one of the most important technologies for the future century [2]. A sensor network is composed of a large number of battery-operated sensor nodes, which is densely deployed either inside the phenomenon or very close it [1]. To enable communication between sensors not within each other's communication range, the sensors form a multi-hop communication network. Sensors in these multi-hop networks detect an event, and then forward to a central location (or sink) the information collected (parameters characterizing these events are estimated) [5].

The cost of transmitting a event is higher than a processing cost and hence it may be advantageous to organize the sensors into clusters. Clustering is fundamental mechanism to design scalable sensor network protocols. Clustering splits the networks into disjoint sets of nodes each centering on a chosen cluster header [4]. Main function of the clustering is to minimize the exchange of flooding messages, there is no point in wasting valuable resources to proactively maintain such an elaborate structure between floods, when there is no traffic that can make use of it.

Although giving the already huge number of routing protocols in wireless sensor networks, we extend an existing cluster-based protocol defined as the low-energy adaptive clustering hierarchy [11] probably the best-known cluster-

based protocol. The position models described in this paper form a relatively skewed distributed position. Cluster headers are concentrated on the right-hand or left-hand side in the sensor network topology. In this case, if the cluster headers rapidly deplete remaining energy, the inter-cluster routing path may fail which can jeopardized the entire mission in some cases. The unbalance of energy depletion is caused by different distance from the sink.

To our best knowledge, [1, 2] have proposed clustering algorithms that minimize the energy of a sensor node. In [5, 9], the authors analytically derived the optimal number of clusters that minimize energy consumption. However, these mechanisms are mostly heuristic in nature and aim at generating the minimum numbers of clusters such that any node in any cluster is at most some hops away from the cluster header. In Fig. 1, cluster headers (or sensors) are concentrated on the right-hand (or left-hand) side in the sensor network topology.

In this paper, we propose a dynamic, distributed algorithm for organizing the sensors network in a hierarchy of clusters with an objective of minimizing the energy spent in the wireless sensor network, we divide the whole network into a few clusters depending on the distance from the sink. This algorithm is helping avoid "hot spots" in the network. Previous works have been aimed at generating the minimum number of clusters, but not at minimizing the energy spent in sensor node. For these reasons, it is very important to design a fast algorithm to organize sensors in clusters to minimize the energy used to communicate information from all nodes to the processing center. Our algorithm was motivated to achieve outlined goals.

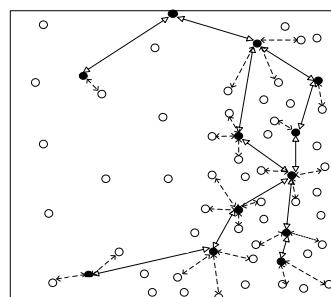


Fig. 1 Network model

Our algorithm validate through the simulation, which show that our algorithm increase the network lifetime by reducing the senor energy consumption since cluster headers are uniformly distributed over the whole network.

The rest of the paper is organized as follows. Section 2 describes a preliminary works. Section 3 presents our algorithm and argues that is satisfies its objectives. Simulation results for evaluating performance are presented in section 4. Finally, Section 5 concludes the paper and discusses possible future research directions.

II. RELATED WORKS

Wireless sensor networks have a character that the forwarding nodes is clearly a balancing act between reduced transmission energy and increased receive energy. Hops that are too short lead to excessive receive energy, and then hops that are too long lead to excessive path loss. There exists considerable previous work addressing the topology control problem of minimizing nodal transmission power, with guarantees of network connectivity.

Bandyopadhyay et al. [5], proposed a clustering-based protocol that utilizes randomized rotation of cluster heads to evenly distribute the energy load among the sensors in the network. In [5], sensor nodes form clusters with one node being the cluster head. However, since the cluster heads would deplete their energy supply much faster than the rest of the nodes, each node can only be a cluster head temporarily, which implies that the clustering global synchronization would have to be done rather frequently.

Handy et al. [8] does not control the number of clusters in current round, since the sensor nodes elect themselves to be local cluster-headers. This algorithm can not maintain optimal number of clusters so that it should consume much energy dissipation.

Youssef et al. [10] proposed routing approach which constraints the minimum transmission range in order to limit the delay. However, which might require the deployment of many gateways to guarantee high sensor coverage.

Heinzelman et al. [12, 13] have assumed that the sensors are equipped with the capability of tuning the power at which they transmit and they communicate with power enough to achieve acceptable signal-to-noise ratio at the receiver.

To meet needs of cluster formation in wireless sensor networks, we proposes a cluster header selection algorithm for establishing virtual clusters of variable length, in which the sink divides the network topology into several segments (or grinds), and then only a single cluster header is selected at each grind based on round-robin fashion. Our algorithm differs substantially from [5, 8], since we do not make any assumptions about its specific locations of sink, and data forwarding do not rely on direct connectivity.

Our goal is to devise dynamic clustering algorithm based on position that can form variable size cluster. In order to adapt the size of cluster in environment, the achieved cluster sizes should be as close as possible to the specified density.

Therefore, once the cluster head is assigned to a cluster, the total number of message sent by each node to one of its neighbor implies that the total forwarding message reduced by at least a faction of neighbor.

III. CLUSTER FORMATION SCHEME

In this section, we describe the clustering protocol based on geographical sensor position. First, we define the optimal parameters for our model. Second, we describe our algorithm used in the cluster headers and sensors per round. Finally, we prove that the protocol meets its requirement.

A. Our Model

To determine the optimal parameters, consider a set of sensors deployed in a field. We assume the following properties about the sensor network.

1. All sensors are arbitrarily deployed in a two-dimensional plane, and have homogeneous capability, i.e. equipped with GPS-capable antennae. We show that location information (x_i, y_i) is available to node i ($i=1,2,\dots,l$), and distance among nodes, d , respectively, for all nodes in the network. We denote the Euclidean distance between x_i and y_j at (x_i, y_j) as

$$d(x_i, y_j) = \sqrt{(x_i - y_j)^2 + (y_i - x_j)^2}$$

2. All sensors transmit at the same power level and hence have the same radio range r . However, the same time or energy cost is required for sending or receiving a packet of unit size.

3. The radios on every node are switched off when its does not need to participate in any communication. Such energy consumption can be founded in the Fig. 2.

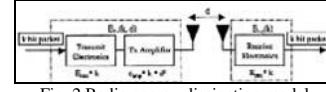


Fig. 2 Radio energy dissipation model

4. We consider the following network model. Prior to selecting cluster header, a sink parts the sensing field into $r \times r$ grid size with received location information from all sensors. Thus, we assume that the radius of cluster is limited by node density. These sensors with higher power levels should cover at least two or more cluster diameters to guarantee that the resulting inter-cluster overlay will be connected.

5. Let the clustering time to re-establishing a grid topology, τ_{grid} be the time interval taken by the sink. Clustering terminates within a fixed number of iterations without regard to cluster range. Assuming that the process for selecting head completed within τ_{head} , and we ensure that $\tau_{grid} \geq \tau_{head}$. Clustering and head selection process is triggered every $\tau_{grid} + \tau_{head}$ second to select new cluster heads.

6. We consider a topology model for sensing field length (R), in which n nodes are randomly distributed in square field.

B. The Proposed Algorithm

The cluster formation algorithm consists of four phases: subscription query, query relay, position aware and cluster header selection. In Fig. 3, the process of position aware is illustrated as follows. Position aware phase starts with the received position information from sensors. When a sink receives a reply from nodes via back path, the sink starts deciding the cluster to the sink along the existing path because it receives the location of route path.

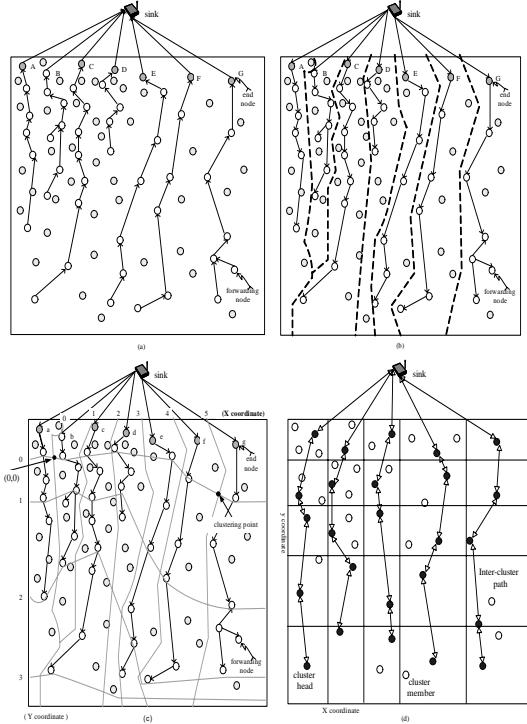


Fig. 3 An example of position aware process. (a) query reply: reporting phase from sensor to the sink. (b) sink broadcasts the partition information to entire nodes. (c) position aware: two hops distance based (d) cluster selection: After broadcasting information from sink, clusters of grid size appear.

At the subscription query phase, a sink directs a join query to the source. At the query relay phase, each sensor node is forward to pre-determined back path via its sensor node. At the position aware phase, our algorithm divides a sensing field into some grid areas; the second phase, referred to as the head selection, locally selects cluster headers on this grid topology. Generally, the size of a cluster is the numbers of nodes belonging to it. However, in our algorithm a density (or size) of nodes, \bar{d} is imposed by the average number of nodes.

Our clustering algorithm starts with skew distributed topology, T_{skew} of wireless sensor networks. In Fig. 3(a), according to received information from each sensor, sink broadcasts an advertisement message using its maximum power range, referred to as the cluster setup (ES) message in

Fig. 3(b), and the ES includes the location of each cluster number, C_i and (x_i, y_i) coordinates, where $i=1, 2, \dots, z$. Upon receiving such an ES, each node a_j , where $j=1, 2, \dots, m$, selects the nearest of its adjacent nodes as cluster header. In Fig 3(c), the source of route path is $r[0]$, e.g. a, b, c, d, e, f, and g the node denotes a gate relay nodes to find the route path from the sink to the gate relay nodes.. Let S_i denote the accumulated sum of the hop count from the terminal node to the gate relay node along route path. Thus, the $r[0]$ has zero.

In Fig. 3(b), let A, B, C, D, E, F, and G be a set of relay $r[0]$ and $r[0]$'s children (i.e. $r[A], r[B], r[C], r[D], r[E], r[F]$, and $r[G] = \{\text{nodes involved in a set of relay } r[0]\}$). The sink finds a set of relay node to minimize the hop count of route path, and maximize the power range, R among elements of relay $r[0]$ satisfying $\{S_i = a_1 + a_2 + \dots + a_{n-1} + a_m\} < \lfloor P_H \rfloor$ and R. Based on P_H and R, and y-coordinate, i.e. 1, 2, 3, ..., k, over the route path, i.e. A, B, C, D, E, F, and G, respectively, the sink is chosen as the relay nodes, i.e. a, b, c, d, e, f, and g. In Fig. 4, the out proposed algorithm is formulated as follows.

```

For each node, j located in  $a_j \in T_{skew}$  to be included at each cluster,  $a_j \in C_i$ :

for re-establishing cluster,
    if  $a_j$  completes then
        repeat
            send request_message from sink to node
            if sink receives information then
                compute grid topology for clustering
                send partition information to nodes
            end if
        until position_aware_time  $\leq$  threshold;
    else
        repeat
            if one round is expired then
                get backoff_time,
                broadcast remaining energy;
                select as a cluster head a node with  $W_p$ ;
            else
                while all node have transmission energy do
                    send its event to cluster head;
                end while
            end if
        until one_round_time;
    end if
end for

```

Fig. 4 Pseudo-code for clustering algorithm

The clustering algorithm is recursively repeated along route path. The failure of a node somewhere in the network requires that the algorithm is executed for the complete network again. It is a fully centralized algorithm since each node determines designated cluster based on information received from sink. Sensor nodes do not have global knowledge of either the hop count or the geometric length of each hop. The geometric distance between nodes is approximately proportional to the hop count between them.

IV. PERFORMANCE EVALUATION

We evaluate performance of our algorithm via a simulation study. For simulation, we used a 100-node network where nodes were randomly distributed $100 * 100$ area and the sink with fixed location. Each data message was 500 bytes long and the packet header for each type of packet was 25 bytes long.

For simulation, we use the same radio model as discussed in [2]. The transmitter dissipates energy to run the radio electronics and the power amplifier, and the receiver dissipates energy to run the radio electronics, as shown in Fig. 2.

For the experiments described here, both the free space (d^2 power loss) and the multi-path fading (d^4 power loss) channel models were used, depending on the distance between the transmitter and receiver. Power control can be used to invert this loss by appropriately setting the power amplifier—if the distance is less than a threshold d_0 , the free space (fs) model is used; otherwise, the multi-path (mp) model is used. Thus, to transmit an 1-bit message a distance d , the radio expends,

$$\begin{aligned} E_{Tx}(l, d) &= E_{Rx}(l) + E_{Tx-amp}(l, d) \\ &= \begin{cases} lE_{elec} + l_{ep}d^2, & d < d_0 \\ lE_{elec} + l_{ep}d^4, & d \geq d_0 \end{cases} \end{aligned} \quad (1)$$

and to receive this message, the radio expends:

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} \quad (2)$$

The electronics energy, E_{elec} , depends on factors such as the digital coding, modulation, filtering, and spreading of the signal, whereas the amplifier energy, $E_{fs}d^2$ or $E_{mp}d^4$, depends on the distance to the receiver and the acceptable bit-error rate, respectively. In [13], the cluster formation algorithm was created to ensure that the expected number of clusters per round is k , a system parameter.

We analytically can determine the optimal value of k in [13] using the computation and communication energy models. Assume that there are N nodes distributed uniformly in an $M*M$ region. If there are k clusters, there are on average N/k nodes per cluster (one cluster header and $(N/k)-1$ non-cluster header nodes). Each cluster header dissipates energy receiving signals from the nodes, aggregating the signals, and transmitting the aggregate signal to the sink. Since the sink is far from the nodes, presumably the energy dissipation follows the multi-path model (d^4 power loss). Therefore, the energy dissipated in the cluster header node during a single frame is

$$E_{CH} = lE_{elec} \left(\frac{N}{k} - 1 \right) + lE_{DA} \frac{N}{k} + lE_{elec} + lE_{mp} d_{toSink}^4 \quad (3)$$

where d_{toSink} is the distance from the cluster header node to the sink and we have assumed perfect data aggregation.

Each non-cluster header node only needs to transmit its data to the cluster header once during a frame. Presumably the distance to the cluster header is small, so the energy dissipation follows the Friss free-space model (d^2 power loss). Thus, the energy used in each non-cluster header node is

$$E_{non-CH} = lE_{elec} + lE_{fs} d_{toCH}^2 \quad (4)$$

where d_{toCH} is the distance from the node to the cluster header.

The communication energy parameters are set as: $E_{elec} = 50\text{nJ/bit}$, $E_{fs} = 10\text{pJ/bit/m}^2$, and $E_{mp} = 0.0013\text{pJ/bit/m}^4$. The energy for data aggregation is set as $E_{DA} = 5\text{nJ/bit/signal}$.

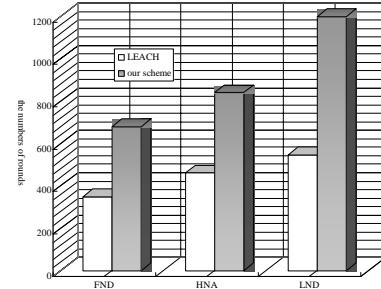


Fig. 5 System life time

Fig. 5 shows the number of rounds when first node dies (FND), half of the nodes (HNA) and last node dies (LND). We can see that proposed algorithm (*our scheme*) provides approximately two times longer life time than [13] in all cases for a $100\text{m} * 100\text{m}$ network. The energy consumption for forming clusters in [13], and our algorithm are similar.

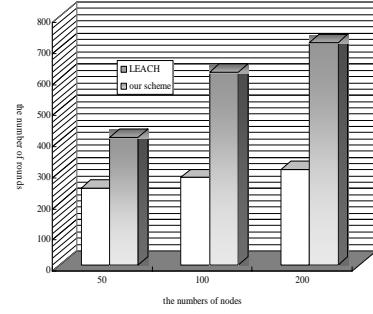


Fig. 6 Life time versus the number of nodes

Fig. 6 shows the number of rounds completed at the FNA with various numbers of nodes. When the node density is high, our algorithm still offers approximately two times longer life time than [13].

Our algorithm has a series of advantage for maintain the optimal number of cluster header and without any negotiation between the sensor nodes for the election of cluster headers. However, proposed algorithm has scalability problems for large sensor networks or is not directly applicable to the support of variant data delivery models such as [9]. Our scheme is more efficient than [13] and less variety of energy consumption. Because this protocol uses cluster header nodes with more energy than the nodes along the shorter routes, the

optimal routes are chosen. Therefore, the remaining energy in all nodes keeps evenly. This is mainly due to the load balance algorithm used in our algorithm so that all nodes try to evenly share their lifetime.

V. CONCLUSION AND FUTURE WORKS

We presented here a cluster formation algorithm based on location in wireless sensor networks with skew distribution that cluster headers work based on non-rechargeable energy. Simulation results show that our algorithm provides a much longer network life time by reducing the sensor power consumption since cluster headers are uniformly distributed over the whole network.

In our evaluation algorithm, however, does not remove all remaining problems in [8]. Therefore, our future work will consider scalability for applicable in large sensor networks, and plan to extend our simulation results by studying additional network parameters or more general topologies.

REFERENCES

- [1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: a survey," *Computer Networks*, vol. 38, 2002, pp. 393-422.
- [2] C. Chong, S.P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," *Proceedings of the IEEE*, vol. 9, no. 8, Aug. 2003, pp. 1247-1256.
- [3] P. Santi and J. Simon, "Silence Is Golden with High Probability: Maintaining a Connected Backbone in Wireless Sensor Networks," in Proc. of 1st European Workshop Wireless Sensor Networks, Lecture Note in Computer Science, LNCS, vol. 2920, Jan. 2004, pp. 106-121.
- [4] H. Chan and A. Perrig, "ACE: An Emergent Algorithm for Highly Uniform Cluster Formation," in Proc. of 1st European Workshop Wireless Sensor Networks, Lecture Note in Computer Science, LNCS, vol. 2920, Jan. 2004, pp. 157-171.
- [5] S. Bandyopadhyay and E.J. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks," in Proc. of IEEE Infocom 2003
- [6] J. Pan, Y.T. Hou, L. Cai, Y. Shi, and S.X. Shen, "Topology Control for Wireless Sensor Networks," in Proc. of MobiCom'03, San Diego, California, USA, Sep. 2003.
- [7] S. Lindsey, C. Raghavendra, K.M. Sivalingam, "Data gathering Algorithms in Sensor Networks Using Energy Metrics," *IEEE Transactions on Parallel and Distributed Systems*, vol. 13 , no. 9, Sept. 2002.
- [8] Handy, M.J.; Haase, M.; Timmermann, D., "Low energy adaptive clustering hierarchy with deterministic cluster header selection," in Proc. of 4th International Workshop on Mobile and Wireless Communications Network, Sept. 2002, pp. 368 – 372.
- [9] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next Century Challenges: Scalable Coordination in Sensor Networks," in Proc. of the ACM/IEEE International Conference on Mobile Computing and Networking, August, 1999, pp. 263-270.
- [10] M. Youssef, M. Younis, K. Arisha, "A constrained shortest path energy-aware routing algorithm for wireless sensor networks," in Proc. of the IEEE Wireless Communication and Networks Conference (WCNC2002), Orlando, FL, March 2002.
- [11] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks," *IEEE Trans. on Mobile Computing*, vol. 3, no. 4, Oct.-Dec. 2004, pp. 366-379.
- [12] Heinzelman W., Chandrakasan A., Balakrishnan H, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Transactions on Wireless Communications*, vol.1, no.4, Oct. 2002.
- [13] Heinzelman W., Chandrakasan A., Balakrishnan H, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," in Proc. of IEEE HICSS, Jan. 2000.
- [14] R. Krishnan and D. Starobinski, "Efficient Clustering Algorithms for Self-organizing Wireless Sensor Networks," *Ad Hoc Networks*, vol. 4, 2006, pp. 36-59.
- [15] Niculescu, D., "Positioning in Ad Hoc Sensor Networks," *IEEE Network*, vol. 18, no. 4, pp. 24-29, 2004.
- [16] E. Yoneki and J. Bacon, "A survey of Wireless Sensor Network Technologies: Research Trends and Middleware's Role," Technical Report, UCAM-CL-TR-646, University of Cambridge, Sep. 2005, pp. 1-43.

The Economic Evaluation of the Active DSRC Application for Electronic Toll Collection System in KOREA

Gunyoung Kim and Kyungwoo Kang

Department of Transportation Engineering, Hanyang University
1271 Sa 1-dong, Ansan, Kyonggi, 425-791, Korea

Abstract-Providing real time traffic information is a key for effective implementation of Intelligent Transport Systems (ITS). The main purpose of this paper is to introduce the recent technological trends of Dedicated Short Range Communications (DSRC) applications for ITS and its economic evaluation, focusing on the City Bus Information System (CBIS) and Electronic Toll Collection System (ETC) in Korea. From a research perspective, it is necessary for the seamless development and maintenance of technical and competitive edges, and the proper budgetary allocation for research and development. Furthermore, the progressive participation of private companies that have the leading technologies on active DSRC is also required.

I. INTRODUCTION

The objective of Intelligent Transport Systems (ITS) is to make the traditional transportation systems safer, faster, and more efficient by establishing real time communications between travelers, vehicles, roads, and the other transportation devices. Thus, providing real time traffic information is a key for effective implementation of ITS. Still the application of telecommunications technology, which is one of the core technologies of ITS, requires the establishment of proper national infrastructure.

In order to achieve the objective of transmitting reliable data, we need to choose the most suitable communications technique. Among various communications requirements in ITS, the communications between vehicles and roads has an important status and collection of the traffic information depends on it. From loop detectors to microwave, infrared or laser, there are many kinds of communications techniques between vehicles and roads.

In Korea, the frequency range of Dedicated Short Range Communications (DSRC) for ITS defined by the Korean Ministry of Information and Communication. It is expected that, based on it, a manifold of ITS services will emerge in Korea. Also, the Korean ITS forum has been handling the first pending problems of 'Dedicated Short Range Communications applications inclusive of Electronic Toll Collection (ETC)' since 2001.

Many ITS related companies and research institutes participated and discussed standardization of DSRC communications over the last 3 years, since 1998. However, the Telecommunication Technology Association (TTA) of

Korea adopted as standard for DSRC radio communications between Roadside Equipment (RSE) and On-Board Equipment (OBE) the 5.8GHz band in August 2000.

The purpose of this paper is to introduce the technological trends of active DSRC application for ITS and its economic evaluation, focusing on the City Bus Information System (CBIS) and Electronic Toll Collection system (ETC) that are most often used in Korea.

This paper has been divided into five sections: Section 2 introduces briefly the concepts of DSRC and standardization of active DSRC and its frequency range distribution in Korea. Section 3 describes national Korean policies on various ITS applications. In section 4, economic evaluation of DSRC application will be presented. Finally, section 5 summarises the relevant findings.

II. OVERVIEW OF DSRC FOR ITS

A. Characteristics of DSRC

Dedicated Short Range Communications (DSRC) is a bi-directional short-range communications between On-Board Equipment (OBE) and Roadside Equipment (RSE). A communications service is only provided during the time a vehicle passes a RSE. The characteristic structure of the DSRC communications is a typical reduced protocol stacks comprised of a physical layer, data link layer, and application layer. Such architectures are very common for real-time environments. The data link layer consists of the MAC (Medium Access Control) sub-layer and the LLC (Logical Link Layer) sub-layer, and it provides its service directly to the application layer.

According to the communications type, DSRC is classified into two types: passive DSRC (transponder) and active DSRC (transceiver). The passive DSRC system has been applied in Europe. This system has a data transmission rate of 100Kbps and 10m-communications coverage. In a passive DSRC system, an oscillator is not mounted in OBE to reduce hardware overhead. Instead, RSE transmits through a continuous carrier for uplink transmission. This restricts cell coverage and service expansion. Therefore, only limited services are available such as Electronic Toll Collection, Parking Management System and so on. For that reason, the price of RSE and OBE are low, compared with that of the active type.

Active DSRC has been mainly applied in Japan and the United States. An active DSRC system has a 1Mbps data

transmission rate and a 100m-communications coverage. An oscillator is mounted in OBE. This provides large radio cell coverage and service expansion. Therefore, various ITS services such as Electronic Toll Collection, City Bus Information System, Commercial Vehicle Operations, wireless Internet service and others can be supported. Because of these performance abilities, the price of active type RSE is somewhat high, compared to passive type RSE. However, the price of dynamic OBE is the same as that of the passive type OBE.

B. Standardization of DSRC in Korea

The Korean government and research institutes have made efforts for the standardization of DSRC. Some important standardization activities are the following.

- Mar. 1998: A research committee for ITS Communications under the Telecommunication Technology Association (TTA) was organized
- Jun. 1998: Draft standard review for active DSRC and passive DSRC (CEN-based).
- Mar. 2000: Active DSRC requirement specification technical review.
- Oct. 2000: Approved DSRC standard in the TTA/Assembly (TTAS.KO-06.0025: Standard of DSRC Radio Communications between Roadside Equipment and On-Board Equipment in the 5.8GHz Band).
- Dec. 2001: Approved ETC interface standard in the TTA/Assembly (TTAS.KO-06.0035: Standard of Application Interface using DSRC for ETC Service).

The Telecommunication Technology Association (TTA), which is one of the standardization organizations in Korea, adopted as active DSRC standard for radio communications between RSE and OBE the 5.8GHz band in August 2000. While passive DSRC uses 2 channels, at 30MHz for communications between RSE and OBE, active DSRC uses 2 channels, at 20MHz. The most recent (2001. 4), Korean Ministry of Information and Communication distributed DSRC frequency bands into 20MHz from 5.795GHz to 5.815GHz for the use of private communications, and into 20MHz from 5.835GHz to 5.855GHz for the use of public communications. Therefore, as the frequency range distribution of DSRC has been settled, it will be expected that the market of relevant equipments and services will rapidly grow.

III. THE VARIOUS ITS APPLICATIONS

A. Overview of CBIS in Korea

Some of the most serious urban traffic problems in Korea, which resulted in poor bus operations, are the inappropriate allocation time of bus operations, problems with schedule adherence, and excessive waiting times. Many bus users complained that there are no alternative bus routes and reliable bus arrival time information due most likely to congestion in the CBD. Thus one should decide whether to wait for the bus or not, without information. In addition, one

wonders about when the bus will come and how much time will be needed.

In Korea, as a model of City Bus Information System (CBIS), two systems were adopted in 2000. One utilizes a beacon, the other a Global Positioning System (GPS) with cellular phone. However, several problems such as accuracy of location, communications delay, and various costs (initial construction, operation, and maintenance costs) were introduced as a result. Today, various CBIS operation scheme using active DSRC are successively applied. Within the ITS model city project for activating ITS in local cities by Korean Ministry of Construction and Transportation, DaeJeon metropolitan government has operated CBIS using active DSRC since January 2003. The important contents will be explained in the next section.

B. CBIS Structure

CBIS consists of four parts: OBE, RSE, information display, and control center. The principal points of CBIS using active DSRC are location tracking and 2-way communications between RSE, which is placed at the roadside, and OBE, which is attached to the vehicle. Transmitting packet data with 1Mbps high speed is available. The requirement information for CBIS is shown in table 1.

TABLE 1
REQUIREMENT INFORMATION FOR CBIS

Location	Required Information
Equipment in Bus	<ul style="list-style-type: none"> - Present position - Public information - Relevant traffic information - Next bust stop name - Weather information - Other information
Bus Stop	<ul style="list-style-type: none"> - Route information - Public information - Bus allocation information - Expected arrival time - Related traffic information - Weather information
Center	<ul style="list-style-type: none"> - Allocation information - Accident information - Bus service plan information - Present position about bus - Other information

Also, table 2 shows the static and dynamic data for CBIS. These data were collected from bus companies and relevant organizations and updated periodically.

TABLE 2
STATIC AND DYNAMIC DATA FOR CBIS

Classification	Required Information
Static Data	<ul style="list-style-type: none"> - Route information - Bus service plan - Allocation time - Distance - Elapsed time - Fare - Local information
Data Dynamic	<ul style="list-style-type: none"> - Position and speed - Traffic condition

The most powerful merits of CBIS using active DSRC are location tracking accuracy as well as low communications cost. And there is no additional cost for various information such as traffic information, incident information, transfer information, news, advertisements and others on bus stops or kiosks. In addition, because of using an exclusive line, there is no communications delay or omitted data. Also, collecting and providing real time traffic information is superior to the cellular phone communications method. CBIS using active DSRC uses 5.8GHz band RF communications between RSE and OBE. Collected information was sent to the traffic information center through the exclusive line.

Then the traffic information center sends various information such as traffic information, road condition, weather information, incident information, and accident information to a bus stop display through an exclusive line. The bus stop display provides information through LED (Light-Emitting Diode), LCD (Liquid Crystal Display) or kiosk. The basic protocols of CBIS consist of three layers; the physical, data link, and application layers.

C. Current Status of ETC Service using DSRC

In Korea, the recently adopted technologies of Electronic Toll Collection (ETC) are developed within the DSRC initiative. Korea Highway Corporation has operated a passive DSRC of ETC type named 'Hi-Pass' for a pilot program since 2000, at 3 points around Seoul metropolitan area such as CheongKye, PanKyo, and SeongNam. The New Airport Highway Co., Ltd. has operated Hi-Pass at 2 points on the Incheon International Airports exclusive expressway that opened in March 2001.

The targeted vehicle classifications are passenger vehicles, regular city bus, and light automobile. As of now, approximately 17,000 OBEs are installed for various vehicle classes. The prepaid Hi-Pass cards are used for all classes except regular city buses that use after payment card.

In the communications link of ETC application, active communications mode is adopted in Japan's DSRC Standard (ARIB T55), while passive communications mode is adopted in European DSRC Standard (ENV 12253). Both active mode and passive mode have clear advantages. The Korean ETC pilot program adopted the passive communications mode for its initial testing, however, active mode is being tested for evaluation purposes.

D. ETC System Configuration

When a car with a Hi-Pass card installed in the OBE passes through the tollbooth with the Hi-Pass system, the antenna on gantry 1 recognizes the OBE and classifies the vehicles. Then it automatically collects the fee from the Hi-Pass card. When the vehicle passes gantry 2, it confirms whether the fee has been paid and indicates the remaining amount on the left of the screen for the driver to view.

E. Major ETC System Components

ETC systems using active DSRC require several different kinds of equipment both in vehicles and along the roadside.

Smart card (Hi-Pass card), and OBE are necessary for vehicles. The smart card has a few microsecond transactions time and includes log file for transaction record, time, serial number, tollgate ID, and so forth. It has its own Chip Operation System for Hi-Pass system, and is compatible to ISO (International Standardization Organization) 7816 and ISO 14423-2. To ensure security, several technologies are embedded by way of a non-readable, non-erasable memory, intrusion detector, and so on.

The OBE has a major role for the Hi-Pass system to guarantee a perfect tolling transaction. It encompasses read/write smart card, LCD (Liquid Crystal Display), buzzer, radio communications interface and others, which are integrated in an ASIC (Application Specific Integrated Circuit). Especially, to provide high security, a built-in SAM (Secure Access Module) chip is also integrated. From a functional point of view, OBE memorizes transaction record, time, serial number, and tollgate ID, just like the smart card. And instead of a consumable battery, it uses a vehicle battery which minimizes environmental impacts. OBE as a communications apparatus has 1Mbps transmission speed in uplink and downlink as well, in which pre-amble data and other synchronization data are not necessary to be optimized to a high speed moving vehicle.

There are also several roadside equipments such as Lane Control System (LCS), Vehicle Classification System (VCS), Vehicle Enforcement System (VES), Driver Feedback Sign (DFS), and Central Computer System (CCS). The Lane Control System (LCS) is installed at the headquarters of the lane equipment division, which controls radio communications links, vehicle classification, and vehicle enforcement. It has its own database containing a toll table, transaction results, critical black list and so forth. This system can manage the Hi-Pass system by itself when the communications link with a central computer is out of order. For this, useful data can be downloaded through the communications link. Major components of this LCS are contained in a weatherproof cabinet so that it can be installed in an island of tollgates.

Tolls are different according to vehicle classes and there will be lots of alternative and problematic situations to correctly identify the vehicles such as to-and-from, bumper-to-bumper, etc. Therefore, accurate vehicle classification and separation techniques will be quite necessary. Currently, a contact type Vehicle Classification System (VCS) consists of an infrared sensor and treadle, in which each vehicle is separated and classified using tire width. In case of other applications for bridges and high-level roads, non-contact type Vehicle Detection System (VDS) using a laser sensor can be introduced; however, the accuracy rate compared with contact type VDS could be worse.

The Vehicle Enforcement System (VES) can take a picture in case of illegal driving, no balance in smart card, no OBE and so forth, in which only a rear side license plate will be stored to avoid a driver's uneasiness. To be sent to the central computer, the picture is compressed. Central computer system consists of several servers for tolling transaction, vehicle

enforcement, and security management for smart card issuing. It manages various management tables such as a basic table, toll tables, and database. Especially, it manages the Hi-Pass system throughout the day using real-time monitoring function for the lane equipments because the system is an unmanned operating system. And there is a strongbox to safely keep the master key value for smart card issuing and tolling transaction. All keys for smart cards, OBE, and issuing smart cards derive from this master key value.

F. Effects of ETC using DSRC

The following benefits are expected from the Hi-Pass system versus a mechanical collection system.

- Efficiency: Automation and managerial efficiency due to electronic systems and enhanced handling of congestion at tollgates.
- TCS lane: 7-9 sec/hr/lane (400-500 vehicles/hr), Daily max. 12,000 vehicles/lane.
- ETC lane: 2.5-3 sec/hr/lane (1,200-1,500 vehicle/hr), Daily max. 36,000 vehicles/lane.
- Environment: Prevents pollution due to traffic. In addition, extends the life of the road.
- Social aspect: Less stress for drivers, higher compliance with the law.

G. Development of ETC using DSRC

In the meantime, Korea Telecom (KT) and the Electronics and Telecommunications Research Institute (ETRI) developed active DSRC standardization and tested it for CBIS in 1999. The ETRI and private companies developed RSE/ OBE test protocols for CBIS and ETC, which use directional antenna. However, KT developed RSE/ OBE test protocols for CBIS and ETC, which use Omni-directional antenna and have a 70m-radius communications range.

As the frequency band of active DSRC was settled at 5.835~5.855GHz, it is expected that various information providing services such as e-mail or wireless Internet services within coverage as parking lots, rest area as well as ATIS (Advanced Traveler Information System), CBIS (City Bus Information System), CVO (Commercial Vehicle Operations) and others will be available in the near future in Korea.

IV. ECONOMIC EVALUATION OF DSRC

A. The Cost-Benefit Analysis for ETC System

Overview: The Korea Highway Cooperation has conducted comprehensive economic analysis for Electronic Toll Collection (ETC) using Dedicated Short Range Communications (DSRC) techniques in order to encourage nation-wide application of ETC systems. The main body of these results of the cost-benefit analysis is based on the recent study done by the Korea Research Institute for Human Settlement (2000). The cost elements consist of construction costs, design and implementation costs for systems, operations costs, and maintenance costs. The social benefits include reduced costs for manpower, manual toll collection system, maintenance costs for its directly related costs. The indirect benefits are travel timesaving, vehicle operating costs, and environmental cost reductions such as pollution reduction impacts.

Economic evaluation time periods are assumed for 7.5 years considering the normal ETC systems economic life and 8 percent discount rates are applied for analysis. The base scenario, the year 2006, is the first full year in which ETC will be fully implemented nation-wide on Korea's highways. Usage rates for ETC systems are assumed to be 10% in year 2003, 20% in year 2004 and 30% in year 2006.

TABLE 3
ETC IMPLEMENTATION SCENARIOS

Operation System	Implementation Stages	Year	Regions	No.
Open System	Full	2002	Seoul metropolitan area	O1
		2003	Seoul metropolitan area	O2
		2004	Seoul metropolitan area	O3
Closed System	Full	2003	Nation-wide	C1
		2004	Nation-wide	C2
		2006	Nation-wide	C3
Integrated Scenarios		Short-term : O1 + C1 Mid-term : O2 + C2 Long-term : O3 + C3		

Costs: Facility investment costs for ETC systems are consist of the vehicle-related costs, road-related costs, tollgates, and main office equipment costs. Maintenance costs include system operation costs and labor costs. Also, the safety-related costs include ETC information facilities, crash absorbing facilities, and road marking costs. As far as users

are concerned, the main cost is OBE costs. Other social costs such as traffic accident costs are ignored in this analysis, because no accident was reported during the Hi-Pass pilot program.

Benefits: The major benefit components of ETC system are labor saving costs, savings from the existing semi-manual toll collection systems and savings for operational costs. The

social benefits are including user timesaving benefits, commercial vehicle operation benefits and environment-related benefits.

Economic Evaluation by Scenarios: In order to simulate the expected cost-benefit analysis for ETC system, we

formulated different assumptions for usage rates for ETC systems as well as time periods, such as short, middle, and long-term use.

TABLE 4
SUMMARY OF THE COST-BENEFIT ANALYSIS FOR ETC SYSTEM ((UNIT: THOUSAND \$))

Usage Rates		10%		20%		30%	
		B/C	NPV	B/C	NPV	B/C	NPV
ETC Operator Aspects	Short-term	1.02	1,157	1.99	26,008	2.92	48,937
	Mid-term	1.02	843	1.91	21,675	2.81	42,713
	Long-term	0.94	-3,094	1.78	14,288	2.63	31,868
Social Aspects	Short-term	2.01	53,481	6.19	236,244	8.52	329,379
	Mid-term	1.92	46,238	5.74	214,900	7.90	299,619
	Long-term	1.65	33,042	4.98	177,448	6.86	247,687
Total	Short-term	3.34	117,181	8.19	336,286	11.44	476,035
	Mid-term	3.17	109,451	7.65	311,571	10.71	441,597
	Long-term	2.79	91,497	4.76	268,357	9.48	381,604

Not surprisingly, the best scenario for ETC systems lies in the high usage rate and short-term scenario, which resulted in 2.9 and 8.5 B/C ratios for operator and social aspects respectively. And these results are translated for \$48.9 million and \$299.6 million net present value.

Also, the usage rate assumption for an ETC system is the critical factor for the success of the nation-wide implementation of the system. For example, every 10% ETC usage rate increase translates to approximately \$17-25 million, net benefit increase in the net present value. Approximately 60-70% of the total net benefits of ETC systems came from the social benefit factors, such as user time savings and pollution reduction costs.

B. User Satisfaction Analysis for the CBIS

Overview: The BuCheon City in Korea operates the City Bus Information System (CBIS), since December 2000 for the 22 intra-city routes. The main operational impact of the BuCheon CBIS is the reliability enhancement of bus arrival time and the results of the user satisfaction survey for the general CBIS.

Costs: The major costs of the CBIS for the BuCheon City consist of the facilities costs for 335 buses and 572 bus stops. The communications costs include about 184 communications modules, 390 location modules and 150 information modules for the bus stops. Total installation costs for the CBIS are estimated about at \$1.25 million and \$27.5 thousand for the annual communications costs.

Benefits: The main benefit components for the CBIS are summarized in table 6. Also, it is reported that revenue of bus companies increased about 1.88% after CBIS operation.

Economic Evaluation: In fact, cost-benefit analysis of CBIS in BuCheon City didn't carry in detail, because bus has been operated by 12 private companies: 3 companies for City bus (general bus), 9 companies for 'MaEul' bus (shuttle bus). The shuttle bus runs with a short-distance service course in the residential area that doesn't have a convenient transportation including a subway or a bus. Usually these buses are smaller and cheaper than the normal buses. From this complicated problems, BuCheon City had some difficulties to analyze the effect of CBIS.

Thus, we tried cost-benefit analysis just considering only increased revenue of bus companies for benefit that surveyed two times by BuCheon City after CBIS operation. Benefit, increased revenue of Bus Company, is calculated at approximately \$5 per bus per day. Economic evaluation time periods are assumed for 5-10 years and 4-8 percent discount rates are applied for sensitivity analysis. Sensitivity analysis for evaluation time periods are summarized in table 5.

TABLE 5
SENSITIVITY ANALYSIS FOR ECONOMIC EVALUATION TIME

Economic Evaluation Time (Year)	B/C RATIO	NPV (Million \$)
5	1.91	1.26
6	2.20	1.69
7	2.48	2.11
8	2.73	2.50
9	2.97	2.88
10	3.19	3.24

And sensitivity analyses for discount rates are summarized in table 6.

TABLE 6
SENSITIVITY ANALYSIS FOR DISCOUNT RATES

Discount Rate (%)	B/C RATIO	NPV (Million \$)
8	2.82	2.65
7	2.94	2.83
6	3.06	3.03
5	3.19	3.24
4	3.32	3.47

Satisfaction Analysis: The user satisfaction survey done by the BuCheon City found that over 50% of bus users rated the CBIS as very reliable and satisfactory. In terms of service improvement, over 67% rated the CBIS as very effective for the bus service improvements.

Based on the preliminary user satisfaction survey for the CBIS of the BuCheon City, it is estimated that the perceived time savings for the CBIS benefit can be calculated at about \$141 million per year. In conclusion, public complaints for the unreliable bus time schedule decreased from 75% to 25% after the CBIS implementation. Also, the bus users are expected to increase about 20%, after the CBIS implementation.

V. SUMMARY

This paper dealt with active Dedicated Short Range Communications (DSRC) application for Intelligent Transport Systems (ITS) and its economic evaluation focused on the City Bus Information System (CBIS) and Electronic Toll Collection (ETC) system, both prominent ITS deployment projects in Korea. Korean government and ITS related organizations tried to standardize ITS communications protocol, frequency band and so on by a trial and error approach. From these experiences and evaluation results, the Korean Ministry of Information and Communication, ITS related research institutes, and the private sector plan to develop the next generation of DSRC equipment that will enable not only wireless Internet but also multimedia services with 10Mbps speed to function by early 2003.

REFERENCES

- [1] Bo-Jeong Kim: An Analysis of the Benefit Bus Information System, Thesis for a Master Degree, Graduate School of Economics, Yonsei University (2002) 22-43
- [2] Deog-Mo Bae: An Analysis on the Efficiency of Bus Information Systems in BuCheon City, Journal of Transportation Research Society of Korea, (2002) 7-18
- [3] Deog-Mo Bae, et al.: An Analysis on the Efficiency of Bus Information Systems, 5th Asia-Pacific ITS Forum Proceedings CD-ROM, Korea (2002)
- [4] Doo-Hee Nam: Intelligent Transportation Systems Model Development Initiatives in Korea, 5th Asia-Pacific ITS Forum Proceedings CD-ROM, Korea (2002)
- [5] Doo-Hee Nam: Dedicated Short Range Communications (DSRC) for Advanced Traveler Information System (ATIS), 9th ITS World Congress Proceedings CD-ROM, (2002)
- [6] Electronics and Telecommunication Research Institute: ETRI: The Status and Prospect of Telecommunications Technology for ITS, Korea (1999)
- [7] Hyun-Mee Choi : Advanced DSRC System Technology, ITS Workshop & Exhibition Proceedings (2000) 129-140
- [8] Jan Kersten: Integrated Chipcards-the future of Payment in DSRC-based EFC-system, 8th ITS World Congress Proceedings CD-ROM, Australia (2001)
- [9] Jan Kersten: Smart Cards in DSRC-based EFC-system, 9th ITS World Congress Proceedings CD-ROM, USA (2002)
- [10] Jeong-Ho Kim, et al: A Study on the ITS-BIS Service and Traffic management using DSRC Protocol, 8th ITS World Congress Proceedings CD-ROM, Australia (2001)
- [11] Ji-Hun Yi, et al: Active DSRC ETC System using Smart Card, 5th Asia-Pacific ITS Forum Proceedings CD-ROM, Korea (2002)
- [12] Korean Ministry of Construction and Transportation: ITS Master Plans 21, Korea (2000)
- [13] Knut Evensen: DSRC-status of a Mature Technology, 9th ITS World Congress Proceedings CD-ROM (2002)
- [14] National Computerization Agency of Korea: A Study on Communications Protocol and Network of ITS (1998)
- [15] Ruimin Li, Quxin Shi: The Application of Dedicated Short Range Communications System in ITS, 5th Asia-Pacific ITS Forum Proceedings CD-ROM (2002)
- [16] Sang-Keon Lee, et al: Performance Analysis for Electronic Toll Collection System, Hi-Pass, Journal of Transportation Research Society of Korea, Vol.19 (2001) 59-69
- [17] Sang-Keon Lee, Yong-Seong Cho: Economic Analysis for Electronic Toll Collection System, Hi-Pass, The Korea Institute of ITS Annual Meeting Proceedings (2002) 108-111
- [18] TTA (Telecommunication Technology Association): Standard of DSRC Radio Communications between Roadside Equipment and On-board Equipment in 5.8GHz Band, TTAS. KO-06.0025 (2001)
- [19] Wan-Chol Ho: ETC Implementation in Korea using HDR (High-speed Data Rate) Radio Communications and Smart Cards, 5th Asia-Pacific ITS Forum Proceedings CD-ROM (2002)
- [20] Wern Yarg Shieh: Some Application of DSRC for ITS in Taiwan, 5th Asia-Pacific ITS (2002)

Adaptive Control of Milling Forces under Fractional Order Holds.

L. Rubio \otimes^* and M. de la Sen \otimes

\otimes Instituto de Investigación y Desarrollo de Procesos, Facultad de Ciencia y Tecnología
Universidad del País Vasco, Apartado 664, 48080-Bilbao (Spain)
 $*$ webrurol@lg.ehu.es

Abstract— This paper introduces a novel discrete-time model reference based control of the tool-work-piece interaction force in a milling process. The novelty of the scheme relies on the use of a fractional order hold (FROH) instead of a traditional zero order hold (ZOH) used in the manufacturing literature to obtain a discrete-time model of the continuous system. The additional degree of freedom introduced by the FROH through its correcting gain allows the designer to improve the closed-loop behavior of the time-varying unknown system by an adequate choice of its value. Simulation examples showing the influence of the correcting gain in the closed-loop response are presented and compared.

I. INTRODUCTION

Milling is a cutting process widely used in the manufacturing of mechanical components. It consists of the relative movement between feeding a work-piece clamped on a table and rotating multi-tooth cutter. In order to avoid machine malfunctions such as tool wear or breakage and to achieve a certain degree of quality in the finishing of the working-piece, the peak cutting force on the working piece has to be maintained below a prescribed safety upper-bound. This fact implies that a control strategy has to be implemented on the system in order to fulfill such safety and performance requirements. Moreover, cutting parameters may be unknown or time-varying as a consequence of a complex milling geometry. Thus, the control law should be able to attain the desired objectives even in the presence of uncertainties or variations in the system parameters. In this way, the nature of the system suggests to use an adaptive controller to address the milling force control problem.

In this work, it is presented the design of an adaptive control law for milling processes which improves the behavior, specially the quality of the finishing of the working piece through a more precise tool-work-piece interaction force control, in comparison with previous approaches.

The key point to achieve such an improved behavior of the system is the use of fractional order holds (FROH) to obtain a discrete-time model of the system. The advantage of using a FROH instead of a traditional ZOH is that

FROHs incorporate an additional degree of freedom, the gain of the FROH, which can be used to modify the overall closed-loop response of the system, improving, for instance, the stability of the discrete zeros or reducing the overshoot or bad transient responses which could lead, for example, to break the cutter shank, tool breakage or tool wear, [1, 2]. Hence, the model reference control is the designed from the so obtained FROH based discrete model.

The use of this kind of more complex hold devices is supported by the actual tendency in manufacturing environments consisting in optimizing the selection of machining parameters, through optimization algorithms, and in controlling the machining process on-line in contrast with the traditional CNC based systems, where the machining constant parameters are usually selected according to handbooks or operators' experience leading to an 'ad-hoc' tuning of the control system.

Thus, the influence of the FROH gain in the system's behavior is studied showing that an adequate tuning of it can lead to an improved closed-loop performance. The study is carried out by means of a cost function which compares the system transient responses when different gains of the FROH are used.

Previous works can be found in references [3-9]. In those papers, linear and time varying parameters models are widely used. Those models are cutting parameters dependent. Then, they will be time varying when complex parts are going to be milled. For this reason, the adaptive control techniques are mainly employed to control the milling process. A successful application of the adaptive control to milling process has potential machining-time savings, among other advantages.

II. SYSTEM DESCRIPTION

A. Continuous Model

The milling system can be modeled as the series decomposition of a Computerized Numerical Control (CNC), which includes all the circuitry involving in the table movement (amplifiers, motor drives), and the tool-work-piece interaction model itself. A feed rate command f_c (which plays the role of the control signal) is sent to the CNC unit. This feed rate represents the desired velocity for the table movement. Then, the CNC unit manages to make

the table move at an actual feed velocity of f_a according to the CNC dynamics. Even though the machine tool drive servos are typically modeled as high order transfer functions, they can usually be approximated as a second order transfer function within the range of working frequencies. Besides, they are tuned to be over-damped without overshoot, so that they can be modeled as the first order system [5]:

$$G_s(s) = \frac{f_a(s)}{f_c(s)} = \frac{1}{\tau_s s + 1} \quad (1)$$

where f_a and f_c are the actual and command velocity values of the table in (mm/s) respectively and τ_s is an average time constant, which depends on the type of the machine tool. In this study, it is assumed to be 0.1 ms.

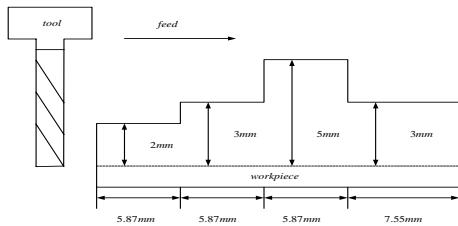


Figure 1: Work-piece profile to test control algorithms.

In addition, the chatter vibration and resonant free cutting process can be approximated as the first order system [5]:

$$G_p(s) = \frac{F_p(s)}{f_a(s)} = \frac{K_c b a(\phi_{st}, \phi_{ex}, N)}{N \cdot n} \frac{1}{\tau_c s + 1} \quad (2)$$

where K_c (N/mm^2) is the cutting pressure constant, b (mm) is the axial depth of cut, $a(\phi_{st}, \phi_{ex}, N)$ is an adimensional immersion function, ranging between 0 and $\sim N$ depending on the immersion angle and the number of teeth in cut, N is the number of teeth on the milling cutter and $n(\text{rev/s})$ is the spindle speed. The axial deep of cut function b in (2) may be time-varying leading to a potential time-varying system. In particular, the cutting process is assumed to be in this work piecewise constant, admitting sudden changes in the cutting parameters at certain time instants while remaining invariant between changes. This assumption allows us to consider the cutting process to be described by the transfer function (2) with the time interval between changes.

The combined transfer function of the system, obtained from (1) and (2) is

$$\begin{aligned} G_C(s) &= \frac{F_p(s)}{f_c(s)} = \frac{B_C(s)}{A_C(s)} = \frac{1}{(\tau_m s + 1) N n (\tau_c s + 1)} = \\ &= \frac{K_p}{(\tau_m s + 1)(\tau_c s + 1)} \end{aligned} \quad (3)$$

where the process gain is K_p ($\text{N} \cdot \text{s}/\text{mm}$) = $K_c ab/Nn$.

Figure 1 shows the sample work-piece depicting basic cutting geometry features with changes in the axial depth of

cut used in the simulations. The spindle speed remains constant, 715 rpm; the work-piece is made of Aluminum 6067 whose specific cutting pressure is assumed to be $K_c = 1200 \text{ N/mm}^2$. A 4-fluted carbide mill tool, full-immersed and roughing milling operation will be taken into consideration in the present paper.

Also, note that the desired final geometry of the piece to be milled involves changes in the axial deep of cut which implies suddenly changes in its value, according to the sudden changes assumption presented before. On the other hand, it has been taken into account that the control law computes new feed-rate command value at each sampling interval. Furthermore, it is worth to be mentioned that the CNC unit has its own digital position law executed at small time intervals in comparison with the sampled time of the control law, even though if high speed milling tool drives are used [5].

B. Discrete model under β -FROH

In this paper, the problem of controlling a continuous plant is addressed by using a discrete controller. The discrete controller is obtained applying a model-reference pole-placement based control design to a discrete model of the plant (3) obtained by means of a FROH with a certain correcting gain β . The additional "degree of freedom" β provided by the FROH can be used with a broad variety of objectives such as to improve the transient response behavior, to avoid the existence of oscillations in the continuous time output of the system or to improve the stability properties of the zeros of the discretized system. Hence, the discretization of (3) under a FROH is calculated as:

$$H_\beta(z) = Z[h_\beta(s) \cdot G_C(s)] \quad (4)$$

where $h_\beta(s) = \left(1 - \beta e^{-sT} + \frac{\beta(1 - e^{-sT})}{Ts} \right) \frac{1 - e^{-sT}}{s}$ is the transfer

function of a β -FROH, where z is the argument of the Z -transform, being formally equivalent to the one step ahead operators, q , used in the time domain representation of difference equations. This allows us to keep a simple unambiguous notation for the whole paper content. The sampling time T has been chosen to be the spindle speed, n , as it is usual for this kind of systems [3-5]. Note that when $\beta = 1$, the FROH hold becomes a first order hold (FOH) and when $\beta = 0$, the zero order hold (ZOH) is obtained, being both particular cases of $\beta \in [-1, 1]$. Furthermore, $H_\beta(z)$ may be calculated using just ZOH devices in the following way:

$$H_\beta(z) = \frac{B_\beta(z)}{z} = \frac{z - \beta}{z} Z[h_o(s)G_c(s)] + \frac{\beta(z-1)}{Tz} Z\left[h_o(s)\frac{G_c(s)}{s}\right] =$$

$$= \frac{B_\beta(z)}{z \delta_\beta \cdot A(z)} = \frac{B_\beta(z)}{z \delta_\beta \cdot \left(z - e^{-T/\tau_m} \right) \cdot \left(z - e^{-T/\tau_c} \right)} = \frac{B_\beta(z)}{z \delta_\beta \cdot (z^2 + a_1 z + a_2)} \quad (5),$$

where $h_o(s) = \frac{1 - e^{-sT}}{s}$ is the transfer function of a ZOH and $\delta_\beta = 1$ if $\beta \neq 0$ and $\delta_\beta = 0$ if $\beta = 0$, which means that a fractional order hold with $\beta \neq 0$ adds a pole at the origin.

$$B_\beta(z) = b_0 z^2 + b_1 z + b_2, \text{ where}$$

$$b_0 = \frac{\tau_m(1 - e^{-T/\tau_m}) - \tau_c(1 - e^{-T/\tau_c})}{\tau_m - \tau_c} + \beta + \frac{\beta}{T} \frac{\tau_c^2(1 - e^{-T/\tau_c}) - \tau_m^2(1 - e^{-T/\tau_m})}{\tau_m - \tau_c}$$

$$b_1 = \frac{\tau_m(1 - e^{-T/\tau_m}) - \tau_c(1 - e^{-T/\tau_c})}{\tau_m - \tau_c} + \beta \frac{\tau_c(1 + e^{-T/\tau_m}) - \tau_m(1 + e^{-T/\tau_c})}{\tau_m - \tau_c} + \\ + \frac{\beta}{T} \left\{ \frac{\tau_m^2(1 + e^{-T/\tau_c}) - e^{-T/\tau_m} - e^{-T/\tau_c} e^{-T/\tau_m}}{\tau_m - \tau_c} \right\} + \\ + \frac{\beta}{T} \left\{ \frac{\tau_c^2(1 + e^{-T/\tau_c}) - e^{-T/\tau_m} - e^{-T/\tau_m} + e^{-T/\tau_c} e^{-T/\tau_m}}{\tau_m - \tau_c} \right\}$$

$$b_2 = \frac{\beta}{\tau_m - \tau_c} \left\{ \tau_c e^{-T/\tau_m} \left(\frac{\tau_c}{T} (1 - e^{-T/\tau_c}) - 1 \right) - \tau_m e^{-T/\tau_c} \left(\frac{\tau_m}{T} (1 - e^{-T/\tau_m}) - 1 \right) \right\}$$

C. Desired response: model reference

A second order system $G_m(s) = \frac{\omega_n^2}{s^2 + 2\xi\omega_n s + \omega_n^2}$ (6) is selected to represent the system model reference. This system is characterized by a desired damping ratio, ξ and a natural frequency, ω_n . It is known that small ξ leads to a large overshoot and a large setting time. A general accepted range value for ξ to attain satisfactory performance is between 0.5 and 1, which corresponds to the so-called under-damped systems. In this way, a damping ratio of $\xi = 0.75$ and a rise time, T_r , equal to four spindle periods is usually selected for practical applications. Furthermore, the natural frequency is then usually suggested to be $\omega_n = 2.5/T_r$ rad/s. This continuous-time reference model is then discretized with the same FROH as the real system was in order to obtain the corresponding discrete-time reference model for the controller. Thus, a number of different discrete models obtained from a unique continuous reference model are considered depending on the value of β used to obtain the discretization.

III. ADAPTIVE MODEL FOLLOWING CONTROLLER

The figure depicts a schematic representation of the

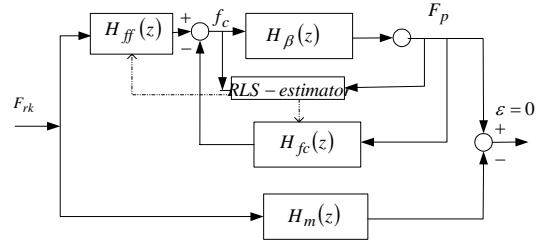


Figure 2: Adaptive model following control scheme.
model reference adaptive control algorithm:

where $H_{ff}(z, k) = \frac{S(z, k)}{R(z, k)}$ is the feed-forward filter from the reference signal, $H_{fb}(z, k) = \frac{T(z, k)}{R(z, k)}$ is the feedback controller, $H(z, k)$ is the discrete plant, $H_m(z, k)$ is the model reference and F_{rk} is the reference force.

The adaptive control algorithm is obtained by adding a RLS estimation algorithm,

$$\hat{\theta}(k) = \hat{\theta}(k-1) + L(k) [F_p(k) - \phi^T(k) \hat{\theta}(k-1)]$$

$$L(k) = P(k-1) \phi(k) \left(\lambda + \phi^T(k) P(k-1) \phi(k) \right)^{-1} \quad (7)$$

$$P(k) = \left(I - L(k) \phi^T(k) \right) P(k-1) \frac{1}{\lambda}$$

simultaneously running in parallel with the control law at each sampling instant, k . $\hat{\theta}^T = \begin{pmatrix} \hat{a}_1 & \hat{a}_2 & \hat{b}_0 & \hat{b}_1 & \hat{b}_2 \end{pmatrix}$ is the

parameter vector and $\hat{\phi}(k)$ is the regressor vector.

The transfer function of the reference model is,

$$H_m(z) = \frac{B^-(z) B'_m(z) A_o(z)}{A_m(z) A_o(z)} = \frac{B_m(z) A_o(z)}{A_m(z) A_o(z)} \quad (8)$$

where $B'_m(z)$ contains the free-design reference model zeros, $B^-(z)$ is formed by the unstable (assumed known) plant zeros and $A_o(z)$ is a polynomial including the eventual closed-loop stable pole-zero cancellations which are introduced when necessary to guarantee that the relative degree of the reference model is non less than that of the closed-loop system so that the synthesized controller is causal. A basic control scheme is displayed in figure 2. Then, it will be considered the polynomials R_k, S_k and T (T depends only on the reference model zeros polynomial

which is of constant coefficients) where $T = B_m A_o$ and R_k (monic), S_k are unique solutions with degrees fulfilling

$$\deg(R_k) = 2n - i, \deg(S_k) = i - 1, \deg(A_m A_o) = 2n$$

of the polynomial Diophantine equation

$$\begin{array}{c} \wedge \quad \wedge \quad \wedge \\ A_k R_k + B_k S_k = B_k^+ A_m A_o \Leftrightarrow \\ \wedge \\ A_k R_{1,k} + B^- S_k = A_m A_o \end{array} \quad (9)$$

$$\text{with } R_k = B_k^+ R_{1,k}.$$

From (8)-(9), perfect matching is achieved through the control signal:

$$f_{c,k} = \frac{\hat{T}(z)}{\hat{R}(z)} F_{r,k} - \frac{\hat{S}(z)}{\hat{R}(z)} F_{p,k} \quad (10)$$

Note that the zeros of the machine tool plant are always stable and within the unit circle. But since the RLS estimator does not predict accurately the parameters of the numerator of the plant, separate control system design are needed for cases when the zeros are stable or unstable.

An additional unstable zero can be introduced by the process discretization. In this paper, only stable discretization zero cases are taken into account.

IV. EXPERIMENTAL RESULTS

There is an extensive literature which carefully explains the algorithms here developed, for example [10, 11], and show the robustness of the adaptive law [12]. The novelty of the control relies on the use of fractional order holds instead of the usual ZOH appearing in the manufacturing literature. In this paper, the correcting gain of β -FROH is handled to show that the system transient response can be enhanced respect to the use of ZOH. This can lead to avoid overloading of the insert, because the maximum removed chip-thickness would not increase the principal tensile stress in the cutting wedge beyond the ultimate tensile strength of the tool material, this can also lead to prevent fracture of the shank, and fulfill the machine tool requirements, such as power and torque availability [6]. Moreover, if the reference force is selected near the tool breakage limit, the large overshoot lead to tool breakage [1, 2, 6]. Then, if the overshoot of the system response is reduced, the reference force can be increased, improving the time production requirements.

An adaptive model following controllers have been developed using different correcting gains of the fractional order hold. The milling system and the model reference are discretized via fractional order hold. The estimation vector has been initialized as the corresponding discretization from estimated continuous transfer function,

$$G(s) = \frac{-3s + 150}{s^2 + 20s + 550} \quad (11)$$

As example, the some representative cases are plotted in figures 3 and 4. The figures present the resultant force keeping at the reference force, which is set to a constant value of 1.2KN. The system registers large overshoots in the transient responses, depending on the β -value and the initial values of the parameter vector.

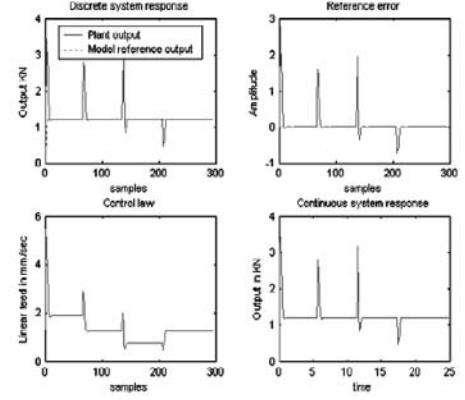


Figure 3: Relevant signals corresponding to $\beta = 0$.

The initial parameter vector has the ability that if it is near to the real values of the plant, the transient response of the system will be smooth and feasible. In contrast, if the initial value of the parameter vector has been selected in arbitrary manner the transient is normally oscillated with a great maximum overshoot and large setting time. In any case, fractional order holds can help to reduce large overshoots.

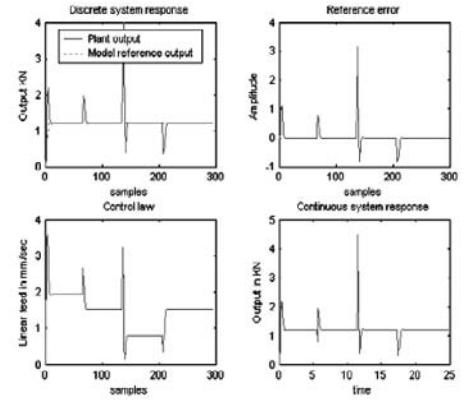


Figure 4: Relevant signals corresponding to $\beta = -0.4$.

On the other hand, there are abruptly overshoots in the output when the axial depth of cut changes suddenly. It is due to the intrinsic structure of the closed-loop output. It is not the main purpose of this paper reducing or avoiding these jumps. But, in that case, some 'a priori' information

about the work-piece geometry is required to design a successful control, as in [6], where a CAD model of the work-piece is used to modify the control command when the axial depth of cut changes in order to minimize the overshoots due to abrupt changes in the transfer function.

V. TRANSIENT RESPONSES CHARACTERIZATION

In order to compare time domain transient behaviors when the designed control scheme respect to the use of traditional ZOHs, a cost function is defined:

$$J_c = \sum_{j=1}^k \int_{(j-1)T}^{jT} |F_p(\tau) - F_{p,m}(\tau)| d\tau \quad (12)$$

where F_p is the output signal and $F_{p,m}$ is the model reference output signal, k is the number of periods which have been taken into account in the transient response characterization.

The cost function calculates a good approximation of the area between the continuous system output and the continuous model reference system response. The smaller this area is, the smaller cost function will be. It leads to choose an adequate value of β which achieves the best output transient response behavior.

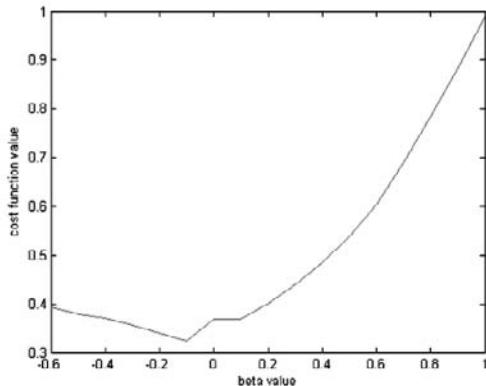


Fig5: Cost function value versus β values of the discrete controllers.

Figure 9 shows the cost function value when β value of the discrete controllers varies. In the figure it can be appreciated that, the use of β -value near to -0.2 leads to minimum values of the cost function. It concludes that better system transient responses will be achieved if the adaptive control algorithm is designed utilizing a FROH respect to the usual ZOH using in the manufacturing literature.

The cases when $\beta < -0.6$ have not been taken into consideration because the plant is non-minimum phase. In those cases, ‘a priori’ knowledge about the system zero is needed to implement a successful control. Information about this case can be found in [11, 12].

VI. CONCLUSION

In this paper an adaptive model following force control scheme has been proposed to deal with unknown time-varying milling systems. The novelty of the control scheme relies on the use of FROH instead of the usual ZOH appearing in the manufacturing literature. The FROH provides an “extra degree of freedom”, which can be manipulated by the programmer to obtain a better transient response as the simulations have pointed out being then confirmed by the proposed cost functional. There is not a rule of thumb to select the adequate β value, only operators’ experience can help to select a satisfying value of β , for a range of working cutting parameters.

On the other hand, the general FROH hold can be implemented by means of ZOH holds, which make this approach fairly feasible to be implemented in the manufacturing industry. Then, an easily implemented device can lead to save machining time in the production, avoid some process malfunctions or damage the tool less than if just a ZOH device is used.

ACKNOWLEDGMENT

The Authors are very grateful to MCYT by its partial support through grant DPI2006-00714/ and to the UPV/EHU through Project 9/UPV00I06.I06-15263/2003.

REFERENCES

- [1] Altintas, I. Yellowley and J. Tlusty, “The Detection of Tool Breakage in Milling Operations”, Journal of Engineering for Industry, November 1988, Vol. 110.
- [2] Y. Altintas, “Prediction of Cutting Forces and Tool Breakage in Milling from feed drive current measurements”, Journal of Engineering for Industry, pp.386-392, November 1992, Vol. 114.
- [3] L.K. Lauderbaugh and A.G. Ulsoy, “Dynamic Modeling for Control of the Milling Process”, Journal of Engineering for Industry, November 1988, Vol. 110.
- [4] L.K. Lauderbaugh and A.G. Ulsoy, “Model Reference Adaptive Force Control in Milling”, Journal of Engineering for Industry, February 1988, Vol. 111.
- [5] Y. Altintas, “Manufacturing Automation”, Cambridge University Press, 2000
- [6] A.Spence and Y. Altintas, “CAD Assisted Adaptive Control for Milling”, Transaction of the ASME, September 1991, Vol. 113.
- [7] Peng, Y.H., “On the performance enhancement of self-tuning adaptive control for time-varying machining processes”, International Journal of Advanced Manufacturing Technology, pp. 395-403, 2004, 24.
- [8] Y.Altintas, F. Sassani and F. Ordubadi, “Design and Analysis of Adaptive Controllers for Miling Process”, Transaction of the CSME, pp.17-25, no.1/2, 1990, Vol. 14.
- [9] Y.Altintas and C.C.H. Ma, “Direct Adaptive Control of Milling Force”, IEEE International Workshop on Intelligent Motion Control, Istanbul 20-22 August 1990.
- [10] K.J. Astrom and B. Wittermark, “Adaptive Control”, 2nd edition, Addison-Wesley, 1995.
- [11] Ioannou, P. and Sun, J., “Robust Adaptive Control”, Prentice Hall 1996.
- [12] S.S. Sastry and M. Bodson, “Adaptive Control: Stability, Robustness and Convergence”. Prentice 1989.

Application of Genetic Algorithms to a Manufacturing Industry Scheduling Multi-Agent System

María de los Ángeles Solari

Facultad de Ingeniería y Tecnologías, UCUDAL
2738, 8 de Octubre Avenue
Montevideo, 11600 Uruguay
msolari@ucu.edu.uy

Ernesto Ocampo

Facultad de Ingeniería y Tecnologías, UCUDAL
2738, 8 de Octubre Avenue
Montevideo, 11600 Uruguay
eocampo@ucu.edu.uy

Abstract - This work presents the research about the application of Genetic Algorithms to a scheduling multi-agent system on a textile manufacturing industry.

Manufacturing industries competitiveness greatly depends on their ability to plan and schedule their processes in the most efficient way, as it impacts on production cost and time. Assigning jobs to scarce resources is not an easy to resolve task, mainly in the complex industrial processes context.

This research's objective is to assess the applicability of Genetic Algorithms to a multi-agent production scheduling system aiming to obtain higher performance levels.

Keywords: Genetic Algorithms, Intelligent Agents, Multiagent Systems, Scheduling, Manufacturing Industry.

I. INTRODUCTION

Currently, industries need to adapt to the increasingly competitive situation of their market. This implies a need to optimize their processes so as to gain efficiency and flexibility. In a manufacturing industry, planning is a key factor to take into account, given that it can drastically affect the reduction of production time and cost. In this research, the applicability of Genetic Algorithms technology to a multi-agent scheduling system for textile industrial environments is assessed. Its goal is to apply this technique in order to achieve greater performance than that of the current scheduling system.

II. INDUSTRIAL MANUFACTURING SYSTEMS

A. Key Concepts

The function of a manufacturing industry is the manufacturing of one or more products, in a process that takes raw materials as input and transforms them into the final product [12] [11]. These systems generally use a centralized architecture, in which the central controller performs the scheduling, that is, the assignment of tasks to be carried out by different machines. These are complex systems, highly dependent on a critical point, expensive, and of poor flexibility.

In decentralized architectures, several smaller controllers or agents are defined, each of them capable of performing its own task independently, making use of the locally available information. Each agent has the ability to interact with its peers, establishing communication and negotiating to

collaborate mutually. These systems are more robust and flexible [12].

Many industrial organizations are adopting a more intelligent control strategy, so as to achieve flexibility to adapt to swift changes in the environment. Two approaches of distributed control systems which have in common the concept of agents are: a) *Multi-agent based Manufacturing Control Systems* (in which agents are associated to machines and products so that they make decisions concerning scheduling, resource assignment, priorities, etc.) and b) *Holonic Manufacturing Systems* (they contain entities called *Holons* which comprise a physical part and a software part, and through which information, materials, and resources are interchanged) [1] [12] [17].

B. Context of Application – The Textile Manufacturing Industry

The industrial process of this research is that of a textile industry, which transforms raw material (wool, yarn) into different kinds of fabric and weave, through a series of processes.

The existing system focuses on two main processes: Spinning and Weaving, where the first generates the input for the second. Roughly, the manufacturing is carried out in this manner: a) the raw wool is combed, mixed, and prepared for unification, forming yarn preparation wicks, b) the Spinning process is carried out in an engine room where the spinning machines, called “Spinning-Frames”, are installed, twisting the wicks until the desired yarn width is achieved, c) these yarns feed the Looms (Room of Looms) which create the weaves of final products in the following way: a certain amount of yarns, which are called yarns of warp, are placed parallel to one another at the input of the loom, and are then crossed with other yarns, called weft yarns, according to some design pattern. d) the products are finalized. Storage is used for intermediate products as well as for final products [12].

III. AGENTS AND MULTI-AGENT SYSTEMS

Nowadays, Agent Oriented Programming is spoken of as a methodology able to overcome the limitations of the Object Oriented Programming [1] [2]. “*An intelligent agent is a computer system located in some environment in which it acts*

in an independent and flexible manner so as to achieve its goals [2] [20] [16]. Wooldridge and Jennings define an agent as “*a unit of software designed to perform a particular task ...*” [20]. Agents exhibit several characteristics, like autonomy, reactivity, proactivity, learning ability and mobility. “*A multi-agent system (MAS) is a collection of computational entities (agents), possibly heterogeneous, each of which have the ability to achieve its own goals in an independent manner, and to interact, eventually pursuing a global objective.*” [12] [17].

In a MAS, agents interact mutually, and there can exist dependency relationships among them (e.g. an agent need help from another to achieve one of its goals) [20]. In such case, decisions taken by one agent may affect the decisions taken by other members of the community.

Agents can be more efficient (at an individual and collective level) if they can communicate beliefs and goals [16]. Languages defines message formats and communication protocols (e.g. KQML, FIPA ACL) [19] [20].

An individual agent does not always hold the necessary competence, resources, or information required to fully solve a problem. Thus, it is important that agents are coordinated, that is, that they organize their actions so as to fulfill their local goals without disregarding the global objective [5].

Collaboration allows agents in MAS to combine their abilities, therefore distributing work (tasks, data, and resources) to carry out a common task. It consists of two phases: a) tasks are divided and b) they are assigned among the available resources [19] [20] [2].

The process in which agents exchange information in order to reach agreements regarding subjects of mutual interest is called negotiation. There exists a variety of techniques: Contract-Net, market, etc. [20].

Given that agents are independent entities, they need to know about their behavior (their abilities) as well as about the behavior of their environment (which agents exist, which are their abilities, how they interact). The representation of knowledge: a) must be done at the level of the agent, b) can be very complex, according to the degree of interactions, and c) it depends on the type of the application [16] [17].

Agents must be able to learn from the environment and to adapt their behavior to the changes in it. This can be seen in a MAS applied to industry, which must execute in real time and adapt to changing conditions that arise as the result of unexpected events, such as a failure in a machine or lack of materials [16] [17].

IV. PLANNING AND SCHEDULING

“*Planning is the process of selecting and serialization of activities whose execution produces one or more objects and that complain with the domain restrictions set. Scheduling is the process to select between alternative plans and of assigning time and resources to the plan's activities*” [1].

The problems involved in these processes are of the NP-complete kind, characteristic that causes that exhaustive search methods cannot be applied in order to get a solution.

The common strategy is to apply some heuristics to bound the solutions space. Some of these heuristics are son: Simulated Annealing, Taboo, Hill Climbing, Best-First Search, Dispatch Rules (e.g. EDD- Earliest Due Date) and Genetic Algorithms [3].

V. GENETIC ALGORITHMS

A *Genetic Algorithms (GA)* is a programming technique that simulates biological evolution, and that has demonstrated to be applicable to different fields with success [8] [7]. In 1975 Holland introduces *GA* definition and presents the related theoretical framework [10] [6].

These are flexible algorithms with built-in target task adaptation capacities. They provide a set of solutions for the considered problem. This technology uses a *Population* composed by a set of individuals called *Chromosomes* (coded by bits, letters or numbers strings), representing possible problem's solutions. These ones are also conceptually divided into *Genes* (minimum information unit, which value is called *Allele*) [10] [8] (see Fig. 1).

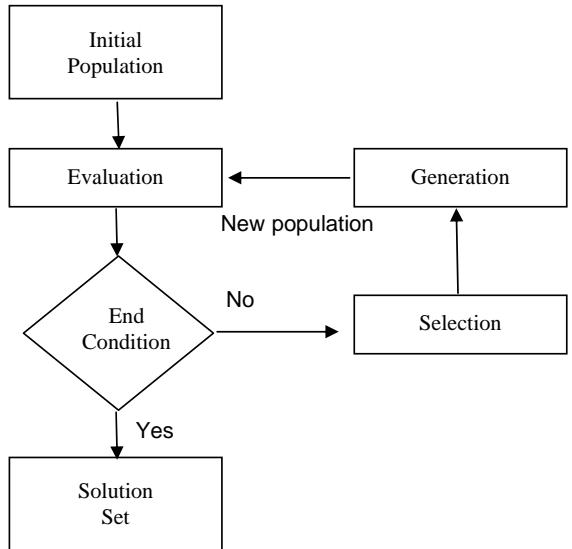


Fig. 1. Genetic Algorithm Process

A GA takes as its input an *initial population*, usually randomly generated, that evolves in an iterative process: a) *Population Assessment* (using a *fitness function* a ranking is applied to each chromosome to indicate how good a problem's solution it is), b) *Finish Control* (process ends after a certain amount of iterations or when a chromosome surpasses certain ranking), c) *Selection* (parents chromosomes are selected for the new population using different methods like *Roulette Wheel*, *Elitism*, *Ranking*, *Tournament*) [18] [10] [6], d) *Generation* (selected chromosomes are reproduced applying genetic operators like *Crossover* – that interchanges parents' chromosomes sections – or *Mutation* – that modifies one gene's allele) [10] [6] [3] [9] [8] [15].

VI. CURRENT SCHEDULING MULTI-AGENT SYSTEM

To develop this research, an existing **MAS** - formerly developed by the research group - has been used. This **MAS** is composed of several different kinds of agents: *Marketing and Selling Agent (SA)*, *Product Agent (PA)*, *Spinning-Frame Agent (SFA)*, *Loom Agent (LA)*, *Yarn Stocks Agent (YSA)* and *Fabric Stock Agent (FSA)*. Here there is a brief outline of their roles and collaborations to successfully schedule and produce the desired products [12] (see Fig. 2).

- **SA:** receives orders from customers, and for each ones it generates a new instance of a Product Agent (**AP**). This instance is killed once the order is either confirmed or cancelled. Selling Agent then removes the related product from Fabric's stock in order to complete the customer's order cycle.

- **PA:** Product Agent decides if it can build the associated product and thus honor the customer's order, negotiating with all the available resources (Spinning-Frames and Looms agents) to get the most suitable cost-benefit relationship. This is accomplished using repeated Contract-Net-like protocols involving all the available Spinning-Frames for each one of the product's composing yarns, and then negotiating with the loom's agents to build the fabric.

- **SFA:** receives calls-for-proposals (**CFP**) from the Product's Agents to quote for producing certain yarn, and reserves time-slots in its internal chronogram until the starting date/time is achieved or else it is cancelled by the related Product Agent. Once the requested yarn has been produced, it sends it to the Yarn Stock, collaborating with the **YSA**.

- **LA:** receives calls-for-proposals (**CFP**) from the Product Agents to build the fabric and reserves time-slots in its internal chronogram until the production starting date/time is achieved or the task is cancelled by the related Product Agent. To build the fabric, it removes the required yarn from the Yarn Stock (collaborating with the **YSA**). When the production finishes, it sends the product – fabric – to the Fabric Stock (collaborating with the **FSA**).

- **YSA:** Receives the yarns that have been produced by the Spinning-Frames, to be later used by the looms. It maintains stocks statistics.

- **FSA:** Receives finished fabrics, from the looms. Sends customer's orders products to **SA**. It maintains stock statistics.

- **Cockpit Agent:** It helps the system's manager to evaluate system's performance and to setup simulation scenarios.

This **MAS** was analyzed and designed using GAIA methodology [21] [13] [12] [4] and AUML software artifacts [14] [4]. It was built using JADE agents development framework [12].

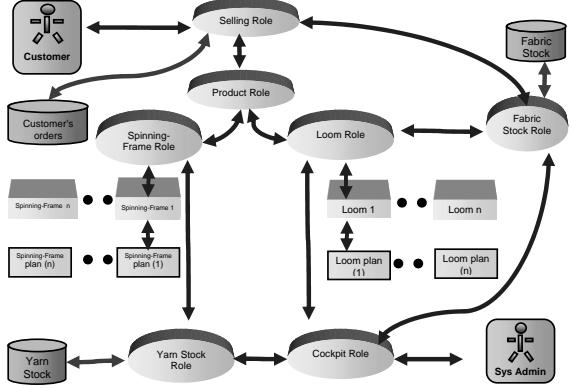


Fig. 2. Manufacturing Scheduling MAS

VII. RESEARCH HYPOTHESIS

“Given a certain Multi-Agent System that allows to plan and program, in a basic level, the activities related to a textile manufacturing industry, it is possible to apply Genetic Algorithms (GA) techniques to attain better performances”.

To prove this statement, the existing multi-agent system has been modified in order to include the GA inside the agents that represent resources (e.g., Spinning-Frames and Looms). This aims to optimize the machines' tasks sequences, minimizing wasted machine times. These times negatively affect the product's costs and time of delivery.

VIII. ANALYSIS

A. Proposed System

In the system proposed the general scenario is preserved, and the difference is that when a new task arrives at a machine (Spinning-Frame or Loom), a **GA** is executed instead of the task being added to the schedule. Once the optimal task sequence has been found, the agent that represents the resource sends a message to the **PA** indicating the date in which the last task would finish. To achieve greater flexibility, there exists the possibility of indicating the moment in which it is intended to schedule using a **GA**.

B. Reasons for applying Genetic Algorithms

The scheduling problem is NP-complete, thus it is not feasible to assess all the possible combinations of tasks associated to a machine to find the best. Given the explosive growth of possible combinations when the amount of elements grows, it is unaffordable to solve this kind of problem by examining all possible solutions. This leads to the necessity of applying a technology capable of reducing the search space and providing a solution within appropriate times. **GAs** are considered to be a suitable option to deal with problems which involve large search spaces.

C. Analysis

In the current schedule process, when a Spinning-Frame (or Loom) receives an order to produce a yarn (or fabric), it is checked that the task can be finished in the specified time frame. This is done by adding the new task at the end of the schedule and checking that the arranged limit date is not surpassed. If this is true then the **PA** is informed of the date in which the task could be finished and it will decide, based on the proposals received from all the Spinning-Frames (or Looms), to which of them will the task be assigned. It can be seen that the schedule for every machine is composed by the tasks that the **PA** assigns to them as time passes.

One improvement to the current system would be to add a mechanism at the level of the machines to determine which combination of tasks (those already scheduled plus the new one) optimizes its resources. The effective time of production of a machine serves a measure of the degree to which the resources are being taken advantage of. Therefore, resource optimizations means reducing the amount of time a machine is inactive, which is the sum of the periods of time from the end of one task to the beginning of the next. Inactive time includes time not producing and time setting-up. The set-up takes place when a machine needs to change its configuration so as to switch from produce one type of product to another.

In the current system, once a **PA** has successfully finished scheduling its order of purchase, the date and machine in which each task is to be executed have been determined. However, in the system proposed, the schedules are dynamic, that is, the tasks assigned to a machine do not change, but their order in the schedule may vary (because of the application of the **GA**).

Each task has a start date and an end date in a machine's schedule. In the system proposed, two new dates are added, minimum start date and the maximum end date possible, which determine the range of dates allowed for the execution of a task. When applying a **GA** at the level of a machine, new sequences of tasks from the schedule will be generated and thus this range of dates will allow to control that each task is carried out within the preset times.

Certain restrictions must be considered, for instance: a task from the schedule of a loom will have as its minimum start date the maximum end date of the production of the threads that will compose the fabric, which will be called Max-End-Date-Order-Threads, and to which must be added the time needed to prepare the loom (including the time of moving the threads to the loom). The maximum end date will be associated with the date of finalization of the order of purchase.

In the system proposed, before the **PA** notifies the **VA** that the manufacturing of an order of purchase has been accepted, if it has, maximum possible end date of each of the thread associated to the order is updated with the Max-Date-End-Order-Threads. Such date must be respected when **GAs** execute at the level of the Spinning Frames, since it has been taken as a reference to start jobs in the loom.

It should also be taken into account that when a new task arrives at a machine to be scheduled in a machine agent, a

copy of its current schedule must be saved before executing the **GA**. This enables to restore the previous schedule, which was an optimum sequence of tasks, in the event that the new task is not finally assigned to the machine.

IX. DESIGN OF THE GENETIC ALGORITHM

In this section the genetic algorithm to be executed at the level of a machine agent is defined, along with its parameters and the way it works.

A. Encoding

The first step to design the **GA** in the scenario of the schedule system to be used consists of identifying what is a gene and what is a chromosome, and to define a suitable encoding method for them.

In this application, a **gene represents a task** to be executed by a machine, while **a chromosome represents its schedule** or sequence of tasks. **Genes** are encoded using a whole number that indicates its position in the schedule.

B. Population

The input of the **GA** is given by a population of individuals (chromosomes), which are generated through the random combination of the tasks which the schedule of a machine comprises. This permits the generation of invalid chromosomes (schedules), but the **fitness function** will allow discarding them in successive evolutions, as shown below.

C. Evaluation or Assessment

The **fitness** function has been designed so as to encourage valid plans that are efficient and to penalize those invalid or inefficient (by assigning them low scores). The evaluation consists of two phases, one that checks that the chromosome or schedule is valid and the other that rates better those plans with less inactive time.

A plan is valid if: a) each task is executed within the arranged date range for it and b) the adjacent pairs of tasks represent a valid sequence in time, that is, the end date of one is not greater than the start date of the next. If this is the case, the plan will be awarded a score of one (1). If only some of the pairs of adjacent tasks are valid, then the score will be given by the proportion of valid pairs and the total of pairs. This promotes the generation of valid individuals. If a plan has no valid sequence, it will have a score of zero (0).

If the plan is valid, it is assigned a score representing the efficiency of usage of the machine resources. This is calculated as the relationship between the time the machine was producing and the total time of the plan (minus the initial setup time).

The biggest score a chromosome can be assigned is two (one for validity and one for resource usage).

D. End condition and solution proposed

After a maximum number of evaluations executed, the solution proposed is the plan with higher fitness.

E. Selection and Generation

In order to obtain the best individuals en each run (evolution) of the **GA**, it has been decided to use *Elitism*-based selection. The generation process consists of applying genetic operators to the selected individuals, so as to create new individuals. The process takes random pairs of chromosomes (ancestors) and applies the selected operators to them (*crossover based on the order and mutation*), thus generating new chromosomes (descendants).

The *crossover based on the order* uses a randomly generated crossover pattern formed by a string of bits (0 and 1) of the same length as the ancestor chromosomes. In those positions in which the pattern has a value of one, the descendant **A** preserves the genes of ancestor **A** and descendant **B** those of ancestor **B**. To complete the missing genes of descendant **A** (in the positions where the pattern has a value of zero), the following procedure is applied: 1º genes from ancestor **A** in the position where the pattern has a value of zero are taken, 2º they are sorted according to the order in which they appear in ancestor **B** and 3º genes are taken one by one from the sorted list and the missing genes of descendant **A** are completed (see Table 1). The genes of descendant **B** are completed similarly, taking one by one the genes form the sorted list (formed with the genes of ancestor **B** where the pattern is zero, and sorting them according to the order in which they appear in ancestor **A**).

TABLE I
APPLICATION OF ORDER BASED CROSSOVER

	Ancestor chromosomes and crossover pattern	Genes to exchange ^a	Generated descendant chromosomes
A	0123456789	2, 3, 9 → 9, 3, 2	0193456782
B	7968342015	6, 8, 5 → 5, 6, 8	7956432018
Pattern	1100111110		

^a At the left of the arrow the genes to exchange (for ancestor A they are 2, 3, and 9) are shown, while at the right of the arrow the genes are shown according to the order in which they appear in the other ancestor (9, 3, 2) for ancestor A.

A *mutation* operator is additionally applied, which consists of randomly choosing two genes from a chromosome and exchanging them. This operator as a mutation rate associated, which indicates how many chromosomes from the population will, on average, experience mutation. After applying the genetic operators, a new population is obtained, but only those which succeed in the evaluation phase (those best awarded) will reach for the next evolution.

X. IMPLEMENTATION DECISIONS

The system has been developed using the Java language. Jade has been used as the development platform for multi-agent systems and JGAP (built with Java) as the platform for the development of the **GA**. Each gene represents a position in a list of tasks that contains: the tasks of the current schedule of a machine plus the new task to schedule.

To determine the population size and the number of evolutions of the **GA** needed to obtain optimum results, an experiment

was carried out consisting of executing the **GA** directly at the level of a single machine, varying the values of the variables to be determined. In each run the size of the population and the number of evolutions were modified and measures of average *fitness* and maximum *fitness* achieved were taken. This allowed to obtain the appropriate value for the number of evolutions and the size of the population, both of them being equal to 250. Other combinations of values for these variables resulted in a remarkable growth of execution times.

XI. SIMULATION AND OBTAINED RESULTS

The test set contains 3240 orders of work which cover 20 weeks of production, generated using a Monte Carlo simulation based on real data provided by a textile industry (350 types of fabric composed by 200 types of thread). In the simulation there were used 56 looms and 15 spinning-frames agents, plus one sales department agent, one yarns depot agent, one fabric depot agent, and uninterrupted availability of raw materials.

Three simulations were performed on the same set of orders, using both the current system and the proposed system (with **GA** technology), so as to obtain conclusions regarding the performance of both systems.

Because of time restrictions in the simulation, the **GA** was only applied to a fraction of the planned schedules.

The values obtained of the weekly income during the period of simulation are samples with which to make a comparison of the performance of both systems.

According to the results of the simulation and the comparison with the base system, it has been possible to verify that a higher performance was achieved by applying the **GA**.

XII. CONCLUSIONS

The quest for effective solutions to solve the problem of scheduling has been the reason for many investigations. The utilization of genetic algorithms for the generation of alternative plans has resulted to be appropriate to generate acceptable solutions for the problem of scheduling.

REFERENCES

- [1] V.J. Botti and A. Giret, *Aplicaciones Industriales de los sistemas multiagente*, Universidad Politécnica de Valencia, 2004.
- [2] J.M. Corchado, *Agencia: Una puerta hacia la convergencia de la inteligencia artificial*, June 2003.
- [3] H. Fang, *Genetic Algorithms in Timetabling and Scheduling*, Department of Artificial Intelligence University of Edinburgh , 1994.
- [4] J.C. García, J. Pérez and A.E. Arenas, *Aplicación de una metodología de desarrollo de sistemas multiagente en la disseminación selectiva de información en la Web*, Universidad Autónoma de Bucaramanga, Colombia.
- [5] N.R. Jennings, *Coordination Techniques for Distributed Artificial* Dept. of Electronic Engineering, Queen Mary and Westfield College, University of London, 1996.
- [6] F. Jorge and R. Piaggio, *Evaluación de Autómatas Celulares mediante algoritmos genéticos*, Memoria de grado, Facultad de Ingeniería de la UCUDAL, 2001.
- [7] C.L. Karr and L.M. Freeman, *Industrial Applications of Genetic Algorithms*, CRC Press, December 1998.
- [8] A. Marczyk, *Algoritmos genéticos y computación evolutiva*, 2004, <http://the-geek.org/docs/algen/>
- [9] J. Martín and D. García. *Seminario: Algoritmos Genéticos*, Curso 2004-2005.

- <http://www.infor.uva.es/~calonso/IAI/TrabajoAlumnos/memoriaAG.pdf>
- [10] M. Mitchell, *An Introduction to Genetic Algorithms*, The MIT Press © 1999 (209 pages)
- [11] G. Nucci, *Aplicação de Sistemas Holdônicos à Manufatura Inteligent*, Universidad Estadual de Campinas, Facultad de Engenharia Mecanica, 2004.
- [12] E. Ocampo, *Aplicación de un sistema multiagente a la planificación y asignación de trabajos en líneas de producción manufacturera*, Trabajo de Doctorado en Ingeniería en Informática, September 2004.
- [13] E. Ocampo, *Ingeniería de Software Orientada a Agentes*, Universidad Pontificia de Salamanca, 2004
- [14] J. Odell, V.D. Parunak and B. Bauer, *Extending UML for Agents*, 2004
- [15] D.S. Orcero, *Los Algoritmos Genéticos*, <http://www.orcero.org/irbis/dissertacion/nod192.html>
- [16] S. Russell and P. Norvig, *Inteligencia Artificial. Un enfoque moderno*, Prentice Hall, 1996.
- [17] W. Shen, D.H. Norrie and J.P. Barthès, *Multi-Agent Systems for Concurrent Intelligent Design and Manufacturing*, 2001.
- [18] L. Val and M. Hernández, *Evaluación del Uso de Programación Genética para la Evolución de Funciones Heurísticas para Juegos de Tablero en un Marco Genérico*, Memoria de grado, Facultad de Ingeniería de la UCUDAL, 2003.
- [19] G. Weiss, *Multiagent Systems. A modern approach to Distributed Artificial Intelligence*, Chapter 2 pp 79-120 - Multiagent Systems and Societies of Agents by Michael N. Huhns and Larry M. Stephens, The MIT Press, <http://puccini.mty.itesm.mx/~rbrena/MAS/Weissc2.pdf>
- [20] M.J. Wooldridge and N.R. Jennings, *Intelligent Agents: Theory and Practice. The Knowledge Engineering Review*, 2(10):115-152, 1995.
- [21] F. Zambonelli, N.R. Jennings and M. Wooldridge, *Developing Multiagent Systems: The GAIA Metodology*, October 2003.

PRE- AND POST- PROCESSING FOR ENHANCEMENT OF IMAGE COMPRESSION BASED ON SPECTRUM PYRAMID

Mariofanna Milanova
UALR
2801 S. University Ave.
Little Rock
Arkansas 72204-1099, USA
mymilanova@ualr.edu

Roumen Kountchev
Technical University of
Sofia
Bul. Kl. Ohridsky, 8
Sofia 1000, Bulgaria
rkountch@tu-sofia.bg

Vladimir Todorov
T&K Engineering
Mladost 3, Pob.12
Sofia 1712
Bulgaria

Roumiana Kountcheva
T&K Engineering
Mladost 3, Pob.12
Sofia 1712
Bulgaria

todorov_vl@yahoo.com kountcheva_r@yahoo.com

Abstract - In the paper is presented a combination of special methods for pre- and post-processing of still images, aimed at compression ratio enhancement and quality improvement of images, processed with pyramidal decomposition in the spectrum domain. The pre-processing is based on the image histogram analysis, in result of which are done adaptive image segmentation and contrast enhancement, performed stretching/skewing the defined segments. As a result, the obtained compression ratio is increased. The post-processing of images, restored after the compression, is performed with a new digital adaptive filter, whose parameters are set in accordance with those, used in the process of the compression. In result, the quality of the images is significantly improved. The presented combination of pre- and post-processing, results in significant enhancement of the compression, based on the pyramidal decomposition.

I. INTRODUCTION

The visible distortions in still images restored after compression/decompression are of great importance for the successful use of compression techniques when efficient archiving of large databases of still images is needed. Such application areas are the distance learning and training, based on visual information, involving large image databases (arts, medicine, geography, or the storage of financial documents (invoices, checks), etc. The size of the databases depends mainly on the efficiency of the used compression algorithms and on the selected compression ratio, but as a rule, for higher compression ratios the quality of the restored images is lower. The reasonable trade-off is to find a way to modify slightly the image contents, retaining the visual image quality (image pre-processing), and to change the image data so that to obtain higher compression ratio. The famous image pre-processing techniques are usually based on some kind of image segmentation, histogram equalization, etc. [1,2]. A new kind of pre-processing, which answers the peculiarities of the spectrum decomposition and compression, is presented below. This pre-processing is based on image histogram analysis and adaptive image segmentation, performed using the analysis results. The post-processing techniques are usually aimed at

the removing of the blocking artifacts, which are the natural consequence of the use of any kind of orthogonal transforms. These artifacts display themselves as artificial boundaries between adjacent blocks or around sharp transitions in the processed images. In order to minimize the artifacts in the processed images are already developed significant number of post-processing algorithms [3,4,5]. The most widely known could be classified in the following groups: 1) direct linear or non-linear smoothing techniques in the spatial domain; 2) combined techniques employing both edge detection or segmentation for detail classification and spatial adaptive filtering; 3) iterative techniques based on the theory of projections on to convex set (POCS) [6], and 4) soft threshold approaches in the wavelet domain [7]. The major issues existing in the current post-processing methods can be summarized as: limitation to a certain type of artifacts (the first group), and such with higher computational complexity – represented with the remaining three groups.

In the paper is offered a relatively simple and efficient post-processing technique for removing the blocking artifacts in decompressed images, obtained with the new pyramidal spectrum decomposition (named "Inverse Difference Pyramid", IDP [8]), using a two-dimensional fuzzy digital filter. In Section 2 is given a brief description of the IDP method for still image decomposition and compression, in Section 3 is presented the algorithm for image pre-processing with adaptive contrast enhancement, in Section 4 is described the approach, used for the adaptation of the filter parameters in accordance with the IDP method, in Section 5 are presented the experimental results of the investigation on the pre- and post-processing for test images compressed with software based on the IDP method and in the Conclusion are pointed the specific features of the presented approach and its main advantages.

II. MULTI-LEVEL IDP DECOMPOSITION

The basic principles of the IDP decomposition [8] are presented below. The original .bmp image [B] with size HxV pixels is divided in K sub-images [B_{k₀}(2ⁿ)] with size 2ⁿ×2ⁿ and sequence number k₀=1,2,...,K. Every sub-image is processed with some kind of 2D linear orthogonal transform, in correspondence with the relation:

$$[B_{k_0}(2^n)] = [\tilde{B}_{k_0}(2^n)] + \sum_{p=1}^{n-1} [\tilde{E}_{p-1}(2^n)], \quad (1)$$

where $p=0,1,2,\dots,n-1$ is the number of the decomposition component.

The IDP decomposition components are defined as follows:
The first component for $p=0$ is defined with the matrix:

$$[\tilde{B}_{k_0}(2^n)] = [T_0(2^n)]^{-1} [\tilde{S}_{k_0}(2^n)] [T_0(2^n)]^{-1}, \quad (2)$$

where $[\tilde{S}_{k_0}(2^n)] = [m_0(u,v) s_{k_0}(u,v)]$ for $u,v=0,1,\dots,2^n-1$,

$$m_0(u,v) = \begin{cases} 1 & \text{when } (u,v) \in V_0; \\ 0 & \text{in all other cases,} \end{cases}$$

$s_{k_0}(u,v)$ are the elements of the spectrum matrix, calculated in accordance with the transform:

$$[S_{k_0}(2^n)] = [T_0(2^n)] [B_{k_0}(2^n)] [T_0(2^n)], \quad (3)$$

$[T_0(2^n)]^{-1}$ and $[T_0(2^n)]$ are the matrices of the 2D direct and inverse orthogonal transforms, represented correspondingly with Eqs. (2) and (3), each with size $2^n \times 2^n$; V_0 is the low-frequency area of the spectrum matrix $[S_{k_0}(2^n)]$, which contains the retained coefficients $\tilde{s}_{k_0}(u,v)$ with spatial frequencies $(u,v) \in V_0$. The place of the retained coefficients $\tilde{s}_{k_0}(u,v)$ is defined by the elements $m_0(u,v)$ of the corresponding matrix-mask $[M_0(2^n)]$.

The next components (1) for $p=1,2,\dots,n-1$ are defined with:

$$\begin{aligned} [\tilde{E}_{p-1}(2^n)] = & \begin{bmatrix} [\tilde{E}_{p-1}^{1,1}(2^{n-p})] & [\tilde{E}_{p-1}^{1,2}(2^{n-p})] & \cdots & [\tilde{E}_{p-1}^{1,4^p}(2^{n-p})] \\ [\tilde{E}_{p-1}^{2,1}(2^{n-p})] & [\tilde{E}_{p-1}^{2,2}(2^{n-p})] & \cdots & [\tilde{E}_{p-1}^{2,4^p}(2^{n-p})] \\ \vdots & \vdots & \ddots & \vdots \\ [\tilde{E}_{p-1}^{4^p,1}(2^{n-p})] & [\tilde{E}_{p-1}^{4^p,2}(2^{n-p})] & \cdots & [\tilde{E}_{p-1}^{4^p,4^p}(2^{n-p})] \end{bmatrix} \end{aligned}$$

Every matrix $[\tilde{E}_{p-1}(2^n)]$ contains the sub-matrices $[\tilde{E}_{p-1}^{k_p}(2^{n-p})]$ with size $2^{n-p} \times 2^{n-p}$ for $k_p=1,2,\dots,4^p$, obtained in result of its quad-tree representation with 4^p square blocks. On the other hand, each sub-matrix is defined as:

$$[\tilde{E}_{p-1}^{k_p}(2^{n-p})] = [T_p(2^{n-p})]^{-1} [\tilde{S}_p^{k_p}(2^{n-p})] [T_p(2^{n-p})]^{-1},$$

where

$$\tilde{s}_p^{k_p}(u,v) = m_p(u,v) s_p^{k_p}(u,v), \text{ for } u,v=0,1,\dots,2^{n-p}-1$$

are the retained spectrum coefficients of the sub-matrix $[\tilde{E}_{p-1}^{k_p}(2^{n-p})]$; $m_p(u,v)$ are the elements of the matrix-mask $[M_p(2^{n-p})]$ with size $2^{n-p} \times 2^{n-p}$, who define the places of the retained spectrum coefficients in correspondence with the relation:

$$m_p(u,v) = \begin{cases} 1 & \text{if } (u,v) \in V_p; \\ 0 & \text{in all other cases.} \end{cases}$$

Here V_p comprises the low-frequency part of the retained coefficients $\tilde{s}_p^{k_p}(u,v)$ from the matrix $[S_p^{k_p}(2^{n-p})]$. This matrix is obtained in result of the 2D orthogonal transform of

the difference matrix $[E_{p-1}^{k_p}(2^{n-p})]$ with the transform matrix $[T_p(2^{n-p})]$ in correspondence with the relation:

$$[S_p^{k_p}(2^{n-p})] = [T_p(2^{n-p})] [E_{p-1}^{k_p}(2^{n-p})] [T_p(2^{n-p})].$$

Here $[E_{p-1}^{k_p}(2^{n-p})]$ is the sub-matrix k_p of the difference matrix $[E_{p-1}(2^{n-p})]$:

$$[E_{p-1}(2^{n-p})] = \begin{cases} [BQ^n] \cdot [\tilde{B}_0(2^n)] & \text{for } p=1; \\ [E_{p-2}(2^{n-p})] - [\tilde{E}_{p-2}(2^{n-p})] & \text{for } p=2,3,\dots,n-1. \end{cases}$$

The last component of the decomposition in correspondence with (1) for $p=n-1$ contains the sub-matrices $[\tilde{E}_{n-2}^{k_{n-1}}(2)]$ with size 2×2 , obtained in result of its quad-tree representation with 4^{n-1} blocks. In order to perform a full decomposition, the number of the retained spectrum coefficients for every sub-matrix should be 4. In this case the elements of the matrix $[M_{n-1}(2)]$ are $m_{n-1}(u,v)=1$ for $u,v=0,1$. The values of the retained spectrum coefficients d from the sub-matrices k_p for the component p , represented in (1) for $k_p=1,2,\dots,4^p$ and $p=0,1,2,\dots,n-1$, build the Inverse Difference Pyramid (IDP). For certain applications, when highest image quality is not necessary, it is suitable to stop the decomposition earlier, reducing the number of pyramid levels.

One of the most important features of the IDP decomposition is that its components for $p=1,2,\dots,n-1$ contain many coefficients with values, equal to zero. Together with this, the spectrum coefficients $\tilde{s}_p^{k_p}(u,v)$ of IDP have irregular amplitude distribution in result of which the entropy coding which follows in the compression procedure becomes more efficient. In order to compress the obtained data, the values of all spectrum coefficients, calculated for the participating IDP levels are arranged in a one-dimensional sequence. This sequence is then processed with adaptive RL and with modified Huffman coding [9], and in result is obtained the compressed data file.

The processed images are restored, performing the already described operations in reverse order. The compression ratio is controlled changing the number of the retained coefficients and the quantization tables for the coefficients' values in all pyramid levels.

The algorithms for image pre-and post-processing, described below, are aimed at the IDP compression enhancement.

III. IMAGE PRE-PROCESSING

The image pre-processing technique precedes the image IDP decomposition. The proposed method performs adaptive image contrast enhancement, comprising two consecutive stages: brightness segmentation based on the image histogram analysis, and transformation of the pixels' brightness in accordance with tables, defined by the segments treatment.

In the first stage is performed the image segmentation, using the thresholds k_1 and k_2 , which divide the histogram in three segments (A, B, C). The thresholds are set so that to define the second segment (B), which contains the main part of the image objects. In order to make the number of participating

brightness levels in the segment B smaller (and correspondingly - to obtain more IDP coefficients with same values without quantization), this part should be skewed to 90-95%. The limits of the central segment (B) are defined performing the following operations:

- The image histogram $h(k)$ is calculated and is defined its maximum:

$$h_{\max} = \max\{h(k)\} \text{ for } k = 0, 1, 2, \dots, k_{\max},$$

- The value $t = \alpha h_{\max}$ is defined, for $\alpha < 1$ (for example $\alpha = 0.8$): this value defines the magnitude of the middle segment of the histogram (B).

- The values of the start and end points of the segment B, defined as k_1 and k_2 , are calculated in accordance with the relations:

$$h(k) \leq t \text{ for } k = 0, 1, 2, \dots, k_1 - 1,$$

$$h(k) \geq t \text{ for } k = k_2 + 1, k_2 + 2, \dots, k_{\max}, \text{ for } |k_2 - k_1| \geq \Delta.$$

(Δ – a value, set in advance).

In case, that the last condition is not satisfied, the value of the parameter α is decreased, for example to $\alpha=0.75$, and using the new threshold value $t=\alpha.h_{\max}$ are defined the corresponding values for k_1 and k_2 . When the requirement $|k_2 - k_1| \geq \Delta$ is satisfied, the calculation cycle ends; if not – the process continues. An example is presented in Fig.1.

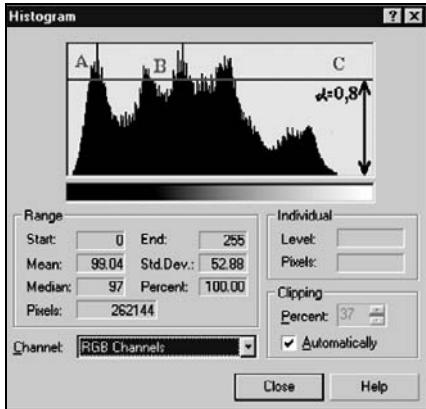


Fig.1.The histogram of the test image "Lena": the three segments of the image histogram (A,B,C) are shown.

In the second stage of the processing, the brightness level k of the pixels in the three segments of the histogram is transformed in accordance with the relations:

$$g(k) = \begin{cases} g_A(k) & \text{if } 0 \leq k < k_1; \\ g_B(k) & \text{if } k_1 \leq k \leq k_2; \\ g_C(k) & \text{if } k_2 < k \leq k_{\max}. \end{cases}$$

The relations $g_A(k)$, $g_B(k)$ and $g_C(k)$ represent the brightness transformation for the pixels in the segments A, B and C correspondingly. In order to perform the required contrast transformation, the boundaries k_1 , k_2 of the segment (B) are skewed to $(k_1+\delta_1)$ and $(k_2-\delta_2)$, and correspondingly are moved the upper limit value of the segment A and the lower

limit value of the segment C. In the presented example δ_1 and δ_2 are parameters, which define the contrast modification of the objects in the segment B and as a consequence – of the segments A and C as well. The brightness transformation tables are defined in accordance with the requirement for histogram equalization of the corresponding segment (A, B or C) with changed (stretched or skewed) brightness range:

$$\begin{aligned} g_A(k) &= (k_1 + \delta_1) \sum_{l=0}^k h_A(l), \\ g_B(k) &= (k_2 - k_1 - \delta_1 - \delta_2) \sum_{l=k_1+\delta_1}^k h_B(l) + (k_1 + \delta_1), \\ g_C(k) &= (k_{\max} - k_2 + \delta_2) \sum_{l=k_2-\delta_2}^k h_C(l) + (k_2 - \delta_2). \end{aligned}$$

In particular, for images in which the histogram of the corresponding segment is uniform, i.e. for:

$$h_A(k) = \frac{1}{k_1} \text{ for } k = 0, 1, \dots, k_1 - 1;$$

$$h_B(k) = \frac{1}{k_2 - k_1} \text{ for } k = k_1, k_1 + 1, \dots, k_2;$$

$$h_C(k) = \frac{1}{k_{\max} - k_2} \text{ for } k = k_2 + 1, k_2 + 2, \dots, k_{\max},$$

the relations for the brightness transformation for every pixel are linear and are defined as follows:

$$g_A(k) = \left(\frac{k_1 + \delta_1}{k_1} \right) k;$$

$$g_B(k) = \left(\frac{k_2 - k_1 - \delta_1 - \delta_2}{k_2 - k_1} \right) (k - k_1) + (k_1 + \delta_1);$$

$$g_C(k) = \left(\frac{k_{\max} - k_2 + \delta_2}{k_{\max} - k_2} \right) (k - k_2 - 1) + (k_2 - \delta_2 + 1).$$

In this case the brightness levels in the range (k_1, k_2) are skewed in accordance with a linear relation and correspondingly - the brightness levels in $(0, k_1 + \delta_1)$ and $(k_2 - \delta_2, k_{\max})$ are stretched.

The contrast enhancement of color (R,G,B) images is performed after their transformation in Y, C_r, C_b format, and then the Y component only is processed. After the end of the processing the three components (Y, C_r, C_b) are transformed back in R,G, B format.

IV. POST-PROCESSING WITH DIGITAL FUZZY ADAPTIVE FILTER

The post-processing of decompressed images is usually based on the use of fuzzy digital filters – this is an approach, widely used recently [3,4]. The filtration is a powerful tool for the improving of the visual quality of compressed images, deteriorated in result of the use of a “truncated” orthogonal transforms and of the quantization of the transform coefficients’ values. The aim of this work was to develop a new digital filter with low computational complexity, whose parameters are easily adapted to the specifics of the IDP decomposition.

The algorithm of the proposed two-dimensional fuzzy adaptive filter (2DFAF), using a sliding window with size $M \times N$ pixels ($M=2R+1$ and $N=2S+1$), is presented below:

$$x_F(i,j) = \begin{cases} \sum_{r=-R}^R \sum_{s=-S}^S \mu(i+r, j+s) x(i+r, j+s) & \text{for } \sum_{r=-R}^R \sum_{s=-S}^S \mu(i+r, j+s) \geq T, \\ \sum_{r=-R}^R \sum_{s=-S}^S \mu(i+r, j+s) & \\ (1/MN) \sum_{r=-R}^R \sum_{s=-S}^S x(i+r, j+s) & \text{- in all other cases.} \end{cases}$$

Here $\lfloor \circ \rfloor$ is a rounding operator; $x(i,j)$ and $x_F(i,j)$ represent correspondingly the pixels of the input and of the filtered output image and T is a threshold.

$$\mu(i+r, j+s) = \begin{cases} 1 & \text{for } \Delta(i+r, j+s) \leq \alpha; \\ \frac{\Delta(i+r, j+s) - \alpha}{\alpha - \beta} & \text{for } \alpha \leq \Delta(i+r, j+s) \leq \beta; \\ 0 & \text{for } \Delta(i+r, j+s) \geq \beta, \end{cases}$$

The relation above, represents the membership function with parameters α and β ($\beta > \alpha$), whose argument Δ is the module of the difference between the central pixel $x(i,j)$ in the filter window and the pixel $x(i+r, j+s)$, which is at a distance (r,s) :

$$\Delta(i+r, j+s) = |x(i,j) - x(i+r, j+s)|; r = -R, +R, s = -S, +S$$

The values of the parameters α and β are defined in accordance with the image contents and the kind of the distortions, which should be repaired. In the case, when they are block artifacts, resulting from the high compression ratio, the values of α and β are defined depending on the compression strength and the compression algorithm used. In this case the 2DFAF filter is used for images, whose block artifacts were obtained as a result of a lossy compression based on the IDP decomposition [8].

V. FILTER ADAPTATION

In order to make the filter performance more flexible, the values of the parameters α and β of the 2DFAF are set in accordance with the relations:

$$\alpha = \delta - \varepsilon, \quad \beta = \delta + \varepsilon,$$

where δ defines the center of the filter fuzziness area, for which the function $\mu(\Delta) = 0.5$, and ε defines the boundaries of the deviation from δ . The value of the parameter δ is defined in accordance with the relation:

$$\delta = \frac{1}{2} |\hat{E}_0(i,j)_{\max}|.$$

Here $E_0(i,j)_{\max}$ is a pixel of the difference matrix $[E_0]$ for which the value of the approximation error between the highest IDP level and the original image is maximum. The parameters ε and T of the 2DFAF filter are set experimentally in accordance with the compression ratio and the noise level.

VI. EXPERIMENTAL RESULTS

The research was done for more than 100 test images compressed with the software TKView, based on the already described IDP decomposition. In the investigation was used the 100-stage quality factor (QF) set, developed for the IDP

decomposition, and defined by a number of parameters (QF100 is for the best quality and the smallest compression, QF1 – for the worst quality and the highest compression ratio). The set of parameters used to define the QF stages comprises the number of pyramid levels, the approximation 2D transform (DCT or Walsh-Hadamard Transform, WHT) used in the consecutive pyramid levels, the participating transform coefficients, the quantization values, etc.

The experimental results show, that the influence of the pre-post processing is more significant when the compression ratio (CR) is high and correspondingly – the restored image quality – worse.

The software implementation of the presented pre-processing method was performed for $\alpha=0.8$. For the investigation of the post-processing was used a filter window with width 3, 5 and 7 pixels (the window height was always 3 pixels), and the center of the filter fuzziness had been changed consecutively from 5 to 65. As a rule, the filter parameters should not be too small so that the noisy edges can be sufficiently smoothed. Since different compression ratios lead to different noise levels, the parameters were optimized to achieve the best tradeoff, taking into account the sub-image size and the maximum difference between the original image and its approximation. The used values for the main IDP parameters defining the QF levels, were:

- Three pyramid levels (0, 1 and 2), with sub-images with size 8×8 , 4×4 and 2×2 pixels correspondingly;
- Approximation – for the lowest level it was CHT and for the higher ones - WHT;
- Retained coefficients: 4 for the lowest level and 8 and 4 for the higher ones;

• Global quantization step: 4;

• Global threshold for the spectral coefficients' values: 2.

The values for the histogram modification parameters were:

• $\alpha = 0.8$;

• Segment B was skewed to 90%;

• Segments A and C were stretched correspondingly.

The values of the ADFAF parameters were:

• Filter window height - 3 pixels;

• Filter window width - 3 pixels for QF in the range from 70 to 10 and 5 pixels for QF from 9 to 1;

• Center of the filter fuzziness - equal to the half of the calculated maximum error between the highest IDP level approximation and the original image;

• δ was set equal to 5.

The results of the dual influence (the histogram modification and the post-filtration) on the quality and the compression ratio of the IDP-processed images are presented graphically in Figures 2,3,4 and 5 below. In Fig.2 is presented the influence of the histogram modification and the adaptive image filtration on the restored image quality (PSNR [dB]). The filtration is efficient for high compression ratios, i.e. for QF in the range from 70 to 1. For lower compressions the image quality is good enough (there are no visible distortions) and the image pre- and post-processing is not necessary.

Note: The results for the pre/post processing in all figures are presented with the curves, named “name_H_F”.

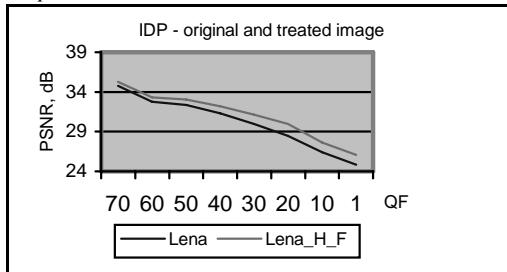


Fig.2. Influence on the image quality for IDP quality factor changing from 70 to 1 after pre- and post processing (test image “Lena”).

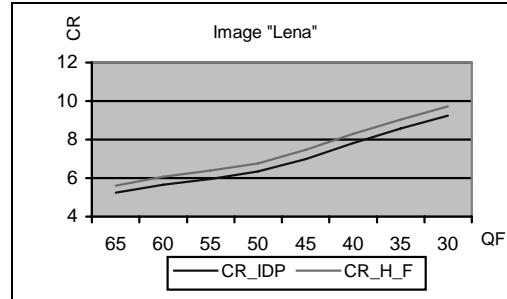


Fig.3. Influence on the IDP compression ratio for quality factor changing from 65 to 30 (test image “Lena”).

Some of the investigation results for the test image “Fruits” are presented in Figs. 4 and 5. In Fig.4 is shown the change of the Compression Ratio (CR) in result of the pre- and post-processing and in Fig. 5 are presented the curves for the obtained CR values with and without pre/post processing.

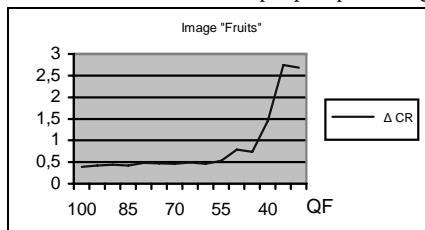


Fig.4. The change of the Compression Ratio (ΔCR) in result of the test image pre- and post-processing for quality factor in the range from 100 to 30.

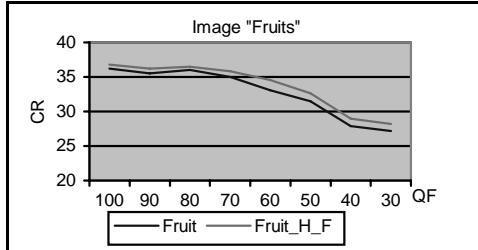


Fig.5. Comparison of the Compression Ratio for the test image “Fruits” without and with pre- and post-processing

In Fig. 6 a,b is presented the visual result of the processing for the test image “Fruits”. The obtained compression ratio for IDP QF 20 (without pre- and post-processing) is 24 and the PSNR = 31 dB.



Fig.6.a. Enlarged part of the test image “Fruits”, restored after IDP compression with QF 20.

The compression ratio obtained for same IDP QF after treatment was 26, and the PSNR = 33,3 dB correspondingly; (the visual quality of the second image is better).



Fig.6.b. The same enlarged part of the test image “Fruits”, restored after IDP compression with QF 20, after treatment in accordance with the described algorithms for pre- and post-processing.

In result of the applied pre-and post-processing the IDP-based image compression is more efficient than JPEG for high compression ratios (for IDP QF in the range from 15 to 1 the compression ratio and the image quality are much higher). The results are presented in Fig. 7 a,b.

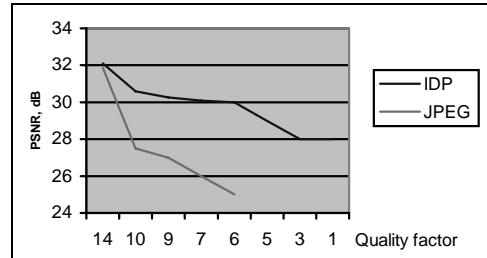


Fig.7. a.

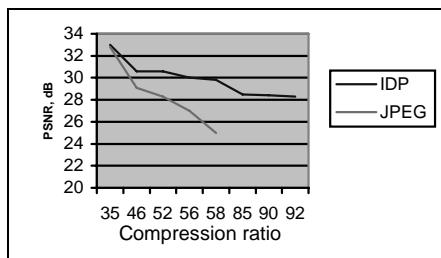


Fig.7.b.

Fig.7. Comparison with JPEG for high compression ratios (test image "Fruits").

In Fig. 7.a are presented the results for lowest values for the IDP quality factor (in the range between 15 and 1). The sizes of the compressed IDP files were much smaller than these, obtained with Microsoft Photo Editor (JPEG compression) and this is why the corresponding JPEG results are missing (such high compressions are not possible for Microsoft Photo Editor). The quality of the corresponding restored images is much better for IDP as well (Fig. 7.b). Specific for the IDP compression is that for such high compression ratios is used the information from the lowest pyramid layer only and it is enough to be visualized as a thumbnail image. The additional information, necessary to restore the image with higher quality is just added to the existing one, without sending twice the same or a part of the compressed data.

VII. CONCLUSION

The basic features of the new methods are:

For the pre-processing:

- The method has low computational complexity and small number of participating parameters, whose values are set in accordance with the result of the image histogram analysis;
- The method is adaptive, which permits to set the parameters and to perform the treatment in accordance with the image contents.

For the post-processing:

- The filter performance is best for cases, when the compression ratio is higher than 10 - for such compressions the blocking artifacts become visible and the filtration is efficient;
- The filter width should not be greater than the number of pixels in the sub-image of the processed image (the last IDP decomposition level). In the presented examples (for a sub-image with size 4 pixels in the highest level) this width is 3, and for the cases, when only one pyramid level is used and the sub-image size is 8 pixels, better performance is obtained for filter width equal to 5.
- The center of the filter fuzziness should be the half of the maximum difference, calculated between the original and its approximation in the last IDP level.
- Additional advantage is the ability to use the filter for JPEG images [10]. In this case the filter parameters are: filter

window width = 5 pixels and Center of the filter fuzziness = 64.

Advantages:

- The computational complexity of the presented methods for pre- and post- processing is low and they could be easily integrated for real-time implementations;

• The filter has high flexibility, because its performance adapts depending on local and global parameters: the center of the filter fuzziness is calculated as a part of the maximum difference (global parameter) and it analyzes and changes the single pixels values (local parameters) framed by the filter window.

- The method ensures the high efficiency of the IDP-based compression (better than JPEG for high compression ratios) and permits easy generation of thumbnail images.

The obtained results prove the method efficiency. The small number of parameters used for the processing permits its application in large number of areas, aimed mainly at distance learning and mobile communications.

ACKNOWLEDGEMENT

This paper was supported by the Bulgarian Ministry of Education and Science (Contract № VU-MI 104/2005).

REFERENCES

- [1] P. Barten. "Contrast sensitivity of the human eye and its effects on image quality". Bellingham, WA: SPIE, 1999.
- [2] S. Winkler, P. Vanderheynst. "Computing isotropic local contrast from oriented pyramid decompositions". Proc. 6th Int. Conf. Image Processing, Kobe, Japan, Oct. 1999, pp. 420-424.
- [3] M. Nachtegael et all. "Fuzzy filters for image processing", Springer-Verlag, 2003.
- [4] Y. Nie, K. Barner. "Optimized fuzzy transformation for image deblocking", IEEE ICME, Vol. I, Mars 2003, pp. 541-544.
- [5] S. Minami, A. Zakhor. "An optimization approach for removing blocking effects in transform coding", IEEE Trans. on Circuit and System for Video Technology (CSVT), Vol. 5, No. 2, Apr. 1995, pp. 74-82.
- [6] Y. Yang, N. Galatsanos, "Removal of compression artifacts using projections onto convex sets and line modeling", IEEE Trans. on Image Processing, 6, October 1997.
- [7] S. Wu, H. Yan, Z. Tan, "An Efficient Wavelet-Based Deblocking Algorithm for Highly Compressed Images," IEEE Trans. CSVT, Vol. 11, No. 11, Nov. 2001, pp. 1193-1198.
- [8] R. Kountchev, M. Milanova, C. Ford, R. Kountcheva. "Multi-layer image transmission with inverse pyramidal decomposition", In Computational Intelligence for Modeling and Predictions, S. Halgamuge, L. Wang (Eds.), Vol. 2, Springer-Verlag, 2005, pp. 179-196.
- [9] M. Milanova, Vl. Todorov, R. Kountcheva. "Lossless data compression for image decomposition with recursive IDP algorithm". 17-th International Conf. on Pattern Recognition (ICPR), Cambridge, UK, 23-26 August 2004, pp. 823-826.
- [10] R. Kountchev, M. Milanova, Vl. Todorov, R. Kountcheva. "Adaptive fuzzy filter for the reduction of blocking artifacts in images compressed with IDP decomposition and JPEG". WSEAS Trans. on Signal Processing, Issue 7, Vol.2, July 2006, pp. 941-948, ISSN 1790-5022.

The Use of *Maple* in Computation of Generalized Transfer Functions for Nonlinear Systems

M. Ondera

Institute of Control and Industrial Informatics, Faculty of Electrical Engineering and Information Technology,
Slovak University of Technology in Bratislava, Ilkovičova 3, 812 19 Bratislava, Slovak Republic
Martin.Ondera@stuba.sk

Abstract - This paper deals with the recently re-discovered concept of generalized transfer functions of nonlinear control systems. It especially addresses the problems connected with the computation of the transfer functions, which are elements of a fraction field of non-commutative polynomials. An algorithm for calculation of generalized transfer functions for both continuous-time and discrete-time nonlinear systems based on the modified Gauss-Jordan elimination method is presented and its implementation in *Maple* computer algebra system is shown.

I. INTRODUCTION

The concept of generalized transfer functions of nonlinear systems (originally introduced in [12] and later independently re-developed in [6], [7] and [8]) is one of the very recent contributions to modern nonlinear control theory and, as such, is not yet included in traditional textbooks dealing with nonlinear control, e.g. [2], [3], [4]. It is based upon the algebraic approach to nonlinear control summarized in [1] and the theory of skew (i.e. non-commutative) polynomials over the field of meromorphic functions. The generalized transfer functions have many interesting properties and in many ways resemble the traditional linear transfer functions (e.g. the block algebra). However, one of the principal difficulties of the approach rests in a far more complicated computation of the generalized transfer functions, as they are elements of a fraction field of skew polynomials defined over meromorphic functions. Such polynomials are, of course, much more difficult to handle than common ones with real coefficients. Moreover, because of the same reason, specialized software tools, e.g. MATLAB's *Control System Toolbox*, developed for manipulating traditional linear transfer functions cannot be used either. This paper tries to cope with the problem using the *Maple* computer algebra system and its *OreTools* package.

The paper is organized as follows. Section II provides the background necessary for understanding the generalized transfer functions of nonlinear systems and briefly reproduces the main principles of the approach. Section III concentrates on the computational aspects and problems connected with manipulating algebraic objects, such as skew polynomials, fractions of these polynomials and matrices whose elements are fractions of skew polynomials, pointing out some of the differences between the commutative and the non-commutative case. The main attention is dedicated to the algorithm of matrix inversion using modified Gauss-Jordan elimination that plays an important role in the computation of the transfer functions from a state-space description of a nonlinear system. Section IV addresses the implementation

problems. It also provides a few illustrative examples. Section V briefly discusses the discrete-time case. Finally, section VI concludes the paper.

II. GENERALIZED TRANSFER FUNCTIONS OF NONLINEAR SYSTEMS

Probably all traditional textbooks dealing with nonlinear control (see e.g. [2], [3], [4]) state that there is no such thing as transfer functions of nonlinear systems. The main reason for this conservative opinion is that the Laplace transform, which plays a key role in the theory of linear transfer functions, is not valid for nonlinear systems. However, as was shown in [6], [7], [8] and [12], the Laplace transform is actually not the most crucial for establishing the transfer functions and, in spite of its absence in the nonlinear case, the transfer functions can be defined for a large class of nonlinear systems, too. Moreover, these transfer functions (throughout this paper referred to as the "generalized transfer functions") are in the linear case identical with those derived via Laplace transform. In this section, only the fundamental principles of the generalized transfer functions (and their necessary prerequisites) will be discussed. For other topics, such as the algebra of the generalized transfer functions or the invariance to regular static state transformations, see [6], [7] or [8]. Similarly, although the generalized transfer functions can be obtained from both state-space and input/output descriptions of nonlinear systems, only the first alternative will be considered in this paper.

A. Algebraic approach to nonlinear control systems

Let us consider a continuous-time nonlinear system described by a system of first-order differential equations of the form

$$\begin{aligned}\dot{x} &= f(x, u) \\ y &= h(x, u)\end{aligned}\tag{1}$$

where f and h are meromorphic functions (meromorphic functions are elements of a fraction field of a ring of analytic functions, see [1] for further details), $x \in R^n$, $u \in R^m$ and $y \in R^p$, respectively, denote the state, the input and the output of the system.

Let \mathcal{K} denote the field of meromorphic functions of x , u and a finite number of derivatives of u , i.e. each element of \mathcal{K} is a meromorphic function of the form

$$F(x, u, \dot{u}, \dots, u^{(k)}) ; k \geq 0\tag{2}$$

Let us define a derivative operator $\delta : \mathcal{K} \rightarrow \mathcal{K}$, such that

$$\begin{aligned}\delta x_i &= \dot{x}_i = f_i(x, u); i = 1, \dots, n \\ \delta u_j^{(k)} &= u_j^{(k+1)}; k \geq 0, j = 1, \dots, m \\ \delta F(x, u^{(k)}) &= \sum_{i=1}^n \frac{\partial F}{\partial x_i} \delta x_i + \sum_{j=0}^m \frac{\partial F}{\partial u_j^{(k)}} \delta u_j^{(k)}\end{aligned}\quad (3)$$

and a vector space spanned over \mathcal{K} by differentials of the elements of \mathcal{K} , i.e.

$$\varepsilon = \text{span}_{\mathcal{K}} \{d\xi; \xi \in \mathcal{K}\}. \quad (4)$$

The elements of this vector space (so-called one-forms) are vectors of the form

$$v = \sum_i \alpha_i d\xi_i; \alpha_i \in \mathcal{K}. \quad (5)$$

Let us define a differential operator d , acting from \mathcal{K} to ε

$$d : \mathcal{K} \rightarrow \varepsilon; dF = \sum_{i=1}^n \frac{\partial F}{\partial x_i} dx_i + \sum_{j=0}^m \frac{\partial F}{\partial u_j^{(k)}} du_j^{(k)} \quad (6)$$

and a derivative operator acting on ε (by abuse of notation also denoted by δ)

$$\delta : \varepsilon \rightarrow \varepsilon; \delta v = \sum_i [\delta(\alpha_i) d\xi_i + \alpha_i d(\delta\xi_i)]. \quad (7)$$

Finally, let us also define the recursive use of the derivative operators (3) and (7), i.e.

$$\begin{aligned}\delta^k F &= \delta(\delta^{k-1} F), \delta^0 F = F; F \in \mathcal{K}, k \geq 1 \\ \delta^k v &= \delta(\delta^{k-1} v), \delta^0 v = v; v \in \varepsilon, k \geq 1.\end{aligned}\quad (8)$$

Note: For the sake of further simplification of the notation, the “dot convention” is often used for the derivative operators instead of the δ symbol, that is, e.g. $\delta x_i = \dot{x}_i$, $\delta^2 u = \ddot{u} = u^{(2)}$, etc.

The equations (1)-(8) form the basics of the algebraic approach to nonlinear systems described in [1] but they are also necessary in order to understand the generalized transfer functions.

B. Some terms from pseudo-linear algebra

Pseudo-linear algebra is the study of common properties of differential and difference operators [5]. Some of its basic terms necessary for understanding the generalized transfer function concept will be explained here.

Let K be a field and $\sigma : K \rightarrow K$ an injective endomorphism of K , i.e.

$$\forall a, b \in K : \sigma(a+b) = \sigma(a) + \sigma(b) \wedge \sigma(ab) = \sigma(a)\sigma(b) \quad (9)$$

Then a mapping $\delta : K \rightarrow K$ satisfying

$$\begin{aligned}\delta(a+b) &= \delta(a) + \delta(b) \\ \delta(ab) &= \sigma(a)\delta(b) + \delta(a)b\end{aligned}\quad (10)$$

is called a *pseudo-derivation*. It is worthy of note that if σ is an identity map, i.e. if $\sigma(a) = a$ for any $a \in K$, then δ is a usual *derivation* acting on K .

The *left skew polynomial ring* given by σ and δ , usually denoted as $K[x; \sigma, \delta]$, is a (non-commutative) ring of polynomials in the indeterminate x over K with the usual addition and the (non-commutative) multiplication given by the commutation rule

$$xa = \sigma(a)x + \delta(a) \quad (11)$$

for arbitrary $a \in K$. Elements of such a ring are called *skew polynomials* or *non-commutative polynomials* [5], [11].

Let V be a vector space over K . A map $\theta : V \rightarrow V$ is called *pseudo-linear* if

$$\begin{aligned}\forall u, v \in V : \theta(u+v) &= \theta(u) + \theta(v) \\ \forall a \in K \forall u \in V : \theta(au) &= \sigma(a)\theta(u) + \delta(a)u.\end{aligned}\quad (12)$$

Again, let us also define this operation recursively, i.e.

$$\theta^k u = \theta(\theta^{k-1} u), \theta^0 u = u; u \in V, k \geq 1. \quad (13)$$

Skew polynomials can act on the vector space V and thus represent operators. We can define an action

$$\cdot : K[x; \sigma, \delta] \times V \rightarrow V; \left(\sum_{i=0}^n a_i x^i \right) \cdot u = \sum_{i=0}^n a_i \theta^i u; u \in V. \quad (14)$$

The symbol \cdot is usually omitted.

C. Generalized transfer functions

Since the derivative operator δ acting on \mathcal{K} (3) is a pseudo-derivation (with σ being an identity map) and, consequently, the derivative operator δ acting on ε (7) is a pseudo-linear map (σ is again an identity map), we can take advantage of the methods of pseudo-linear algebra (B.) and apply them to the one-forms defined in A. (see [6] or [7]).

If we consider a left skew polynomial ring over the field of meromorphic functions, with σ being an identity map, i.e. the (non-commutative) ring $\mathcal{K}[s; 1, \delta]$, then (14) will turn into

$$\cdot : \mathcal{K}[s; 1, \delta] \times \varepsilon \rightarrow \varepsilon; \left(\sum_{i=0}^n a_i s^i \right) \cdot v = \sum_{i=0}^n a_i \delta^i v; v \in \varepsilon \quad (15)$$

and the commutation rule (11) will be

$$sF = Fs + \dot{F}; F \in \mathcal{K} \quad (16)$$

As was proven in [6], [7] and [8], the derivative operator δ (3) and (7), respectively) and the differential operator d (6) are commutable, i.e.

$$\delta^k (dF) = d(\delta^k F) = dF^{(k)} \quad (17)$$

This is a fundamental result, which lets us introduce the generalized transfer functions of nonlinear control systems in the following fashion:

$$\begin{aligned}\dot{x} &= f(x, u) \\ y &= h(x, u)\end{aligned}\quad (18)$$

$$\begin{aligned}d\dot{x} &= Adx + Bdu \\ dy &= Cdx + Ddu\end{aligned}\quad (19)$$

where

$$A = \frac{\partial f(x,u)}{\partial x}, B = \frac{\partial f(x,u)}{\partial u}, C = \frac{\partial h(x,u)}{\partial x}, D = \frac{\partial h(x,u)}{\partial u}. \quad (20)$$

Considering the skew polynomial ring $\mathcal{K}[s;1,\delta]$, the mapping (15) and the property (17), we can write (19) as

$$\begin{aligned} (sI - A)dx &= Bdu \\ dy &= Cdx + Ddu \end{aligned} \quad (21)$$

and finally as

$$dy = [C(sI - A)^{-1}B + D]du = F(s)du \quad (22)$$

where $F(s)$ represents the *generalized transfer function* (or the *generalized transfer matrix* in the MIMO case) of the nonlinear system (18). The expression

$$F(s) = C(sI - A)^{-1}B + D \quad (23)$$

is formally identical with the well-known one that holds for the traditional transfer functions. However, it is important to keep in mind that now the matrices A, B, C, D are not constant but matrices whose elements are meromorphic functions and that the multiplication (15) is non-commutative, i.e. it has to be carried out strictly according to the commutation rule (16) and the order of the terms has to be maintained. As a result, the computation of the inverse matrix to $(sI - A)$ is much more complicated (see e.g. [7], [9] or [10]). Besides, further mathematical constructions are necessary to justify (22) and (23) – these will be introduced in the next section.

III. FRACTIONS OF SKEW POLYNOMIALS, CALCULATING THE GENERALIZED TRANSFER FUNCTIONS

Since the left skew polynomial ring $\mathcal{K}[s;1,\delta]$ defined in the previous section contains no zero divisors and satisfies the so-called left Ore condition (i.e. each two elements of $\mathcal{K}[s;1,\delta]$ have a common left multiple, see [7], [8], [9], [10] or [11]), it can be embedded to a non-commutative *fraction field* (also known as a *field of fractions* or a *quotient field*) by defining fractions as

$$\frac{a}{b} = b^{-1} \cdot a \quad (24)$$

where $a, b \in \mathcal{K}[s;1,\delta]$ and $b \neq 0$. Addition and multiplication of the fractions of skew polynomials are defined as

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{\beta_2 a_1 + \beta_1 a_2}{\beta_2 b_1}, \text{ where } \beta_2 b_1 = \beta_1 b_2 \quad (25)$$

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{\alpha_1 a_2}{\beta_2 b_1}, \text{ where } \beta_2 a_1 = \alpha_1 b_2 \quad (26)$$

These are the basic operations that have to be performed with corresponding elements of the matrices involved in (23) in order to calculate the generalized transfer function $F(s)$. Although generally elements of each of the matrices in (23) can be considered fractions of skew polynomials and, therefore, all the individual additions and multiplications can be carried out according to (25) and (26), in fact, there is no need to do everything in the strictly “non-commutative” way –

recall that the elements of the matrices A, B, C, D are actually meromorphic functions whose multiplication is commutative (the commutation rule (16) makes a difference only for expressions involving the indeterminate s).

Nevertheless, there still remains the problem how to invert the $(sI - A)$ matrix, i.e. a matrix whose elements are skew polynomials. Obviously, because of the non-commutative multiplication (15), we cannot use any of the known methods of matrix inversion directly as it was designed for conventional matrices. Besides, not only the multiplication (15) of individual elements is non-commutative; the matrix multiplication itself is non-commutative, too, which brings further difficulties – this “double” non-commutativity e.g. causes that the left inverse matrix is different from the right one (from (21) one can see that we are interested in the left inverse matrix in this case) and the same goes for the determinants. And yet, known methods of matrix inversion can be modified so as to handle the non-commutative multiplication properly.

For example, in [10] linear equations in non-commutative fields are discussed and left- and right-hand determinants are defined. These can be useful in modifying the method of matrix inversion based on a determinant and an adjugate matrix. However, according to our belief, a method which is even more easily adaptable to matrices of skew polynomials is the well-known Gauss-Jordan elimination (see e.g. [13]). The original algorithm requires only slight modifications, the only actual difference being the way how the operations with individual elements are performed in order to get zeros above and below the diagonal. The procedure is illustrated below.

Let us consider a 2nd-order case first. Our task is to calculate the left inverse of the matrix

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad (27)$$

where $a_{ij} \in \mathcal{K}[s;1,\delta]$, i.e. a matrix whose elements are skew polynomials. In accordance with the Gauss-Jordan elimination algorithm we will augment the 2nd-order identity matrix to the right of (27), forming the 2×4 block matrix

$$\begin{pmatrix} a_{11} & a_{12} & 1 & 0 \\ a_{21} & a_{22} & 0 & 1 \end{pmatrix}. \quad (28)$$

From this matrix we need to eliminate the a_{21} and a_{12} elements, i.e. we need to put zeros at the positions of a_{21} and a_{12} by means of elementary row operations. Let us deal with the a_{21} element first – in order to eliminate it we need to find skew polynomials $\beta, \gamma \in \mathcal{K}[s;1,\delta]$ such that

$$\beta a_{11} = \gamma a_{21}. \quad (29)$$

The equation (29) represents the left Ore condition where the value of βa_{11} and γa_{21} , respectively, is the common left multiple of the two elements a_{11} and a_{21} (obviously, in the commutative case, the β and γ would be $\beta = a_{21}$ and $\gamma = a_{11}$). With this done, we can perform the elimination on (28) and get

$$\begin{pmatrix} a_{11} & a_{12} & 1 & 0 \\ 0 & \gamma a_{22} - \beta a_{12} & -\beta & \gamma \end{pmatrix}. \quad (30)$$

In the same way we can eliminate the a_{12} element. The Ore condition corresponding to this case is

$$\phi(\gamma a_{22} - \beta a_{12}) = \phi a_{12} \quad (31)$$

and the resulting matrix will be as follows:

$$\begin{pmatrix} \phi a_{11} & 0 & \phi + \phi \beta & -\phi \gamma \\ 0 & \gamma a_{22} - \beta a_{12} & -\beta & \gamma \end{pmatrix}. \quad (32)$$

Finally, the left inverse of (27) is

$$\begin{pmatrix} \frac{\phi + \phi \beta}{\phi a_{11}} & \frac{-\phi \gamma}{\phi a_{11}} \\ \frac{-\beta}{\gamma a_{22} - \beta a_{12}} & \frac{\gamma}{\gamma a_{22} - \beta a_{12}} \end{pmatrix}. \quad (33)$$

However, it is often possible to simplify (33) further by cancelling the numerator and the denominator of each of the fractions by their greatest common left divisor.

Let us also sketch a few first steps of the 3rd-order case. The initial augmented matrix is

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & 1 & 0 & 0 \\ a_{21} & a_{22} & a_{23} & 0 & 1 & 0 \\ a_{31} & a_{32} & a_{33} & 0 & 0 & 1 \end{pmatrix}. \quad (34)$$

In the first step, we will eliminate the a_{21} and a_{31} elements. The corresponding left Ore conditions are

$$\begin{aligned} \beta_2 a_{11} &= \gamma_2 a_{21} \\ \beta_3 a_{11} &= \gamma_3 a_{31} \end{aligned} \quad (35)$$

and the matrix (34) after the elimination will be

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & 1 & 0 & 0 \\ 0 & \gamma_2 a_{22} - \beta_2 a_{12} & \gamma_2 a_{23} - \beta_2 a_{13} & -\beta_2 & \gamma_2 & 0 \\ 0 & \gamma_3 a_{32} - \beta_3 a_{12} & \gamma_3 a_{33} - \beta_3 a_{13} & -\beta_3 & 0 & \gamma_3 \end{pmatrix}. \quad (36)$$

Now we shall eliminate the $\gamma_3 a_{32} - \beta_3 a_{12}$ element using the condition

$$\phi(\gamma_2 a_{22} - \beta_2 a_{12}) = \phi(\gamma_3 a_{32} - \beta_3 a_{12}). \quad (37)$$

The resulting matrix (because of the space limitations the matrix is split and written in two lines) will be

$$\left| \begin{array}{ccc|ccc} a_{11} & a_{12} & & a_{13} & & & \\ 0 & \gamma_2 a_{22} - \beta_2 a_{12} & & \gamma_2 a_{23} - \beta_2 a_{13} & & & \\ 0 & 0 & \phi(\gamma_3 a_{33} - \beta_3 a_{13}) - \phi(\gamma_2 a_{23} - \beta_2 a_{13}) & & & & \\ & & 1 & 0 & 0 & & \\ & & -\beta_2 & \gamma_2 & 0 & & \\ & & -\phi \beta_3 + \phi \beta_2 & -\phi \gamma_2 & \phi \gamma_3 & & \end{array} \right|. \quad (38)$$

The $\gamma_2 a_{23} - \beta_2 a_{13}$, a_{13} and a_{12} elements can be eliminated analogically. The final inverse matrix will be a matrix of

fractions of skew polynomials whose numerators will be the elements of the right 3×3 block matrix and denominators the corresponding diagonal elements of the left 3×3 block matrix of the 3×6 matrix resulting from the elimination.

IV. MAPLE IMPLEMENTATION, ILLUSTRATIVE EXAMPLES

The *Maple* computer algebra system (version 9.5) provides support for pseudo-linear algebra through its *OreTools* package. The package contains commands for defining and manipulating Ore (i.e. skew, non-commutative) polynomials that simplify the calculation of the generalized transfer functions. Some of the useful commands in the package are:

- *SetOreRing* – define an Ore polynomial ring,
- *LCM*, *GCD* – compute the least common left or right multiple and the greatest common left or right divisor, respectively, of two or more Ore polynomials,
- *Quotient* – compute the right or left quotient of two Ore polynomials,
- *Add*, *Minus*, *Multiply* – add, subtract and multiply, respectively, two Ore polynomials,
- *Convertors[FromPolyToOrePoly]* – convert a polynomial to the corresponding *OrePoly* structure,
- *Convertors[FromOrePolyToPoly]* – convert an *OrePoly* structure to the corresponding polynomial.

On the other hand, the *OreTools* package cannot directly handle fractions of Ore polynomials nor matrices whose elements are fractions of Ore polynomials; therefore, custom procedures have to be programmed for this purpose.

Although, of course, there are no rigid rules as to the implementation of the fractions of Ore polynomials in *Maple*, in our opinion it is advantageous to:

1. represent the fraction as a list with two elements of the *OrePoly* type (the numerator and the denominator),
2. create procedures for the two basic operations with fractions of Ore polynomials, i.e. the addition (25) and the multiplication (26) of the fractions,
3. create a procedure for inverting a matrix of Ore polynomials via the modified Gauss-Jordan elimination method, as described in the previous section,
4. create the main procedure for calculation of a generalized transfer function (23) from a state-space description of a nonlinear system (18) that calls the two above procedures,
5. convert the result (the generalized transfer function) from the *OrePoly* form to the usual transfer-function representation (i.e. fraction of regular polynomials in s).

Because of the space limitations, the *Maple* source code cannot be presented completely. However, some of the procedures are listed in the appendix and the calculation of generalized transfer functions in *Maple* is also illustrated by the examples below.

Example 1: Let us compute the generalized transfer function of the nonlinear system

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 u \end{pmatrix} \quad (39)$$

$y = x_1$

From (20) it follows that

$$A = \begin{pmatrix} 0 & 1 \\ u & 0 \end{pmatrix}; B = \begin{pmatrix} 0 \\ x_1 \end{pmatrix}; C = (1 \ 0); D = (0) \quad (40)$$

To be able to calculate the generalized transfer function (23) we need to find the left inverse of the matrix $(sI - A)$. Using the modified Gauss-Jordan elimination algorithm described in the section III we can find out that the left inverse is

$$(sI - A)^{-1} = \begin{pmatrix} \frac{s}{s^2 - u} & \frac{1}{s^2 - u} \\ \frac{u}{s^2 - \frac{\dot{u}}{u}s - u} & \frac{s - \frac{\dot{u}}{u}}{s^2 - \frac{\dot{u}}{u}s - u} \end{pmatrix} \quad (41)$$

Finally, the generalized transfer function will be

$$F(s) = \frac{x_1}{s^2 - u} \quad (42)$$

The generalized transfer function can also be computed using a custom procedure (named *TransFunc*) implemented in *Maple*:

```
> f1:=Matrix([[x2],[x1*u]]);
> h1:=Matrix([x1]);
> Fs1:=TransFunc(f1,h1,1);

f1 := [x2]
      [x1 u]

h1 := [x1]

Fs1 := [x1(t)
      -u(t) + s^2]
```

Example 2: Let us compute the generalized transfer matrix of the nonlinear MIMO system

$$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{pmatrix} = \begin{pmatrix} x_3 u_1 \\ u_1 \\ u_2 \end{pmatrix} \quad (43)$$

$y = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

Similarly as in the previous case, we can again take advantage of the *TransFunc* procedure implemented in *Maple*:

```
> f2:=Matrix([[x3*u1],[u1],[u2]]);
> h2:=Matrix([[x1],[x2]]);
> Fs2:=TransFunc(f2,h2,2);

f2 := [x3 u1]
      [u1]
      [u2]
```

$$h2 := \begin{bmatrix} x1 \\ x2 \end{bmatrix}$$

$$Fs2 := \begin{bmatrix} \frac{x3(t)}{s} & \frac{u1(t)}{\left(\frac{d}{dt}u1(t)\right)s + s^2} \\ \frac{1}{s} & 0 \end{bmatrix}$$

V. THE DISCRETE-TIME CASE

Although originally developed for the continuous-time case, the approach can be applied to discrete-time nonlinear systems as well (a comprehensive description is available in [9]). Most of the definitions and properties introduced in the previous sections remain the same, however, certain constructions have to be reformulated in the discrete-time case. These will be mentioned below (the notation used will be slightly different from the one introduced in [9]).

Let us consider a discrete-time nonlinear system described by a system of first-order difference equations of the form

$$\begin{aligned} x(k+1) &= f(x(k), u(k)) \\ y(k) &= h(x(k), u(k)) \end{aligned} \quad (44)$$

where the symbols f , h , x , u , y stand for the same as in the continuous-time case (1). The discrete-time case analogies to (2) and (3) are

$$F(x(k), u(k), u(k+1), \dots, u(k+l)); l \geq 0 \quad (45)$$

and $\sigma: \mathcal{K} \rightarrow \mathcal{K}$

$$\begin{aligned} \sigma x_i(k) &= x_i(k+1) = f_i(x(k), u(k)); i = 1, \dots, n \\ \sigma u_j(k) &= u_j(k+1); j = 1, \dots, m \\ \sigma F(x(k), u(k+l)) &= F(\sigma x(k), \sigma u(k+l)); l \geq 0 \end{aligned} \quad (46)$$

Note that σ (46) is a shift operator, whereas δ (3) was a derivative operator. The other two constructions that have to be adjusted for use with discrete-time systems are the definitions of the differential operator (6), $d: \mathcal{K} \rightarrow \mathcal{E}$:

$$dF = \sum_{i=1}^n \frac{\partial F}{\partial x_i(k)} dx_i(k) + \sum_{j=0}^m \frac{\partial F}{\partial u_j(k+l)} du_j(k+l) \quad (47)$$

and the derivative (now shift) operator acting on \mathcal{E} (7):

$$\sigma: \mathcal{E} \rightarrow \mathcal{E}; \sigma v = \sum_i \sigma(\alpha_i) d(\sigma \xi_i) \quad (48)$$

Similarly as in the continuous-time case we will consider a left skew polynomial ring over the field of meromorphic functions \mathcal{K} . However, σ will now be the shift operator (46) and $\delta = 0$, which can be considered a trivial pseudo-derivation according to (10). Therefore, we can denote the ring as $\mathcal{K}[z; \sigma, 0]$, define the \cdot operator (14) as

$$\cdot: \mathcal{K}[z; \sigma, 0] \times \mathcal{E} \rightarrow \mathcal{E}; \left(\sum_{i=0}^n a_i z^i \right) \cdot v = \sum_{i=0}^n a_i \sigma^i v; v \in \mathcal{E} \quad (49)$$

and the commutation rule (11) as

$$zF = \sigma(F)z; F \in \mathcal{K} \quad (50)$$

These are the most important differences between the continuous- and the discrete-time case, the rest of the constructions either remains unchanged, e.g. (25)–(26), or the necessary modifications are obvious, e.g. (18)–(23). As to the *Maple* implementation, apart from the (optional) change of notations (e.g. z instead of s), the only real difference is the second parameter of the *SetOreRing* command, which has to be ‘shift’ in the discrete-time case.

Example 3 (adapted from [9]): Let us compute the generalized transfer function of the discrete-time nonlinear system

$$\begin{pmatrix} x_1(k+1) \\ x_2(k+1) \end{pmatrix} = \begin{pmatrix} x_2(k) + u^2(k) \\ u(k) \end{pmatrix} \quad (51)$$

$$y(k) = x_1(k)$$

We can solve the problem using a custom *Maple* procedure named *TransFuncDisc*:

```
> f1:=Matrix([[x2+u^2],[u]]);
> h1:=Matrix([[x1]]);
> Fz1:=TransFuncDisc(f1,h1,1);
f1 := [x2 + u^2]
u
h1 := [x1]
Fz1 := [1 + 2 u(k + 1) z]
z^2
```

VI. CONCLUSION

In this paper the problem of computation of generalized transfer functions for nonlinear systems from a state-space description was addressed. The *Maple* computer algebra system and its *OreTools* package were used for the purpose. This is one of the first attempts to implement the generalized transfer functions on a computer in some way but certainly not the last one – in our opinion, computer implementation can stimulate the further development and increase the popularity of the generalized transfer function theory itself. Therefore, our future goals include both the enhancement of the existing *Maple* procedures as well as their migration to *MATLAB*, which is probably a more popular tool within the control engineering community.

APPENDIX

Two custom *Maple* procedures, *AddOreFractions* and *MulOreFractions*, for addition (25) and multiplication (26), respectively, of two fractions of Ore polynomials are listed below.

```
AddOreFractions:=proc(f1,f2::list)
local beta,beta1,beta2,S;
use OreTools in
S:=SetOreRing(t,'differential');
beta:=LCM['left'](f1[2],f2[2],S);
beta2:=Quotient['right'](beta,f1[2],S);
beta1:=Quotient['right'](beta,f2[2],S);
```

```
[Add(Multiply(beta2,f1[1],S),
      Multiply(beta1,f2[1],S));
   Multiply(beta2,f1[2],S));
end use;
end proc:
```

```
MulOreFractions:=proc(f1,f2::list)
local beta,alpha1,beta2,S;
use OreTools in
S:=SetOreRing(t,'differential');
if f1[1]<>OrePoly(0) then
  beta:=LCM['left'](f1[1],f2[2],S);
  beta2:=Quotient['right'](beta,f1[1],S);
  alpha1:=Quotient['right'](beta,f2[2],S);
  [Multiply(alpha1,f2[1],S),
   Multiply(beta2,f1[2],S)];
else
  [OrePoly(0),OrePoly(1)];
end if;
end use;
end proc:
```

These procedures form an element-oriented basis for the matrix-oriented procedures *InvOreMatrix* (left inverse of a matrix of Ore polynomials) and *TransFunc* (calculation of a generalized transfer function), which are not listed here because of space limitations.

ACKNOWLEDGMENTS

This work was supported in part by the Slovak Scientific Grant Agency (VEGA) Project No. 1/3089/06 "Development and integration of methods of the nonlinear systems theory". The author would also like to thank M. Halás for his valuable comments and suggestions.

REFERENCES

- [1] G. Conte, C. H. Moog, and A. M. Perdon, *Nonlinear Control Systems: An Algebraic Setting*. London: Springer, 1999.
- [2] A. Isidori, *Nonlinear Control Systems: An Introduction*, 2nd ed. New York: Springer, 1989.
- [3] J. J. Slotine, and W. Li, *Applied Nonlinear Control*. New Jersey: Prentice Hall, 1991.
- [4] M. Huba, *Nonlinear Systems [in Slovak]*. Bratislava: Vydavateľstvo STU, 2003.
- [5] M. Bronstein, and M. Petkovšek, "An introduction to pseudo-linear algebra," *Theoretical Computer Science*, 157, pp. 3–33, 1996.
- [6] M. Halás, "Quotients of Noncommutative Polynomials in Nonlinear Control Systems", In: *Proceedings of 18th European Meeting on Cybernetics and Systems Research*, Vienna, Austria, 2006.
- [7] M. Halás, and M. Huba, "Symbolic Computation for Nonlinear Systems Using Quotients Over Skew Polynomial Ring", In: *14th Mediterranean Conference on Control and Automation*, Ancona, Italy, 2006.
- [8] M. Halás, "An Algebraic Framework Generalizing the Concept of Transfer Functions to Nonlinear Systems," to appear in *Automatica* (provisionally accepted).
- [9] M. Halás, and Ü. Kotta, "Extension of the Concept of Transfer Function to Discrete-Time Nonlinear Control Systems, submitted to *European Control Conference 2007*.
- [10] O. Ore, "Linear Equations in Non-Commutative Fields," *Annals of Mathematics*, 32, pp. 463-477, 1931.
- [11] O. Ore, "Theory of Non-Commutative Polynomials," *Annals of Mathematics*, 34, pp. 480-508, 1933.
- [12] Y. Zheng, and L. Cao, "Transfer Function Description for Nonlinear Systems," *Journal of East China Normal University (Natural Science)*, 2, pp. 15–26, 1995.
- [13] "Gaussian elimination," "Gauss-Jordan elimination," *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Gaussian_elimination.

A Game Theoretic Approach to Regulating Mutual Repairing in a Self-Repairing Network

Masakazu Oohashi¹ and Yoshiteru Ishida^{1, 2}

¹ Department of Knowledge-Based Information Engineering,

Toyohashi University of Technology,
Tempaku, Toyohashi, 441-8580 Japan

² Intelligent Sensing System Research Center
Toyohashi University of Technology,
Tempaku, Toyohashi, 441-8580 Japan

Abstract-When *Cooperate* and *Defect* of the Spatial Prisoner's dilemma are corresponded to repair and not repair in a self-repair network, a major problem is that agents stuck at a Nash equilibrium of mutual defection, and the network ended in all abnormal states. To resolve the problem, we have studied game theoretic regulation schemes of selfish agents. Payoff for each agent is modified to include not only its own resources left but all the resources of the neighbor agents.

I. INTRODUCTION

When information systems grow into large-scale systems such as the Internet, autonomous decentralized regulation may be needed for regulation and maintenance of the system. Recovery oriented computing (ROC) has been studied [1] with such motivations. We also proposed a self-repairing network, and studied its mutual repairing schemes: one uniform repairing scheme by which all the agents repair other agents with a uniform rate; another strategic repair scheme by which agents determine the rate based on the local information they get from the neighbor agents.

The uniform repairing scheme has been modeled by a probabilistic cellular automaton (pCA) [2] which turns out to be a generalization of the well known model [3]. Self-repairing cellular automata have been attracting a broad attention including in the field of statistical physics [4]. A critical phenomenon has been observed for such models, which will suggest the rate by which eradication of abnormal agents is possible.

As a more sophisticated scheme that is suitable for autonomous selfish agents: a strategic repair scheme has been studied [5]. The strategic repair incorporates a game theoretic framework known as Spatial Prisoner's Dilemma.

When the self-repair is done in an autonomous distributed manner, each agent does not voluntarily repair other agents to save their own resources, thus leaving many abnormal agents not repaired. This situation is similar to the dilemma that would occur in the Prisoner's Dilemma. Thus, we use an approach of a spatial version of Prisoner's Dilemma [6-10] for emergence of cooperative collectives and for controlling copying to save resources.

While this paper amounts to a macroscopic studies on the network with many interacting agents, another paper in this volume [13] amounts to a microscopic analysis focusing on conditions when two interacting agents have incentive to cooperate (i.e. mutually repair).

Section II explains motivations and background of the models. The network cleaning problem and the self-repair network model will be presented. Simulations with uniform repair rate will be briefly explained for comparison with the subsequent models. Section III proceeds to the strategic repair for the self-repair network. Two different strategic repair schemes (one involving spatial strategies and another with modified payoff) will be presented and compared. Section V will compare the strategic repair with uniform repair.

II. NETWORK CLEANING WITH UNIFORM REPAIR RATE

A. Network Cleaning Problem

We consider the possibility of cleaning up the network by mutually copying. The repair by copying in information systems is also the "double edged sword" and it should be identified when the network can really eradicate abnormal elements from the system. We consider a probabilistic CA to model the situation where computers in a LAN mutually repair by copying their content. Since the problem involves the "double edged sword" leading to a critical phenomenon, repairs have to be decided giving consideration to the resources used and remained in the system and the network environment.

B. A Self-Repair Network Model

The self-repairing network consists of agents capable of repairing other agents connected.

In the model by pCA [2], agents do not have a failure rate and do not become abnormal by themselves, however, the agents in the model here implement failure rate (λ). Repairing is controlled by repair rate (γ). When repair is carried out, it will be successful with repair success rate (α), and the repaired agents are made normal. The adverse impact by the abnormal agents is implemented as raising the failure rate (by the amount of damage rate δ) of the repaired agents (when repaired by the abnormal agents). Further, the agents are

assumed to use some resources (R_λ) in repairing. This amounts to a cost for cooperation, and hence motivates selfish agents for free-riding. The agents have to do the tasks assigned to them; but without doing repair, abnormal agents increase and hence the performance in the system decreases; hence a dilemma. The agent is able to repair more than one agent, provided that the quantity of maximum resource R_{\max} is not exceeded. We consider the available resource (the resource that is not used for repairing) as score of an agent.

Throughout this paper, simulations are conducted in the following parameters.

TABLE I
List of Parameters for Simulations

	Description	Value
L x L	Size of the Space	50 x 50
N	Number of Agents	2500
$N_f(0)$	Initial Number of Abnormal Agents	100
λ	Failure Rate	0.01
γ	Repair Rate	0.01
α	Repair Success Rate	0.1
δ	Damage Rate	0.1
r	Strategy Update Cycle	100
R_{\max}	Maximum Resource	25
R_λ	Resource Used for Repairing	1

C. Simulations with Uniform Repair Rate

Simulations are conducted in a 2-dimensional lattice shown in Figure 1. To contrast the results with the selfish repair rate control in Section III, simulations are conducted for the above



Figure 1. An initial configuration of agents. Black color indicates a normal agent and gray color an abnormal agent.

self-repair network with a uniform repair rate.

This model has a threshold for the damage rate δ as shown in Figure 2. Over the threshold of the damage rate, all the agents become abnormal.

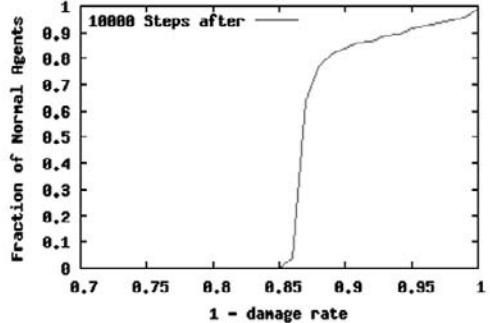


Figure 2.
Fraction of
normal agents
when damage
rate varies.

III. REPAIR RATE CONTROL BY SPATIAL PRISONER'S DILEMMA: A MACRO MODEL

Although actions of agents in the above models are controlled by a uniform repair rate, selfish agents in the current model will determine their actions by accounting their payoffs. To implement this selfish framework, we first introduce a Spatial Prisoner's Dilemma.

A. Spatial Prisoner's Dilemma as an Autonomous Control Mechanism

Spatial Prisoner's Dilemma has been studied to investigate when, how, and why the cooperation emerges among selfish agents when they are spatially arranged, hence interactions are limited only to their neighbors. In SPD pioneered by [8], each player placed at each lattice of the two-dimensional lattice. Each player has an action and a strategy, and receives a score. Each player plays PD with the neighbors, and changes its strategy to the strategy that earns the highest total score among the neighbors. We will use this deterministic SPD. In stochastic version, the agent will decide its action based on probability proportional to the difference between its own payoff and the highest payoff in the neighbors' agents (similarly to the replicator dynamics [11,12]).

As shown in Fig. 2, framework of selfish agents with only C and D actions is good enough. This situation could be rescued by extending payoffs as in the microscopic model; however, since the macroscopic models allow other extensions, spatial extension in particular, we focus on the spatial one for enhancement and promotion of cooperation.

The SPD is generalized by introducing spatial strategy [10]. Spatial strategy determines the next action dependent upon the

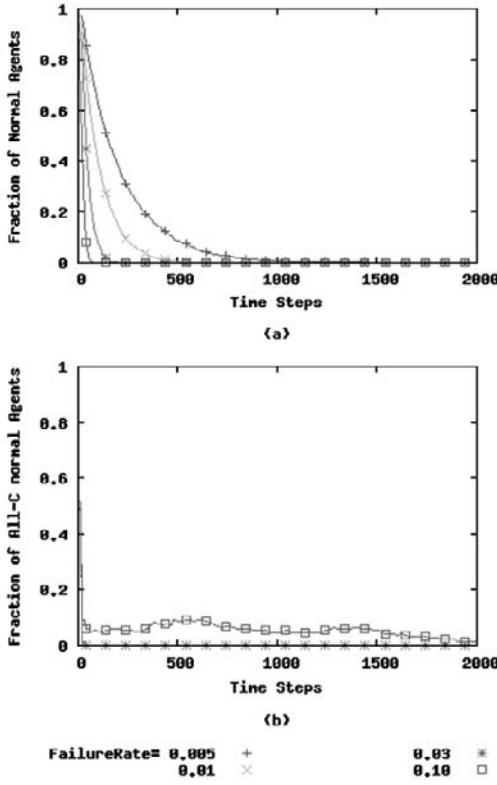


Figure 3. SPD with simple payoff measured by available resources of the agent. Parameters are: failure rate 0.005 - 0.10, repair success rate 0.1, damage rate 0.1, strategy update cycle 20, max resources 9, cost for repair 1. Randomly chosen 100 agents are made abnormal and randomly chosen a half of agents takes all-D initially.

spatial pattern of actions in the neighbors. Score is calculated by summing up all the scores received from PD with 8 neighbor players. After r (strategy update cycle) steps of interactions with neighbors, the strategy will be chosen from the strategy with the highest score among the neighbors.

To specify a spatial strategy, actions of all the neighbors and the player itself must be specified. For simplicity, we restrict ourselves on a “totalistic spatial strategy” that depend on the number of D (defect) action of the neighbor, not on their positions.

In the simulations shown in Figure 3, only two trivial strategies are used: All-C and All-D. However, the following simulations (Figure 4) use kD strategy instead of All-C. In the kD strategy, the agent does the action of C if the number of D agents is less than k ; and it does the action of D if the number of D agents is greater or equal to k . The kD strategies amount to a spatial generalization of well-known TFT, since k indicates how many D's are tolerated in the neighbors.

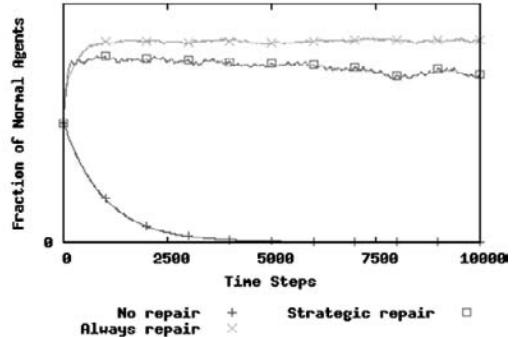


Figure 4. Time evolution of the fraction of abnormal agents when strategic repair with spatial strategies kC are compared with two extreme repairs: All-D (no repair) and All-C (always repair). Parameters are as in TABLE I except repair success rate 0.01, strategy update cycle 200, maximum resources 8 and resources used for repairing 2. Randomly chosen a half of agents are made abnormal initially.

In the simulation shown in Figure 3, All-D will eradicate All-C strategies; hence all the agents will remain silent without repairing any agents. Thus, eventually all the agents will be abnormal with a positive failure rate. We studied two mechanisms for preventing all the agents from taking D actions and from being abnormal:

- Spatial strategies involving copying the strategy of repairing agent when repairing.
- Modified payoff incorporating not only its own resources left but all the resources in the neighbor.

The one with spatial strategies will be explained in the following subsection B, while the one with modified payoff will be presented in the subsection C.

B. Repair Rate Control with Spatial Strategies

This subsection investigates a repair rate control by spatial strategies. When the agent copies its content (software that can be copied and be contaminated), the strategy of the agent is also copied. Thus, the strategy will be changed at copying in addition to every strategy update cycle. This strategy copying will bias strategies toward All-C, since All-C (not All-D) will repair by copying the content and the strategy (All-C) is copied at the same time.

Computer simulations are conducted for three strategies: a spatial strategy kC , All-D (no repair), and All-C (always repair). Figure 4 plots the time evolution of the fraction of abnormal agents. A half of agents, randomly chosen, are set to be abnormal in these three strategies initially. It can be observed that strategic repair (kC) can reduce abnormal agents with a performance comparable to always repair (All-C).

C. Repair Rate Control with Systemic Payoff

This subsection deals with a repair control by allowing agents to take only All-C (repair) or All-D (not repair) as in the

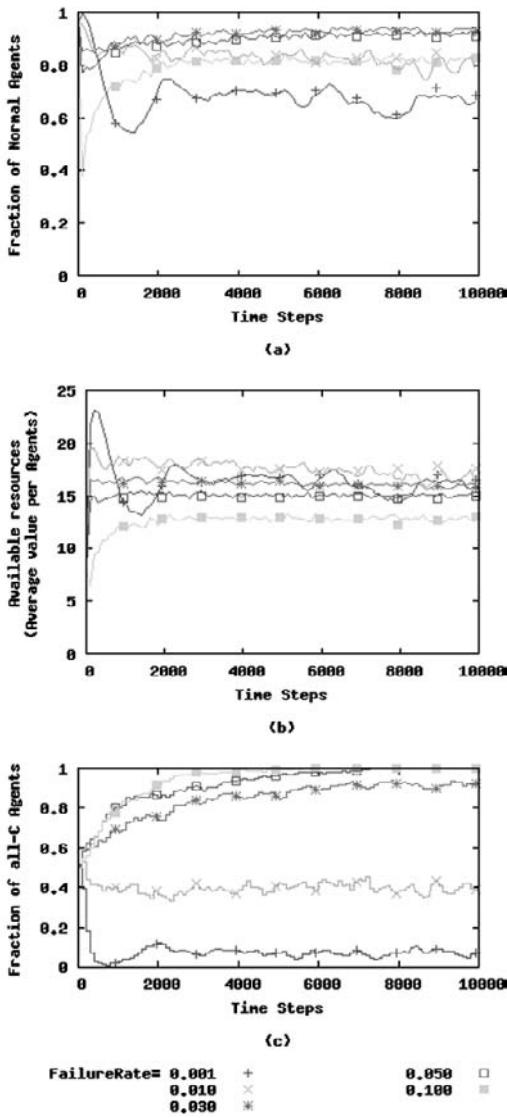


Figure 5. SPD with strategic control with the modified payoff (available resources of the neighbor agents are added to payoff) (a) fraction of normal agents, (b) available resources, (c) fraction of All-C agents. Parameters are as in TABLE I and initial configuration with half of All-D agents and 100 failure agents randomly chosen.

simulations shown in Figure 3. However, the payoff if modified to include all the resources in the neighbor. This modified payoff has an impact on making agents more attentive by caring neighbor agents that would possibly repair the agent in the future.

Simulations are conducted for the strategic repair with modified payoff: not only resources left for the agent but the resources of the neighbor agents are added into the payoff. Figure 5 plots the time evolution of the fraction of normal agents (a), available resources left in the system (b), and the fraction of agents with All-C (c).

It can be observed that this strategic repair with modified payoff can adapt to the failure rate: when the failure rate is low fraction of All-C agents is kept small (Figure 5 (c)) limiting unnecessary repair, while when the failure rate is high the fraction of All-C agents is also made high. As a result of this flexible change of repair rate, the fraction of normal agents (Figure 5 (a)) as well as available resources (Figure 5 (b)) are made stable and the difference of failure rate is absorbed.

Figure 6 shows a snapshot of agent configurations at 4663 time step when simulation is carried out with the same condition as that in Figure 5. Fraction of All-C agents (cooperators) is small compared to All-D agents at this snapshot, which can be also observed in Figure 5 (c). A black cluster of Abnormal Defectors in the center is being corroded by repairing by Normal Cooperators (light gray), leaving Normal Defector (white) at the perimeter of the cluster. Dotted Abnormal Defectors (black) appear in the sea of Normal Defectors (white) due to failure and no repair.

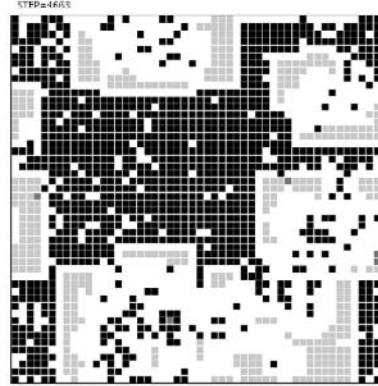


Figure 6. A snapshot of agent configurations at 4663 time step when simulation is carried out with the same condition as that in Figure 5, failure rate 0.001. Light gray is Normal Cooperator, dark gray is Abnormal Cooperator, white is Normal Defector and black is Abnormal Defector.

IV. DISCUSSIONS

The strategic control with the modified payoff (available resources of the neighbor agents are added to payoff) has been compared with the control by a uniform rate.

Figures 7, 8, and 9 are simulation results with max resource varied: 25, 13, and 9 respectively. Changes of the max resource will make the relative cost of repair. At each figure, fraction of normal agents (a) as well as available resources (b) are

monitored. Available resources, which are correlated with the fraction of normal agents, are rough measure of performance.

It can be first observed that performance of the uniform rate control varies in these three simulations, while that of the strategic rate control shows reasonable performance. For example, the available resources by the uniform rate control with repair rate 0.5 is worst when failure rate 0.1 and max resource 25 (Figure 7 (b)), however, it is the best when max resource 12 (Figure 8 (b)) and 9 (Figure 9 (b)).

Thus, the comparison of performance between the uniform and strategic rate control can be summed as:

- The strategic rate control is neither best nor worst;
- The strategic control is robust against parameter changes.

The simulations indicate that an appropriate uniform rate could be set when parameters were identified correctly. However, it is often the case that parameters are difficult to

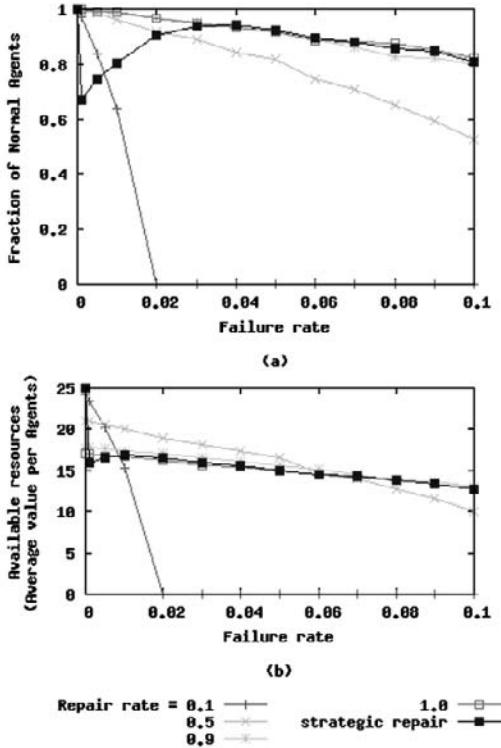


Figure 7. Comparison between strategic control with the modified payoff (available resources of the neighbor agents are added to payoff) and control with uniform rate (a) fraction of normal agents and (b) available resources.
Parameters are as in TABLE I and initial configuration with a half of All-D agents and 100 failure agents.

identify, or they may change dynamically. In such cases, strategic rate control can be used.

The above discussion hold only when the damage rate is below threshold (see Figure 2). Although not shown in these Figures 7, 8, and 9, the strategic rate control does not necessarily show the robust performance when the damage rate exceeds the threshold.

So far, we have not yet identified the cause for degrading performance of the strategic rate control when the damage rate exceeds the threshold. In fact, many things remained to be studied for the strategic repair when the threshold is exceeded.

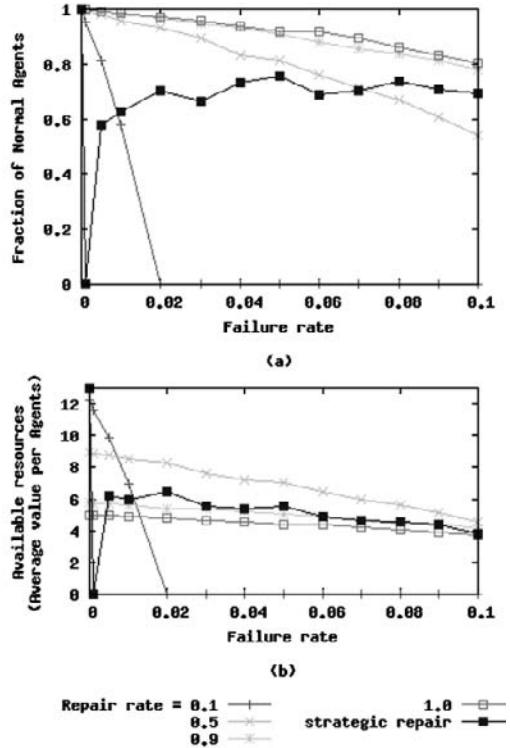


Figure 8. Comparison between strategic control with the modified payoff (available resources of the neighbor agents are added to payoff) and control with a uniform rate (a) fraction of normal agents and (b) available resources.
Parameters are the same as the previous simulations shown in Figure 7 except the max resource is 13.

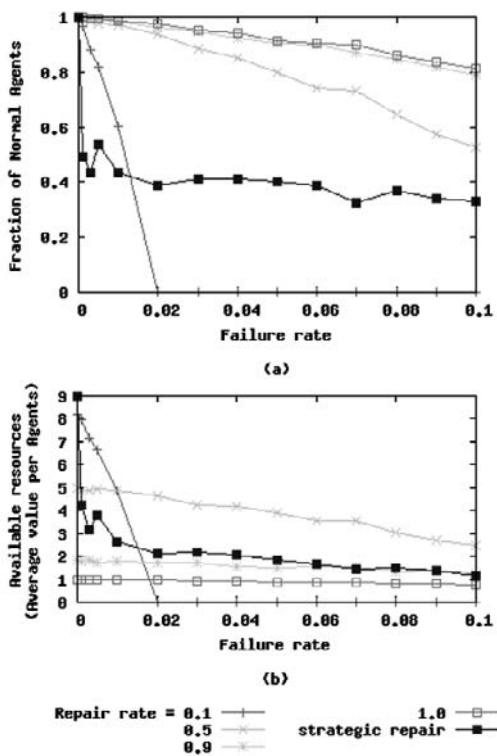


Figure 9 Comparison between strategic control with the modified payoff (available resources of the neighbor agents are added to payoff) and control with a uniform rate (a) fraction of normal agents and (b) available resources.

Parameters are the same as the previous simulations shown in Figure 7 except the max resource is 9.

V. CONCLUSIONS

It has been shown that strategic repair that leaves decision of repairing neighbor agents to each selfish agent. This game theoretic framework is suitable for autonomous and distributed decision-making context that is again suitable for regulation and maintenance of large-scale information systems.

A major problem of using spatial prisoner's dilemma in regulating repair rate of agents is that agents tend to remain silent and stuck at the Nash equilibrium of mutual defection.

This paper presents a new resolution on this problem: that is involving more systemic payoff incorporating not only its own resources left but all the resources in the neighbor. With this modified payoffs, agents not only have an adaptive decision-making dependent on the environmental parameters such as failure rate and damage rate but have more favorable resource allocation when compared with a uniform regulation of repair rate.

ACKNOWLEDGMENT

This work was supported in part by Grants-in-Aid for Scientific Research (B) 16300067, 2004. This work was partly supported also by the 21st Century COE Program "Intelligent Human Sensing" of the Ministry of Education, Culture, Sports, Science and Technology of Japan.

References

- [1] Brown, A. and Patterson, D.: Embracing Failure: A Case for Recovery-Oriented Computing (ROC), High Performance Transaction Systems Workshop (TTPS '01) (2001)
- [2] Ishida, Y.: A Critical Phenomenon in a Self-Repair Network by Mutual Copying, LNAI, (2005) this volume
- [3] Domany, E. and Kinzel, W.: Equivalence of cellular automata to Ising models and directed percolation, Phys. Rev. Lett. 53 (1984) pp. 311
- [4] Gacs, P.: Reliable Cellular Automata with Self-Organization, J. Stat. Phys. 103(2001), pp. 45-267
- [5] Ishida, Y. and Mori, T.: A Network Self-repair by Spatial Strategies in Spatial Prisoner's Dilemma, Knowledge-Based Intelligent Information and Engineering Systems (KES'2005), Lecture Notes in Artificial Intelligence (LNAI 3682), 79-85 (2005)
- [6] Matuo, K. and Adachi, N. : Metastable Antagonistic Equilibrium and Stable Cooperative Equilibrium in Distributed Prisoner's Dilemma Game, Proc. Int. Symp. Syst. Res. Infor. Cybern. (1989)
- [7] Boyd, R.: Mistakes Allow Evolutionary Stability in the Repeated Prisoner's Dilemma Game, J. theor. Biol., vol. 136 (1989) 47-56
- [8] Nowak, M.A. and May, R.M.: Evolutionary games and spatial chaos, Nature, Vol. 359 (1992) pp.826-829
- [9] Grim, P.: The greater generosity of the spatialized prisoner's dilemma, J. theor. Biol., Vol. 173, (1995) pp. 353-359
- [10] Ishida, Y. and Mori, T.: Spatial Strategies on a Generalized Spatial Prisoner's Dilemma, J. of Artificial Life and Robotics, (2005) to appear
- [11] Taylor, P. D., and Jonker, L. B.: Evolutionarily Stable Strategies and Game Dynamics Math. Biosci. 40, (1978) pp. 145-156
- [12] Hofbauer, J. and Sigmund, K.: Evolutionary game dynamics Bull. Am. Math. Soc. 40, (2003) pp. 479-519
- [13] Ishida, Y.: A Game Theoretic Analysis on Incentive for Cooperation in a Self-Repairing Network, International Joint Conferences on Computer, Information and Systems Sciences and Engineering (CIS2E 06), (2006) in this volume

An Automated Self-Configuring Driver System for IEEE 802.11b/g WLAN Standards

Mathieu K. Kourouma and Ebrahim Khosravi
Southern University and A&M College
Department of Computer Science
Baton Rouge, LA 70813

Abstract – This paper presents a prototype for an automated self-configuring driver system (ASDS) for the IEEE 802.11 WLANs. This software system provides a new way of running multiple IEEE 802.11 wireless standards on laptops and other mobile devices on the fly anywhere around the world.

Most current drivers for 802.11 standards are static; that is during the installation, the installer has to specify the region or country in which the laptop or PC will be used. This requirement, as we will explain later, is due to the multitude radio regulations in different countries. To be more specific, we consider the drivers from NETGEAR.

Keywords: IEEE 802.11b/g, ASDS, Netgear, FCC, ART

I. INTRODUCTION

The IEEE 802.11 or the Wi-Fi standards, represents a set of wireless LAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee, IEEE 802. The 802.11 followed by some specific letter denotes the varieties of standards. The 802.11b was the first widely accepted wireless networking standard, followed by 802.11a and 802.11g. The current 802.11a/b/g WLAN standards offer the convenience of wireless connections with adequate performance for most of today's wireless networking applications. The standard 802.11n is under development which targets higher data throughput as the next generation of wireless emerges [1]. The 802.11b and 802.11g standards use the 2.4 GHz band, operating in the United States under Part 15 of the Federal Communication Commission (FCC) Rules and Regulations. Because of this choice of frequency band, 802.11b and 802.11g equipment can incur interference from Bluetooth devices, cordless telephones, and microwave ovens, and other appliances operating in this frequency band. The 802.11a standard uses the 5 GHz band, and is therefore not affected by the above mentioned products which operated at 2.4 GHz. 802.11a/b/g standards provide wireless connectivity in the home, office and some commercial establishments.

Most of the early dual-band 802.11a/b products became dual-band/tri-mode, supporting a, b, and g in a single mobile adapter card or access point. Articles [2] and [3] discuss the transceiver designs for 802.11a/b/g. Note that these articles

discuss the hardware issues implementation of these IEEE standards. Many 802.11 WLAN products (wireless PC card adapters, router, access point, wireless USB, etc) from a number of companies such NETGEAR, Intel, Sony, CISCO, Dell, Linksys, etc available in today's market come in combination of 802.11.b/g or 802.11.a/b/g in order to allow more flexibility. In order to narrow down our studies and, that is the design of an automated self-configuring driver system for IEEE 802.11b/g, the most widely used standard, we mainly focus on a specific product, the Wireless PC (WPC) card, which connect to the PCMCIA slot, from the NETGEAR [4]. There is no specific reason why we are choosing this company's product. But if you would, we chose this product because of our many years of experience using it, of course along with many other products. However, regardless of the type of products and whether the WPC card is internal or external (can be easily removed), there are two main components, which are provided in the Netgear Wireless PC Card product package shipped to consumers, to be considered: (a) the WPC card and (b) the driver and configuration utility software CD. For the internal WPC card, the installation is done by the manufacturer of the laptop, notebook, or PC as opposed to the external WPC card, whose installation is carried by the user. The installation process in either case is static and is based on the country in which the WPC card is installed. Figure 1 shows some sections of the Netgear PC Card WG51T driver installation. Figure 1a shows the starting point of the card installation after the software installation has completed. Figure 1b and Figure 1c show the windows for configuring the driver based on the selected country. Once a country is selected and the installation is final, no reconfiguration is possible in this case. To reconfigure, the software and associated utility programs have to be uninstalled and the overall reinstallation is carried out in order to select a different country. Wireless radio frequencies are highly regulated and diverse. We propose a dynamic/automated self-configuring driver system which can be used in any country in the world.

This article is organized as follows. In section II, we provide a brief overview of the 802.11a/b/g standards. Section III discusses the regulatory issue. Section IV presents the

architecture and the implementation of the universal driver. In this section, we will also present the Netgear driver specifications. Note that we do not intend to alter this product. A request for a joint collaborative research work with the Netgear is in process. Finally, a summary of the overall work is presented in section V.

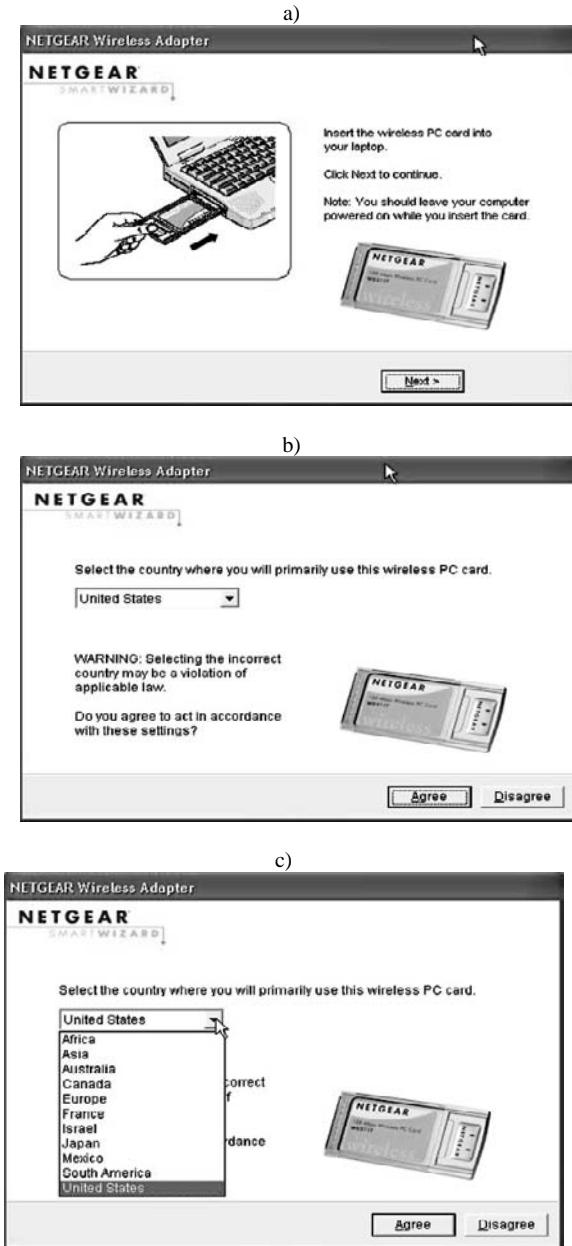


Fig. 1. Some steps in Netgear's [4] driver installation.
Copyright of Netgear ®

II. OVERVIEW OF IEEE 802.11a/b/g STANDARDS

Table 1 provides a summary of the most widely used standards, 802.11b/g, in the U.S., Europe, and ASIA. Series of standards in the family of 802.11 (c through f, h, j) are service extensions or enhancements to previous standards. Many other standards are under development including the 802.11n projected to support all major platforms, including consumer electronics, personal computing, and handheld platforms, and will be usable throughout all major environments, including enterprise, home, and public service areas [5]. In addition, the standard 802.11d is used for international, country-to-country; roaming that it is used in

TABLE 1
SUMMARY OF 802.11a/b/g STANDARDS

Standard	802.11a	802.11b	802.11g
Release in	1999	1999	2003
Operating freq.	5 GHz	2.4 GHz	2.4 GHz
Max. data rate	54 Mbps	11 Mbps	54 Mbps
Modulation	OFDM	DSSS & CCK	CCK & OFDM
Average range	80 feet	175 feet	175 feet
Channels	12 (all non available)	11 (3 non overlapping)	3

countries where systems using other standards in the IEEE 802.11 family are not allowed to operate. The standard 802.11j was finalized in 2004; the standard works in the 4.9 GHz to 5 GHz band to conform to the Japanese rules for radio operation for indoor, outdoor and mobile applications.

The 802.11.a uses a 52-subcarrier orthogonal frequency-division multiplexing (OFDM) and it has 12 non-overlapping channels, 8 dedicated to indoor and 4 to point to point. It is not interoperable with 802.11b, except if using equipment that implements both standards.

The 802.11.b uses Complementary code keying (CCK) as its modulation technique. The modulation scheme used in 802.11g is OFDM for the data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s, and reverts to (like the 802.11b standard) CCK for 5.5 and 11 Mbit/s and DBPSK/DQPSK+DSSS for 1 and 2 Mbit/s. The 802.11.g is backward compatible with 802.11.b. Standards 802.11b/g can both be used in ad-hoc and infrastructural modes. In ad-hoc mode, these two standards would need to support 11 Mbps. However, to get higher performance, it is better to use infrastructure mode instead. Table 2 presents the channels available with the 802.11b/g.

TABLE 2
802.11b/g RADIO FREQUENCY CHANNELS

Channel	Center Frequency	Frequency Spread
1	2412 MHz	2399.5 MHz - 2424.5 MHz
2	2417 MHz	2404.5 MHz - 2429.5 MHz
3	2422 MHz	2409.5 MHz - 2434.5 MHz
4	2427 MHz	2414.5 MHz - 2439.5 MHz
5	2432 MHz	2419.5 MHz - 2444.5 MHz
6	2437 MHz	2424.5 MHz - 2449.5 MHz
7	2442 MHz	2429.5 MHz - 2454.5 MHz
8	2447 MHz	2434.5 MHz - 2459.5 MHz
9	2452 MHz	2439.5 MHz - 2464.5 MHz
10	2457 MHz	2444.5 MHz - 2469.5 MHz
11	2462 MHz	2449.5 MHz - 2474.5 MHz
12	2467 MHz	2454.5 MHz - 2479.5 MHz
13	2472 MHz	2459.5 MHz - 2484.5 MHz

III. REGULATORY ISSUES

A. Federal Communication Commission Guidelines

- In order to comply with RF exposure limits established in the ANSI C.95.1 standards, the user is advised to maintain a distance of at least 1 inch (2.5 cm) from the antenna of the NETGEAR WPC card.

- The devices may not cause harmful interference and the device must accept any interference received, including interference that may cause undesired operation.

- The product's firmware has to limit operation to only channels allowed in particular region and country.

- Some restrictions on exporting the encryption code outside U.S and Canada.

- The bottom line is the user is required to carefully read and comply with the usage and operation requirements of a particular product. In addition, the final product has to show the symbol of compliance, FC, for FCC [6].

B. European Community

- The user should run the client utility program provided with the WPC product to check the current channel of operation and confirm that the device is operating in conformance with the spectrum usage rules for European Community countries.

- During the installation of the driver, a list of European country's names (France, Germany, Italy, Spain, Portugal, Sweden, etc.) is displayed. The user has to confirm the declaration of conformance for the country selected.

- In France, for example, the radio spectrum regulator, Autorité de Régulation des Télécommunications (ART), reinforces the rules with respect to use of 2.4 GHz spectrum in various locations in France [7]. The symbol, CC, is used for European Community.

- Finally, compliance rules must also be confirmed for Canada and Asian countries.

As mentioned at the beginning of this paper, the model of the driver installation used is static. If a laptop user in the U.S goes to France for example, he/she will have to go over the

overall installation setting for France in order to be able to use the wireless network in the specific location. This model, therefore, lacks flexibility and is time consuming. In the following section we show our dynamic model of driver installation.

IV. A NEW DRIVER MODEL FOR 802.11b/g

The following is assumed in the proposed implementation. It is assumed that hardware models implementing the tri-mode band are available [2] and [3]. The model of the proposed driver is presented in Fig. 1.

A. Description of the Driver Units

The architecture of the driver is divided into three main blocks:

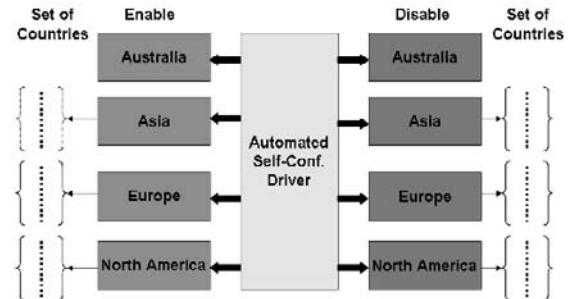


Fig. 2. Architecture of the proposed driver.

- Enable and Disable blocks: these blocks are similar in design. Each block is used to represent each continent. Note that the African continent is listed under the European block. The Enable block will be activated during the first time installation of the wireless PC card driver based on the location of the portable user. The Disable block is the de-allocation section. The section of the Enable block activated is deactivated to adapt to the new location. This allows power and resource savings.
- Set of Countries block: these blocks are arrays or data structure of all the required countries in the specific continent block (Enable and Disable blocks).
- Automated Self-Configuring Driver (ASCD) block: this block is the central block; it is like the central processing unit of a computer or the main function in a C# or JAVA code, or a digital switching fabric in telecommunications. During the driver installation, this module calls either one of the subroutine in the Enable's block. Then a list of countries is displayed from which the installer will select. Once the country is selected, the conformance window is displayed. Following this window is the list of some European countries. A careful selection in order to avoid any malfunction and/or harm. Finally, the installation goes through the normal basic wireless settings procedures. When the location of the user changes and a new connection is

needed at a different country per say, then the ASCD will deactivate that initial country's procedure and not necessary the associated continent's block if another country of that same block is requested; otherwise, the whole continent block is deactivated and another continent block is enabled.

B. Implementation

Fig. 2 shows a partial implementation of the automated self-configuring driver architecture presented in Fig. 1. As this work is in progress, we have left out full details of the implementation until the final work is accomplished. Fig. 3 displays the conformance window of the European's regulation. Fig. 4 shows a list of the European countries' that can be configured. The overall driver utility program is implemented in C#.

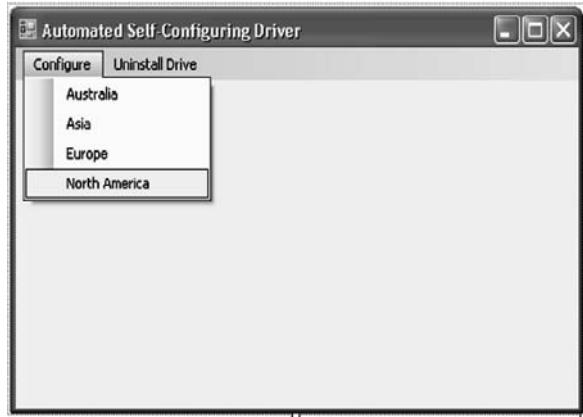


Fig. 3. Driver main window.

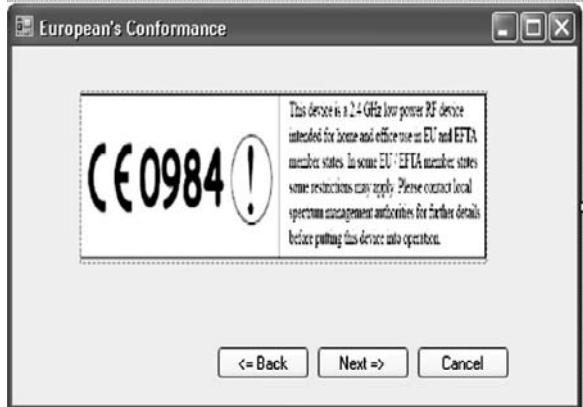


Fig. 4. Conformance window.



Fig. 5. Countries selection window.

C. Partial Implementation of the Code

Figure 6 shows a partial coding of our proposed driver. Note that code is implemented in C# using Microsoft Visual Studio 2005 [8]. A record of the selected continent and its associated country is kept for the uninstall and the reconfiguration procedures.

```
// The Proposed Automated Self-Configuring Driver
```

```
public class AutomatedSelfConfiguringDriver{
    public static void Main(string[] args){
        Configure configureClass = new Configure();
    }

    public class Configure{
        string[] continent = {"Australia", "Asia", "Europe",
        "North America"};
        string selection // This uses Figure 3
        switch(selection){
            case continent[0]: call method Australia; break;
            case continent[1]: call method Asia; break;
            case continent[2]: call method Europe; break;
            case continent[3]: call method North America; break;
        }
    }
}
```

Fig. 5. Partial driver code.

C. The Driver Specifications

The proposed Automated Self-Configuring Driver is based on the Netgear WG511T hardware and software and utility programs specifications, see Figure 7. Therefore, as implementation follows the same specifications. As a result, in this section, we present the general specifications of the Netgear 108 Mbps Wireless PC Card, 32-bit CardBus WG511T. A prior written consent will be obtained from Netgear when there is a need to decompile or decrypt the software. Note that this is an ongoing work at the Southern University and A&M College in Baton Rouge, Louisiana.

Physical Specifications

- Dimensions (l x w x h): 4.68 x 2.12 x .25 in (119 x 54 x 6 mm)
- Weight: 1.6 oz (46 g)

Frequency

- 2.412 ~ 2.462 GHz (US)
- 2.412 ~ 2.472 GHz (Japan)
- 2.412 ~ 2.472 GHz (Europe ETSI)
- 2.457 ~ 2.462 GHz (Spain)
- 2.457 ~ 2.472 GHz (France)

Network Speeds

- 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 & 108 Mbps (auto rate capable)

Modulation Type

- OFDM with BPSK, QPSK, 16QAM, 64QAM, DBPSK, DQPSK, CCK

Encryption

- Hardware-based 40/64-bit & 128-bit WEP encryption
- WPA-PSK, WPA2-PSK

Electromagnetic Compliance

- FCC Part 15 Class B

System Requirements

- Notebook PC with Pentium 300 MHz - compatible processor or higher
- Available CardBus PC Card Type II slot
- Microsoft® Windows® 2000 or XP

Fig. 7. Netgear WG511T driver specifications.
Copyright of Netgear ®

IV CONCLUSION

This paper presents a prototype for an automated self-configuring driver system (ASDS) for IEEE 802.11 WLAN. This software system provides a new way of running multiple IEEE 802.11 wireless standards on laptops and/or other mobile devices on the fly anywhere around the world. The paper starts with a brief overview of the 802.11 standards. Regulatory issues related to radio frequency in the ISM band were investigated in section III. The proposed architecture was introduced in section IV. This architecture is totally dynamic

and self-configuring. The authors would like again to mention that this is an on going work. The model presented here provides wireless LAN mobility flexibility and is projected to be to be power efficient with the added deactivation technique of the blocks (continents) not being used. To be more specific in our implementation, we focused on Netgear WG511T Wireless product, which generated the motivation behind this work. The WG511T is based on the 802.11 b/g standards. In order to add the 802.11a, the specifications provided here will have to change and the overall hardware design adjusted consequently.

REFERENCES

- [1] www.ieee.org
- [2] Masoud Zargari, Manolis Terrovitis, *et all.* "A Single-Chip Dual-Band Tri-Mode CMOS Transceiver for IEEE 802.11 a/b/g Wireless LAN," *IEEE Journal of Solid State Circuits*, Vol. 39, NO. 12, December 2004.
- [3] K. Vavelidis, A. Vassilion, *et all.* "A Dual-Band 5.15-5.35 GHz, 2.4-2.5 GHz 0.18μm CMOS Transceiver for 802.11a/b/g Wireless LAN, *IEEE Journal of Solid State Circuits*, Vol. 39, NO. 7, July 2004.
- [4] www.netgear.com
- [5] www.intel.com
- [6] www.fcc.gov
- [7] www.art-telecom.fr/eng/index.htm
- [8] Microsoft Studio, www.microsoft.com

DEVELOPMENT OF A VIRTUAL FORCE-REFLECTING SCARA ROBOT FOR TELEOPERATION

Mehmet Ismet Can Dede, and Sabri Tosunoglu

*Florida International University
Department of Mechanical Engineering
10555 West Flagler Street
Miami, Florida 33174*

Abstract – Teleoperation control methods have been studied for decades by several researchers. The testing systems used in these studies often consist of duplicates of the same robot. Deploying different robotic systems in teleoperation requires mapping between the motions of the two. This mapping should be optimized so that telemanipulation would get the maximum use of each system's capabilities. This study presents an alternative slave system for an existing teleoperation system. A version of a SCARA robot is selected for this purpose. The task is to draw on or carve into the surfaces as motion commands are received from the operator. A parallel position/force controller is investigated and the mapping between the master input and the slave output is explained. The test results are presented for a specific task of the slave constructed in virtual environment. As a result, the designed slave showed that it is capable of following the commands sent from the master with the help of the mapping created. The parallel position/force controller also proved to be successful in following the trajectory and providing force reflection while maintaining stability.

I. INTRODUCTION

A teleoperation system usually consists of a master robot, a slave robot and the communications line that provides the signal transfer between these two robots. Master usually sends commands to control the slave motion. The master robot in this study is a force-reflecting two-degree-of-freedom (DOF) joystick.

The objective of this study is to build a slave system which is capable of following surfaces and provide force reflection information which is often the case in some maintenance, assembly and quality control operations. The slave is selected as a SCARA robot that has a total of three DOF. The task to be accomplished by the slave is described as drawing on or carving into various surfaces. This specific task requires position/force controllers as well as customary control laws for the slave manipulation. Another objective of this study is to evaluate the necessity of position/force controllers as well as their performance for the specific type of teleoperation and in general bilateral (force-feedback) teleoperation. Modified versions of the position/force controllers are examined for possible communication loss in which the slave system may lose the track of the trajectory provided by the master. One other objective of this study can

be described as creating a virtual reality simulation model from a CAD model using Matlab[®] Simulink blocks.

First step of the design is to decide on the workspace size of the slave robot. The size of the robot is determined as a result of this decision. The CAD model of the robot is created utilizing the previously set manipulator size. Then the CAD model is translated into a VRML file to be used in virtual reality representation of the system. Size, mass, inertia and joint axis properties are also translated into a Matlab[®] SimMechanics model. This model is then integrated with the VRML file so that the motion of the model is viewed via a virtual reality screen. The model is further expanded by creating a contact model for the manipulator and the surface friction. The friction force created is used as force feedback information for the master. The simulation model utilizes customary position and position/force controllers. Various controllers are tested in simulation tests and the findings are presented.

The significance of the study is that a new teleoperation slave is developed that requires mapping of the motion received from the master. It is not a replica of the master system unlike the most teleoperation test systems [7,8]. Another significance is the evaluation of a position/force controller to be used in teleoperation systems. Also, the virtual rapid robot control prototyping [1] is used to virtually construct the slave system.

II. TELEOPERATION SYSTEM OVERVIEW

Teleoperation is a robotics system where two robots interact with each other to accomplish a task via remote control. The robotic systems are called master and slave. Master robot is operated by the human operator and slave robot is controlled by the commands sent from the master. Teleoperation is usually utilized in two conditions. One condition is where the task to be accomplished is at a distant site from the operator. Second condition is where the task is carried on in an environment, which is hazardous for a human to work in. In both conditions, slave robot takes place of the human that is expected to work on the task. The human operator is placed at the other end of the teleoperation system, sending signals to control the slave robot via a master system.

A special and probably the most common type of teleoperation, bilateral teleoperation involves transmitting control signals in both directions. A special type of bilateral teleoperation schematic is shown in Fig. 1. Master robot is operated by the human to send velocity signals to control the slave robot. As a result of the slave robot and environment interaction, slave sends back force measurements to the master. This architecture is designed for the operator to feel slave-environment interaction during the manipulation. As a result, operator can control the force he/she wants to apply to the environment while controlling the motion of the slave system via velocity inputs.

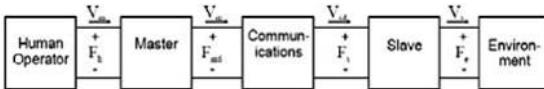


Fig. 1 Force-feedback teleoperation.

There are different master system designs that depend on the task to be accomplished. In this study, a two-degree-of-freedom (DOF) gimbal-based joystick is used as the master [6]. The joystick has uncoupled motions about the two axes as a result of its design. Therefore, the motion about one axis does not affect the motion about the other axis. Fig. 2 shows the master joystick with its x and y rotation axes.

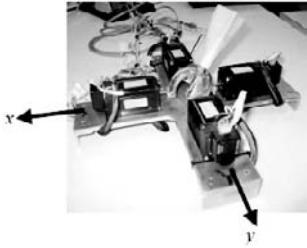


Fig. 2 Two-DOF master joystick.

A fault-tolerant holonomic mobile platform has already been designed as a slave system [2]. This system was used as a slave in the tests that were conducted using the real-time joystick and a virtual reality model of the mobile platform. There had to be a mapping between the joystick and mobile platform motion due to the limitations of the joystick motion. Therefore, the position commands received from the joystick were taken as velocity inputs on the slave side. The mapping provided a limitless workspace for the mobile platform as intended.

In this study, it is proposed to build a slave system that has a limited workspace and requires a mapping between the joystick motion and the slave motion. The proposed slave system is a three-DOF SCARA robot that is designed to be used in following surfaces by exerting controlled forces. The commands received in x - and y -axes are transmitted to the slave as Cartesian coordinate inputs. Then the forces created during the telemansipulation as a result of interaction and surface friction are fed back to the master.

III. CONTROLS BACKGROUND

The task for the SCARA is solely to follow the commands sent from the master. Thus, it follows the inputs of the operator. During the telemansipulation, it may be required for the slave to have contact with the surface and even exert forces on the surface for either carving or writing purposes. The surface rigidity varies for different environments and tasks.

It is obvious that a pure position controller is not sufficient enough to accomplish the operations mentioned above. Therefore, in this study the use of a position/force controller is proposed. Among a variety of parallel position/force controllers listed in [3], admittance controller is selected.

A. Admittance Controller

Admittance control tracks not only the position trajectory but also the force trajectory. A pure position controller works on the principle of rejecting disturbance forces while following a reference motion. Instead of rejecting it, admittance control using a force compensator complies with the environmental interaction and reacts to contact forces by modifying the reference motion trajectory [4]. The mechanical admittance is defined by the equation below.

$$\dot{X}(t) = AF(t) \quad (1)$$

This equation can be written in the s domain as

$$X(s) = K(s)F(s) \quad (2)$$

where

$$K(s) = \frac{1}{s} A \quad (3)$$

In above equations and in Fig. 3, X and \dot{X} are the position and velocity vectors of the end-effector, A is the admittance matrix. Fig. 3 shows the schematic representation of a customary admittance control scheme.

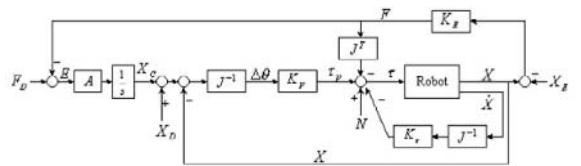


Fig. 3 Customary Admittance Control.

The admittance matrix A relates the force error vector E ($E = F_D - F$) to the required modification in the end-effector velocity vector. This leads to the following additive modification on the reference trajectory:

$$X_c = \int A(F_D - F)dt \quad (4)$$

Usually the admittance term, A , is not selected as a constant. It involves a variable matrix such as

$$A(s) = k_d s^2 + k_p s + k_i \quad (5)$$

which then results in the following PID force compensator when the Eq. 3 is applied:

$$K(s) = \frac{1}{s} \cdot A(s) = k_d s + k_p + \frac{k_i}{s} \quad (6)$$

The formulation of the customary admittance control uses the assumption that the error between the position demand and the actual position in Cartesian space is small. Therefore, it can be transformed into the joint space using the approximation in Eq. 7.

$$(\theta_{ref} - \theta) \approx J^{-1}(X_{ref} - X) \quad (7)$$

This assumption does not hold if there is a communication loss during telemanipulation and the robot loses the track of its Cartesian coordinates. With the first command received the error range becomes unacceptable for this assumption.

On the contrary, the modified admittance control algorithm presented in [5] provides a solution that does not use the assumption mentioned above. The modification is on exact calculation of the error in joint space. Therefore, both the position demand and the actual position measured in Cartesian space are transformed to the joint space using inverse kinematics (IK) as shown in Eq. 8. Usually the actual positions of the joints are received from the joint sensors in joint space. Then the reference trajectory and the actual position can be compared in joint space without any assumptions. This solution is valid for the manipulators that have inverse kinematics solutions.

$$(\theta_{ref} - \theta) = IK(X_{ref}) - IK(X) \quad (8)$$

The block diagram of the modified version is presented in Fig. 4. As it can be observed the only modification is made in the inner position control loop where the error is calculated.

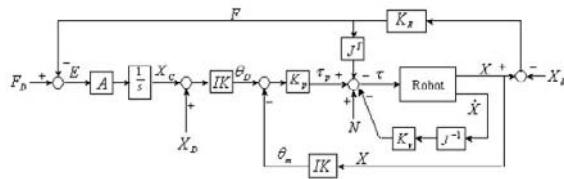


Fig. 4 Modified Admittance Control.

In this study, the modified admittance control is utilized as a parallel position/force controller.

IV. SIMULATION DESIGN

The SCARA robot in this study is designed as a slave system for teleoperation tests. It is constructed as a virtual slave so that there is no need to construct the manipulator. Therefore, the simulation requires a virtual reality representation of the robot. The link and joint parameters of the SCARA robot used in this work are given in Table 1.

TABLE I
LINK AND JOINT PARAMETERS OF THE SCARA

Joints	α_k (deg)	s_k (mm)	a_k (mm)	θ_k (deg)
1	0	0	750	θ_1
2	0	0	480	θ_2
3	0	s_3	0	0

The concept presented in [1] is used to construct the robot in virtual environment. First the manipulator is constructed in a computer-aided-design software environment. Then the material, inertial and mechanism parameters are translated into the Matlab® environment. Fig. 5 shows the link parameters on the visual representation of the manipulator.

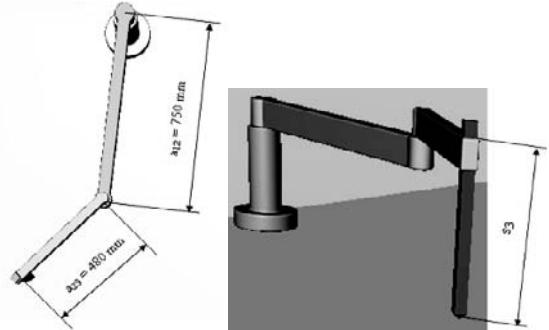


Fig. 5 Link Parameters of the SCARA.

The forward kinematic and dynamic modelling of the manipulator is created automatically using the translation tool mentioned in [1]. Interaction model between the end-effector and the surface is created using a planar contact. The material of the end-effector is selected to be lead with a modulus of elasticity of 36.5 GPa. The surface is assumed to be rigid.

The force applied by the end-effector on the surface, N , is used to describe the magnitude of the surface friction. The direction of the friction force is determined by the motion of the end-effector as shown in Eq. 9.

$$x_f = -\frac{V_x}{\sqrt{V_x^2 + V_y^2}} \Rightarrow F_x^f = \mu \cdot N \cdot x_f \quad (9)$$

$$y_f = -\frac{V_y}{\sqrt{V_x^2 + V_y^2}} \Rightarrow F_y^f = \mu \cdot N \cdot y_f$$

$$F^f = \begin{bmatrix} F_x^f \\ F_y^f \end{bmatrix} \quad (10)$$

The friction force information created in the Cartesian space is then translated into the joint space as disturbance torques acting on the revolute joints of the manipulator. The Jacobian matrix is used to translate the Cartesian forces into joint forces as shown in Eq. 11.

$$\tau = J^T \cdot F^f \quad (11)$$

The Jacobian matrix of this manipulator is defined by:

$$J = \begin{bmatrix} -a_{12} \cdot \sin \theta_1 - a_{23} \cdot \sin \theta_{12} & -a_{23} \cdot \sin \theta_{12} \\ a_{12} \cdot \cos \theta_1 + a_{23} \cdot \cos \theta_{12} & a_{23} \cdot \cos \theta_{12} \end{bmatrix} \quad (12)$$

where $\theta_{12} = \theta_1 + \theta_2$. The mapping between the joystick commands and the SCARA joint motion is calculated through inverse kinematics. The following equations present the calculation of each joint position as a result of this mapping.

$$\theta_2^{a,b} = \pm \arccos \left(\frac{x^2 + y^2 - a_{12}^2 - a_{23}^2}{2 \cdot a_{12} \cdot a_{23}} \right) \quad (13)$$

$$\theta_1^{a,b} = \arctan \left(\frac{(a_{12} + a_{23} \cdot \cos \theta_2^{a,b}) \cdot y - a_{23} \cdot \sin \theta_2^{a,b} \cdot x}{(a_{12} + a_{23} \cdot \cos \theta_2^{a,b}) \cdot x + a_{23} \cdot \sin \theta_2^{a,b} \cdot y} \right) \quad (14)$$

The operator through an input screen specifies the desired force to be applied to the environment, which also can be called the force trajectory. The friction forces in Cartesian space are then fed back into the servomotors of the joystick's respective axes.

V. SIMULATION TEST RESULTS

For all the simulation studies, independent joint control is used. In the first set of simulations, Proportional-Derivative (PD) control was used in every joint. After tuning the PD parameters, the overall control was in acceptable error range when there was no contact with the surface. In order to control the force applied on the surface with this controller, the desired position trajectory was modified to penetrate into the surface so as to create the desired amount of contact force.

It was expected that a pure position controller for the prismatic joint would not be effective enough to follow the force trajectory while following the position trajectory. Another solution is to use dual controls. A position controller makes the end-effector approach the surface and create the contact. Then the control algorithm has to be switched to a pure force controller to follow the force trajectory. This type of switching between the controls can cause instabilities and chattering in a teleoperation system where the communication can be delayed in an unacceptable amount.

One other possibility for a system that is required to follow both position and force trajectories is to use a parallel

position/force controller. The controller proposed in this study is the modified admittance controller presented in [5].

The following set of simulations is carried out by using an admittance controller for the prismatic joint and PD controller for the revolute joints. The PD control parameters were modified to compensate for the disturbances created by the friction forces at revolute joints.

The task used in the simulations is to follow a square path inside the workspace of the manipulator by applying a constant force. The task was made more demanding by specifying the speed of the end-effector constant. It was expected to cause problems especially at the corners of the square where the end-effector is required to change its direction by 90°. The maximum amount of error is seen at the change of direction at 20, 30 and 40 seconds as illustrated in Figs. 6 and 7.

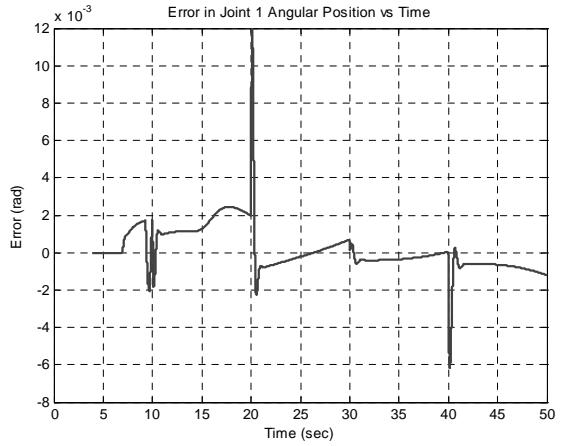


Fig. 6 Angular Position Error in Joint 1.

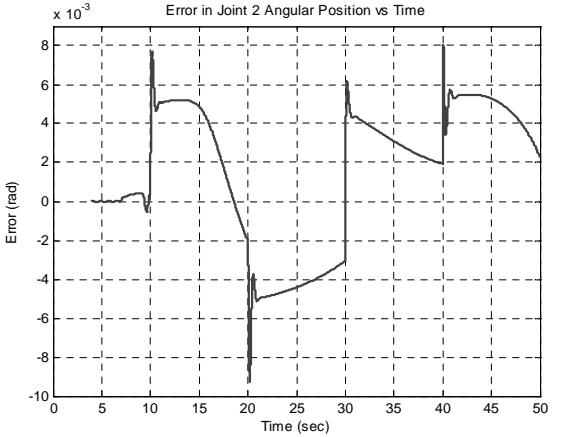


Fig. 7 Angular Position Error in Joint 2.

The change of direction acts as a step input because of the design of the task. This can be observed clearly from the velocity response of the manipulator in Cartesian space in Fig. 8.

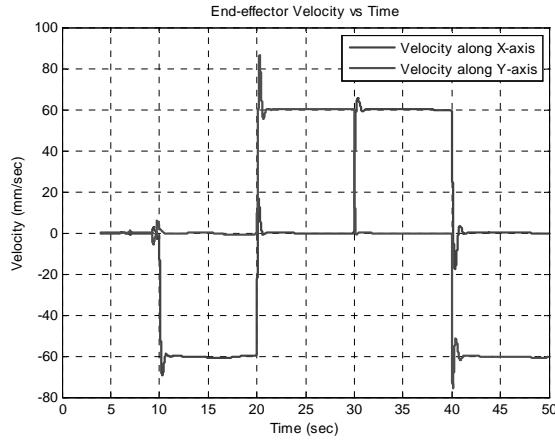


Fig. 8 End-effector Velocity in X and Y- Axis.

The square drawn by the end-effector also has the characteristics of transition states after each change of direction. The simulation creates an output for the lines drawn. Fig. 9 is the output for the lines drawn on the surface.

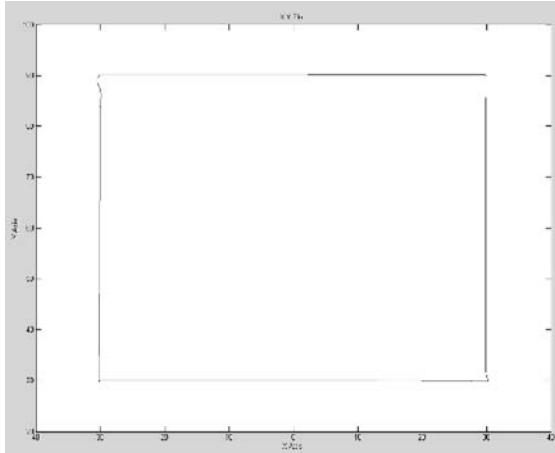


Fig. 9 Lines Drawn on the Surface.

The force applied to the surface is presented in Fig. 10. It is observed that after an acceptable transition period, the contact force is kept stable at the designated amount without any overshoots. The transition state characteristics can be changed by modifying the admittance term of the controller. The position control law however is kept constant as a PD controller. It was not necessary to modify the position control

parameters. The position was tracked in acceptable error range with the inner position loop of the admittance controller.

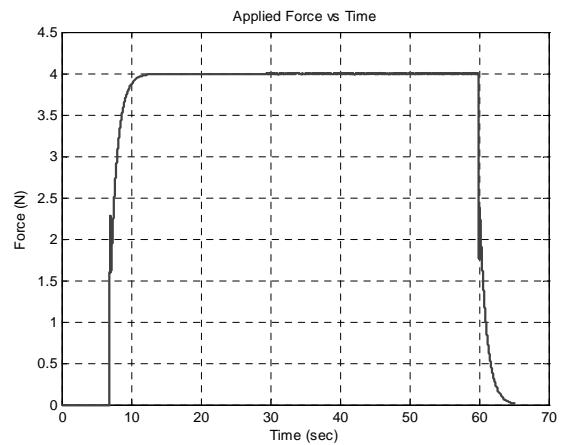


Fig. 10 Force Applied by the End-Effector to the Surface.

The friction force created in the Cartesian space is presented in Fig. 11. This information is to be transmitted to the servomotors of the joystick as torque inputs in each axis. It is also observed from this figure that the friction force alters with the change of direction of motion.

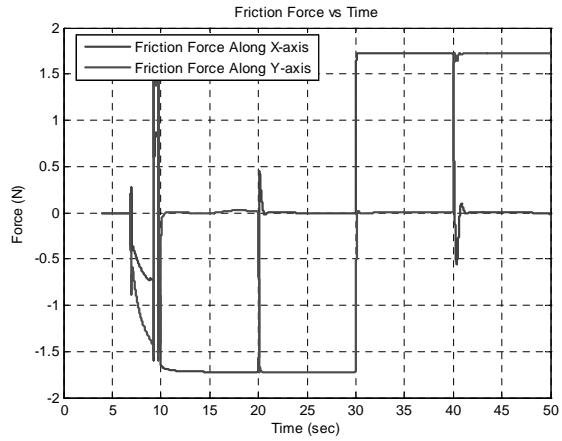


Fig. 11 Friction Force Observed Along Each Axis.

Friction force information is then transformed into joint disturbance torques. It was necessary to have this transformation so that the friction forces created would affect the manipulator motion as expected. The disturbance torques are presented in Fig. 12.

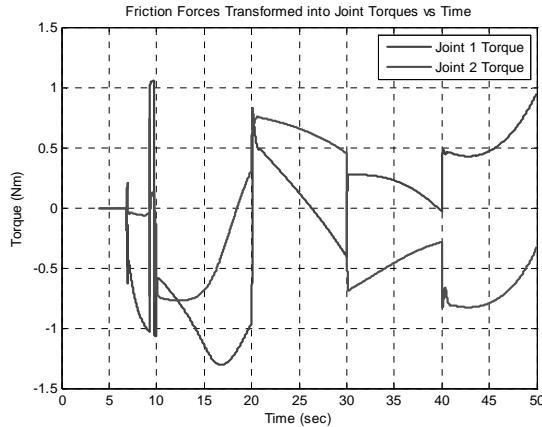


Fig. 12 Disturbance Torques Created due to Surface Friction.

The tests show that the virtual slave manipulator can follow the position and force trajectories within an acceptable error range. It also creates the force feedback information to be used in providing the feel of the environment for the operator.

VI. CONCLUSIONS

A SCARA robot is virtually constructed in CAD environment. Its physical properties and virtual representation are then translated into a Matlab® model. Several simulations are run testing different control algorithms using this model.

Admittance controller is employed for the prismatic joint for tasks involving contact with the environment. Possible communication loss or loss of data during communication made the assumption of having small errors in Cartesian space invalid for customary admittance control. Therefore, modified admittance control algorithm is used in this study. The modified version of the admittance controller is advised for

use in teleoperation applications that require parallel position/force control.

A customary position control (PD) is also used for the remaining revolute joints. If faster manipulation speeds are required, the computed-torque method can be incorporated to compensate for larger Coriolis and centrifugal forces.

The test results indicate that the virtually-constructed slave is capable of following position and force commands sent by the slave using the mapping explained in this paper. Also, it reflects force information to the master as intended in a force-reflecting bilateral teleoperation system.

REFERENCES

- [1] M. I. C. Dede, and S. Tosunoglu, "Virtual Rapid Robot Prototyping," ASME Early Career Technical Journal, Volume 5, Number 1, October 2006.
- [2] M. I. C. Dede, and S. Tosunoglu, "Design of a Fault-Tolerant Holonomic Mobile Platform," Proceedings of the 19th Florida Conference on Recent Advances in Robotics, Florida International University, Miami, Florida, May 25-26, 2006.
- [3] G. Zeng and A. Hemami, "An Overview of Robot Force Control," *Robotica*, Volume 15, 1997, pp. 473-482.
- [4] H. Seraji, "Adaptive Admittance Control: An Approach to Explicit Force Control in Compliant Motion," IEEE International Conference on Robotics and Automation, 1994, pp. 2705-2712.
- [5] M. I. C. Dede, and M. K. Ozgoren, "A New Approach for the Formulation of the Admittance and Hybrid Position/Force Control Schemes for Industrial Manipulators," 10th Robotics & Remote Systems Mtg. Proceedings, Gainesville, Florida, March 28-31, 2004.
- [6] M. I. C. Dede, and S. Tosunoglu, "Development of a Real-Time Force-Reflecting Teleoperation System Based on Matlab® Simulations," Proceedings of the 19th Florida Conference on Recent Advances in Robotics, Florida International University, Miami, Florida, May 25-26, 2006.
- [7] Munir, S., "Internet-Based Teleoperation," Ph.D. Dissertation, Georgia Institute of Technology, 2001.
- [8] Chopra, N., Spong, M. W., Hirche, S., and Buss, M., "Bilateral Teleoperation over the Internet: the Time Varying Delay Problem," In Proceedings of the American Control Conference, Denver, 2003.

Improving HORSE Again and Authenticating MAODV

Mingxi Yang¹, Layuan Li¹, Yiwei Fang²

¹School of Computer Science and Technology, Wuhan University of Technology, Wuhan, China

²Dept. of Electronics and Information Eng., Huazhong University of Science and Technology, Wuhan, China.

Abstract-Providing source authentication of message for multicast is necessary to guard against malicious nodes. In this paper we developed a novel efficient cryptographic mechanism HORSEI2 by improving HORSE for the second time and apply it to secure multicast as source authentication scheme for ad hoc networks. Comparing with HORSE, HORSEI2 reduces the memory-times-computational complexity of verifying a signature and the communication overhead without drop in security. The related security analysis and efficiency analysis about the main results have been given. And the network simulation on NS-2 proved that the performance of HORSEI2 based authenticating MAODV protocol is better than HORSE/RSA based authenticating MAODV protocol.

I. INTRODUCTION

Multicasting is a popular mechanism for supporting group communication. However, ensuring secure multicast involves source authentication, which allows all receivers and forwarding nodes to verify the origin of the data. An ideal multicast authentication scheme for mobile ad hoc networks (MANET) should be efficient for the senders and receiver nodes (low memory-times-computational complexity for signature and verifying), have a small communication overhead, be tolerant of packet loss, need not time synchronization between senders and receivers, provide instant authentication without buffering of data at the sender or receiver side and can verify the signature interrelated to dynamic packet message, etc.. To the best of our knowledge, few previous studies that satisfy all above requirements. The following is a brief overview of possible cryptography used as authentication tool in MANET and the shortcomings.

1) *Asymmetric cryptography*: The main drawback of the asymmetric cryptography is its expensive computational cost for MANET. According to the measured data [1], asymmetric cryptographic primitives are generally two to three orders of magnitude slower than Symmetric cryptography. The examples of the secure route scheme for MANET that uses public key digital signature are ARAN [2] , Ariadne [3] and the framework of securing MAODV [4], etc.

2) *Symmetric cryptography*: It has to share a secret key between senders and receivers hence it is difficult to prevent receivers from forging sender's signature, especially in the multicast scenarios. It could be used to Ariadne as far as know.

3) *Hash chain*: It is also a low computational cost authentication. It is based on one-way function. One of its drawback is that some encryption mechanism is needed to relate itself with the signed messages. Besides it works with signature amortizing and requires time synchronization. The typical example

is TESLA [5] , which is an efficient and secure source authentication for multicast. TESLA is applied to several protocols such as ARAN, Ariadne and SEAD [6] and so on. But it is a pity that it requires time synchronization between senders and receivers. Besides TESLA needs buffers to store data temporarily and can not to provide instant authentication. In our opinion, it is not practical enough for MANET.

4) *Hash tree* [12]: Although it needs not time synchronization, takes a few processing time and memory space for authentication, hash tree is not adapted to authenticate the dynamic packet message because it's root interrelated to packet message is generated prior to sending the packets. Hence hash tree can be used to authenticate "hop count" in route discovery, whose value changes from 0 to "max hop count" only, etc..

5) *HORSE* [7]: It is a potential perfect cryptography to authenticate multicast messages for MANET. But it has still some disadvantages on communication overhead and verifying signature cost.

Further studies are necessary on multicasting authentication. In the following sections, we will focus on improving HORSE and its applying to MAODV authentication in MANET.

II. IMPROVING ON HORSE

A. HORSE Review

HORSE is an extension of HORS [8]. HORS is an r -time signature scheme with fast signing and verification. It is similar to a public-key scheme in that it is can be used to create unforgeable signatures on messages that can be verified by making use of public information. These signatures are generally faster to compute than public-key signatures. But the higher speed of HORS is gained at the expense of larger key sizes. HORSE extends HORS by introducing hash chains and it can sign thousands to millions of messages efficiently and securely using keys that are orders of magnitude smaller than would be required for HORS signature scheme. With HORSE, source authentication can be produced in the group setting like a public-key signature scheme, only with signature and verification time much closer to those of a MAC (when the chain synchronization is held). With HORSE, every sender has his own initial secret and public keys, SK_i and PK . When a signature is computed and revealed, the sender can refresh his secret key by replacing any exposed key values with their predecessors SK_{i+1} in the hash chains. Receivers will verify the signature with the hash relation between the predecessors and successors in the hash chains.

B. HORSEI: Improving HORSE

One of the main drawbacks of HORSE is the cost of verifying authentication. We have presented HORSEI [9] to improve HORSE described below.

For signature, HORSE maps each message, m , to a unique k -element subset of a t -element key pairs set which is belong to the hash chains. In fact, because of $k \ll t$ (generally $t=1024$, $k=16$), when a receiver verifies a element of signature, s_{i_j} , the probability of the element's nearest predecessor in the hash chain, $s_{(i+1)_j}$ ($H(s_{i_j}) = s_{(i+1)_j}$), has been received and stored in the receiver's memory is just $1/t$ and that of every predecessor for all k elements of the signature is only $(1/t)^k$, so the chain synchronization between sender and receiver couldn't be held generally. Consequently the memory-times-computational complexity of verifying a signatures may be $O(tkd)$, where, d is the length of the hash chains ($d = 2^{10}$ generally). This will increase evidently the processing latency of forwarding nodes or receiving nodes.

We reduce the memory-times-computational complexity by introducing Intermediate Hash Joints into HORSE, which are shown in Fig. 1.

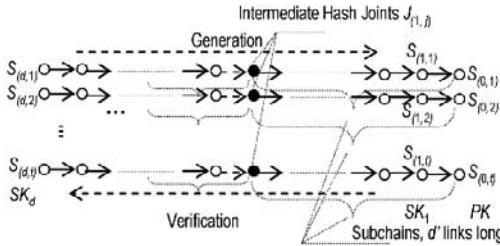


Fig. 1 HORSEI: the subchains and the Intermediate Hash Joints

There are t hash chains which are d links long in HORSE. In the algorithm HORSEI, we split each hash chain into d' ($d'=int(\sqrt{d})$) subchains and set up $(d'-1)$ Intermediate Hash Joints every other d' links at the juncture of both subchains initially, and set the value of the r th Intermediate Hash Joint in the j th hash chain is

$$J_{(r,j)} = H(s_{(r*d',j)} // PK_j), \text{ where } d'=int(\sqrt{d}), 1 \leq j \leq t$$

$$r=0, 1, 2, \dots, int(i/d'), \dots, (d'-1),$$

$$\text{When } i=0, J_{(0,j)} = PK_j = s_{(0,j)}.$$

Where H denotes a hash function, PK_j is the public key corresponding to $s_{(i,j)}$ belonged to the j th hash chain.

When verify an element of signature, s_{i_j} ,

"accept" if for each j , $1 \leq j \leq k$, $H(s_{i_j}) = s_{(i-1)_j}$;

or $J_{(r,j)} = H(H^{(i \bmod d')}(s_{i_j})) // PK_j$.

"reject" otherwise.

Therefore by HORSEI algorithm, although the space needed to store public key pairs(include Intermediate Hash Joint) are expanded, the largest computational times per step is decreased to \sqrt{d} . The computational complexity of verifying a subset of

signature is reduced from $O(d)$ to $O(\sqrt{d})$. It can be used to the ad hoc networks which have enough memory.

C. HORSEI2: Improving HORSE Again

In HORSE, a signature is constructed by k elements. The size of an element is 160b (using SHA-1 function) and a signature is $k*160b$ long thus the communication overhead is 320B/signature, which is 2.5 times of that of RSA1024. Besides the hash operations need to be performed at most $k*d$ ($16*2^{10}=16384$) times for verifying all k elements of a signature in HORSE and $k*\sqrt{d}$ times in HORSEI. The max process delay caused by HORSE/HORSEI is longer than that caused by RSA. In addition these will create a potential denial-of-service vulnerability. We impromved HORSEI by developing HORSEI2 as below.

For signing, HORSE or HORSEI splits the output of the hash function, $h=H(m)$, into k substrings $h_1, h_2, \dots, h_j, \dots, h_k$ of length $\log_2 t$ bits each; Interpret each h_j , as an integer i_j for $1 \leq j \leq k$, and use i_j as subscript of s_{i_j} to select the k elements from the t -element key pairs set, then makes out the signature as:

$$\sigma = (s_{i_1}, s_{i_2}, \dots, s_{i_k}).$$

The new approach of HORSEI2 is simple and efficient:

After splits $h=H(m)$ into $h_1, h_2, \dots, h_j, \dots, h_k$,

let $i_j = h_1 \text{ } h_2 \dots \text{ } h_j \dots \text{ } h_k$.

instead, then $\sigma = s_{i_j}$.

When verifying a signature only an element need to be checked.

D. Full detailed description of HORSEI2

Step1: Key Generation

1) Set Parameters l, k, t ,

where $k\log_2 t \leq H(\bullet)$,

$k < t$,

$H(\bullet)$ is a cryptographic hash function
and $l = H(\bullet)/2$;

2) Generate t random l -bit strings s_1, s_2, \dots, s_t ;

3) Use them as $s_{(d,1)}, s_{(d,2)}, \dots, s_{(d,t)}$ as seeds to construct t hash chains of length d (refer to Fig. 1):

$s_{(d,1)} \rightarrow s_{(d-1,1)} \rightarrow s_{(d-2,1)} \rightarrow \dots \rightarrow s_{(0,1)}$;

$s_{(d,2)} \rightarrow s_{(d-1,2)} \rightarrow s_{(d-2,2)} \rightarrow \dots \rightarrow s_{(0,2)}$ };

...

$\{s_{(d,t)} \rightarrow s_{(d-1,t)} \rightarrow s_{(d-2,t)} \rightarrow \dots \rightarrow s_{(0,t)}$;

where $s_{(d,i)} = H^i(s_{(d,j)})$,

that is $s_{(i,j)} = H^{d-i}(s_{(d,j)})$, ($0 \leq i \leq d, 1 \leq j \leq t$)

4) Set up Intermediate Hash Joints

Let $J_{(r,j)} = H(s_{(r*d',j)} // PK_j)$,

where $d'=int(\sqrt{d})$,

$r=0, 1, 2, \dots, int(i/d'), \dots, (d'-1)$,

when $r=0, J_{(0,j)}=PK_j$.

5) Store these hash chains for use as a series of keys and the initial secret keys SK_1 and the Intermediate Hash Joints (IHJ for short) in the memory of sender, where:

$SK_1 = (s_{(1,1)}, s_{(1,2)}, \dots, s_{(1,t)})$,

$$IHJ = (J_{(1,j)}, J_{(2,j)}, \dots, J_{(d'-1,j)}), (1 \leq j \leq t).$$

6) Distribute the public keys PK to networks, where

$$PK = (v_1, v_2, \dots, v_t)$$

$$= (s_{(0,1)}, s_{(0,2)}, \dots, s_{(0,t)})$$

$$= (H(s_{(1,1)}), H(s_{(1,2)}), \dots, H(s_{(1,t)}));$$

Step2: Signing

1) For Message m_i , search out the secret key SK_i from memory, where

$$SK_i = (S_{(i,1)}, S_{(i,2)}, \dots, S_{(i,t)})$$

$$= (H(S_{(i+1,1)}), H(S_{(i+1,2)}), \dots, H(S_{(i+1,t)}))$$

$$= H^{d-i}(SK_d),$$

Where m_i is the i th message packet, i.e. i is the originator sequence number.

$$2) \text{Let } h = H(m_i); \quad (1)$$

3) Split h into k substrings h_1, h_2, \dots, h_k , of length $\log_2 t$ bits each;

4) let $i_j = h_1 \ h_2 \ \dots \ h_j \ \dots \ h_k$, (2) and take i_j as a subscript to select a element from SK_i , so that the signature of the m_i is :

$$\sigma = S_{i_j}; \quad (3)$$

Step3: Sending

Send the message m_i with the signature and the corresponding Intermediate Hash Joint:

$$(m_i || \sigma || J_{(r, j)}); \quad (r = \text{int}(i/d'), j = i_j) \quad (4)$$

Step4: Verifying by Receiver

1) for the received Message m_i and signature

$$\sigma = (s'_{i_j}),$$

search out the corresponding $S_{(i-1)_j}$ (if received) or public key PK_0 from the memory;

2) Let $h = \text{Hash}(m_i)$;

3) Split h into k substrings h_1, h_2, \dots, h_k , of length $\log_2 t$ bits each ;

4) let $i'_j = h_1 \ h_2 \ \dots \ h_k$;

5) “accept” if for the unique i'_j ,

$$H(s'_{i_j}) = S_{(i-1)_j}, \quad (\text{if } S_{(i-1)_j} \text{ is received.}) \quad (5)$$

$$\text{or } J_{(r, j)} = H(H^{(i \bmod d')}(s'_{i_j})) // PK_j, \text{ where } r = \text{int}(i/d'). \quad (6)$$

“reject” otherwise.

E. Related Analysis

1) **Security Analysis:** The focus of HORSEI2 is to decrease k from 16 to 1, which advance the efficiency without any drop in security. The security of HORSEI2 relies entirely on cryptographic hash functions which are thought to be infeasible to invert. This is the same as that of HORSE when they all adapt a same hash function.

2) **Efficiency Analysis:** In HORSEI2 the max computational times per step on verifying a signature is only \sqrt{d} , and the size of the public key is not changed with the Intermediate Hash Joints are delivered in company with the signature. Therefore the memory-times-computational complexity of verifying a signature is reduced from $O((tkd))$ to $O(t\sqrt{d})$.

The comparing results of the different efficiencies about RSA, HORSE, and HORSEI2 are shown in Table 1.

TABLE 1^a
Efficiency Comparison of RSA and HORSE and HORSEI2

scheme	Size of Public key (Byte)	Comm. Cost (Byte)	Max No of hash operation verifying (times)	Max verifying delay/pkt (ms)	Complexity of verifying a signature
RSA1024	128	128	—	4.77/p1 117.6/p2	—
HORSE	20K	320	16385	0.236/p2	$O(tkd)$
HORSEI2	20K	80	33		$O(t\sqrt{d})$

Hash function: SHA-1. $t = 1024$, $k = 16$, $d = 1024$.

Size of packets: p1=128B, p2=512B

^aAll of the max delay time is calculated according to the measured data[1].

III. APPLYING TO MAODV AUTHENTICATION

Assume some appropriate distributed access control and key management schemes like URSA [9,10] and so on have been provided prior to HORSEI2 based MAODV authentication. In other words, the public key pairs sets of every node have been distributed to all multicast group member nodes in advance and being updated dynamically.

A. Authenticating MAODV based on HORSEI2

In the scheme of authenticating MAODV based on HORSEI2, we sign the hop count with HORSEI2 also. Besides we verify the signatures hop by hop, which will protect the bandwidth from been exhausted by malicious messages and the destination nodes from deny-of-service attack by huge number of forged messages due to the distributed authentication made by the forwarding nodes.

Suppose A, B, C and S are group members. S wants to join the multicast session [4], and only C is the tree node.

1) Authenticating Route Discovery:

(1) Sender S sends the route request message and the signature with the Intermediate Hash Joints.

$$S : m_{s,i1} = (\text{Join-RREQ}, IP_{Grp}, ReqID, i1);$$

// $m_{s,i1}$ is the i th message sent by S .

$$S \rightarrow *: (m_{s,i1})_{\sigma 1_{s,i1}} || (S, 0, i1)_{\sigma 2_{s,i1}} || J_{s(r1, j1)};$$

// the signature σ is made out according to equation (1) (2) (3) (4) and using SK_{i1} of S , and $\sigma 1$ is signed for the message m , the $\sigma 2$ is signed for the hop count, which is 0 here. $J_{s(r1, j1)}$ is calculated using SK_{i1} of S referring to formula (6) and $r1=\text{int}(i1/d')$. The following is similar to these.

$$(2) A : \text{verify } \sigma 1_{s,i1} \text{ and } \sigma 2_{s,i1};$$

if past, do the following:

$$A \rightarrow *: ((m_{s,i1})_{\sigma 1_{s,i1}} || J_{s(r1, j1)}) || ((A, 1, i2)_{\sigma 2_{A,i2}} || J_{A(r2, j2)});$$

Else, reject.

$$(3) B: \text{verify } \sigma 1_{s,i1} \text{ and } \sigma 2_{A,i2};$$

if past, do the following:

$$B \rightarrow *: ((m_{s,i1})_{\sigma 1_{s,i1}} || J_{s(r1, j1)}) || ((A, B, 2, i3)_{\sigma 2_{B,i3}} || J_{B(r3, j3)});$$

Else, reject.

$$(4) C: \text{verify } \sigma 1_{s,i1} \text{ and } \sigma 2_{B,i3};$$

if past, do the following:

$$m_{c,i4} = (\text{Join-RREP}, IP_{Grp}, ReqID, Seqn_{Grp}, i4, (ABC));$$

$$C \rightarrow B: (m_{c,i4})_{\sigma 1_{c,i4}} || J_{c(r4, j4)};$$

Else, reject.

(5)B: check $\sigma_{c,i4}$, if past, do the following:

$B \rightarrow A: (m_{c,i4})_{\sigma1_{c,i4}} || J_{c(r4, j4)}$;

Else, reject.

(6)A: check $\sigma_{c,i4}$ also, if past, do the following:

$A \rightarrow S: (m_{c,i4})_{\sigma1_{c,i4}} || J_{c(r4, j4)}$;

Else, reject.

(7)S: received the route response message, check $\sigma1_{c,i4}$, if passed, accept the route and modify the route table. Else, reject.

2) *Authenticated Link Activation: (Omit the verification.)*

$S: m_{s,i5} = (\text{JoinMACT}, IP_{Gp}, \text{SourceSeqnAtS}, i5, 0)$;

$S \rightarrow A: (m_{s,i5})_{\sigma1_{s,i5}} || (S, 0, i5)_{\sigma2_{s,i5}} || J_{s(r1, j5)}$;

$A \rightarrow B: ((m_{s,i5})_{\sigma1_{s,i5}} || J_{s(r5, j5)}) || ((A, 1, i6)_{\sigma2_{A,i6}} || J_{A(r6, j6)})$;

$B \rightarrow C: ((m_{s,i1})_{\sigma1_{s,i5}} || J_{s(r5, j5)}) || ((A, B, 2, i7)_{\sigma2_{B,i7}} || J_{B(r7, j7)})$;

The other authenticaed MAODV operations are similar to the above two, which could be past over.

B. Simulated Network Performance

We used the network simulator NS-2 to simulate the performance of HORSEI2 based MAODV authentication. We implemented it by referring to and modifying the code [11]. For comparing, RSA1024 and HORSE based MAODV authentication for ad hoc networks were simulated also, where SHA-1 was used as the hash function. The results were showed as Fig. 2. and Fig. 3..

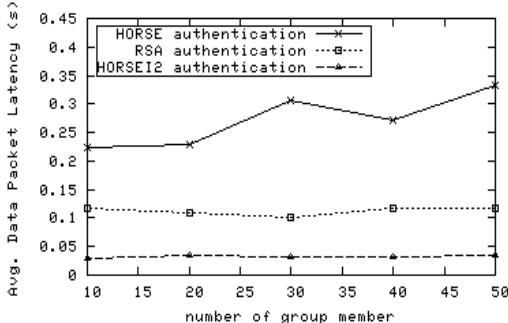


Fig. 2. Average End to End Latency of Data Packet

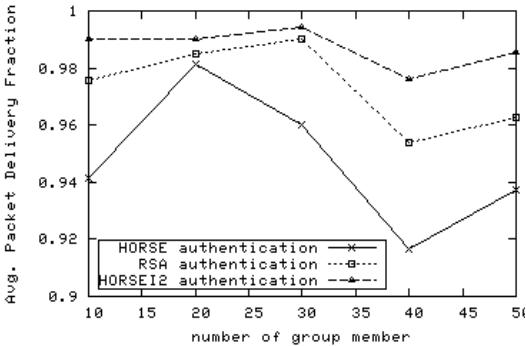


Fig. 3. Average Packet Delivery Fraction

The simulation parameters were: 1)Area: 1500 x 300 meters. 2)The number of nodes is 50 and sender is 1. 3)Simulation duration: 50 seconds; 4)Physical/Mac Layer: 802.11b with 11Mbps bandwidth. 5) Each packet is 256 bytes long. 6)The moving speed of each node is from 0 to 1m/s randomly with no pause time. 7) 7 CBR sessions was in each run. 8)A hash operation delay was 0.00359ms and the number of the hash operation in the hash chains was set up as a random number between 1 to d or d' in verification due to HORSE or HORSEI2. And also a signature generation delay of 0.36ms and a verification delay of 9.54ms for RSA based scheme.

IV. CONCLUSION

As mentioned above, we can find that HORSEI2 has almost reached the requirements of the ideal multicast authentication scheme for MANET described at section 1. It is efficient to sign and verify a signature, has low communication overhead, needs no time synchronization and hash chain synchronization, and it is tolerant of packet loss, can provide instant authentication and verify dynamic packet messages. The simulation results proved that HORSEI2 based authentication produces less average end-to-end packet latency and gains higher average packet delivery fractions than HORSE based and RSA based authentication at almost every data point.

The future works may be reducing the size of the public key for HORSEI2.

ACKNOWLEDGMENT

This research was supported by the National Natural Science Foundation of China (under Grant No. 90304018 ,60672137) and Specialized Research Fund for the Doctoral Program of Higher Education of China (under Grant No. 20060497015).

REFERENCES

- [1] Wei Dai, Crypto++ 5.2.1 Benchmarks, [Online]. Available: <http://www.eskimo.com/~weidai/>.
- [2] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP '02), IEEE Press, 2002, pp. 78–87
- [3] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. e8th Ann. Int'l Conf. Mobile Computing and Networking (MobiCom 2002), ACM Press, 2002, pp. 12–23.
- [4] Roy, S., Addada, V.G.; Setia, S., Jajodia, S., "Securing MAODV: attacks and countermeasures," Sensor and Ad Hoc Communications and Networks. IEEE SECON 2005. Second Annual IEEE Communications Society Conference on 26-29 Sept., 2005 Page(s):521 – 532.
- [5] A. Perrig et al., "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc. IEEE Symp. Security and Privacy, IEEE Press, 2000, pp. 56–73.
- [6] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 02), IEEE Press, 2002, pp. 3–13.
- [7] William D Neumann, "HORSE: An Extension of an r-Time Signature Scheme With Fast Signing and Verification," International Conference on Information Technology: Coding and Computing (ITCC'04), Las Vegas, NV, USA, 05-07 April 2004.

- [8] Adrian Perrig. "The BiBa one-time signature and broadcast authentication protocol." In Eighth ACM Conference on Computer and Communication Security, pages 28-37. ACM, November 5-8 2001
- [9] Mingxi Yang, Layuan Li, Yawei Fang, "Securing Multicast Route Discovery for Mobile Ad Hoc Networks," Wuhan University Journal of Natural Sciences, vol. 12, No.1, 2007. to be published.
- [10] Luo Haiyun, Kong Jiejun, Zerfos P, et al. URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks, IEEE/ACM TRANSACTIONS ON NETWORKING, 2004, 12, (6): 1049 - 1063.
- [11] Yufang Zhu and Thomas Kunz, "MAODV Implementation for NS-2.26, Systems and Computing Engineering," Carleton University, Technical Report SCE-04-01, January 2004.
- [12] Ralph C. Merkle. Protocols for Public Key Cryptosystems. In Proceedings of the IEEE Symposium on Research in Security and Privacy, pages 122.133, April 1980.

CURVELET TRANSFORM BASED LOGO WATERMARKING

Thai Duy Hien¹, Kazuyoshi Miyara¹, Yasunori Nagata¹, Zensho Nakao¹, & Yen Wei Chen²

¹Faculty of Engineering, University of the Ryukyus, Okinawa 903-0213, Japan

²College of Information, Science and Engineering, Ritsumeikan University, Shiga 525-8577, Japan

{tdhien, miyara, nakao}@augusta.eee.u-ryukyu.ac.jp

{ngt}@eee.u-ryukyu.ac.jp

{chen}@is.ritsumei.ac.jp

Abstract- Apart from existing representation such as DCT, wavelets, and steerable pyramids, recently, curvelet is introduced as a new multiscale presentation suited for images which are smooth away from discontinuities across curves. In this paper we propose a new watermarking method based on curvelet domain. Since the curvelet transform was developed in order to represent edges along curves much more efficiently than the traditional transforms, we apply the transform to digital watermarking and evaluate the effectiveness of the method. Our watermarking algorithm embeds a watermark in curvelet coefficients which are selected by a criterion whether they contain as much edge information as possible. We evaluated the effectiveness of the method against some well-known watermark attacks. Experimental results show that the performance of the proposed method against most prominent attacks is good and promising.

1. INTRODUCTION

In the recent past, several watermarking algorithms have used image representations where most information is concentrated in to a small number of coefficients. In this fashion, watermarking methods operating in the wavelet domain [5], discrete cosine transform domain (DCT) [4], principle component analysis (PCA) domain [6], and independent component analysis (ICA) domain have been proposed [11] [12].

The novel algorithm is developed in this work as the solution to the problems of data copyright, content protection and ownership; it is the process of inserting a logo watermark into digital image, which can be detected or extracted later to make an assertion about the data proof based on curvelet transform domain. The curvelet transform is a relatively new technique and is motivated by the needs of image analysis. The transform is designed to present the edges much more efficiently than the traditional transforms.

The proposed watermarking algorithm embeds a watermark in curvelet coefficients which are selected by a criterion whether they contain as much edge

information as possible. In the following sections, we present an outline of the curvelet technique and explain the proposed method.

2. CURVELET TRANSFORM

Recently, Candes and Donoho [1] developed a new multiscale transform which they called the curvelet transform. The transform was designed to represent edges and other singularities along curves much more efficiently than the traditional transforms, i.e. using much fewer coefficients for a given accuracy of reconstruction. Thus, already it has been applied to processing of edge properties e.g., noise removal [3] and contrast enhancement [10].

The curvelet transform executes some processing in order to attain those properties. Figure 1 shows the detailed process of curvelet transform of an image. The idea is to first decompose the image into a set of wavelet bands, and to analyze each band by a local ridgelet transform. The block size can be changed at each scale level. Roughly speaking, different levels of the multiscale ridgelet pyramid are used to represent different subbands of a filter bank output. At the same time, this subband decomposition imposes a relationship between the width and length of the important frame elements so that they are anisotropic and obey $width \approx length^2$.

The curvelet decomposition is the sequence of the following steps [1, 7, and 8]:

1. Subband Decomposition: The object is decomposed into sub-bands by “à trous transform” algorithm.
2. Smooth Partitioning: Each sub-band is smoothly windowed into “squares” of an appropriate scale (of side length $\approx 2^{-s}$).
3. Ridgelet Analysis: Each square is analyzed via the discrete ridgelet transform [9].

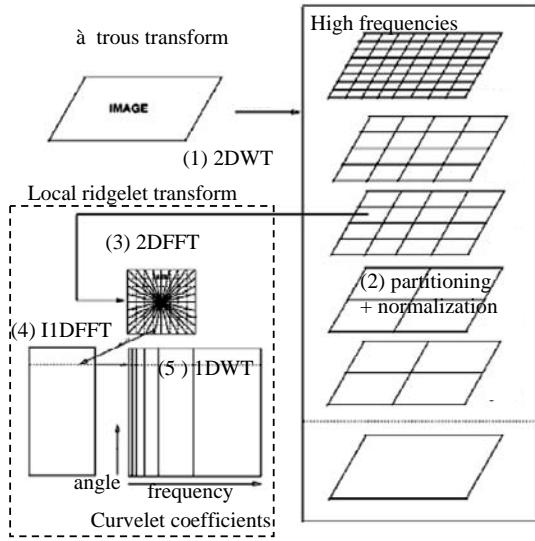


Fig.1. Curvelet transform

In this definition, the two dyadic sub-bands $[2^{2s}; 2^{2s+1}]$ and $[2^{2s+1}; 2^{2s+2}]$ are merged before applying the ridgelet transform. In the result, we achieve curvelet coefficients with involvement of edge information.

3. WATERMARK EMBEDDING/DETECTION

In our watermarking embedding system, watermarking gives priority to embedding of the edges of the given image. Given the original image, we take the curvelet transform and get the curvelet coefficients.

It is noted that in the same finite frequency scale, the edges have more important information. Since the coefficient where absolute value is large gives close agreement with the edge information of the image. Specifically, the watermarking algorithm embeds a watermark in curvelet coefficients which are selected by a criterion whether they contain edge information.

Selection of the coefficients to which a watermark is embedded is based on a pre-defined threshold and the watermark is cast into coefficients whose absolute values are larger than the threshold.

3.1. Embedding algorithm

The proposed algorithm is based on three input arguments: "scale," "pctg," and "alpha" to embed a watermark. "scale" is to select watermark embedding

scale coefficients, e.g., if we are selecting input scale = [4, 5], then the watermark embed to from scale 4 coefficients to scale 5 coefficients until it is all embedded. Then in each selected scales, the coefficients are sorted and find the criterion for choosing watermark embed position by "pctg" parameter. It were the number of index of sorted coefficients, e.g., "pctg" = 0.8, the length (sorted coefficients) = 1000, then we determine that watermark embed threshold is the value of coefficient of index number = $0.8 * 1000 = 800$. "alpha" is a strength parameter. Finally, the watermark is embedded to coefficients to satisfy the conditions: "larger than threshold." The architecture of our programs is shown in the Figure 3.

3.2. Watermarks

In this algorithm, the watermark is a logo image whose 32x32 pixels and marked a kanji character 'Oki' which is the first character of place name 'Okinawa' (Figure 2). In embedding process, the logo changes the form into binary bit stream (the length is 1024 bit), $W = w_1, w_2, \dots, w_{1024}$, and then cast to the curvelet coefficients. The embedded coefficients were modified by the following equation:

$$C' = C + \text{alpha} \cdot w_i \quad (1)$$

where C is a curvelet coefficient to satisfy the conditions, alpha is a strength parameter (this parameter is the same as the input argument alpha).



Fig. 2. The logo watermark

3.3. Watermark Detection

A logo is detected from the altered curvelet coefficients, and binarized with specific threshold. We used the Normalization Correlation (NC) to evaluate the quality of detected logo watermark. NC is calculated using the following equation:

$$NC = \frac{\sum_{m=1}^{N/2} \sum_{n=1}^{N/2} [W_k(m, n) \cdot W_k^*(m, n)]}{\sum_{m=1}^{N/2} \sum_{n=1}^{N/2} [W_k(m, n)]^2} \quad (2)$$

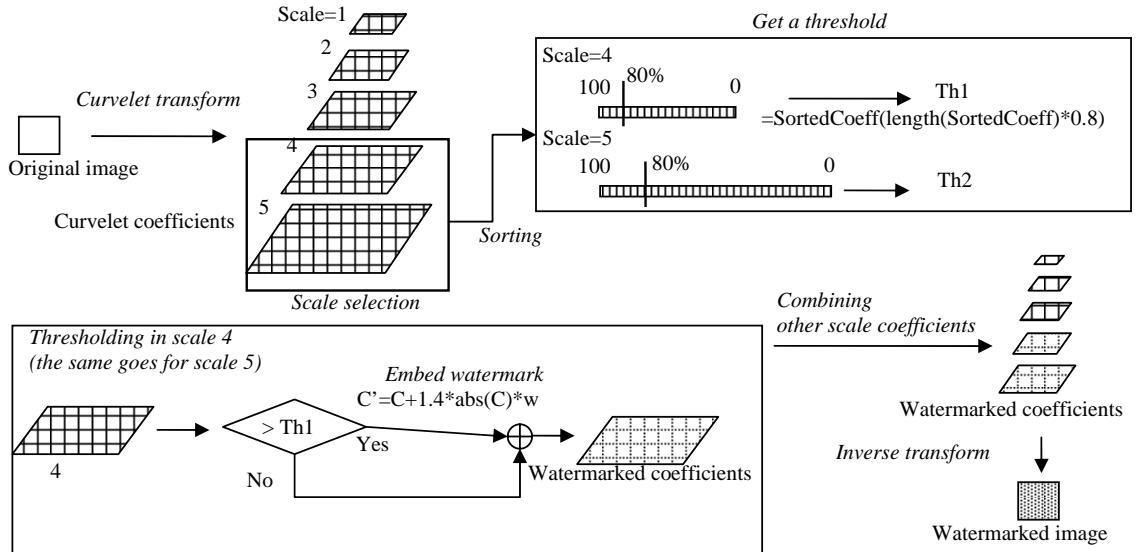


Fig. 3. The embedding algorithm ($\text{scale}=[4,5]$, $\text{pctg}=0.8$, $\text{alpha}=1.4$)

where W_k is original logo and W'_k is detected logo. The value of NC has the unit range $[0, 1]$, and if we get at higher NC values, the embedded watermark is more similar to the detected one.

4. EXPERIMENTAL RESULTS

We use standard 512x512 pixel image ‘Lena’ for evaluation of our proposed method. In our program, the image is transformed through fast discrete curvelet transform via wrapping [2].

We conducted experiments logo watermarking with the noted above parameters is $\text{scale}=[3]$, $\text{pctg}=0.31$, $\text{alpha}=50.0$. For watermarking evaluation we used the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

We apply the proposed method to the image ‘Lena,’ the obtained watermarked image (Figure 4) shows that there is no noticeable difference between the watermarked and the original image, which confirms the invisibility requirement in our watermarking method.

Its PSNR is 48.73 [dB] and MSE is 0.87 and The NC value of detected logo is 0.9063 (Figure 5). From figure 5, we can confirm that the recognition of the watermark in the experimental images is giving satisfactory results.

In addition, we perform further experiments to evaluate for the robustness against more commonly used image processing attacks such as JPEG compression, surrounding cropping, adding noise, image resizing and so on. We apply the attacks to the watermarked image and then detect the watermark. Variation in the detector response depending on a parameter changing of various attacks is displayed in Figure 6.



Fig. 4. Watermarked image
($\text{PSNR} = 48.73$ [dB] and $\text{MSE} = 0.87$)



Fig. 5. Detected logo ‘Oki’ (NC = 0.9063)

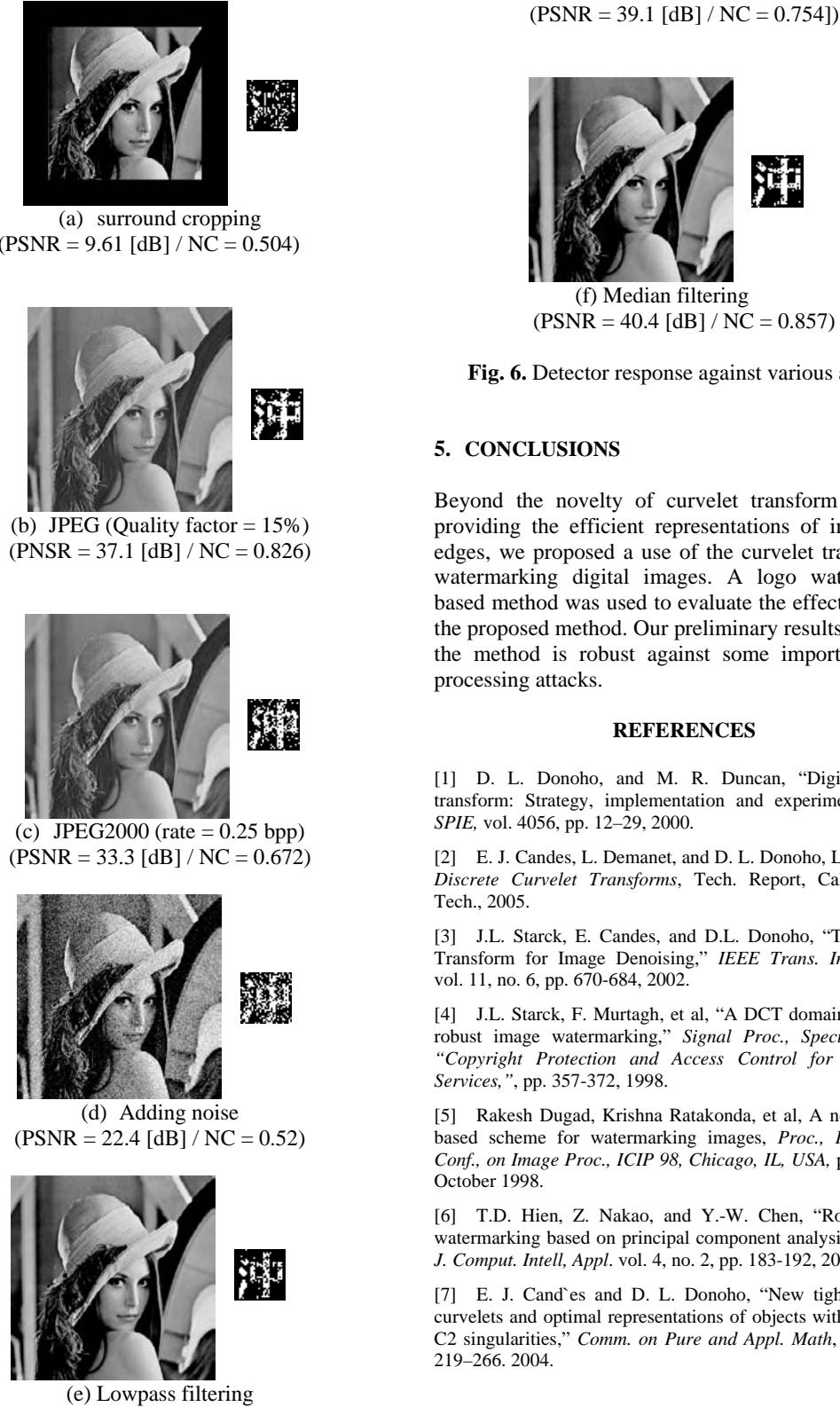


Fig. 6. Detector response against various attacks

5. CONCLUSIONS

Beyond the novelty of curvelet transform in which providing the efficient representations of image with edges, we proposed a use of the curvelet transform in watermarking digital images. A logo watermarking based method was used to evaluate the effectiveness of the proposed method. Our preliminary results show that the method is robust against some important image processing attacks.

REFERENCES

- [1] D. L. Donoho, and M. R. Duncan, "Digital curvelet transform: Strategy, implementation and experiments," *Proc. SPIE*, vol. 4056, pp. 12–29, 2000.
- [2] E. J. Candes, L. Demanet, and D. L. Donoho, L. Ying, *Fast Discrete Curvelet Transforms*, Tech. Report, Calif. Inst. of Tech., 2005.
- [3] J.L. Starck, E. Candès, and D.L. Donoho, "The Curvelet Transform for Image Denoising," *IEEE Trans. Image Proc.*, vol. 11, no. 6, pp. 670-684, 2002.
- [4] J.L. Starck, F. Murtagh, et al, "A DCT domain system for robust image watermarking," *Signal Proc., Special Issue in "Copyright Protection and Access Control for Multimedia Services,"*, pp. 357-372, 1998.
- [5] Rakesh Dugad, Krishna Ratakonda, et al, A new wavelet-based scheme for watermarking images, *Proc., IEEE Inter. Conf., on Image Proc., ICIP 98, Chicago, IL, USA*, pp. 419-423, October 1998.
- [6] T.D. Hien, Z. Nakao, and Y.-W. Chen, "Robust digital watermarking based on principal component analysis," *Internat. J. Comput. Intell. Appl.* vol. 4, no. 2, pp. 183-192, 2004.
- [7] E. J. Candès and D. L. Donoho, "New tight frames of curvelets and optimal representations of objects with piecewise-C2 singularities," *Comm. on Pure and Appl. Math*, vol. 57, pp. 219–266. 2004.

- [8] J.L. Starck, D.L. Donoho, and E.J. Candes, "Astronomical Image Representation by the Curvelet Transform," *Astronomy and astrophysics(Berlin. Print)*, vol. 398, pp. 785-800, 2003.
- [9] P. Campisi, D. Kundur, and A. Neri, "Robust Digital Watermarking in the Ridgelet Domain," *IEEE Signal Processing Letters*, vol. 11, no. 10, pp. 826-830, October 2004.
- [10] J.-L. Starck, F. Murtagh, E. Candes, and DL Donoho, "Gray and Color Image Contrast Enhancement by the Curvelet Transform," *IEEE Transaction on Image Processing*, vol. 12, no. 6, pp. 706-717, 2003.
- [11] T.D. Hien, Z. Nakao, and Y.-W. Chen, "Robust multi-logo watermarking by RDWT and ICA," *Signal Processing archive*, Vol. 86, pp. 2981-2993, December 2005.
- [12] T.D. Hien, Z. Nakao, and Y.-W. Chen, "RDWT/ICA for Image Authentication," *The 5th IEEE International Symposium on Signal Processing and Information Technology*, Athens, Greece, pp. 18-21, December 2005.

Fairness Enhancement of IEEE 802.11 Ad Hoc Mode Using Rescue Frames

Mohamed Youssef

Department of Electrical Engineering
and Computer Engineering
Université de Sherbrooke
Sherbrooke, QC, Canada, J1K 2R1
M.Medhat@USherbrooke.ca

Eric Thibodeau

Department of Electrical Engineering
and Computer Engineering
Université de Sherbrooke
Sherbrooke, QC, Canada, J1K 2R1
Eric.Thibodeau@USherbrooke.ca

Alain C. Houle

Department of Electrical Engineering
and Computer Engineering
Université de Sherbrooke
Sherbrooke, QC, Canada, J1K 2R1
Alain.Houle@USherbrooke.ca

Abstract- The IEEE 802.11 standard suffers from severe fairness problems when used in multi-hop ad hoc networks. There are situations where some nodes are transmitting at a much lower throughput than other members of the network. These nodes are unable of realizing their underprivileged situation compared to their neighbors. Neither are they able to communicate with the transmitters causing this unfairness due to the short transmission range compared to the larger carrier sense range. The classical RTS/CTS mechanism cannot solve this problem. This paper presents an algorithm called Fairness Enhancement through Rescue frames (FER) that suggests a solution to the 802.11 unfairness problem using information about transmission delays in the network. The delay values pass through a simple weighted average process that takes account the node history in order to make our algorithm robust against temporary conditions. This delay information is conveyed using Beacon frames. We introduce a new frame type called “Rescue frame” which is transmitted when an unfair situation is perceived in the network. This is followed by decreasing the contention window size of the disadvantaged node and hence, increasing its throughput. The proposed algorithm shows a significant enhancement in fairness of the IEEE 802.11 in ad hoc mode. It is also proven to be effective in dynamically varying environments. Finally, it is fully compatible with other nodes using legacy IEEE 802.11 versions.

I. INTRODUCTION

IEEE 802.11, a.k.a. Wi-Fi, has become the predominant option for the physical and the medium access control (MAC) layers of wireless local area networks (WLANs) [1]. Wi-Fi equipments are low cost and widely used for indoor and outdoor applications. The 802.11 standard is simple and is indeed a good choice for single hop infrastructure networks. However, 802.11 shows noteworthy quality of service (QoS) gaps when used in ad hoc networks. Hidden/exposed nodes problems [1], degradation of the performance of upper layers protocols, specially the Transmission Control Protocol (TCP) [2, 3], and unfair bandwidth distribution [4] are examples of 802.11 misbehavior.

In this paper, we solve the unfairness problem of the IEEE 802.11 standard by manipulating the size of the contention window. This solution has been explored by several previous works such as [5] and [6]. However, the novelty of our algorithm resides in the way it solves two main issues. The

first issue is how to make the disadvantaged emitter detect its unfair situation. The second issue is that the algorithm has to be fast enough so that the detection of the unfair situation, the reaction to restore fairness conditions of the network, and the return to normal behavior once abnormal conditions are gone occur as fast as possible.

In the following sections, we first describe the unfairness problem of the 802.11 ad hoc mode (Section II). The problem is exposed through two scenarios, the first featuring a static node topology while the second is dynamic. Section III is dedicated to the explanation of the Fairness Enhancement through Rescue frames (FER) algorithm. We start by highlighting the characteristics of a generic solution to the 802.11 unfairness problem. Then, we detail the proposed FER algorithm and simulation results of the FER implementation are reported. Finally, Section IV concludes the paper and discusses future work.

II. 802.11 UNFAIRNESS IN AD HOC NETWORKS

A. Transmission Range and Carrier Sense Ranges

Contrary to 802.11 infrastructure networks where all the terminals reside within the transmission range of the access point, 802.11 ad hoc networks have to differentiate between two ranges [1]:

1. The Transmission (TX) range: where a transmitted frame is received correctly if no collisions occur.
2. The Carrier Sense (CS) range: where the frame transmission is being detected and the medium is considered busy. However, the receiver is unable to understand the ongoing transmission because the received power falls under the receiver sensitivity limit.

The TX range depends mainly on the transmission power, the propagation properties and the transmission rate. Effectively, different TX ranges coexist in an 802.11 network due to the support of different transmission rates. For example, 802.11b supports transmission at 1, 2, 5.5 and 11 Mbps [7]. Since the 802.11 standard allows transmission at constant power, transmitted frames at lower rates have more energy per symbol and can then travel longer distances at equivalent Bit Error Rate (BER). Only unicast data/management frames shall be sent on any supported data rate. All other frames (broadcast, multicast and control) are transmitted with a basic rate (1 or 2 Mbps). Most wireless

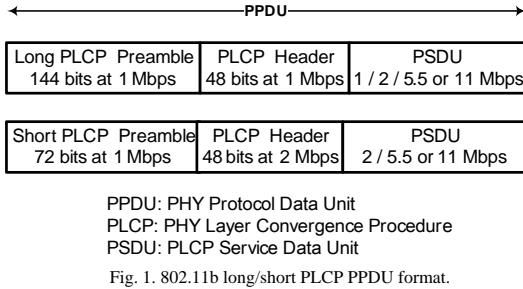


Fig. 1. 802.11b long/short PLCP PPDU format.

cards support some kind of techniques like Auto Rate Fallback (ARF) that allows a dynamic change of the transmission rate depending on the BER to maximize the performance and the transmission range [8]. Moreover, even a single 802.11 frame is normally transmitted with different rates and hence has different transmission ranges. Fig.1 shows an example of an 802.11b frame transmitted with different rates.

The CS range depends mainly on the receiver sensitivity and the radio propagation properties. It is independent of the transmission rate and is larger than twice the TX range at 1 Mbps. For example, Anastasi et al. estimated the TX range for their 802.11b cards to be around 120 m for the 1 Mbps case and 30 m for the 11 Mbps case, whereas the CS range was assumed to be approximately 250 m [1].

A node that exists within the CS range of a transmitting node while being outside of its TX range will consider the medium as busy and will defer any pending transmissions. When the medium gets back to idle, the node should wait for an EIFS (Extended InterFrame Space) interval of time which is larger than the DIFS (Distributed InterFrame Space) normally used if the node was in TX range of the transmitter and could receive the transmitted frame correctly.

B. The Extended Hidden/Exposed Terminal Problem

The extended hidden/exposed terminal problem was addressed by authors in [1] and is shown in Fig. 2. The ongoing transmission between terminals C and D blocks communication between A and B. Terminals C and D are outside the CS range of A. Therefore, terminals C and D are hidden to A. B may not be able to correctly receive the frames sent by A because of the interference from the ongoing transmissions between C and D. Additionally, terminals C and D reside within the CS range of B that senses the medium as busy and cannot initiate a transmission to A unless C and D become silent. Terminal B is then exposed to the transmissions between C and D.

The Request-To-Send/Clear-To-Send (RTS/CTS) mechanism is unable to solve the problem since any RTS/CTS frame transmitted by either of the A/B or C/D pairs doesn't reach the other pair. The problem may be seen as follows: we have two segments in the same network that mutually influence each other but they are unable to exchange information since their TX ranges don't intersect.

We have called this problem "the extended hidden/exposed terminal problem" since it extends beyond

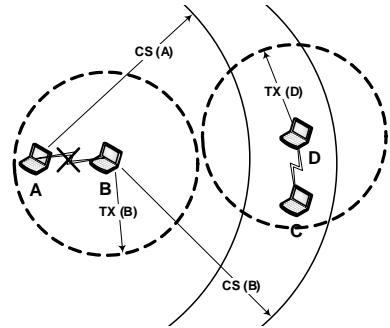


Fig. 2. The extended hidden/exposed terminal problem.

the limits of the well known hidden/exposed problem that considers only the TX range. The extended hidden/exposed terminal problem will be exposed in the following sections through two simulation scenarios.

C. The Simulation Environment

The simulations are made using Network Simulator (ns-2) [9]. We modified the 802.11 MAC model to simulate the Announcement Traffic Indication Message (ATIM) period and the transmission of the Beacons. Moreover, ns-2 doesn't simulate the presence of different TX ranges in the network. All frames travel a same distance which is defined by the parameter RXThresh_ that represents the receiving power threshold of frames within the TX range. We substituted RXThresh_ by two other parameters: BRXThresh_ that defines the receive threshold for a frame transmitted with a basic rate and DRXThresh_ that defines the receive threshold for a frame transmitted with a data rate. We didn't simulate the dynamic rate selection feature in order to simplify the analysis. We preferred to simulate the extreme TX ranges for the case of the 802.11b standard, i.e. 11 Mbps as data rate and 1 Mbps as basic rate. We also disabled the RTS/CTS mechanism in our simulations as it doesn't provide – in most of the cases – any performance improvement while causing a throughput degradation due to the introduced overhead [1].

The transport protocol used is UDP. We didn't use TCP to isolate the behavior of the 802.11 and to avoid the conflictual interaction between TCP and 802.11. The UDP packet size is 1000 bytes. In order to saturate the medium, we used Constant Bit Rate (CBR) traffic with 1 ms time interval between two successive UDP packets. Hence, the required throughput is 8 Mbps which is much larger than the channel capacity.

We considered the physical characteristics of a wireless *ORINOCO™ 11b PCI* card in an open range which gives a TX range of 160 m for the 11 Mbps and 550 m for the 1 Mbps [10]. Since the specifications of the card don't mention the CS range, we assumed a difference of 14 dB between the receive threshold at 1 Mbps and the CS threshold which gives a CS range of 1231 m. We found that CS adequate as it is larger than the double of the TX range at 1 Mbps. This difference of 14 dB is inspired from the default configuration of ns-2 which gives a TX range of 250 m and a

CS range of 550 m. The results of the simulations will be valid for other types of cards having similar ratios between TX and CS ranges.

D. The Three Pairs Static Scenario

This is a classical scenario that clearly reveals the extended hidden/exposed terminal problem. It has been addressed by previous works [11]. We have three pairs of transmitter/receiver, as shown in Fig. 3. The pair in the middle (2-3) is outside the TX range of the exterior pairs (0-1 and 4-5) but within their CS ranges. Therefore, the middle pair detects the transmissions of the exterior pairs but is unable to understand them. Meanwhile, the exterior pairs are outside the CS of each other and don't detect their respective transmissions. The terminals 6 and 7 are necessary to build a single Independent Basic Service Set (IBSS).

Results of that scenario are shown in Fig. 4. The central pair has an average throughput of 0.48 Mbps compared to 4.55 Mbps for each exterior pair. The throughput of the central pair is 10.5% of the throughput of an exterior pair, which clearly shows the unfairness problem. This percentage may be a little less if we decrease the frame size and vice versa. This percentage is higher than the 1-5% suggested by [11] where the transmission of Beacons and the presence of the ATIM period are not considered.

This severe unfairness is caused by the asymmetrical case where the transmission of the central pair should wait for a moment of silence by both the two exterior pairs whereas each exterior pair waits for the central pair only. The situation is worsened for the central pair because of its excessive use of the EIFS. The network is seen as fragmented into two segments, each composed of the central and an exterior pair. The throughput of each exterior pair approaches the maximal throughput which is 5.1 Mbps in our simulation conditions.

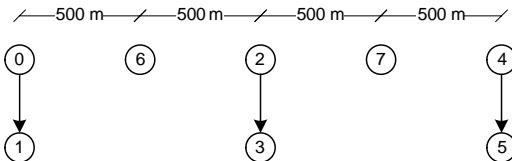


Fig. 3. The three pairs static scenario

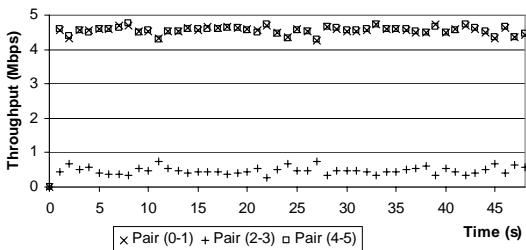


Fig. 4. The throughputs of the three pairs static scenario.

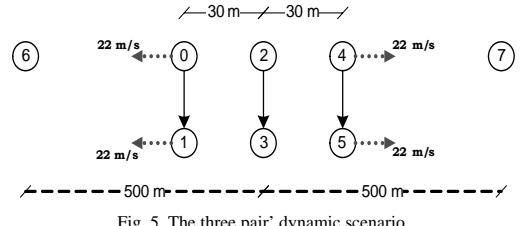


Fig. 5. The three pair's dynamic scenario.

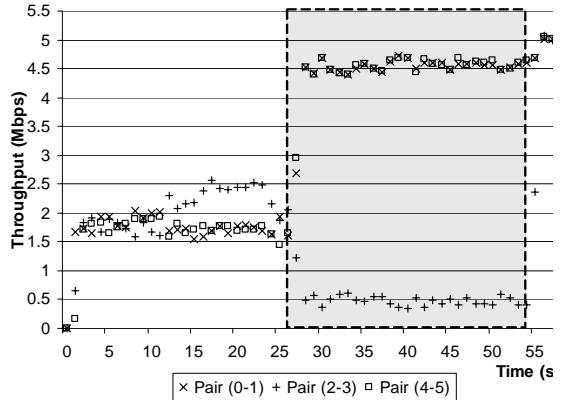


Fig. 6. The throughputs of the three pairs' dynamic scenario

E. The Three Pairs Dynamic Scenario

This scenario aims at strengthening the observations in the first scenario when nodes mobility is taken into consideration. A similar simulation has been made in [12]. Here again, we added terminals 6 and 7 to create a single IBSS.

As shown in Fig. 5, the three pairs start close so that they are all in the same TX range. Then, the two exterior pairs start moving outwards with a constant speed of 22 m/s. The results are shown in Fig. 6. We can see that the bandwidth is almost fairly distributed until the three pairs get in the symmetric and unfair situation shown in the static scenario where the central pair exists in the CS range of the exterior pairs whereas the exterior pairs evolve independently of each other. This situation is marked by the gray zone in Fig. 6 (between [26.75,54.6] s).

III. THE FAIRNESS ENHANCEMENT THROUGH RESCUE FRAMES (FER) ALGORITHM

A. Characteristics of the Proposed Solution

In this section, we resume the general characteristics that should be present in a generic algorithm that suggests a solution to the 802.11 unfairness:

1. A terminal should be able to evaluate its transmission performance compared to its neighbors.
2. As the unfairness problem appears normally when the medium is already congested, a terminal should have a *backdoor* communication channel in order to communicate with its neighbors.

3. The wireless channel is prone to temporary variations as obstacles or interference. Therefore, a fairness algorithm has to start in real situations of unfairness and should be robust against conditions that cause a temporary decrease of the performance.
4. An ad hoc network is a dynamic and a fast changing environment. The algorithm should start as soon as possible after the start of the unfairness situation and should end as fast as possible after it ends.
5. Modification to the 802.11 standard should be minor and shouldn't cause any interoperability problems with other terminals using legacy versions of 802.11.
6. As in our scenarios, the disadvantaged terminal may be unable to communicate with the transmitters causing its unfair situation as they are outside of its TX range. Therefore, we need a bridge terminal that takes the responsibility of such connection.

B. Illustration and Justification of the Algorithm

In order to allow a certain terminal to evaluate its performance compared to its neighbors, we use information about the transmission delay (TD) of a frame. The TD calculation starts from the time where a terminal decides to transmit (or to retransmit) a frame and until reception of an Acknowledgment (ACK) or the expiration of the waiting timer. Therefore, TD includes all the backoff and defer times. Our simulation results showed that the TD of the central pair in the unfair situation is more than nine times the TD of an exterior pair.

Each terminal has a Transmission Delay Queue (TxDelayQueue) that contains the last eleven TD values. Each time a new TD is inserted, the TxDelayQueue passes through a simple weighted moving average giving emphasis to the most recent TD values, as shown in Fig. 7. An average value is then calculated and will be called Weighted Transmission Delay (WTxDelay_{_}). This value represents a measure of the TD encountered by the terminal considering its history and giving more weight to the recent values. This weighted moving average process produces the robustness of our algorithm: although the new TD values have more weight, one or two large temporary TDs will not cause unnecessary triggering of our algorithm if the terminal's history indicates a low TD.

Each terminal includes its most recent value of WTxDelay_{_} with its transmitted Beacons. We chose the Beacons to transmit this TD information for the following reasons:

1. Beacons are periodic frames that are used for network synchronization. The time interval between Beacons (aBeaconPeriod) is in the order of 0.1 s. We find this interval suitable for updating the TD information in the network.
2. Beacons are broadcasted. Therefore, they are transmitted with the basic rate and will travel longer distances. They will be received by the entire neighborhood as well.
3. Beacons are Management frames. They may include new variable length information fields without causing

- incompatibility problems with previous 802.11 versions.
4. Beacons have their own backoff mechanism that starts for all terminals at almost the same time and uses the same Contention Window (CW). This gives a higher chance for a terminal in an unfair situation to transmit a Beacon that includes its TD information.

When a terminal receives the TD information of a neighboring terminal, it enqueues this value in the Received Delay Queue (RxDelayQueue) which is also a queue of eleven values. Then the RxDelayQueue passes through the same weighted moving average process shown in Fig. 7 in order to calculate the value of the Weighted Received Delay (WRxDelay_{_}) that is a measure of the average TD in the terminal neighborhood.

Once a terminal receives a Beacon including a TD and just before enqueueing the new value in the RxDelayQueue, the terminal makes the unfairness check. It simply checks if the received TD is higher than eight times the value of WRxDelay_{_}. If so, the terminal declares a case of unfairness and sends a Rescue frame. Considering the results in the first scenario where the TD of a terminal in the unfair situation was more than nine times higher than the TD of the exterior pairs, we wanted to use a ratio which is little less than nine as the first scenario represents an extreme case. However, that ratio shouldn't be too small in order to avoid false alarms of unfair situations. We found that eight gives good results.

The Rescue frame is introduced by this work and is shown in Fig. 8. The Receiver Address (RA) is a broadcast address. The Emergency Address (EA) is the address of the terminal suffering unfairness. The Emergency Delay (EmDelay) field is the value of the TD of the disadvantaged terminal (it is equal to the value WTxDelay_{_} sent by the disadvantaged terminal in its Beacon frame). The Emergency Weighted Received Delay (EmWRxDelay) includes the value of the WRxDelay_{_} used by the terminal when making the unfairness check.

The Rescue frame is sent in the ATIM period, right after

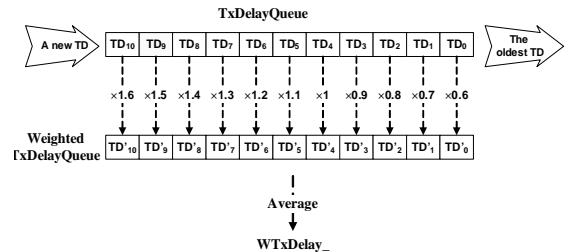


Fig. 7. The WTxDelay_{_} is the average value of the weighted TxDelayQueue

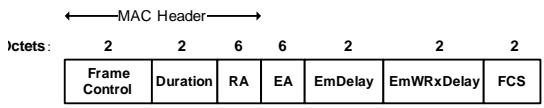


Fig. 8. The Rescue frame format.

the Beacon. All terminals should wake up during that period that is reserved for Beacons and power management frames. It is much less congested, which justifies its usage for sending the Rescue frames. Hence, the Beacons and the ATIM period play the role of the backdoor information channel used when the medium is highly congested.

When a terminal receives a Rescue frame, it checks if the EA corresponds to its address. If so, the terminal gets aware of its unfair situation compared to its neighbors. It then sets its emergency flag meaning that the terminal is in the emergency mode and will be using a CW of $(\text{CWmin}-1)/2$. After each aBeaconPeriod, a terminal in the emergency mode will increment its emergency counter. Once the counter reaches 20, the terminal resets its emergency flag and gets back to its normal 802.11 operation. The emergency counter is reset every time the terminal receives another Rescue frame indicating the persistence of its unfair situation. Hence, the minimum period for being in the emergency mode is around 2 seconds (20×0.1). This value has been chosen empirically. It has to be long enough to avoid severe peaks and valleys in the throughput graph, while it has to be short enough so that the terminal gets back to normal operation once the unfair conditions are gone.

C. Results

In order to compare between the fairness level before and after the implementation of the FER algorithm, we made use of the Coefficient of Variation (CV) which is a dimensionless value defined by the ratio of the standard deviation of the throughput (σ) to its mean (μ). The CV is useful for comparing the degree of variation from one data series to another even if the means are different from each other. It is reported as a percentage:

$$CV(\%) = \frac{\sigma}{\mu} \times 100$$

The $CV(\%)$ will be used as the fairness coefficient. A large value of the fairness coefficient indicates more data dispersion around the mean which subsequently indicates an unfair medium where the throughputs are highly deviated.

The fairness enhancement for the case of the first scenario is shown in Table I. The average throughput of every pair (in Mbps), the total average throughput (in Mbps), the standard deviation (in Mbps) and finally the fairness coefficient (in %) are shown.

We note a seven-fold increase of the fairness level in the network. The price of such enhancement is a decrease of the total throughput which was expected as the two exterior pairs should be more silent because of the throughput increase of the central pair. Nevertheless, when we compare the 12% decrease of the total average throughput to the significant increase in the medium fairness we find the results satisfactory.

Table II shows the improvement brought to the dynamic scenario. The fairness coefficient is more than thirteen times better. Again, the total average throughput had a slight decrease (8%). However, the most important results drawn

from that scenario are about the robustness and the rapidity of the algorithm. Fig. 9 shows the throughput of the three pairs in the dynamic scenario after the implementation of the FER algorithm. We can see that the graphs before (see Fig. 6) and after the FER implementation are identical until the gray zone that denotes the interval where the central pair suffered from severe unfairness. This shows the robustness of our algorithm against provisional long TDs, thanks to the weighted moving average process. Also, we note that the nodes start the FER algorithm as soon as they get in the unfair zone and end it just after the unfair conditions are gone. Therefore, even in high mobility conditions ($22 \text{ m/s} \approx 80 \text{ km/h}$), the FER algorithm shows a remarkable performance.

TABLE I
FAIRNESS ENHANCEMENT OF THE STATIC SCENARIO

	μ_{0-1}	μ_{2-3}	μ_{4-5}	μ_{total}	σ	$CV(\%)$
Before	4.55	0.48	4.55	3.19	2.35	73.67
After	2.95	2.46	2.99	2.8	0.29	10.36

TABLE II
FAIRNESS ENHANCEMENT OF THE DYNAMIC SCENARIO

	μ_{0-1}	μ_{2-3}	μ_{4-5}	μ_{total}	σ	$CV(\%)$
Before	3.33	1.51	3.3	2.71	1.04	38.38
After	2.49	2.55	2.42	2.49	0.07	2.81

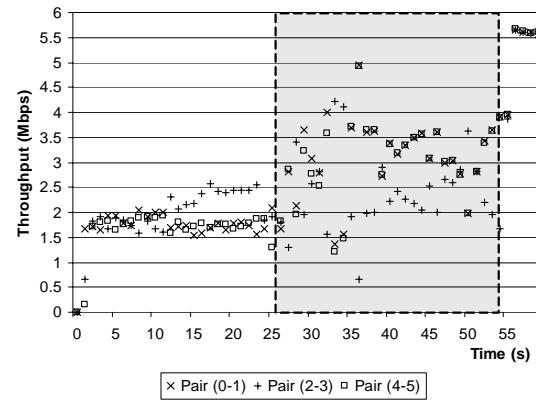


Fig. 9. The throughputs of the three pairs' dynamic scenario after the FER implementation

IV. CONCLUSION AND FUTURE WORKS

In the paper we presented the FER algorithm which greatly enhances the fairness of the IEEE 802.11 standard in ad hoc mode. The FER algorithm uses the TD information as a measure of performance. A weighted moving average process that takes account of the TD history of a terminal allows making our algorithm robust against a provisional long TD. As the disadvantaged terminal is unable to detect its unfair situation by itself and unable to communicate with transmitters causing the unfairness, the unfairness check is made by neighboring terminals acting as bridge nodes: they receive the delay information and diffuse a Rescue frame when necessary. We used the Beacons and the ATIM window as communication tools to overcome the congested channel. In order to enhance its throughput, the disadvantaged node reduces its CW to half of the minimum window length. A counter is used to ensure that the terminal gets back to normal operation once the unfair situation gets to an end. The FER algorithm doesn't cause a harmful traffic overhead because the Rescue frames are transmitted in the ATIM window so they don't compete with DATA frames. FER is a simple and efficient algorithm that doesn't require much processing or memory buffers and doesn't cause incompatibility problems with legacy 802.11 standards.

In some scenarios, we cannot enhance the fairness of the medium without causing a certain degradation of the global performance. In the scenarios shown in this paper, the total average throughput has decreased because the central pair is having more transmission chances and the exterior pairs are having more silence periods. However, the gain in fairness enhancement is of much greater value than the decrease in the overall average throughput.

The proposed FER algorithm opens the door to substantial future work. This algorithm should be tested with TCP. It should also be tested in a multitude of scenarios such as hybrid networks (wired and wireless) and other situations of unfairness. Also, the FER algorithm should be secured against malicious modifications of the CW that are not justified by a real unfair situation. It is worthy to note that the fields EmDelay and EmWRxDelay included in the Rescue frame currently don't have a defined function. In fact, we left those two fields that include the values used when making the emergency test to remind their potential importance for security reasons. For example, a terminal that finds its address in the EA of a rescue frame may check the EmDelay field to be sure that it really matches its TD. Finally, a practical test of the efficiency of the FER algorithm could be done using a test bed with real Wi-Fi equipments.

REFERENCES

- [1] M. C. E. G. Giuseppe Anastasi, "IEEE 802.11 AD HOC Networks: Protocols, Performance, and Open Issues," in *Mobile Ad Hoc Networking*, M. C. S. G. I. S. Stefano Basagni, Ed., 2004, pp. 69-116.
- [2] S. Xu and T. Saadawi, "Revealing the problems with 802.11 medium access control protocol in multi-hop wireless ad hoc networks," *Computer Networks*, vol. 38, pp. 531-548, 2002.
- [3] X. Kaixin, B. Sang, L. Sungwook, and G. Mario, "TCP behavior across multihop wireless networks and the wired internet," in *Proceedings of the 5th ACM international workshop on Wireless mobile multimedia*. Atlanta, Georgia, USA: ACM Press, 2002.
- [4] C. Chaudet, D. Dhoutaut, and I. G. Lassous, "Performance issues with IEEE 802.11 in ad hoc networking," *IEEE Communication Magazine*, 2005.
- [5] B. Brahim, W. Yu, and K. Chi Chung, "Fair medium access in 802.11 based wireless ad-hoc networks," in *Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing*. Boston, Massachusetts: IEEE Press, 2000.
- [6] L. Bononi, M. Conti, and E. Gregori, "Runtime optimization of IEEE 802.11 wireless LANs performance," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 15, pp. 66-80, 2004.
- [7] "IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirement. Part 11: wireless LAN medium access control (MAC) and Physical layer (PHY) specifications. Amendment 2: higher-speed physical layer (PHY) extension in the 2.4 GHz band - corrigendum 1," *IEEE Std 802.11b-1999/Cor 1-2001*, 2001.
- [8] L. M. Ad Kameran, "WaveLAN-II: a high-performance wireless LAN for the unlicensed band," *Bell Labs Technical Journal*, vol. 2, pp. 118-133, 1997.
- [9] T. V. Project, "The Network Simulator Main Page," http://nsnam.isi.edu/nsnam/index.php/Main_Page.
- [10] PROXIMwireless, "ORiNOCO® 11b Client PC Card datasheet." http://www.proxim.com/learn/library/datasheets/11bpcard_A4.pdf.
- [11] C. Chaudet, I. G. Lassous, E. Thierry, and B. Gaujal, "Study of the impact of asymmetry and carrier sense mechanism in IEEE 802.11 multi-hop networks through a basic case," in *Proceedings of the 1st ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks*. Venezia, Italy: ACM Press, 2004.
- [12] D. Dhoutaut, "Etude du standard IEEE 802.11 dans le cadre des réseaux ad hoc: de la simulation à l'expérimentation," Ph. D. Thesis, INSA de Lyon, December, 2003.

Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective

Mohammad Momani¹, Subhash Challa¹, Khalid Aboura¹

¹University of Technology, Networked Sensors Technologies Lab. (NeST)

Information & Communication Technology Group

1 Broadway, Sydney 2007, Australia

mmomani@eng.uts.edu.au

Abstract - This paper surveys the state of the art trust-based systems in Wireless Sensor Networks (WSN); it highlights the difference between Mobile ad hoc networks (MANET) and WSN and based on this observed difference (monitoring events and reporting data) a new trust model is introduced, which takes sensor reliability as a component of trust. A new definition of trust is created based on the newly introduced component of trust (sensor data) and an extension of node misbehaviour classification is also presented based on this new component of trust.

1. INTRODUCTION

Wireless sensor networks (WSN) as a special type of mobile ad hoc networks (MANET) has an additional function to the traditional functions of an ad hoc network, which is monitoring events and reporting data. This observed difference is the foundation of our new approach to model trust in WSN.

Trust in WSN plays an important role in constructing the network and making the addition or deletion of sensor nodes from a network very smooth and transparent. The creation, operation, management and survival of WSN are dependent upon the cooperative and trusting nature of its nodes, therefore the trust establishment between nodes is a must.

Trust as prerequisite to secure communication between nodes, somebody might ask, How can we be sure that all nodes are trusted in order to establish a secure communication between them? There must be a new mechanism to establish trust in top of the existing mechanisms, so we introduce a new approach of establishing trust (assessing the node behaviour) using the sensor data as discussed in section 3. So our main contribution in this paper is introducing the sensor data as an additional metric (decisive component) to check the trustworthiness of a node which is to the best of our knowledge has not been addressed before.

In this paper we redefined trust in WSN based on the existing definitions and the newly introduced component of trust (sensor data) and we introduce a new trust computational model based on that. And we presented a survey on WSN trust based systems to help researchers getting a brief description of the problem and also to use it as a starting point to do a further research in the area. The rest of the paper is organised as follows: Section 2 presents our new trust definition and the properties of trust in WSN. We present all the related work

done in the area in section 3. Section 4 presented modelling trust in WSN using the newly introduced component. In section 5 we introduced a new approach of trust formation and section 6 concludes the paper.

2. TRUST DEFINITION AND PROPERTIES

Trust has been defined differently by researchers belong to different research communities. Even in the same research field trust can be defined in a different way depends on the application and the methodology used to calculate trust. We believe that properly defining trust in WSN is the key to understand the meaning of trust and to easily model trust, which is not yet done properly. So firstly we will try to define trust based on the trust classification discussed in [1] and the newly introduced component of trust (sensor data) as discussed later in the paper and from the definition we will be extracting the properties of trust.

Here we will use the same approach given in [1] and [2] to redefine trust with the introduction of the sensor data as a major player of defining trust. The main trust construct as discussed in [1] are: trusting behaviour, trusting intention, trusting beliefs and dispositional trust (risk). According to [2] trust can be classified into two types; reliability trust (trusting behaviour) and decision trust (trusting intention, trusting beliefs and risk). Here we are introducing sensor data as a trust component, so we are redefining trust from communication and data point of views, based on that our new definition of trust is; *Trust is the node's belief in the competence and the reliability of another node*. In other words; *Trust is the subjective probability by which node A depends on node B to fulfil its promises in performing an action and at the same time being reliable in reporting its sensor data* (here we are checking the competence of the node and its reliability and truthfulness of reporting data).

2.1. Properties of trust

From the above definition we can extract the following trust properties to help modelling trust efficiently.

- Trust is subjective - It is based on observations and evidence made available to the node in a specific situation.
- Trust is linked with risk - There is no reason to trust if there is no risk involved.

- Trust is intransitive - If node A trusts node B and node B trusts node C, this does not necessarily imply node A trusts node C.
- Trust is dynamic - Trust may decrease or increase by the time based on new evidence or experience.
- Trust is Asymmetric - Two nodes do not need to have similar trust in each other or about the trustworthiness of another node.
- Trust is reflexive - A node always trusts itself.

3. RELATED WORK

Trust in general has been the focus of many researchers for the last decade, many of them were addressing trust using different techniques to model reputation in different scenarios, mainly peer to peer networks and the internet such as in [3-7]. Trust in WSN is a new area of research and only very few people started to look at the problem such as in [1, 8-13]; however a number of people addressed some of the trust management aspects in mobile ad hoc networks (MANET), which closely resembles the WSN operation such as in [14-18]. In this section we will focus only on the work specifically addressing trust in WSN.

The authors of [8] are proposing to use a single trust value to a whole group (cluster), they are using a group trust management scheme based on their belief that sensor nodes mostly fulfil their responsibilities in a cooperative manner rather than individually. Therefore instead of calculating individual trust, it is more appropriate to calculate the trust for the entire group. This design might help saving node resources as the authors claim but it suffers from the following drawbacks, if one node is compromised (the cluster head for ex.) it will affect the whole group and also malicious nodes within the cluster will have the same trust value as the normal nodes (malicious nodes are difficult to be excluded). Trust in groups might be beneficial when the node has the choice to join a group that can bring it most benefit [3] and also when there is a high mobility in the network, which is not the case in WSN as the nodes are mainly deployed to monitor an event. In section (5) we are proposing a new approach to calculate trust, which we believe is more robust and more efficient than the suggested approach in [8] and addresses its drawbacks.

The authors of [8] are calculating the group trust in three phases, trust calculation at the node, at the cluster head and at the base station. The authors are assuming each node to have a unique ID in the group, and that is not the case in WSN as they are deployed in tens of thousands of nodes and the assignment of unique IDs is not possible and the authors are recognising that as a problem in their conclusion remarks. In their scheme [9], which is based on a distributed trust model to produce trust relationship for sensor networks, they use personal reference and reference as inputs parameters to define trust value (intention). Personal reference according to [9] consists of cryptographic operations parameters, which represent the security mechanisms and node interactive behaviour parameter,

which reflects node availability. We think the scheme in [9] is very complicated especially the security part as they are assuming the communication is happening between base station and node, which is going to generate lots of traffic, (Base stations should not and can not communicate with all nodes, as the range of a node is small, instead nodes in a cluster talk to their cluster head, and cluster heads talk to a sink or a base station).

The authors of [10] were the first to introduce sensor data in their scheme as a function of the watchdog mechanism to calculate trust and according to them the web of trust embedded in every network is used to predict the behaviour of nodes in the network. In their scheme presented in [10], reputation is not a physical quantity but it is a belief; and trust is obtained by taking the statistical expectation of the probability distribution representing the reputation between the two nodes. The scheme operates on the principle of Bayesian decision theory (past behaviour of a node can be used to predict its future behaviour). In their Bayesian representation (BRSN) given in [10], they are assuming the presence of some sort of node authentication technique, which is required to achieve a trustworthy sensor network but on the other hand we argue that due to the mass deployment of sensor nodes in a WSN, it will be very difficult to authenticate nodes.

The authors of [13] are using in their proposed scheme (DRBTS) special nodes known as beacon nodes (BNs) to assist other sensor nodes (SNs) to determine their location based on a simple majority principle. They are proposing a trust system for excluding malicious BNs that provide false location information. In the proposed scheme BNs are monitoring other BNs behaviour, but what about the SNs themselves? If a sensor node is compromised, what is the solution? These questions are not addressed. They are modelling the network as an undirected graph $G = (V; E)$, with the set of vertices V being the set of SNs and BNs and the set of edges E being the link between them. The proposed system has some additional overhead and also requires extra memory to store the reputation tables [13].

4. MODELLING TRUST IN WSN

Trust modelling represents the trustworthiness of each node in the opinion of another node, thus each node associates a trust value with every other node [4], and based on that trust value a risk value required from the node to finish a job can be calculated. As illustrated in Fig. 1, node X might believe that node Y will fulfil 40% of the promises made, while node Z might believe that node Y will fulfil 50% of the promises made.

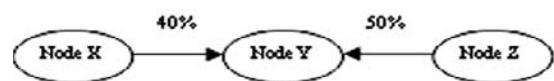


Fig. 1. A simple trust map [4]

In other words trust modelling is simply the mathematical representation of a node's opinion in another node in a network. We argue that almost all the previous work of modelling trust are approaching the problem from a communication point of view and to the best of our knowledge no one is using sensor data as a trust component other than the authors of [10], which are looking at it as a function of the watchdog mechanism, which we believe is not sufficient as the main goal of deploying a WSN is to gather and report information regarding an event, so we are treating the sensor data as a decisive component of trust as shown in Fig. 2. At the beginning the reputation will be calculated based on the direct and indirect communication with the node as discussed in our previous work in [12].

The new approach is calculating trust in a different way, the output of the reputation is coupled with the validity of the sensor data reported from that node and based on that the trust value will be calculated (the trustworthiness of a node will be determined). The sensor data reported from the node will be tested against a predefined threshold, and if the reputation value is enough to do the job (greater or equal to a threshold) and the sensor data is above or equal the predefined threshold, then the node will be considered as trustworthy otherwise a question mark will be put on the node and it will be given another chance to report data in a predetermined period of time, and so on. Detailed analysis of the data and how is it going to be tested will be in our future work.

Trust formation can be divided into 3 stages, the stage of initializing trust, the stage of building trust and the stage of updating trust.

The initialization process, when the network first constructed or when a new node is introduced to the network can be in any of the following methods:

- 1) All nodes are considered to be trustworthy. This is the quickest method of establishing trust, but it is very risky as malicious node can be given a higher trust value. It is a practical method when the network deployment is not for a critical mission (reading temperature)
- 2) All nodes are considered to be untrustworthy. It is very slow method (trust formation takes very long time to be established, but on the other hand it is very robust and can be used in a critical mission networks (battlefields).
- 3) All nodes are neutral; they are neither trustworthy nor untrustworthy. It is in between compared to the other mentioned methods.

The building stage is the process of forming (calculating) trust from direct interactions, which can be achieved by using a watchdog mechanism as in [10] and [13] to monitor the surrounding nodes and indirect interactions (recommendations received from surrounding nodes). Most systems are using both direct and indirect interactions (positive and negative or just either one of them) to update trust, some use only direct interactions and others use only indirect information. In [10], only positive direct experience is exchanged with the surrounding nodes, while in [13], both positive and negative information is exchanged.

The evolution stage is the process of updating trust, which can be achieved using the first hand information, the second hand information or both. Most systems proposed so far use both first hand and second hand information. The main issue here is how to weight that information? Some systems give more weights to the old experience, other systems give more weight to recent experience (aging) such as in [10] and [13].

Trust values regarding other nodes should be maintained locally and updated periodically as new evidence (direct or indirect observation) becomes available. Thus, trust evolves with time as a result of evidence [5]. The evolution process can be regarded as iterating the process of trust formation as additional evidence becomes available. The level of trust must be modified as additional evidence becomes available and that will change the risk assessment of the node [6].

Fig. 2. Trust computational model for WSN

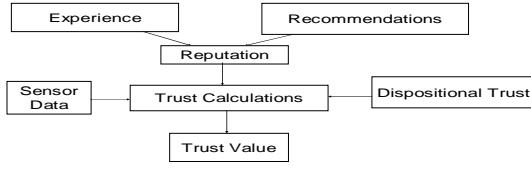
4.1. Trust Formation in WSN

Trust is calculated based on the QoS characteristics (reliability, availability, power, processing speed, memory, data rate...) the main sources for calculating trust as given in Fig. 2 are:

- Sensor Data - Data authentication, expected value
- Observation (experience) - Direct, from the node itself
- Recommendations - Indirect, from surrounding nodes
- Dispositional Trust - The risk, a node is ready to take (new node)
- Reputation (past experience) - In case no observation and experience are available

4.2. Node Misbehaviour in WSN

The main idea behind reputation and trust-based systems is to discover the misbehaving nodes and also to be very robust solutions against insider attacks (to exclude misbehaving nodes and to minimise the damage caused by inside attackers). Most of the researchers are classifying node misbehaviour from the communication point of view, however as discussed so far, WSN are deployed to sense events and report data, so we are



expanding the node misbehaviour diagram given in [11] by introducing a new branch to node misbehaviour addressing sensor data (misinforming) as a new classification of node's misbehaviour as shown below in Fig. 3.

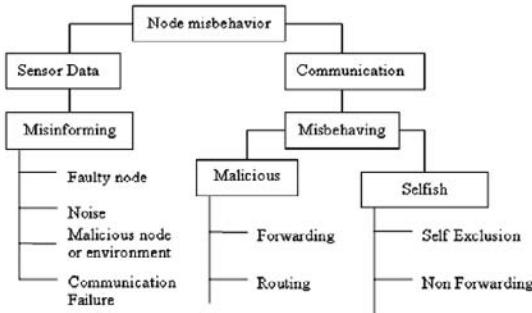


Fig. 3. Node misbehaviour classification

As can be seen from the diagram in Fig. 3, the new branch dealing with sensor data includes the misinforming behaviour of a sensor node which can be caused due to a faulty node (damaged or expired), a noise (as sensor data is not without noise), a malicious node or environment (node get captured or the environment is stuffed) or a communication failure (communication between nodes is cut off for some reason). Readers are advised to refer to [13] to get a detailed information regarding the node misbehaviour communication branch of the diagram given in Fig. 3.

5. A NEW APPROACH OF TRUST FORMATION

Up to this moment and to the best of our knowledge all the research been done in MANET and WSN is taking into considerations the components of trust from a communication point of view. In WSN there is more than just communication and computation, there is a sensing data, as the main goal of distributing sensor is to monitor some events and to gather some data. We argue that to the best of our knowledge we are the first researchers to address trust in WSN in terms of sensing data. We based our new approach in this section based on the existing work done by [8] with the following modifications:

Due to the massive deployment of nodes, the large area of coverage and the short communication range (distance) between nodes in WSN; nodes are grouped in a small ad hoc networks (clusters) and every node is keeping a record of only the surrounding nodes (to save resources). Each cluster has got a cluster head (reporting node) which communicates with other cluster heads or directly with the base station and off to the outside world (Internet). Here we are not giving a single trust value for each group as the authors of [8] suggested, instead we are using the default repeated small world phenomena, which means as individual nodes forms an ad hoc network

between themselves, cluster heads and base stations do exactly the same with their surrounding counterparts and so on, until reaching the coverage of the whole network.

For example, as shown below in the Fig. 4; nodes A, B, C, D, E form a cluster with node R as a cluster head; nodes, F, G, H, I, J form another cluster with node S as a cluster head and nodes K, L, M, N, O forms a third cluster with node T as a cluster head. Nodes R, S and T form a cluster of cluster heads and so on, until the convergence of the whole network; with the assumption that every node belongs to only one cluster.

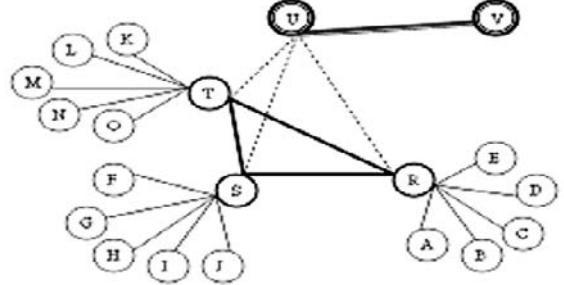


Fig. 4. A new trust model

The approach we are presenting here is different from the approach given in [8]; according to them the cluster head will aggregate all trust values for all nodes to base station and the base station will calculate the group trust value and report it back; which produces in our opinion an extra overhead on the cluster head as communication is the major resource consumer in the whole process. And as we discussed before group trust value is not recommended as the whole group can be affected in case of a cluster head get captured. Instead, in our approach we suggest that individual nodes in the cluster will have trust values for all the nodes in the cluster based on their direct and indirect interactions as shown in our previous work [12].

In addition we introduced in this approach a new trust component, which is the actual sensing data as a decisive component of node trustworthiness. We argue that, the same phenomena is valid for the cluster heads; every cluster head is keeping a record of every other cluster head in the surroundings as was the case within the cluster, and cluster heads report their trust in each other as a recommendation to the base station. The base station compares and calculates the trust in each cluster head based on the direct and indirect interactions with the cluster heads and also on the data reported from the cluster head. Following this design, we can exclude misbehaviour nodes from within the cluster at the cluster level and misbehaviour cluster heads from within the cluster heads cluster at the cluster heads level and so on till reaching the entire network level. Here we assume clusters are more powerful than normal nodes and base stations are of more power than the cluster heads. Also in our approach, we are

combining the communication process and the sensor data to calculate trust not just the communication process as been the case with almost all the previous work done by all researchers to this moment.

The authors of [8] are calculating trust in three different phases to get the group trust value and in our opinion if one phase is wrong the whole result will be wrong and that is the dangerous thing about it, our scheme is calculating trust (the whole trust) at different stages (node, cluster, base station). The model suggested in [8] also does not say how to formulate trust with newly joining nodes (or what is the initial trust between nodes, just as they meet for the first time with no experience or recommendations available).

Scenario; let us consider the following design, we have deployed a network as shown in Fig. 4. where sensors are gathering the temperature of a specific area, the trust between nodes in the cluster is calculated as discussed in our work in [12]. The cluster head is periodically gathering data from all nodes in the cluster. If the data gathered from a node deviate more than a predefined threshold of the actual and estimated value, then the trust value will be affected as we will be discussing in our future work. Sensor readings are not without noise, so when we judge a reading we take into consideration the noise which can be represented as a Gaussian noise.

6. CONCLUSION AND FUTURE WORK

In this paper we introduced a new decisive component of trust in WSN (sensor data) and based on that component we redefined trust in WSN, we introduced a new approach of modelling trust and we also introduced a new classification of nod misbehaviour in WSN. We also presented a survey on all the trusted systems in WSN. The newly presented approach is believed to be very robust as it addresses all the drawbacks from the existing approaches. In our future work we are going to select a mathematical tool to represent our trust model and simulate a network using a network simulator to verify results and finally we are planning of setting up a test bed of WSN to further verify results.

ACKNOWLEDGEMENT

We acknowledge funding for this research through a postgraduate scholarship from the University of Technology, Sydney and partial funding through the ARC Linkage Grant LP0561200.

REFERENCES

- [1] M. Momani, J. Agbinya, G. P. Navarrete, and M. Akache, "Trust Classification in wireless sensor networks," in *8th International Symposium on DSP and Communication Systems, DSPCS'2005*. Noosa Heads, Queensland, Australia, 2005.
- [2] A. Jøsang, C. Keser, and T. Dimitrakos, "Can we manage Trust?," presented at the third international conference in Trust Management, Rocquencourt, France, 2005.
- [3] Y. Wang and J. Vassileva, "Bayesian Network-Based Trust Model," presented at IEEE/WIC International Conference on Web Intelligence, 2003. WI 2003., 2003.
- [4] B. N. Shand, "Trust for resource control: Self-enforcing automatic rational contracts between computers," University of Cambridge Computer Laboratory UCAM-CL-TR-600, 2004.
- [5] G. D. M. Serugendo, "Trust as an Interaction Mechanism for Self-Organising Systems," presented at International Conference on Complex Systems (ICCS'04), Marriott Boston Quincy, Boston, MA, USA, 2004.
- [6] C. English, P. Nixon, S. Terzis, A. McGettrick, and H. Lowe, "Dynamic Trust Models for Ubiquitous Computing Environments," presented at Ubicomp2002 Security Workshop, GÖTEBORG, SWEDEN, 2002.
- [7] A. Abdul-Rahman and S. Hailes, "A Distributed Trust Model," presented at Proceedings of the 1997 workshop on new security paradigms, Langdale, Cumbria, United Kingdom 1997.
- [8] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song, "Trust Management Problem in Distributed Wireless Sensor Networks," presented at 12th IEEE international conference on Embedded and Real-Time Computing Systems and Applications, 2006.
- [9] Z. Yao, D. Kim, I. Lee, K. Kim, and J. Jang, "A Security Framework with Trust Management for Sensor Networks," presented at Workshop of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks, 2005.
- [10] S. Ganeriwal and M. B. Srivastava, "Reputation-based Framework for High Integrity Sensor Networks," presented at the 2nd ACM workshop on Security of ad hoc and sensor networks Washington DC, USA 2004.
- [11] A. Srinivasan, J. Teitelbaum, H. Liang, J. Wu, and M. Cardei, "Reputation and Trust-based Systems for Ad Hoc and Sensor Networks," in *Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks*, A. Boukerche, Ed.: Wiley & Sons, 2007.
- [12] M. Momani, J. Agbinya, R. Alhmouz, G. P. Navarrete, and M. Akache, "A New Framework of Establishing Trust in Wireless Sensor Networks," in *International Conference on Computer & Communication Engineering, (ICCCE '06)*. Kuala Lumpur, Malaysia, 2006.
- [13] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation-based Beacon Trust System," in *2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06)*, 2006.
- [14] L. Eschenauer, "On Trust Establishment in Mobile Ad-Hoc Networks," in *Department of Electrical and Computer Engineering*, vol. Master of Science: University of Maryland, College Park, 2002, pp. 45.
- [15] J. S. Baras and T. Jiang, "Dynamic and distributed trust for mobile ad-hoc networks," presented at 24th Army Science Conference, Orlando, FL, 2004.
- [16] Z. Liu, A. W. Joy, and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks," presented at Distributed Computing Systems, 2004. FTDCS 2004.
- [17] A. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad-hoc Networks," presented at ACM International Conference Proceeding Series, Dunedin, New Zealand, 2004.
- [18] C. R. Davis, "A localized trust management scheme for ad hoc networks," presented at 3rd International Conference on Networking (ICN'04), 2004.

Performability Estimation of Network Services in the Presence of Component Failures*

Mohammad-Mahdi Bidmeshki, Mostafa Shaad Zolpirani, and Seyed Ghassem Miremadi

Computer Engineering Dept.

Sharif University of Technology, Tehran, Iran

{bidmeshk, m_shaad}@ce.sharif.edu, miremadi@sharif.edu

Abstract-This paper presents a performability estimation approach which measures the ability of a network to deliver its services in the presence of component failures. The measurement is based on two important network service parameters, the end-to-end delay and the packet loss. To evaluate the approach, different network topologies are studied using the OPNET Modeler. The results of simulations for four random topologies and two routing protocols, the RIP and the OSPF are presented and compared. The OSPF protocol with different delay timer values is also evaluated.

Keywords

Network Performance, Network Measurement, Failure Injection.

I. INTRODUCTION

Internet advances with new applications in our every-day life signal the importance of the reliability and availability of Internet services. All Internet services and applications basically depend on the Internet routing infrastructure [19]. Data packets are forwarded hop-by-hop in datagram networks according to the routing information located in forwarding tables made by dynamic routing protocols such as BGP [20], OSPF [17], and RIP [13]. In theory, the combination of dynamic routing protocols and sufficient redundancy in network can guarantee data delivery even in case of several severe component failures [1] [19]. In practice, however, the Internet is a complex large-scale loosely-coupled distributed system including many imperfect components [19] [11] which may result in temporary disruption of network services in the presence of failures [10]. Studies show that failures with various effects and severity occur frequently at different locations in the Internet [6] [11]. Dynamic routing protocols can find alternate routes, but it takes time both to detect a failure and to spread necessary update-messages throughout the network. The convergence time of existing routing protocols may be as long as multiple seconds, or even minutes [6] [10]. Many packets may lost or dropt during this time because of transient loops or inconsistent forwarding information [3] [23].

Service Level Agreements (SLAs) are used to characterize services of Internet Service Providers (ISPs). However the main problem with the existing SLA specification is that they do not capture the effects of instantaneous network conditions like failures and congestions [9]. Some analytical models and methods are also introduced to measure the network's reliability or performability. However these methods are mainly based on the loss of traffic and do not model the behaviors of routing protocols [8]. In [9] some metrics for service availability are defined and using them, a set of goodness factors are computed. These factors are used to characterize and compare different topologies in the presence of single link failures. But its method is restricted to OSPF routing protocol and single link failures.

For users, it is important to get an acceptable service quality from the network. Network services can tolerate a maximum delay and/or packet loss and beyond these values, the service quality would become unacceptable. For example, ITU-T G114 recommends a maximum of 150ms one-way latency and less than 1% packet loss for VoIP [7]. Failures can affect the network's packet loss and delay. So the service quality can be used to evaluate different network topologies, protocols and configurations in the presence of failures.

In this paper, to evaluate network's dependability a performability measure that is based on network's end-to-end delay and packet loss is estimated using simulation. This performability measure which is the probability that the network is able to perform the requested service with desired quality in a specified time in the presence of failures can be used to compare different networks, topologies and configurations. OPNET Modeler [18] is used to model and simulate several networks. A failure injector node is placed in the network's model to fail and recover network components during simulation. OPNET supports many network models and configurations and real networks can be modeled with almost no change. Failure injector node uses stochastic model which can lead to simultaneous failures in links and nodes of the network. To evaluate the approach, results of simulations for four random topologies with OSPF and RIP as routing protocol and OSPF protocol with different delay timer values are presented and compared.

The rest of this paper is organized as follows: section 2 reviews related work. In section 3, impacts of failures on network performance are described briefly. Section 4 presents

* This work was partially supported by a grant from Iran Telecommunication Research Center (ITRC)

the performability estimation approach. In section 5 some experimental results are presented. And section 6 concludes the paper and describes future work.

II. RELATED WORK

To evaluate network's reliability or performability, some analytical models are introduced. A review of these models can be found in [8]. However these models only take into account loss of traffic due to failures and do not model the behaviors of routing protocols.

Failures and their effects on routing performance are studied in several works. It is generally believed that a shorter convergence time reduces packet losses [19]. So the main concerns of many studies were convergence time of routing protocols. In [24] the convergence behaviors of several routing protocols are simulated. The authors measured the convergence time, number of routing messages, and the routing loops after node or link failures. Authors in [10] studied the convergence time of BGP routing protocol through the experimental instrumentation of key portions of the Internet, including both passive data collection and fault-injection machines at major Internet exchange points. Based on these data, they described the unexpected properties of BGP convergence such as long convergence time.

Routing loops can also increase the delay of packets in the network. In [5] off-line analyses of trace information containing the header of every packet traversing a link on a backbone ISP are used to detect loops. The authors observed that the forwarding loops are rare, and the delay of packets which do escape a routing loop is increased by 25 to 1300ms.

The loop-free MS distance vector algorithm [15], the ExDBF algorithm [4], and a link state protocol (SPF) are simulated in [22]. It used the NSFNET backbone topology and measured the packet throughput, packet delay and routing bandwidth consumption. The authors observed that although SPF and ExDBF algorithms are known to have transient loops, their packet delivery performance is better than that of loop-free MS algorithm. The packet delivery performance of three routing protocols: RIP, DBF [2], and BGP are studied in [19] using simulation. The authors showed that the packet delivery ratio improves as the network connectivity becomes richer but different routing protocols have different abilities to fully utilize the topological redundancy in the presence of failures. Active and passive measurements are used in [3] to study the impacts of link failures on VoIP performance. It discovered that new protocols and mechanisms are needed to provide a better protection against link failures.

Whatever effects that failures can have on the networks, users expect to be able to get their desired services from the network with acceptable quality. In [9] service availability metrics were defined and are used to characterize different topologies. These metrics were traffic disruption and service disruption time during routing convergence and additional end-to-end delay after routing convergence. In order to quantify network behavior, the authors defined a set of goodness factors based on service availability metrics to

characterize each topology and/or configuration. An offline method was used to calculate service availability and only single link failure was considered. Congestions, multiple link and node failures, and routing protocols other than OSPF, however, were not considered in their work.

In this study, we use simulation to estimate the performability of the network in the presence of failures. Using this performability measure, which is the probability that the network can provide the expected service quality, we investigate the effects of failures on different network topologies and routing protocols. This approach is not restricted to single failures or one type of routing protocol and can provide an insightful view of the network's ability to deal with failures.

III. IMPACT OF FAILURES ON NETWORK PERFORMANCE

In packet switched networks, routing protocols are responsible for finding a path between each pair of active nodes in the network. When a node or link failure occurs, these protocols try to find an alternate route. The time between failure occurrence in a network and updating nodes' routing table is called convergence time [9], and consists of time needed for detecting failure (detection time), sending new updates throughout the network (notification time) and recalculating the new routes (route update).

Routers are equipped with several mechanisms to detect failures, but all of them are based only on local information exchanged between neighboring nodes [9]. Exchanging periodic check messages is a common mechanism used for failure detection by routing protocols [20] [17] [13]. Although these messages consume bandwidth and processing time, they are essential to detect failures. To limit resource consumption and to reduce number of wrong failure detections because of several short-time link-noise periods or temporarily processors' overload, long time interval between consecutive check messages is preferred [12], e.g. in recommended configuration of OSPF [17] failure detection can take 40 to 120 seconds.

When a node detects a failure or recovery of a link or node in the network, i.e. a topology change, according to network's routing protocol, it informs other nodes through topology update messages. It takes time for all nodes in the network to be notified of the topology change. After receiving update messages, each router calculates new routes and updates its routing table. The time needed for recalculation of new routes depends on the number of destination nodes in network. The greater the number of hops and links, the more time required to recalculate and update routing tables. Studies show that routing convergence time may take longer than several minutes [10] [6]. During these long convergence times, some routing tables may be inconsistent and result in transient loops [3] [23], packet loss, and also increase in delay. Besides, the new route may have longer delay than the primary route [9] and can not satisfy service requirements. So failures in network components can influence network's delay and packet loss. These two parameters are also important in

determining the Quality of Service of the network. If traffic generation be continuous, connectivity of the network could also be captured by monitoring packet loss because any disconnection in the network can increase the packet loss.

In this paper, these two parameters are used to evaluate network's service level and estimate its performability. This measure can show how it can provide services in the presence of failures.

IV. PERFORMABILITY ESTIMATION

To evaluate network in face of failures, a measure is needed that reflects the effects of failures on network's ability to provide services. Since network is a *graceful degraded* system, performability would be a good measure that can be used for network dependability evaluation. Performability $P(L, t)$ of a system is a function of time, defined as the probability that the system performance will be at or above some level L at the instant of time t (Eq. 1) [16].

$$\text{Performability}(L, \tau) = \text{prob}\{\text{ServiceLevel} \geq L \mid t = \tau\} \quad (1)$$

As mentioned in section 3, two important network parameters which are affected by failures are end-to-end delay and packet loss. So, in this paper these parameters are used to show network's service level. Using simulation, these parameters are captured during network operation and occurrence of link/node failures. Based on the simulation results, the performability of the network is calculated.

Network applications need a minimum service level to operate properly. For example, ITU-T G114 recommends a maximum of 150ms one-way latency and less than 1% packet loss for VoIP service [7]. This can be different for other network services. In this paper, to estimate the network's performability, a maximum level for the network service level, composed of end-to-end delay and packet loss, which depends on the application type, is assumed. Based on these data, to calculate the network's performability, using Equation 2 the probability that the network can satisfy the assumed service level is computed. In this equation d and p are acceptable maximum end-to-end delay and packet loss in the network. τ is the time at which performability is estimated.

$$\begin{aligned} \text{Performability}(d, p, \tau) &= \\ \text{prob}\{\text{Delay} < d, \text{PacketLoss} < p \mid t = \tau\} \end{aligned} \quad (2)$$

Our simulations are done using OPNET Modeler [18]. The network can be modeled using devices and technologies existed in OPNET's model library. New models can also be built by user. To inject failures into the network, a special node is implemented which gets probability distribution functions of links and nodes failure and recovery times as inputs. OPNET supports many popular distribution functions such as Exponential, Uniform, and Erlang, so user has the flexibility in choosing distributions. Selection of the link or

node to be failed is also done using a probability distribution function. In order to model traffic in the network, some services must be assigned to the network host nodes. OPNET supports many kinds of network services such as file transfer, web browsing, and voice. In our simulations, a number of LAN clients are connected to the edge routers in the network and voice application is used for traffic generation. Voice application in these hosts is set up to generate traffic continuously. Therefore packet loss in network can also capture the connectivity of the network.

V. EXPERIMENTAL RESULTS

In this section in order to show the usefulness of performability estimation approach, some experimental results are presented. To do this, four random topologies with 20 nodes are generated using BRUTE [14]. The characteristics of these topologies are shown in Table I. In these topologies, link delays are assigned randomly between 10 and 30ms based on a uniform distribution. The diameters of all of these topologies are 4.

Probabilistic distributions of failure and recovery times are considered to be exponential. Table II shows the mean of failure and recovery times for network links and nodes. These times were chosen so that the rate of failures would be high enough and the effects of failures would be more distinct in the limited time of simulation. Link or node to be failed is selected based on a Uniform distribution. Simulations are repeated 5 times with different seeds for random generator and the results are averaged.

TABLE I
CHARACTERISTICS OF THE SIMULATED TOPOLOGIES

Topology	1	2	3	4
No. of Links	32	41	43	35
Min Node Degree	2	2	3	3
Max Node Degree	5	8	7	5

TABLE II
SELECTED MEAN FAILURE AND RECOVERY TIMES FOR FAILURE INJECTION

Mean node failure time	500 sec
Mean link failure time	200 sec
Mean node recovery time	300 sec
Mean link recovery time	100 sec

In addition to the network topology and link characteristics, there are some other parameters that can be configured by the network administrator which can affect network performance. Routing protocol is one of these parameters. RIP (a distance vector protocol) and OSPF (a link state protocol) are used as routing protocol in the experiments and the results are presented in sections B and C. Section A compares the network's performability in two cases: without failures and in the presence of failures.

Routing protocols have many configuration parameters which affect their behavior in dealing with failures. For example in OSPF implementation, two timers are used to control the time of SPF calculation after reception of topology change packets. *Delay* timer specifies the delay before SPF

calculation. *Hold Time* specifies minimum time between two consecutive SPF calculations. Because shortest path calculation is a CPU-intensive task, these delays give the router a chance to receive more update-messages that may indicate changes in the topology and amortize the cost of an SPF calculation over a number of update-messages requiring such calculation [21]. On the other hand this delay can increase the time at which the router's forwarding table is invalid. In section D the effects of OSPF delay timer on the network's performance are studied.

A. Effects of Failures on Performability of the Network

In the first experiment, we simulated the network topology 1 and OSPF as routing protocol in two cases: without any failure and in the presence of component failures according to Table II. OSPF was configured to be in LSA driven route update mode, OSPF delay timer was set to 0, and hold timer was set to 1sec. As mentioned earlier as an example, ITU-T G114 recommends a maximum of 150ms one-way latency and less than 1% packet loss for VoIP service. Because the simulated network is small, the end-to-end delay in it is not as much as 150ms. Here we choose 90ms and 100ms for end-to-end delay and 0.5%, 1%, and 1.5% for packet loss to represent the required service levels. Fig. 1 shows the results of one hour simulation for topology 1 with failures. Without component failures the performability of the simulated topology in all chosen service levels is close to 1 and is not shown in the figure. There is a sharp decrease in network's performability at the beginning times of simulation. It's because of low number of data points captured at the beginning of simulation. Thus any low service level point can result in high fluctuation in network's performability. Fig. 1 shows that failures have severe effects on this network and its performability in one hour and selected service levels varies between 0.63 and 0.75.

B. Performability of Different Network Topologies with OSPF Protocol

In this experiment we simulated the topologies of Table I using OSPF as routing protocol. OSPF configuration is similar to section A. Failure rates are as in Table II.

Fig. 2 shows the performability of these networks in one hour of simulation with $p=1\%$ and $d=90\text{ms}$ and Fig. 3 shows the results for $p=1\%$ and $d=100\text{ms}$. Performabilities of the networks in other service levels are similar to these figures and are not shown here. As can be seen in these figures, higher number of links means higher performability. But it is not always true. Although topology 3 has two more links than topology 2, its performability is lower. Adding links should be done carefully in order to increase the performance of the network in presence of failures. There is an apparent difference between the performability of topology 1 and 2, and the effect of network topology on its performability can be clearly discovered.

C. Performability of Network Topologies with RIP Protocol

In this experiment we simulated the topologies of Table I using RIP as routing protocol. RIP was used in its default configuration. Failure rates are chosen as in Table II.

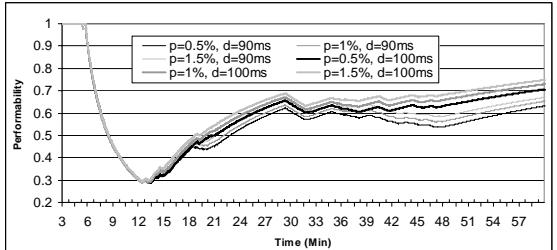


Fig. 1. Performability of topology 1 with failures at different service levels

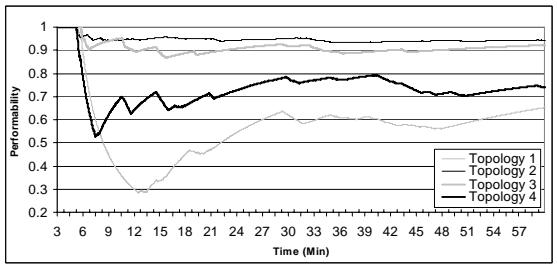


Fig. 2. Performabilities of four simulated topologies using OSPF protocol
($p=1\%$, $d=90\text{ms}$)

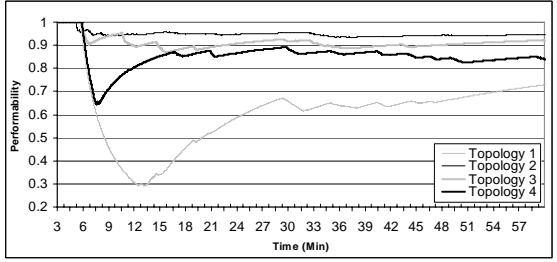


Fig. 3. Performabilities of four simulated topologies using OSPF protocol
($p=1\%$, $d=100\text{ms}$)

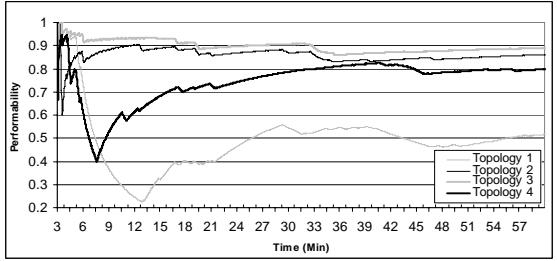


Fig. 4. Performabilities of four simulated topologies using RIP protocol
($p=1\%$, $d=90\text{ms}$)

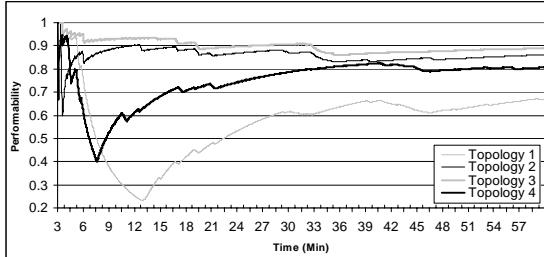


Fig. 5. Performabilities of four simulated topologies with RIP protocol ($p=1\%$, $d=100\text{ms}$)

Fig. 4 shows the simulation results for $p=1\%$ and $d=90\text{ms}$ in one hour of simulation. Fig. 5 shows the results for $p=1\%$ and $d=100\text{ms}$. Performabilities in other service levels are similar to these figures. As can be seen in these figures, using RIP as routing protocol, topology 3 has the best performability. But in case of OSPF, topology 2 has the best performability. However comparison of the results for OSPF and RIP shows that the performability of the OSPF (with the specified configuration) is more than the RIP in these topologies. These results show the importance of routing protocol in determining the performance of the network in presence of failures. For a more general result in comparing these protocols, more simulations on various network topologies and configurations are needed.

D. Effects of OSPF Delay Timer on Network's Performability

In this section we simulated topology 1 with 3 different values for OSPF delay timer. In these simulations, OSPF was configured to be LSA driven and its delay timer was set to 0, 5, and 10sec. The OSPF hold timer was set to 1sec. The results are shown in Fig. 6, 7, 8, and 9 for different service levels.

In Fig. 6 and 8, the performability decreases slightly with the increase of OSPF delay. As the expected delay for the service level increases (for example 100ms instead of 90ms), the OSPF delay timer will have little effect on the performability of this network (see Fig. 7 and 9). The optimum value for the OSPF delay depends on the failure rate of the network components and can be obtained using this approach.

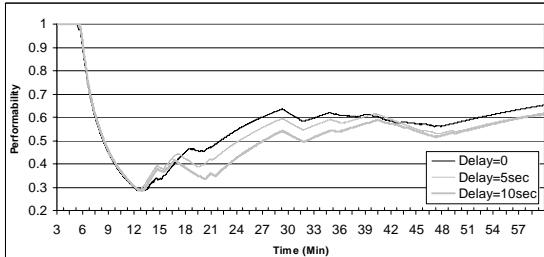


Fig. 6. Effects of OSPF delay timer on network's performability ($p=1\%$, $d=90\text{ms}$)

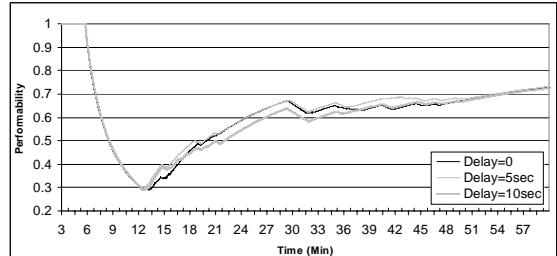


Fig. 7. Effects of OSPF delay timer on network's performability ($p=1\%$, $d=100\text{ms}$)

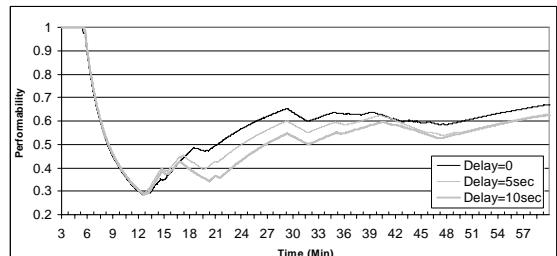


Fig. 8. Effects of OSPF delay timer on network's performability ($p=1.5\%$, $d=90\text{ms}$)

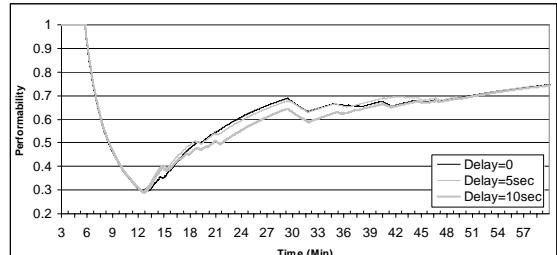


Fig. 9. Effects of OSPF delay timer on network's performability ($p=1.5\%$, $d=100\text{ms}$)

VI. CONCLUSIONS AND FUTURE WORK

In this paper a performability estimation approach was presented to evaluate the network in the presence of component failures. The offered performability measure is based on the network's end-to-end delay and packet loss. Performability is a measure of network's ability to provide services at desired level of quality and can be used to characterize the network behavior in the presence of failures. Usefulness of this measure was shown in this paper with some simulation results for different networks.

The future work would be use of this approach to evaluate and compare other common used topologies, routing protocols and network configurations and study the effects of different failure rates on network's performability. The relations between the topology characteristics such as its diameter and performability are being investigated. We are also working to

extend the performability measure and include other network service parameters in it.

REFERENCES

- [1] P. Baran, "On Distributed Communication Networks," *IEEE Transactions on Communications*, Vol. 2, No. 1, 1964, pp. 1-9.
- [2] D. Bertsekas, and R. Gallager, *Data Networks*, Prentice-Hall, 1992.
- [3] C. Boutermans, G. Iannaccone, and C. Diot, "Impact of Link Failures on VoIP Performance," in *Proceedings of NOSSDAV*, Miami Beach, FL, May 2002.
- [4] C. Cheng, R. Riley, S. Kumar, and J. Garcia-Lunes-Aceves, "A Loop-Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect," in *Proceedings of ACM Sigcomm*, Aug. 1989, pp. 224-236.
- [5] H. Hengartner, S. Moon, R. Mortier, and C. Diot, "Detection and Analysis of Routing Loops in Packet Traces," in *Proceedings of ACM IMW*, Marseille, France, Oct. 2002.
- [6] G. Iannaccone, C. Chuah, R. Mortier, S. Bhattacharya, and C. Diot, "Analysis of Link Failures in an IP Backbone," in *Proceedings of ACM IMW 2002*, Marseille, France, Oct. 2002.
- [7] International Telecommunication Union (ITU). Transmission systems and media, general recommendation on the transmission quality for an entire international telephone connection; one-way transmission time. Recommendation G.114, Telecommunication Standardization Sector of ITU, Geneva, Switzerland, March 1993.
- [8] L. Jereb, "Network Reliability: Models, Measures and Analysis," in *Proceedings of 6th IFIP Workshop on Performance Modeling and Evaluation of ATM Networks*, Tutorial Papers, Ilkley, UK, 1998, pp. T02/1-T02/10.
- [9] R. Keralapura, A. Moerschell, C. N. Cuah, G. Iannaccone, and S. Bhattacharya, "A Case for Using Service Availability to Characterize IP Backbone Topologies," *Journal of Communications and Networks*, Vol. 8, No. 2, June 2006, pp. 1-12.
- [10] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed Internet Routing Convergence," in *Proceedings of ACM SIGCOMM 2000*, Stockholm, Sweden, Aug. 2000, pp. 175-187.
- [11] C. Labovitz, A. Ahuja, and F. Jahanian, "Experimental Study of Internet Stability and Wide-Area Backbone Failures," in *Proceedings of 29th International Symposium on Fault-Tolerant Computing (FTCS)*, Madison, Wisconsin, June 1999.
- [12] G. Litchwald, U. Walter, and M. Zitterbart, "Improving Convergence Time of Routing Protocols," in *Proceedings of 3rd International Conference on Networking (ICN'04)*, Gosier, Guadeloupe, French Caribbean, Mar. 2004.
- [13] G. Malkin, Routing Information Protocol Version 2. RFC 2453, SRI Network Information Center, Nov. 1998.
- [14] A. Medina, A. Lakhina, I. Matta, and J. Byers, "BRITE: An Approach to Universal Topology Generation," in *Proceedings of 9th IEEE Int. Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (MASCOTS'01)*, Cincinnati, Ohio, USA, Aug. 2001.
- [15] P. M. Merlin, and A. Segal, "A Fail-Safe Distributed Routing Protocol," *IEEE Transactions on Communications*, Vol. 27, No. 9, Sep. 1979, pp. 1280-7.
- [16] J. F. Meyer, "On Evaluating the Performability of Degradable Computing Systems," in *Proceedings of 8th IEEE International Symposium on Fault-Tolerant Computing (FTCS-8)*, Toulouse, France, June 1978, pp. 44-49.
- [17] J. Moy, OSPF Version 2. RFC 2328, SRI Network Information Center, Sep. 1998.
- [18] *OPNET Modeler documentation*, OPNET Technologies Inc. <http://www.opnet.com>
- [19] D. Pei, L. Wang, D. Massey, S. Felix Wu, and L. Zhang, "A Study of Packet Delivery Performance during Routing Convergence," in *Proceedings of IEEE International Conference on Dependable Systems and Networks (DSN)*, San Francisco, CA, June 2003.
- [20] Y. Rekhter, and T. Li, Border Gateway Protocol 4, RFC1771, SRI Network Information Center, July 1995.
- [21] A. Shaikh, and Albert Greenberg, "Experience in Black-box OSPF Measurement," in *Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement*, San Francisco, CA, USA, 2001, pp. 113-125.
- [22] A. U. Shankar, C. Alaettinoglu, K. Dussa-Zieger, and I. Matta, "Transient and Steady-State Performance of Routing Protocols: Distance-Vector Versus Link-State," *Journal of Internetworking: Research and Experience*, Vol. 6, 1995, pp. 59-87.
- [23] A. Sridharan, S. Moon, and C. Diot, "On the Causes of Routing Loops," in *Proceedings of ACM Sigcomm Internet Measurement Conference*, Oct. 2003.
- [24] W. T. Zumen, and J. J. G.-L. Aceves, "Dynamics of Distributed Shortest-Path Routing Algorithms," in *Proceedings of ACM SIGCOMM*, Aug. 1991, pp. 31-42.

RBAC Model for SCADA

Munir Majdalawieh¹, Francesco Parisi-Presicce², Ravi Sandhu³

¹ American University of Sharjah, mmajdalawieh@aus.com,

² George Mason University, fparisi@ise.gmu.edu

³ George Mason University and NSD Security, sandhu@gmu.edu

Abstract - This paper focuses on recommending the usage of the Role-Based Access Control (RBAC) model to define the users' security roles, permissions, authorization, and role hierarchy to access the SCADA system. Achieving the desired level of authorization and access control will involve integrating the security system with SCADA operations and building role based access control capabilities in the application level.

Keywords: DNP3, DNPsec, SCADA, RBAC

1.0 Introduction

The Supervisory Control and Data Acquisition (SCADA) systems and the communication network they operate in are moving from proprietary and legacy environment to more open standard, modern microprocessor, and networking technologies. These systems have evolved over the years from totally centralized mainframe systems to distributed systems built with Commercial Off-The-Shelf (COTS) hardware and custom software. Figure 1.0 illustrates the components of SCADA systems. The availability of reliable communications between the SCADA components and the advanced functionality of the software used to manage the hardware systems are the major factors in the renovation and the growth in these systems.

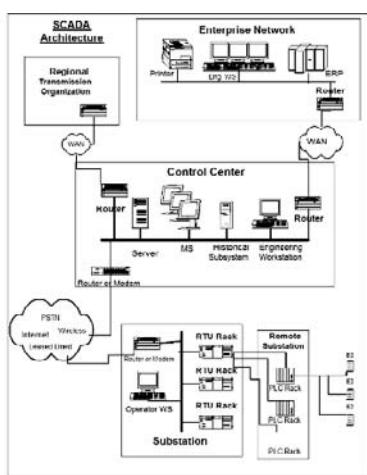


Figure 1.0: SCADA Components

Traditionally, network and security community in the utilities industries have focused virtually most of their

attention on the “enterprise network”, generally ignoring the other part of the network associated with the supervisory control and data acquisition systems in the belief that SCADA resides physically on a separate, standalone network [16]. Combining this assumption with the adoption and the deployment of these new technologies is creating a vulnerable environment for sophisticated terrorist, malicious attacks, cyber assaults, and inside assaults to target and break into the SCADA information systems. As a result, the fundamental principles of security (confidentiality, integrity, and availability) is compromised and the results will create unsafe conditions, which could lead to loss of the critical infrastructure assets, loss of lives, and loss of consumer confidence.

In October 1997, the security of the energy industries became a major focus, when the United States President's Commission on Critical Infrastructure Protection highlighted the risk of successful cyber attacks on the SCADA systems used in these industries as part of the critical infrastructures assets, stating that “the widespread and increasing use of SCADA systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means.” In February 2003, the United States President provided additional attention to these systems and highlighted concern about “the threat of organized cyber attacks capable of causing debilitating disruption to our Nation’s critical infrastructures, economy, or national security,” noting that “disruption of these systems can have significant consequences for public health and safety” and the protection of control systems has become “a national priority.” [20]

This created more urgent need for the SCADA decision makers to take corrective actions to tighten up their security components and protect their assets from such attacks by the use of new security measures. These security measures start by developing a comprehensive security policy to cover all the elements of security infrastructure, and work with the vendors to apply more strict security capabilities in their systems and applications. In addition, the public sector needs to take a practical initiative to partner with the private sector to help in promoting the security’s best practices that have been implemented successfully in its infrastructure. This partnership requires some incentives for the private sector to allocate resources and budget to deal with these issues.

This paper focuses on the access control aspect of the security policy. Our approach is built on the Role-Based Access Control (RBAC) model to define the users' security roles, permissions, authorization, and role hierarchy to access the SCADA system. Achieving the desired level of authorization and access control will involve integrating the security system with SCADA operations and building role based access control capabilities in the application level throughout the entire life-cycle of the development of these applications. Enforcement of access control decisions at the time of assigning roles to users and during a real time operation will prevent malicious commands from reaching the field instruments and thus prevent harm.

RBAC provides great flexibility in the way administrators assign permissions to roles and roles to users. Users have access to the permissions that are associated with roles and users are made members of appropriate roles. Users can be assigned to a role based on their job description and function and easily can be reassigned from one role or another or removed altogether from the system without modifying the underlying access control structure. Role can be granted new permission when necessary, and permission can be removed from role as needed.

Identifying the data types used in SCADA system, the function codes used to communicate between the SCADA objects, and the users who access the SCADA system and defining their roles and responsibilities are the first steps in developing such a policy. In the following subsections we examine each of these elements and their characteristics to motivate our approach.

2.0 Access control security policy

In general, the security policy goal is to protect the organization assets and to ensure that mechanisms are established to protect the assets' confidentiality, integrity, and availability. There are many elements that are part of an enterprise-wide security policy. Few other papers provide high level framework and guidance for SCADA enterprise security policy [10] [21] [22], but very little has been done in providing models for all the elements of the security policy.

SCADA access control security policy starts by identifying critical and important resources, then determining who can access these resources, and knowing exactly what kind of access is provided. The roles within SCADA organization need to be defined and the type of access to these critical resources, activities, and operations need to be detailed.

This paper focuses on the access control security policies within the SCADA resources, mainly in and between the control center (CC), the Substation (SS), and the Remote Substation (RS). The interaction between CC, the Enterprise Network (EN) and the Regional Transmission

Organization (RTO, e.g. electric power industry), is out of the scope of this paper. It is not practical to propose one approach for the entire utilities. Our approach is general since each organization using the SCADA system needs to adjust our model to fit its own specific roles and operations.

RBAC is a framework to help in articulating access control policies. One of the main design principles of the RBAC model is to minimize the potential for inside security violations by providing greater control over users' access to applications, information, and resources. Another design principle of the RBAC model is to allow administrators to assign access control to users based on their function in the organization. RBAC accomplishes this by introducing a new element called role. Roles can be granted new permissions as new functions and actions are incorporated, and permissions can be revoked from roles as needed.

A general RBAC model was defined by Sandhu [15] and a reference model is shown in Figure 2.0a [8]. The core RBAC elements are users, roles, objects, permissions, and operations. A user has access to an object based on his/her assigned role which is defined based on his function in the organization. The object is concerned with the user's role and not the user. Permissions are defined based on job authority and responsibilities within a job function. Operations on an object are invoked based on the permissions.

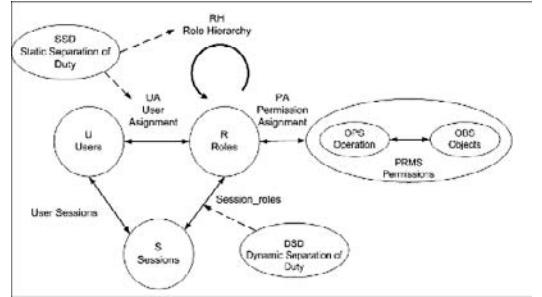


Figure 2.0a, RBAC Reference Model [8]

In RBAC, the administrator uses the role to manage permissions and assignments. For example, a utility company using a SCADA system may create a role called "Senior Operator" that has the permissions to access specific function codes and specific objects that he/she needs to conduct to carry his/her day-to-day job. When a senior operator is hired, he/she is assigned the "Senior Operator" role and directly has all required permissions to do his job.

Section 2.1 introduces the objects of a SCADA system. Section 2.2 describes the first three elements of RBAC: users, roles, and operations on objects. Section 2.3 describes our recommendation for a SCADA role hierarchy. Section 2.4 describes our approach for the permitted operations on objects and functions for the predefined roles

in SCADA systems. Section 2.5 highlights the policy rules in RBAC for SCADA systems.

2.1 SCADA Objects

Objects in SCADA are composed of sets of resources that contain or receive information. Figure 2.1a highlights the objects in SCADA. The Control Center's main function is to monitor and control remote equipment. The control may be automatic, or initiated by operator commands. The CC initiates all communications, gathers and stores data, sends control commands, and interfaces with remote devices directly or through the substations; it provides the infrastructure to the operators to handle these functions. The Historical Server (HS) logs real-time data in the database and is configured for a predefined set of remote devices and equipments. This data is used by the corporate office to conduct business analysis, auditing, and provide reporting.

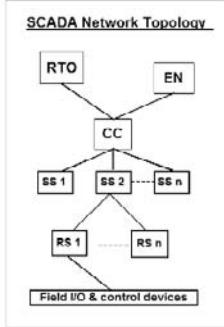


Figure 2.1a, SCADA Objects

The SubStation initiates communication with the Remote Substations or the field devices and works as the middle man between the Control Center and the field devices.

The Remote Substation gathers information from its remote devices, like valves, meters, alarms and pumps and reports it back to the CC or the SS based on the setup and the pre-defined flow of data. The CC or the SS scans IEDs or the IEDs report back data to the Master Station or to the SubStation.

Figure 2.1b [4] depicts some of the inputs and the outputs from and to the three main SCADA components, CC, SS, and RS.

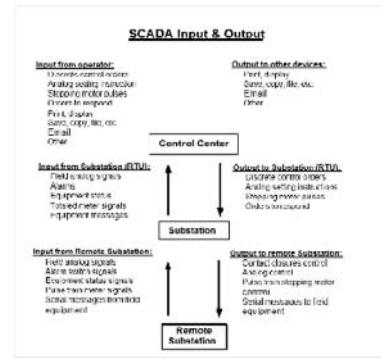


Figure 2.1b, SCADA inputs and outputs per component

The SCADA objects listed above, in addition to the operations and the functions permitted on these objects, need to be listed as part of RBAC permissions in the SCADA application level and in turn to be assigned to roles.

2.2 Users, Roles and Operations

The SCADA internal and external roles need to be identified and the type of access each of these roles requires for the SCADA system should be outlined. The external role is defined as any external user accessing the SCADA system. Access should be allowed only to the HS database and not to any other data in the SCADA system. The flow of this data should be from the SCADA system to the corporate enterprise network. We call this role an External User (EU) Role and the permission type need to be restricted and assigned by the SCADA System Administrator (SA) and the organization should decide what type of security controls should be put in place to enforce such policy.

Several internal roles need to be defined. In a SCADA environment, we find a Manager (MR), a Supervisor (SU), a Senior Operator (SO), a Junior Operator (JO), an Instrument Technician (IT), and an Engineer (EG) role. The permissions to access SCADA objects for these users should be restricted to the role of each user. SCADA applications provide the infrastructure for the CC to communicate with the rest of the SCADA objects. The SCADA Operator initiates the communications with these objects. For example, CC through the MS sends requests (commands) to SS and RS and receives data from SS, RS, and the field devices. It receives requests from EU to access HS.

The policy for the interaction of CC with SS and RS should be centered around the input, the output, and control functions between these identities. CC receives different types of data from SS. For example, CC could receive field analog data, alarms, equipment status, totaled meters signals, and equipment messages. A “Junior Operator” (JO) could have permission to poll and view such data.

Also, CC controls field instruments by executing some operational commands. As a result, MS could send discrete control orders, analog setting instructions, stepping motor pulses, and orders to SS to respond. A Supervisor (SU) could have permission to conduct such functions. In Figure 2.2a, we show the different users, roles, and operations [4] in the SCADA systems.

A utility company using the SCADA system may create the roles and functions we identified in Figure 2.1a. When a user is hired, he/she is assigned the role based on his/her job description and in turn he/she will be carrying his/her job function based on the permissions assigned to his/her role. For example, when the company hires an “Instrument Technician”, the administrator will assign the “Instrument Technician” role to the user. Based on the pre-assigned permission to this role, the user will be able to carry the following operations: view any screen, tune controllers, analyze all alarm reports, and conduct simple configuration. When the user leaves the company, he will be removed from the position of “Instrument Technician” role and no longer has the permission to access the system.

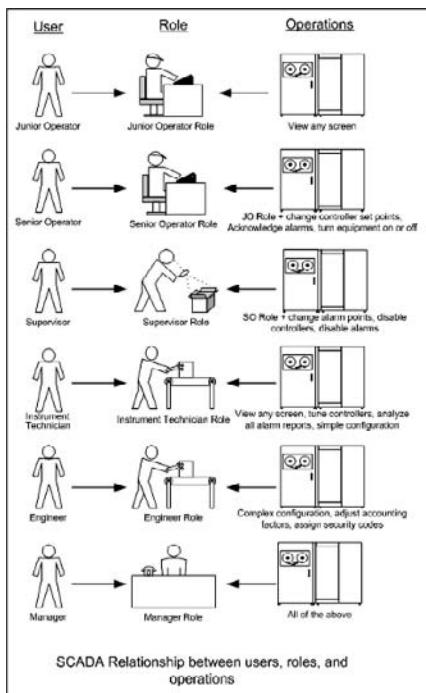


Figure 2.2a, Relationship between users, roles, and operations In SCADA

A user can be assigned to one or many roles, and a role can be assigned to one or many users. In our model we assume that we have a single administrator who assigns users to roles and roles to users. For example, the supervisor is assigned a junior operator, senior operator, and supervisor roles. The supervisor needs all of these roles to conduct his job.

2.3 Role Hierarchy

The Role Hierarchy reflects the organizational structure based on job's authorities and responsibilities. In some organizations, one role can include the tasks and permissions that are associated with another role. In such case, RBAC role hierarchy provides an efficient way to avoid specifying common tasks. Tasks and roles depend on organizational policies. When tasks overlap, you can establish hierarchies of roles.

The President's Critical Infrastructure Protection Board, and the Department of Energy, has developed 21 steps to help a utility organization improve the security of its SCADA system [19]. Step number 12 defines the importance of taking an action to “Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.” To address this issue we recommend a role hierarchy structure for a SCADA organization as described in Figure 3.3a. For example, the “Supervisor” role overlaps with the “Senior Operator” role. SU will have authority to carry the tasks of SO, which is established by assigning SO role to SV.

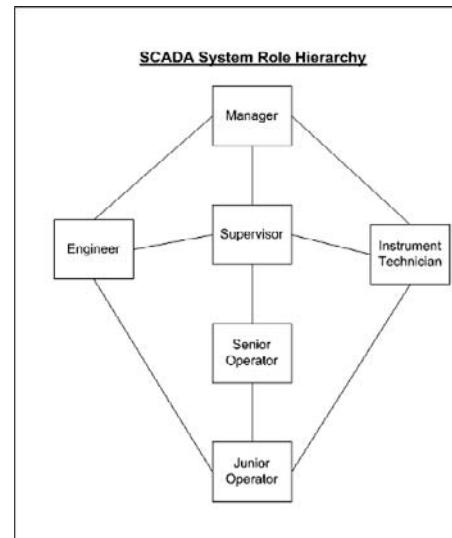


Figure 2.3a, SCADA Role Hierarchy

2.4 Roles and Permissions at the Application Level

Sandhu [13] indicated that the nature of permissions and operations mediated by RBAC depends on the nature of the system in which RBAC is embedded. The authorization decisions associated with the operations are based on factors that can be known only to the application. Similarly, the request (commands) and reply (status/data) control operations must be programmed as part of the SCADA application access control. Vendors should provide functionalities for application programmers to effectively build such application programs that provide abstract application-level operations and to protect them by means of RBAC capabilities. The use of role-based con-

trols at the application level will enable enforcement of policies that closely conform to the intentions of stakeholders, while causing minimal interference with legitimate operator actions.

SCADA abstract application operations and permissions are centered around the system objects and the interface objects. In section 3.1 we discussed the system objects which are composed of CC, SS, RS, and IEDs.

The interface objects are presented by the system communication protocols. There are several protocols that are supported in the SCADA communications architecture. For the purpose of this paper we will use the DNP3 protocol [6] [9]. The DNP3 or Distributed Network Protocol version 3.3 (DNP3) is a telecommunication standard protocol that defines communications between MS, SS, RS, and IEDs. In the Master/Slave architecture, the master communicates with the slaves using the application layer message function.

The DNP frame format is limited to 292 bytes. One important structure of the frame fields is the frame control byte. The control byte is used to communicate the function codes (commands) from the master-to-slave (request) and the slave-to-master (reply). The request commands need to be carefully examined and assigned to the right role and the roles be assigned the right permissions based on the function code of such command. Such assignment should occur at the application user level. The application should have some mechanisms to verify that the user has permission to use such code function when a user attempts to perform an operation on an object. At the same time, mechanisms should be implemented at the slave side to verify that the command code function is coming from a trusted source.

The request and response function codes specified in the frame control byte are described in the DNP3 specifications [6]. The function code identifies the purpose of the message and indicates what function is required to be performed. For example, the Freeze Functions type could be assigned to the “Supervisor” role and excluded from the “Junior” role. At the time of operation the SCADA application should provide mechanisms to allow the Supervisor to execute (request) such function on a specific object and deny the “Junior Operator” access to such functions. As an example, table 2.1a shows the freeze request function codes.

Table 2.1a: Freeze Request Function Codes

Code	Function	Description
7	Immediate Freeze	Copy the specified objects to a freeze buffer and respond with status of the operation.
8	Immediate Freeze – No Ack	Copy the specified objects to a freeze buffer; do not respond with a message.
9	Freeze and clear	Copy the specified objects to a freeze buffer, then clear the objects; respond with the status of the operation.
10	Freeze and clear – No Ack	Copy the specified objects to a freeze buffer, then clear the objects; do not respond with a message.

11	Freeze with time	Copy the specified objects to a freeze buffer at the specified time and intervals; respond with status.
12	Freeze with time – No Ack	Copy the specified objects to a freeze buffer at the specified time and intervals; do not respond with a message.

In RBAC, a session relates one user to possibly one or more roles. A user establishes a session during which he or she activates some subset of roles that he / she is a member of. The permissions available to the user are the union of permissions from all roles activated in that session. Each session is associated with a single user. Permissions are assigned and granted to roles in order to access the object. The permission for a specific role could be restricted to access specific objects, which in turn deny the user with such role to send and receive information from such object. In addition the permission for the same role could be restricted to access specific function codes, which in turn deny the user with such role to access other function codes.

A user assigned to a role is authorized to perform an operation on the object only if the operation is a member of the set of permitted functions for that object (See Figure 2.4a). As such, the operations for an object need to be defined and the object access types need to be identified and permissions need to be authorized to perform a function on an object at the SCADA application level. For example, a user assigned to the “Senior Operator” role must be able to view screens, send control signals to controllers, and receive and acknowledge alarm alerts. Thus, the “Senior Operator” has permission to read information displayed on the Human Machine Interface, send (request) control signals (ON/OFF) to the controllers attached to the Substations and the Remote Substations, and receive (reply) and acknowledge alarm alerts from the controllers attached to the Substations and the Remote Substations. On other hand, the “Senior Operator” does not have permission to send (request) signals (ON/OFF) to change alarm points, to send signals (ON/OFF) to disable controllers, or to send signals (ON/OFF) to disable alarms attached to the Substations or to the Remote Substations. These operations need to be mapped by the SCADA application and allocated specific function codes that can carry such operations.

Associating permissions with function codes and objects has the potential to create a level of difficulty to the policy to be understood and developed without further knowledge about the SCADA application and its protocols. Since the function codes and the objects (by name and address) are predefined, the SCADA application vendors need to provide some tools to help the SCADA administrators to associate roles with permissions and vice versa. Such tools will help also to provide the mechanisms to associate objects and function codes with permissions.

Also, there is a need in using application specific factors in authorization decisions. The sophisticated access control policies in SCADA systems are due to the major

effect these systems have on the service to the public and the liability requirements imposed by state and federal legislation. Ideally, authorization decisions in the SCADA systems should be based on the following factors: the size of operations, subject affiliation (EN, RTO), subject role, subject location, access time, and relationship between the subject and the SCADA objects whose data are to be accessed.

By introducing role based access control on the application level, authorization decisions and objects access types for SCADA systems and the affiliation with other subjects are two important topics for future work.

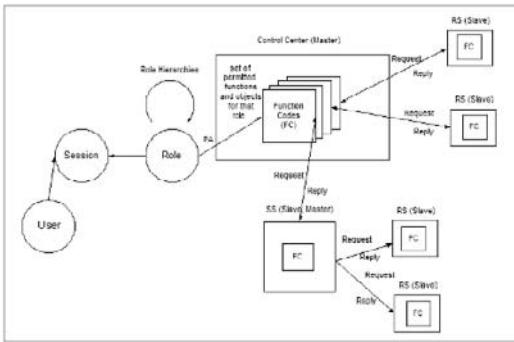


Figure 2.4a, SCADA System Topology: Multiple Master

3.5 Policy Rules in the RBAC model

The main purpose of a policy is to be sure that the resources are protected and information is transmitted in secure and appropriate manner. In addition, all users who access the system are using appropriate permissions based on their roles to conduct specific tasks and operations in a secure and control manner. RBAC supports several security principles and policies that can be implemented as a set of rules to be used in defining and enforcing access control policy for a SCADA system. Some of these are: the role authorization, the enforcement of least privilege for administrators and users, the dynamic separation of duties, and the cardinality property.

These policies can be enforced at the time operations are authorized for a role, at the time users are assigned a role, at the time of role activation, or when a user attempts to perform an operation on an object. The SCADA vendors can design and build such policies in their applications and provide some mechanisms to implement such policies in the SCADA systems. For example, a Senior Operator can be constrained to change controller set points but not to change alarm points. This is possible because of the RBAC capability to associate the operations with the roles. The decision to grant or deny an SO from changing the controller set points or changing the alarm point could be enforced at the time when SO attempts to perform such operation or at the time such SO assigned to a role.

In the role authorization policy, a user can never have an active role that is not authorized for that user. To perform an operation on an object controlled under RBAC, a user must be active in some role. Before the user can be active in a role, that user must first have been authorized as a member of the role by an administrator. In Figure 2.2a we described the major roles in the SCADA systems and the operations associated with each role. For example, the administrator assigns an “Engineer” role to a new employee whose job function is to carry complex configuration operations. When this user accesses the SCADA system, the granting or denying access to this operation will take place at the time the user is assigned to the role and will be in effect when the user uses the system.

The enforcement of the least privilege principle is based on allocating the minimum amount of permissions in a role to access an object. In the same principle, the user is assigned to a role that allows him/her to perform only what's required for that role. In addition no single role is given more permission than the same role for another user. As discussed earlier, the norm in SCADA environment is to trust the users when they are inside the control station center. With RBAC, users are authorized to access objects based on pre-assigned permissions and pre-defined operations. These permissions and operations should be at a minimum to allow the user to conduct his/her day-to-day job and be responsible for such actions.

The Dynamic Separation of Duty (DSD) rule provides the capability to address potential conflicts of interest issues at the time a user's membership is authorized for a role. However, in some organizations it is permissible for a user to be a member of two roles which do not constitute a conflict of interest when acted independently, but introduce policy concerns when allowed to be acted in simultaneously. DSD places constraints on the users that can be assigned to a set of roles, thereby reducing the number of potential permissions that can be made available to a user. The objective behind DSD is to allow more flexibility in operations. DSD places constraints on the simultaneous activation of roles. So for example, a SCADA “Senior Operator” can be authorized for both the acknowledgement of alarms and the change of the alarm points, but can dynamically assume only one of these roles at the same time. This could happen when a “Senior Operator” is covering for a “Supervisor” Role.

Some roles can only be occupied by a certain number of employees at any given time. This policy is enforced by the cardinality property. For example, consider the role of a Manager. Although other employees may act in that role, only one employee may assume the responsibilities of a Manager at a certain time. A user can become a new member of a role as long as the number of members allowed for the role is not exceeded.

An important design principle of RBAC model is the administrative capabilities it supports. In other access control models, the administrative process is very complex and requires a specific capability and knowledge. In

RBAC, users become members of roles based on their functions and responsibilities in the organization. Users are not granted permission to perform operations based on individual basis, but operations are associated with roles, and users are associated with roles. Under RBAC, new operations can be added to a role and operations could be removed from a role. All of this could happen without affecting the assignment of a user to a role.

Another administrative advantage of RBAC is that administrators control access at an abstraction level. This is established by introducing the “role” principle. Users are assigned to roles based on their job function and responsibility. After creating the RBAC framework, the administrator’s actions will be limited to granting and revoking users into and out of roles. Therefore, RBAC simplifies the administrator role and makes it very efficient.

4 Conclusion

SCADA systems were not designed with security capabilities in mind. The SCADA vendors can build such capabilities by utilizing the RBAC functions with a minimum time and cost and without a major impact on the systems components. RBAC strong administration capabilities can help simplifying the process of security management in SCADA systems.

In this paper we developed a security access control framework using RBAC for the SCADA systems. We described the capabilities of RBAC in providing abstract application level operations such as request (send) and reply (receive) signals (ON/OFF) from and to the Control Center, the SubStation, and the Remote Substation. A security model to verify the authorization at the time of operations on the system objects using the DNP3 could be a topic worth more investigation.

In addition, the external users (EN, RTO) accessing the SCADA systems could be a topic worth of further investigation. Moreover, the flow of data between the major SCADA objects could be another topic for research in the contents of access control policy.

References

1. Gail-Joon Ahn and Ravi Sandhu, “Role-Based Authorization Constraints Specification”
2. John Barkley, Anthony Cinotta (NIST), “Managing Role/Permission Relationships Using Object Access Types”
3. L. Beaver, D.R. Gallup, W. D. NeuMann, and M.D. Torgerson., “Key Management for SCADA”
<http://www.sandia.gov/scada/documents/013252.pdf>
4. Stuart Boyer 2004, “SCADA, Spervisor Control and Data Acquisition, 3rd edition”
5. Brian Broyles and Frank Kling, “Is there anything new under the SCADA sun?”
http://www.rigzone.com/insight/insight.asp?i_id=32
6. DNP User Group, <http://www.dnp.org>
7. DF Ferraiolo, “Role-Based Access Control (RBAC): Features and Motivations”, 11th Annual Computer Security Applications Proceedings, December 1995
8. David Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli, “Proposed NIST Standard for Role-Based Access Control”
9. Munir Majdalawieh, Francesco Parisi-Presicce and Duminda Wijesekera, DNPsec: A Security framework for DNP3 in SCADA Systems, in International Joint Conference on Computer Information and Systems Sciences and Engineering, Bridgeport, CT. December 10-20, 2005.
10. NERC, Version, June 14, 2002. Security Guidance for the Electricity Sector: Cyber – Access Controls.
11. Jaehong Park and Ravi Sandhu , “The UCONABC Usage Control Model”
12. The Register, “Hacker jailed for revenge sewage attacks”
http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_reveng_e_sewage
13. Ravi Sandhu, “Issues in RBAC”,
<http://www.list.gmu.edu/workshop/issue.pdf>
14. Ravi Sandhu, Venkata Bhamidipati, and Qamar Munawer, “The ARBAC97 Model for Role-Based Administration of Roles.”
15. Ravi Sandhu, Edward J. Coyne, Hal Feinstein, and Charles Youman, “Role-Based Access Control Models”
16. Riptech, Inc. January 2001 “Understanding SCADA System Security Vulnerabilities”,
<http://www.iwar.org.uk/rerources/utilities/SCADAWhitewpaperfinal1.pdf>
17. Sandia National Laboratories, The Center for SCADA Security, SCADA Brief History <http://www.sandia.gov/scada/history.htm>
18. Joe St Sauver, Ph.D. University of Oregon. SCADA Security, <http://darkwing.uoregon.edu/~joe/scada/>
19. U.S. Department of Energy, “21 Steps to Improve the Cyber Security of SCADA Networks,”
<http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf>
20. U.S. General Accounting Office, “Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems”
<http://www.gao.gov/new.items/d04354.pdf>
21. William F. Young, Jason E. Stamp, and John D. Dillinger. “Communication Vulnerabilities and Mitigation in Wind Power SCADA Systems”
22. Bill Young and Mark Rumsey . “Communication Vulnerabilities and Mitigations in Wind Power Supervisory Control and Data Acquisition.”

DNPSec Simulation Study

Munir Majdalawieh¹, Duminda Wijesekera²

¹ American University of Sharjah, mmajdalawieh@aus.com

² George Mason University, dwijesek@gmu.edu

Abstract: The main objective of this simulation study is to investigate the performance effects of adding the DNPSec functionality to SCADA DNP3 protocol.

Keywords: DNP3, DNPSec, SCADA, OPNET

Introduction

Majdalawieh et al. [2] proposed a new Distributed Network Protocol Version 3 Security (DNPSec) framework to enable confidentiality, integrity, and authenticity placed directly in the DNP3 [1]. The main goal of such framework is to address the threats related to these security principles in the DNP3 as part of SCADA architecture, with a minimum performance impact on the communication link. The main objective of this simulation study is to investigate the performance effects of adding the DNPSec functionality to SCADA DNP3 protocol.

In order to accurately simulate the performance of SCADA and end nodes, specific traffic attributes are configured corresponding to the implementation of DNP3. Traffic profiles include multiple attributes that are used to configure the level of traffic transmitted throughout the network. The simulation studies considered the typical request (poll) / response processing in DNP3. In addition, the configuration of the DNP3 and DNPSec includes packet-by-packet data transfer with each transmit which is modeled as a discrete event. The size of the generated packets is exponentially distributed with a mean size of 292 bytes per packet. The appropriate adjustment of these packet-by-packet data transfers will determine the level of traffic placed on the:

- End-nodes
 - Master: Human Machine Interface (HMI)
 - Slaves: Remote Terminal Units (RTU), and
 - Intelligence Equipment Devices (IED)
- and communication network.

In a typical Master-Slave configuration, the Master (client) requests information and the Slave (server) responses by providing such information. In such arrangement, the Master gives instructions, asks for information updates, and orders the Slave to respond. The Master then listens for the response. The Slave gathers

information (status points, alarm points, measurement meters, and analog points) from the IED nodes (sensors, actuators, etc.), then responses as soon as the Master has finished requesting, then stops and listens for more requests. The Master moves to the second Slave and goes through the same procedure. The Master requests information from each Slave then returns back to the first to begin the cycle all over again.

The process of requesting information from each Slave in order and then going back to the first Slave to begin the cycle all over again is called “scanning” or ‘polling’. Scan interval determines by number of RTU nodes, amount of data that must be passed on each scan, the data rate of the communication link, and the communication efficiency.

The performance of SCADA using DNP3 and DNPSec architectures is measured and compared during the simulation by collecting statistics in OPNET Modeler for the following metrics:

- Packet throughput at both the Master and the Slave nodes
- The utilization of the Master to Slave nodes link
- Total control action round trip delay time.

All the simulations for network performance characterization have been performed using the discrete event simulator OPNET Modeler™ [3]. The packet format editor, node model editor, network editor, link model editor, probe editor, simulation tool, analysis tool, and project editor are used to model and simulate the topologies and scenarios, which are described in this chapter. OPNET is commonly used for network simulation and provides a powerful network modeling and simulation tools and it offers a comprehensive library of detailed protocols, network, and application models. We use OPNET as the development and simulation platform for its friendly GUI and flexibility.

In the following sections we will describe the DNP3 and DNPSec packets, the link models, the node models, and the network models. Then we will choose the statistics, run simulation, and view & analyze results.

DNP3 and DNPsec Packets

The packet format editor is used to create DNP3 and DNPsec packets as shown in Figures 1, and 2 respectively.



Figure 1: DNP3 packet

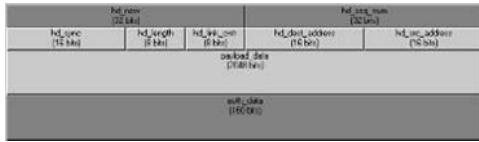


Figure 2: DNPsec packet

These packets are used as a main source for creating traffic at both the Master and Slave nodes in our topology. The size of the generated packets is exponentially distributed with a mean size of 292 bytes per packet.

Link Model

The link model for this study was chosen to be a point-to-point duplex link with a data rate of 19200 bps between the RTU and the IED nodes and a data rate of 9600 bps between the HMI and the RTU nodes. The 9600 link model is configured with DNP3 and DNPsec packet formats. We are assuming that the communication link efficiency is 60%. Accordingly, the actual data rate for the HMI to the RTU link is 5670 bps and the actual data rate for the RTU to the IED link is 11520 bps.

In addition to setting the supported packet format type, the following attributes in the attribute table has been chosen:

- The error correction model ecc model is set to ecc_zero_err .
- The error model is set to error_zero_err .
- The point-to-point propagation delay model propodel model is set to dpt_propodel .
- The point-to-point transmission delay txdel model is set to dpt_txdel .

To collect statistics for the link, we included the link_delay function from Opnet using the Declare External Files option.

SCADA Network Model

The SCADA network consists of three types of nodes:

- **Intelligent Electronic Device Nodes:** These nodes collect data using their relays. The collected data is then passed to the attached RTU node through the network. There may be as many relay nodes as needed depending on the area to be covered. Figure 3 depicts the IED node structure.

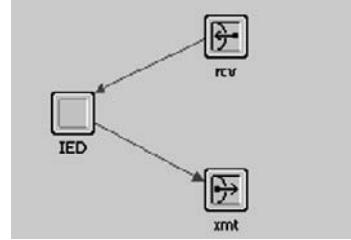


Figure 3: IED node

The IED process model is a finite state machine (FSM). It represents the logic and behavior of a module. An FSM defines the states of the module and the criteria for changing the states. FSM uses states and transitions as shown in figure 4. The complete code for the IED node is described in appendix A3.

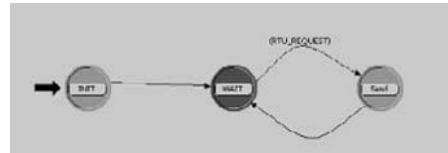


Figure 4: IED process – FSM

- **Slave Nodes:** Slave nodes are responsible for collecting data from IED nodes. The slave node collects information from all the IED nodes attached to it. The collected data then passed to the Master node when it polls the slave node.

The RTU functions as a single slave device to collect, scale, aggregate, and present all substation data to the SCADA master. This system collects status and measurement data from the substation and provides a control interface for SCADA (for example, open or close a circuit breaker using the IED as a control interface device).

The RTU process model (see figure 5) is a finite state machine (FSM). It represents the logic and behavior of a module. The complete code for the RTU node is described in appendix A2.

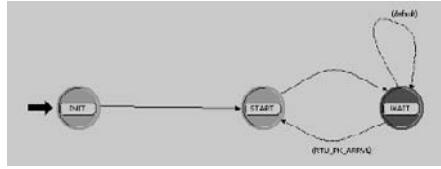


Figure 5: Slave (RTU) Process – FSM

- **Master Node:** Master node is responsible for collecting data from Slave nodes. The master node polls the slaves in turns and the slave responses by sending the information that the master asked for.

As in the RTU process model, the HMI process model (see figure 6) is a finite state machine (FSM). It represents the logic and behavior of a module. The complete code for the HMI node is described in appendix A1.

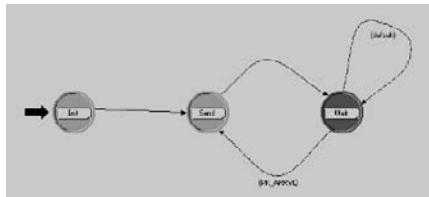


Figure 6: Master (HMI) Process – Finite State Machine (FSM)

For each topology, we built two network models:

- **RTU-To-Intelligence Electronic Device (IED) network:** to simulate the network and the traffic between the RTU and the IED nodes, and
- **HMI-To-RTU network:** to simulate the network and the traffic between the HMI and the RTU nodes. I included eight RTU nodes in each network. The RTU nodes are connected to the Master node by a link model.

RTU-To-Intelligent Electronic Device (IED) Network

For each topology, we built an RTU to IED network with the architecture and protocol to be tested. We included one RTU and twelve IED nodes in each network. The twelve IED nodes represent transformer, line, and feeder relays for a typical twelve-feeder station. The IED nodes are connected to the RTU node by a link model. Figure 7 shows the RTU to IED networks.

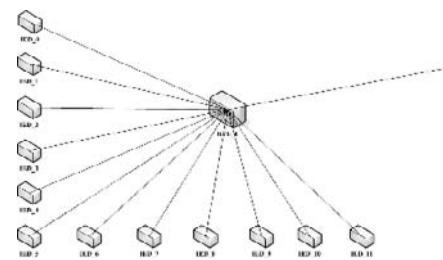


Figure 7: RTU-To-IED network

Upon receiving the POLL command from the HMI, the RTU scans all the IED nodes attached to it, collects the requested information, stores the information in its buffer, and sends the collected information to the HMI.

HMI-To-RTU Network

For each topology, we built an HMI to RTU network with the architecture and protocol to be tested. We included one HMI and eight RTU nodes in each network. The eight RTU nodes represent a typical eight-input-output station. Figure 8 shows the HMI to RTU network.

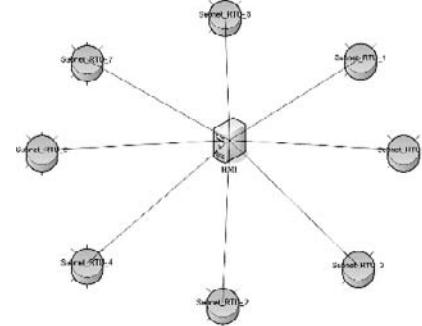


Figure 8: HMI-To-RTU network

HMI polls the RTU nodes in order starting from RTU-0 to RTU-7 and then back to RTU-0, see figure 9. After receiving the requested information from each RTU, the HMI node destroys the packets and starts with fresh buffer.

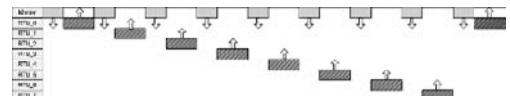


Figure 9: Master – Slaves Scan (Poll) Scheduling Algorithm

While these networks do not describe all possible SCADA systems, they provide a benchmark for relative comparisons. By testing each network, we also gained an understanding of the main factors affecting performance,

and we can use this information to understand performance in other installations.

SCADA invocations consist of several steps as shown in figure 10. On the Master side, HMI issues a POLL command. The HMI process model processes the request and passes the message onto the network. On the RTU side, the RTU acquires messages from the network and passes the arguments to the RTU process model. For purposes of this study "Scan Interval I" is defined as the HMI to RTU nodes process and "Scan Interval II" is defined as the RTU to IED nodes.

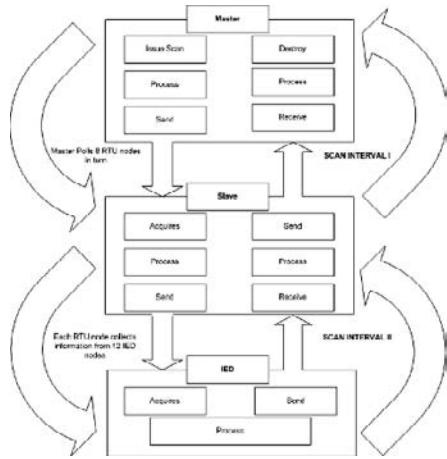


Figure 10: Master polling information steps from RTU and IED nodes

RTU process model is responsible for reassembling the arguments and sending the request to the attached IED nodes. RTU collects information from all the attached IED nodes and stores the information in its buffer. The RTU node then sends the message onto the network stream. Similarly, HMI receives the reply message and forwards the message parameters to the HMI process for reassembling the reply message parameters before it destroys the message. The similar process continues from the Master to the RTU to the IED nodes until the Master polls all the RTU nodes in its network. Then, the same process is repeated as described above.

Network topology

We performed simulations to determine the overall performance of one Master node connected to eight RTU nodes in which each RTU is connected to IED network that consists of twelve nodes. In the baseline model scenario, we simulated typical base loading of the system using DNP3 and then determined the overall scanning speed.

We simulated the collection of about 40 status points (40 bits), 12 alarm points (12 bits), 4 measurement meters (64

bits), and 3 binary points (48 bits) of typical SCADA information acquisition from each IED including currents, voltages, other analog values, and relay targets. As for the design of the DNP3 protocol, the RTU node will send an acknowledgement message for each message that the HMI sends to RTU.

We duplicated the same scenario and created the same model network using DNPsec by applying a delay at the HMI and the RTU. The delay at the HMI and RTU simulates the encryption delay, authentication delay, and fetching the database for the shared key. As a worst case scenario I used .012 sec delay each time HMI assembles and sends a message to RTU and each time RTU assembles and sends a message to HMI.

Simulation Results

Table 1 provides a comparison of the average delay time results between DNP3 and DNPsec. HMI time delay for Scan Interval I using DNP3 is .595. The time delay jumped to .631 during the same interval when we used DNPsec. The time delay during Scan Interval II is constant since we did not apply any new delay when I introduced DNPsec. The assumption that we made, is the Distributed Network Protocol is configured only between the Master and the Slave and the configuration between RTU and the IED is using another protocol. This is consistent with the majority of the SCADA installations.

Table 1: DNP3 and DNPsec Delay

Statistic	DNP3	DNPsec
HMI ETE Delay	.595	.631
RTU ETE Delay	.429	.429
IED ETE Delay	.027	.027

Table 2 shows the results of the throughput between the HMI and the RTU nodes and the RTU node and the IED nodes.

Table 2: Throughput between HMI, RTU, and IED nodes

Node - Node	point-to-point throughput (bits/sec)
HMI > RTU	981
RTU > HMI	1962
RTU > IED	35
IED > RTU	108

The assumption that we made is that the size of all the RTU nodes are the same. All RTU nodes collect the same amount of point count from the IED nodes and send one packet to the HMI. We used the same assumption for the IED nodes.

The graphs below summarize the results of the simulation. These graphs show that there is a very small change in over all SCADA time delay on the network by adding DNPsec functionality. The security calculation

added some delay time but it is not significant to effect the scanning cycle of the defined SCADA network topology.

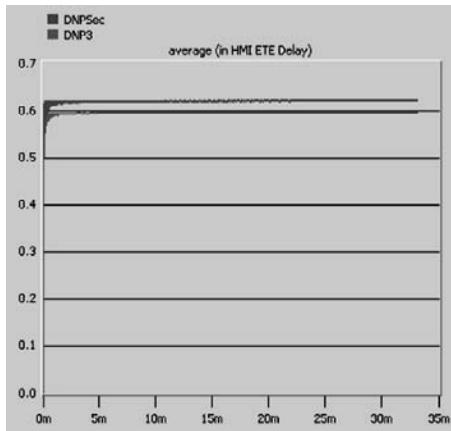


Figure 11: HMI ETE Delay

The average HMI delay time is the time from the creation of the packet at HMI until the time the HMI receives a packet from RTU. The difference of delay time between DNP3 and DNPsec is $.631 - .595 = .036$ seconds. HMI receives in average 1962 bps from each RTU.

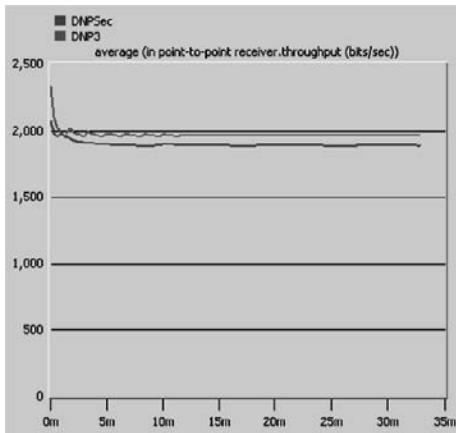


Figure 12: HMI Receiver Throughput

Simulation Analyses

In the first scenario (using DNP3), the time delay is .595 seconds in Scan Interval I (HMI polls each RTU) and the time delay is .429 seconds in Scan Interval II (RTU collects information from each IED.) In the second scenario (using DNPsec), the time delay is .631 seconds in Scan Interval I and .429 seconds in the Scan Interval II.

The difference in Scan Interval I between the two scenarios is .038 seconds. The question that I will try to

answer is: How the addition of .038 seconds affects the simulation results? The total time in the first scenario (using DNP3) for Scan Interval I of the first complete cycle (HMI to 8 RTU nodes and each RTU to 12 IED nodes) is:

$$\text{DNP3-HMI_to_8RTU_to_12IED_delay} = \text{DNP3-HMI_to_RTU_delay} * 8 = .593 * 8 = 4.744 \text{ sec}$$

It would be good design practice to round this 4.744 seconds up to 6 seconds in order to get the “best rate” at which for the HMI to scan all RTU nodes for data. Having calculated this number, it would be wise to ensure that no process functions will be adversely affected by a delay of 6 seconds.

The total time in the second scenario (using DNPsec) for Scan Interval I for the first complete cycle (HMI to 8 RTU nodes and each RTU to 12 IED nodes) is:

$$\text{DNPsec-HMI_to_8RTU_to_12IED_delay} = \text{DNPsec-HMI_to_RTU_delay} * 8 = .631 * 8 = 5.048 \text{ sec}$$

Accordingly, it will take 4.744 seconds for the HMI to re-poll the same RTU node in the second round of scanning in the first scenario (DNP3) and it will take 5.048 seconds for the HMI to re-poll the same RTU node in the second round of scanning in the second scenario (DNPsec.)

If we use the same design practice established in the DNP3, it would be wise to increase a delay from 6 seconds to 7 seconds to ensure that no process functions will be adversely affected by this delay.

Conclusion

The sizing of the SCADA HMI server, the RTU nodes, and the communication links is very important and it needs to take in consideration scan intervals between RTU nodes. Scan intervals determines by the following factors:

- Number of Slaves: the larger the number of Slaves the larger the scan interval needs to be.
- Amount of data that must be passed on each conversation: The higher the amount of data, the higher the scan interval needs to be.
- The data rate: the higher the data rate, the smaller the scan interval needs to be.
- The communication efficiency: the higher the communication efficiency the lower the scan interval needs to be.

As described above the RTU delay based on the defined network topology is about .429 seconds. This delay could be accumulated very fast based on the criteria described above. Having calculating the delay number, it would be wise to ensure that no process function (like collecting information from any IED) will be adversely affected by this delay. If

such functions do exist but only at one or two of the RTU nodes, the problems may be addressed by scanning each of those RTU nodes twice in the scan. For example, if the scan rate were acceptable for all except RTU number 5 in a system of n RTU nodes, the scanning program could be set up as follows:

RTU 0, RTU 1, RTU 2, RTU 3, RTU 4, **RTU 5**, RTU 6, RTU 7, **RTU 5**, RTU 8, RTU 9, RTU 10, **RTU 5**, ..., RTU n, RTU 0, ...

If most of the RTU nodes show process functions that are marginally good or bad from a timing point of view, the best solution may be to increase the data rate. For example, upgrading the data rate between HMI and RTU from 9600 bps to 33600 bps, or upgrading the data rate between RTU and IED nodes from 19200 bps to 33600 bps.

References

1. DNP User Group, <http://www.dnp.org>
2. Munir Majdalawieh, Francesco Parisi-Presicce and Duminda Wijesekera, DNPsec: A Security framework for DNP3 in SCADA Systems, in International Joint Conference on Computer Information and Systems Sciences and Engineering, Bridgeport, CT, December 10-20, 2005.
3. OPNet, <http://www.opnet.com>

A Client-Server Software that Violates Security Rules Defined by Firewalls and Proxies

Othon M. N. Batista, Marco A. C. Simões, Helder G. Aragão, Cláudio M. N. G. da Silva , Israel N. Boudoux

Information Security Research Group

Bahia University Center – FIB

41.770-130 – Salvador/BA – Brazil

{othon, marcosimoes, holder}@fib.br, csmanoel@gmail.com, israeljava@hotmail.com

Abstract – This paper presents a client-server software that violates security rules defined by firewalls and proxies. A firewall is a set of components, interposed between two networks, that filters the traffic according to rules based on a security policy. Several techniques may be used to make firewalls obsolete, for instance: tunneling and cryptography. The software presented in this paper is composed by two modules: a client and a server one. the client module must be installed in any host of the local network that is not protected by a firewall or a proxy. The server module must be installed in the Internet, in a host accessible by the client module. With this software, it's possible to bypass firewalls and proxies.

Keywords: information security, firewall, proxy.

INTRODUCTION

Each day, computer networks gain more importance. The Internet is a practical example of a computer network that grows in an accelerated manner. With this growth, there is a preoccupation with information security, since every day we have news about virtual robbery, information theft and new computer viruses [1] [2].

New vulnerabilities arise constantly. Being explored or not, they motivate the work of the information security community that must supply any solution. Two possible solution already supplied are: firewall and proxy [3].

A firewall is a set of components, interposed between two networks, that filters the traffic according to rules based on a security policy [4]. Typically, a firewall is installed between a private network and the Internet. A security policy may demand that all the traffic is forbidden, except the web access from the private network, that occurs, by default, through ports 80 and 443.

Several techniques may be used to make firewalls obsolete [5]. Two of them are special because, in a certain way, they are explored by the software described in this paper:

- many ways to establish tunnels allow that individuals bypass all security mechanisms supplied by traditional firewalls;
- end-to-end cryptography may also be a threat to firewalls, since they impose difficulties to the analysis process of the fields to filter packages.

An alternative to an isolated firewall is the addition of a proxy with firewall functions. Therefore, a system must execute a proxy server with firewall functions and the hosts

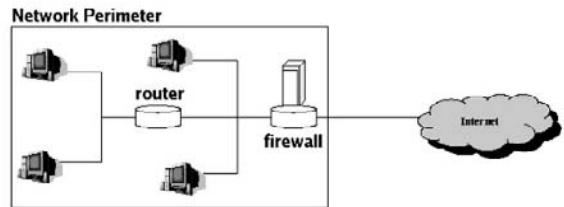


Figure 1. Firewall localization.

must access the web only by this proxy. With this proxy, more filters may be configured, such as: forbid the access to determined sites and/or forbid to download files considered huge by the system administrator [6]. A firewall works in the network layer, while a proxy with firewall functions works in the application layer of the TCP/IP architecture [1] [2].

The software presented in this paper is divided in two modules, a client and a server one. It violates the filters imposed by firewalls and/or proxies. This software only needs the communication with the web permitted by the Hyper Text Transfer Protocol (HTTP) [7] [8], because it encapsulates the information that should be forbidden in HTTP messages.

FIREWALLS

This section is an overview of firewall concepts. For further explanation, read [4].

A firewall has the goal to control the access (incoming and outgoing) of the network it is acting over. There are two types of firewalls: package filters, running in the network layer, and gateways in the application layer.

The package filters have the objective to allow, or not, access to network datagrams, based on pre-established rules. Because firewalls are responsible to control the access of the network datagrams, they are often situated in routers, since they represent the connection point with another networks.

Figure 1 shows a network protected by a router with package filter capabilities. The filtering mechanism realized in the router make it possible to control the kind of traffic that may exist in each network segment.

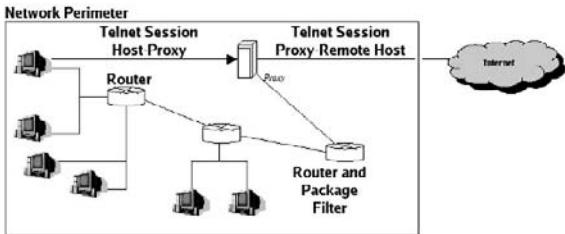


Figure 2. Firewall composed by an application gateway and a filter.

The filtering rules used by most of the routers are mainly based in these informations:

- source address;
- destination address;
- type of protocol;
- source ports;
- destination ports.

The application gateways extend the services offered by a firewall. One type of application gateway is the proxy with firewall functions. One example of its use is depicted by an organization that needs to provide Telnet access to a restricted group of users.

In this case, a firewall would not help, because it has no information to cope with that. A possible solution is to configure a firewall with all the source address related to the users belonging to the group allowed to use Telnet. Although this solution fails when a user gets a host with a forbidden address.

The real solution to this problem is based on the user authentication. A network proxy would gather the information when the user authenticates itself in the system. Therefore, the user would have (or not) Telnet access.

A gateway runs transparently to the user. All requisition made by the users of a network with a proxy, must explicitly pass by it. It intermediates all requisitions from the network it resides in. Taking the Telnet example already quoted, when a user is allowed to access a Telnet server, he (she) is implicitly connected to the proxy, and, by this way, the proxy is connected with the Telnet server (figure 2).

THE SOFTWARE

The software is composed by two modules: a client and a server one. The client module must be installed in any host of the local network that is not protected by a firewall or a proxy. The server module must be installed in the Internet, in a host accessible by the client module (figure 3).

All communication with Internet servers must be intermediated by the software, otherwise, they run the risk of being forbidden by the firewall or proxy. The software runs in a very simple way. The client module receives a requisition, encapsulates it into a HTTP message and sends it to the server module. The server module desencapsulates the message and make the solicitation, acting as an intermediary. After receiving the answer, the server module encapsulates it in a HTTP message and sends it back to the client module.

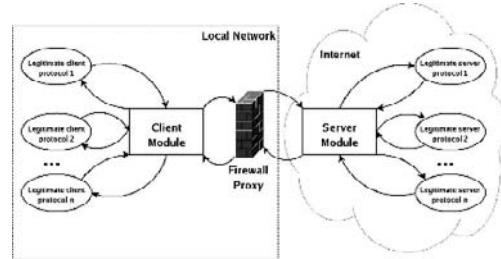


Figure 3. Basic software functions.

The client module receives the message, desencapsulates it and pass it to client that made the requisition.

Considering that a firewall lets the web traffic pass without any filtering and the proxy allows communication between the client and server modules of the software, the security rules are bypassed.

Figure 4 shows the internal architecture of the client module, which is divided into four parts: the internal servers for each protocol that must be intermediated. They receive legitimate client solicitations of each protocol and pass them to the encapsulator.

The internal servers must exist in a proportion of one to each protocol that must be intermediated. They receive legitimate client solicitations of each protocol and pass them to the encapsulator.

The encapsulator only assembles a HTTP message and encapsulates the information into the data area of the message. It adds a header containing information about the used protocol, such as: protocol name, used ports and IP addresses. The assembled messages are passed to the HTTP client that sends them along to the server module.

When the server module answers, the HTTP client receives the message and passes it to the desencapsulator. It, by its means, desencapsulates the contents and pass it to the correspondent internal server. The protocol additional informations are used at this moment. The internal server responds to the legitimate client that contacted it initially.

Figure 5 shows the internal architecture of the server module, composed by: HTTP server, desencapsulator, encapsulator and internal clients for each protocol.

The internal clients must exist in the same proportion of the internal servers in the client module, one for each internal server.

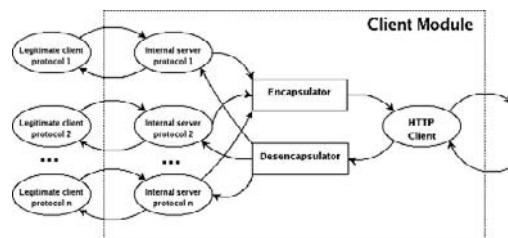


Figure 4. Client module architecture.

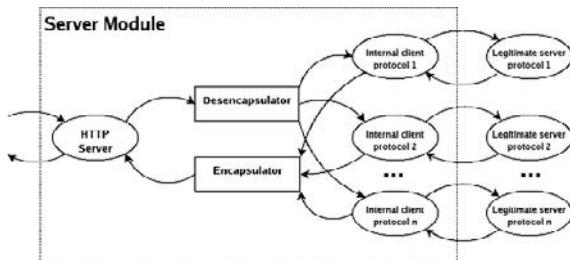


Figure 5. Internal architecture of the server module.

The HTTP server receives messages from the client module and passes it to the desencapsulator. The desencapsulator takes the useful informations and passes them to the correspondent internal client, thanks to the header added by the client module encapsulator. The internal client communicates with the protocol legitimate server and receives an answer.

The answer is sent to the encapsulator. It encapsulates it into a message, and passes it to the HTTP server that responds to the client module of the software.

With this behavior, the software opens a HTTP tunnel between client and server modules. Since web communication is allowed by almost all firewalls, and a proxy doesn't forbid the server module, because it's unknown, this software permits the communication for all protocols.

RESULTS

The software client module was tested in a host belonging to a Local Area Network (LAN) connected to the Internet. The server module was installed in a host in the Internet. In the border between the LAN and the Internet, there was a firewall and a proxy. Figure 6 shows the LAN, with seven hosts connected by a switch, the firewall/proxy in the border and the Internet.

The firewall permitted only traffic coming to and from the proxy. The proxy filtered the access by three ways: some sites were forbidden, such as www.orkut.com, it didn't allow download of files bigger than 4 Mbytes and it didn't allow access to the MSN Messenger server.

In the client host, the one in which the client module of the software was installed, we used Firefox, version 1.5.0.6, as a web browser, and Kopete acting as a Microsoft Network (MSN) Messenger client. All of them running on Linux Fedora Core 5.

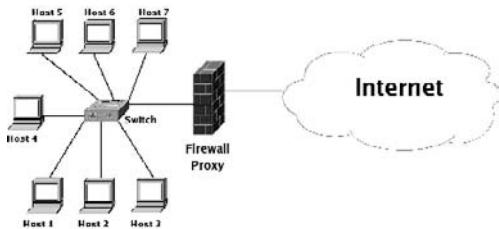


Figure 6. Test environment.

The proxy client of Firefox and Kopete was set to the Internet Protocol (IP) address of the client module (127.0.0.1, in this case), port 1563. This was necessary because all communications must pass by the client module of the software first.

With the client, two tests were realized: access to a forbidden site, www.orkut.com, and access to the MSN Messenger server by its client. Without using the software, both requisitions were denied. But, when the software was used, both firewall and proxy were inefficient, allowing information that should be forbidden.

POSSIBLE DEFENSES

The software exploits valid HTTP requisitions to encapsulate any forbidden requisition. Even though, some defenses may be tried:

- proxy or firewall may be configured to forbid accesses to the server module of the software;
- each host in the LAN may have a mechanism that avoids the client module execution;
- an Intrusion Detection System (IDS) may be configured to recognize HTTP messages generated by the modules of the software.

Other defenses may be tried, but for each defense implemented, the software may evolve and avoid it or bypass it. For example:

- multiple server modules may be installed in the Internet;
- client module may change to avoid local detection;
- the HTTP messages interchanged between client and server modules may be cryptographed.

CONCLUSION

The software presented in this paper has the goal to show vulnerabilities in traditional firewalls and proxies. Defenses to the software are also proposed.

As future works for the software and defenses, we point:

- design a pattern for the communication interface with the encapsulator/desencapsulator to allow the internal clients and servers to be designed as plugins;
- use cryptography in the encapsulated content;
- fragment messages to allow downloading of files bigger than any limit established by a proxy;
- test the software in an environment with an IDS installed and running.

REFERENCES

- [1] TANENBAUM, A. S. Computer Networks. 4th Edition. Prentice Hall. 2002.
- [2] KUROSE, J. F. ROSS, K. W. Computer Networking: A Top-Down Approach Featuring the Internet. 3rd edition. Addison Wesley. 2004.

- [3] MCCARTHY, L. IT Security: Risking the Corporation. Prentice Hall. 2003.
- [4] CHESWICK, W. R. Firewalls and Internet Security: Repealing the Wily Hacker. Addison-Wesley. 1994.
- [5] IOANNIDIS, S. KEROMYTIS, A. D. BELLOVIN, S. M. SMITH, J. M. Implementing a Distributed Firewall. Proceedings of the ACM Computer and Communications Security (CCS) 2000. p.p. 139-151. San Diego, CA, USA. 2001.
- [6] HUNT, C. TCP/IP Network Administration. 2nd edition. O'Reilly. 1997.
- [7] BERNERS-LEE, T. FIELDING, R. FRYSTYK, H. Request For Comment 1945 - Hyper Text Transfer Protocol 1.0. 1996.
- [8] FIELDING, R. GETTYS, J. MOGUL, J. FRYSTYK, H. MASINTER, L. LEACH, P. BERNERS-LEE, T. Request For Comment 2616 - Hyper Text Transfer Protocol 1.1. 1999.

Mobile communication in real time for the first time. User evaluation of non-voice terminal equipment for people with hearing and speech disabilities

Patricia Gillard, Gunela Astbrink and
Judy Bailey
University of Newcastle
Callaghan, NSW, Australia 2308

Abstract – Fifteen people with very diverse backgrounds were interviewed and asked to test one of two mobile non-voice terminal devices. The participants were people who were Deaf or had a hearing or speech impairment. The interviews with some Deaf and hearing impaired participants were signed in Auslan and videotaped. The study reports detailed differences in their uses and needs, places these in the context of their current patterns of communication and argues for technology development that provides for the rich array of requirements, uses and possibilities.

I. INTRODUCTION

The following study had two main aims:

- to identify the needs of the different user groups, and
- to identify the effectiveness of the terminals assessed for each user group.

The need for a comprehensive study of the effectiveness of new non-voice terminal equipment was identified by the Australian Communications Industry Forum (ACIF), now merged into the Communications Alliance, who established the TATA Working Group (Any-to-Any Text Connectivity). Their final report suggested a range of text communication alternatives to the existing analogue TTY to ‘better meet the text communication needs of the end user for both fixed and mobile networks’ (TATA, 2004). It proposed a range of text communication protocol options and a national Text Server to provide interworking between existing TTYS (text telephones) and the new textphone protocols. The regulatory authority, the Australian Communications and Media Authority (then the Australian Communications Authority) and telecommunications carriers Optus¹, Telstra and Hutchison had also conducted testing that was encouraging (eg.Telstra, 2004) but there had not been any user testing of terminal devices to establish how they worked for the very people who needed them: people who are Deaf or have a hearing or speech impairment.

For the Deaf and hearing-impaired community, SMS capability of mobile phones and the cross-networking of mobile phone service providers, has resulted in much higher use than among hearing people (Power & Power, 2004).

However, SMS does not provide ‘real time’ communication and it cannot be relied upon in an emergency.

In Australia text telephone technology (TTY) and the National Relay Service (NRS) currently provide ‘real time’ communication, but these have several disadvantages, especially the lack of privacy and time delays involved in using an intermediary. An interpreter in Auslan (Australian Sign Language) signs at between 240 and 300 words per minute. The Baudot 50 technology used to relay calls via the NRS can handle no more than 67 words per minute. Therefore, it takes Deaf people three to five times longer to make a phone call by TTY or using the NRS, than it does to sign face-to-face in Auslan.

The new generation of video mobiles are moving technology another step closer to the aim of signing face-to-face but such a service has not been established in Australia and these devices are not necessarily the sole answer. For people with a speech impairment, reaching the phone in time to answer, not needing to lift and hold a handset, having access to voice and text, and the ability to see and manipulate the keypad accurately, are still vital issues. Nguyen & Garrett (2005) found that the requirement for customized adaptation of available technology and education of users in the current capabilities of mobile phones, were the major issues in providing satisfying telecommunications solutions to people with mild, moderate and severe physical disabilities. Technical developments such as customized access to infrared controls, wireless keypads, hands-free devices and image talk software may be essential to the ability of people with speech impairments to access mobile phone technology at all.

II. RESEARCH DESIGN AND METHODS

The design of this research reflected the need to test equipment with people with a wide range of disabilities and personal circumstances, covering people with Deafness, hearing or speech impairments. To maximize the usefulness of findings in this study, it was decided to test the uses of the equipment in the everyday contexts of participants.

In-depth interviews were conducted with fifteen individuals, each using one piece of equipment in the environments where they usually made calls, such as homes, schools or offices. Purposive sampling was used, to make it possible to locate five people with a variety of backgrounds within each disability group.

¹ This research was generously funded by a grant from Optus who also loaned equipment, provided SIM cards and covered the costs of all calls.

A. Recruitment of participants

The project aimed to recruit a minimum of five participants from each of the groups: people who are Deaf, people with a hearing impairment and people with a speech impairment. Recruitment of people who were Deaf or had a hearing impairment was conducted in Sydney through personal contacts and networks. In contrast to this, recruitment of people who were speech impaired was a difficult and lengthy process.

Those six men and four women who were Deaf or had a hearing impairment were aged 23-45 years. Seven were employed (one on a casual basis).

The five participants with speech impairments were male. Four were aged over 50. Speech impairments showed much variation and included:

- breathiness and loss of vocal volume due to Parkinson's Disease
- voice production using a speech valve or Servox following laryngectomy
- almost mute following a stroke, communicating using a Lightwriter
- mild speech impairment after acquired brain injury.

B. Interviews

In depth interviews of one to two hours were designed to gain detailed information about the users' everyday context and their use of phones or other communications. Patricia Gillard and Gunela Astbrink designed the interviews and tested them in a pilot study. The interview consisted of three sections:

i. Researchers outlined the project, and obtained written permission to audiotape and/or videotape the interview, followed by a set of questions concerning the participant's usual modes of communication, use of landlines, mobile phones and SMS.

ii. Three phone calls were made by the participant (and answered by another project researcher) simulating the making of a doctor's appointment, asking a friend out for coffee, and lastly contacting either:

- a lecturer at university or technical college to ask for an extension on an assignment
- a person at work to report in sick and notify of a day's absence, or
- a government agency to check on a Disability Service Pension

iii. Researchers asked questions concerning the participant's opinion of the success and ease of making the calls, including suggestions for improvements and a rating of the device used.

Interviews were conducted in contexts where the individuals made phone calls, mainly in the participant's home (7), sometimes at work (3), in the researcher's home (3), in the social room of a local hospital (1) or at school (1).

When the study was first conceived it had been assumed that for interviews with Deaf participants there would need to be interpreters to sign, in addition to the interviewer. Instead, we were very fortunate to engage a researcher who was also a fluent interpreter so that she could conduct the interviews by signing and hence communicate with Deaf participants in their native language, Auslan.

The interviews were videotaped and later transcribed by the same researcher.

The second interviewer was an experienced speech pathologist. Her ability to understand and adapt to the very individual circumstances of people with speech impairments ensured the success of the project in interviewing and in recruitment of this group. A third researcher provided co-ordination, phone interviewing, persistence in dealing with equipment issues and detailed administrative work.

The sound and video interviews were transcribed by the interviewers themselves as a basis for analysis of the entire group. Analysis was conducted by tabulating those results that could be summarized or quantified and seeking patterns, consistencies and unique cases within the transcribed interviews. Great care was taken to understand the perspective of users themselves, their disability and personal context, and to describe similar findings within disability groups and across the entire sample where this was possible. Multiple comparisons were made for this purpose.

The detailed results and suggestions for improvement arising from this study confirm the importance of testing equipment with a broad range of users within the complexity of their everyday lives.

C. Training and Equipment

A one-day workshop was held where researchers were trained in the use of the equipment by an engineer from the Australian Communications and Media Authority (ACMA) who provided detailed sets of instructions for each device. The equipment was tested successfully during the training session, within one cell of reception distance.

All three devices were tested successfully on project training day. While some difficulties associated with the appearance of nonsense symbols were initially experienced using the DSPG Textlink 9100M, the device was used successfully to send and receive messages within the same room on the training day. Pre-interview trials conducted on the Nokia Communicator 9210i and O2 XDA were successful, although some reception problems were experienced using the devices inside brick structures.

Further pre-interview trials conducted on the DSPG Textlink 9100M over longer reception distances (within Newcastle) yielded nonsense symbols when the call was connected.

Following advice from the ACMA representative, three operational improvements were recommended:

- Ensuring the Textlink was in 'mobile' mode
- Physically separating the Textlink and mobile phone as much as possible during calls
- Adjusting the mobile phone volume to medium setting.

Further trials implementing ACMA recommendations continued to yield nonsense symbols, some incomplete messages from one operator, or no transmission of message. Both Optus and Telstra mobile phone SIM cards were tested with the same unsuccessful result. At this point, the decision was made to remove the DSPG Textlink 9100M from the study because it could not be made to operate successfully in fieldwork conditions.

The two devices used in the interviews were supplied by ACMA and Optus, with the aim of using each device with 7 or 8 participants. The text terminal equipment and software were specifically configured for the purposes of the trial.

i. Nokia Communicator 9210i.

The Nokia Communicator 9210i has a mobile phone on the lid of the case, which is about the size of a solid sunglasses case. The cover flips open to reveal a keyboard and screen. This device could be used to make and receive calls from another Nokia Communicator, and from the O2 XDA.

ii. O2 XDA

The O2 XDA is a Personal Digital Assistant, which may be connected to a customized fold-out keyboard. Text messages may be typed using the keyboard, which is larger than that of the Nokia Communicator, or using a stylus and an on-screen keyboard. The device may be charged using a cradle or using a more compact USB port for mobility. Due to software limitations at the time of conducting this research, the device could not receive text-based calls, and so could only be used to make calls.

The equipment was supplied with add-on software that was not the commercial software normally available on the Communicator or the O2 XDA.

III. RESULTS

A. Usual modes of communication

Participants were asked about their routine uses of telephones, SMS, TTY and other devices to communicate.

i. Deaf participants

Participants who were Deaf used a variety of communication modes for different purposes. All used mobile phone SMS mode, for reasons including immediacy, to make appointments, to pass on a message of a business or social nature, or as part of an education network. The Deaf participants made more SMS calls than other participant groups (between 2 and 20 SMS calls each day). The vibration alert for arrival of SMS messages was mentioned as a useful feature.

Most Deaf participants used TTYs either at home or at work, some messaging directly to another text terminal, and others used the intermediary of the National Relay Service. Some Deaf participants mentioned that they use email, and one uses fax for transferring information that must be saved.

ii. Participants with hearing impairments

Participants with hearing impairments have the most varied profile of phone use. One person uses only landline, to make 30 to 50 business calls each day, avoids the use of mobile phones entirely, and uses email for business and family purposes. In another extreme case, a participant uses landline only to speak to familiar people in her native language, preferring to avoid difficulties with volume control on the hearing aid loop; she also uses mobile phone, SMS messaging for jokes and fun, and TTYs on some occasions.

For these participants, use of landline varies from 1-2 calls per day, to 30-50 calls per day. Frequency of use of SMS varies from 10-15 messages per day, to complete avoidance of SMS, and of mobile phones.

iii. Participants with speech impairments

These participants prefer to use voice rather than text for their communication wherever possible. This group of people use mainly landline to make phone calls, making the lowest number of calls of all three participant groups, from 5-6 per day to 1 per week. Three out of five in this group use voice on a mobile phone only in emergencies, or to arrange transport (1-2 calls/day). The remaining two participants do not use mobile phones at all, and no one in this group uses SMS messaging. Only one participant in this group, who is essentially unable to use voice for communication, uses a TTY, and communicates by email.

B. Evaluation of Text Terminal Functions

At the conclusion of the interview, participants rated the device they used for ease of use of the six functions: keyboard use, reading the display, physical use, portability, size and comfort. Each function was rated on a four-point sliding scale: Very easy, Easy, Bit difficult and Very difficult. A higher score indicates the function was easier to use.

Average ratings for ease of use of the six functions for the two text terminals are shown in Table 1.

i. Keyboard use

For ease of keyboard use, the two text terminals were rated almost evenly by the 15 participants. The Nokia Communicator scored 3.2, marginally ahead of the O2 XDA, at 3.1. Seven out of eight Nokia users rated its keyboard use 'Very easy' or 'Easy'. Those who used the O2 XDA were more divided in their judgement, with just over half rating its keyboard 'Very easy' to use, and the remainder finding it a 'Bit difficult'. No participants found the text terminals 'Very difficult' to use.

TABLE 1.
AVERAGE 'EASE OF USE' RATING OF EACH TEXT TERMINAL FOR SIX FUNCTIONS (HIGHER NUMBER = EASIER)

Equipment Function	Nokia Communicator 9210i	O2XDA
Keyboard use	3.2	3.1
Reading display	2.3	2.7
Physical use	2.7	2.7
Portability	3.4	3.1
Size	2.9	3.0
Comfort	2.4	3.4

ii. Reading display

Reading the display on the screens was rated more difficult than any other function. The O2 XDA scored 2.7, higher than the Nokia Communicator at 2.3. About half the participants using both devices found reading the display a 'Bit difficult', and one user found the Nokia screen 'Very difficult' to read.

iii. Physical use

Both text terminals were rated equally easy in terms of physical use (score 2.7 each). This belies rather different distributions of ratings, however, with a Gaussian distribution

peaking on an 'Easy' rating for the Nokia Communicator, compared to a broader, more platykurtic distribution for the O2 XDA. There were some users who found each device 'Very difficult' in terms of physical use.

iv. Portability

The portability of the Nokia Communicator (score 3.4) was found preferable to that of the O2 XDA (score 3.1), probably due to the fact that the O2 XDA consists of two parts, a keyboard which must be opened, folded out, and attached to the PDA. Overall the portability scores for the devices were the highest for any function. All but one participant found the portability of the text terminals 'Very easy' or 'Easy'.

v. Size

The benefits of the size of both devices were rated very closely by the participants, with the O2 XDA marginally ahead (score 3.0) of the Nokia Communicator (score 2.9). Again the evenness of the scores belies a different distribution of ease ratings for the two text terminals. Rating of size for the Nokia Communicator showed a Gaussian distribution, peaking on a rating of 'Easy.' The scores for the O2 XDA covered a broader range, with three out of seven users finding its size 'Very easy', and the remaining users judging it 'Easy', 'Bit difficult' and 'Very difficult'.

vi. Comfort

The comfort of using the O2 XDA (score 3.4) was found to be greater for the participants, than using the Nokia Communicator (score 2.8). The rating of comfort shows the greatest contrast of all functions, although no participants found comfort 'Very difficult'.

Four out of seven of those who used the O2 XDA gave 'Comfort' a rating of 'Very easy'. In view of the detailed information recorded during the interviews, it appears the greater comfort of the O2 XDA related to the use of its stylus for driving the screen menu, the larger keyboard and keys, and the higher and perhaps more ergonomic position of the PDA screen when the text terminal is set up on a table or desk.

C. Adapting the text terminals to the body

When the six functions of the two text terminals were compared the O2 XDA was given a total of 18.0 points, slightly ahead of the Nokia Communicator at 16.9 points.

The most difficult function of both text terminals was reading the display. At the time of conducting the project, the text terminal software did not allow an increase of font size on the display without loss of information at the screen margins. Participants and researchers alike found reading the small text challenging. This perceived deficit in the equipment may be ameliorated slightly by increasing text-screen contrast, and by modifying the software to begin each new speaker's conversation on a new line in contrasting text. However, the tiny font could realistically prevent potential users from taking up the technology, and this aspect of text terminal use should be addressed.

The display of the O2 XDA was rated easier to read than that of the Nokia Communicator, despite the font being very similar in size. One possible reason for this may be different display colors; the O2 XDA having a blue screen with white text, and the Nokia Communicator having a white screen with black text. In addition, the O2 XDA occupies a higher position above the desk surface when plugged into the keyboard USB

port, which places the user in a better ergonomic position to read the text without bending down to see the screen.

This ergonomic difference probably explains the significantly higher comfort rating given to the O2 XDA. It is also inextricably linked to the user's rating of physical use of the terminals. Both text terminals have keyboards designed for multi-finger, or two-hand typing, and so must be placed on a surface for use. For this reason, neither can be used as a live text terminal while walking or standing up, say on public transport, so physical use (2.7) was rated almost as low as reading the display (2.3, 2.7).

Having accepted the fact that the devices must be placed on a surface, and generally operated with two hands, users rated the keyboard use quite high among the functions assessed (3.2, 3.1). However, a recurring theme on the keyboard issue was the desire for regular QWERTY keyboard design, and discrete keys for the 'GA' and 'SK' functions which signal changeover of speaker, and end of conversation. Users want to be able to transfer their other keyboard skills directly to the text terminal, especially those mature users who have acquired disabilities later in life, and may be learning keyboard skills for the first time. The keys on the O2 XDA keyboard are larger in size, accounting for the slightly higher rating given the O2 XDA in terms of size (3.0 O2 XDA, 2.9 Nokia).

However, the O2 XDA loses its advantage, in terms of the portability function. One simple case with a mobile on the 'lid' for the Nokia Communicator was judged to be significantly more portable (3.4) than the two or three part assembly required for the O2 XDA (3.1).

D. Adapting the text terminals to the disability

While the current trend in mobile phone design for the general population appears to be toward more compact phone terminals with a large range of extra functions, these trends do not serve populations with speech and hearing impairments equally well. People with speech impairments occupy a special niche of text terminal user, because a significant proportion of this population have impaired speech as a result of a congenital condition or syndrome, a degenerative illness, a traumatic brain injury or an acquired brain injury due to stroke; all conditions which may affect other functions, such as motor skills, and vision. People who are Deaf or have a hearing impairment but no other disability are often able to operate mobile phones in a similar way to the general population.

Two main issues arise from these observations. The first is that while the trend toward smaller mobile phones and text terminals makes for greater compactness while not affecting usability for the Deaf and hearing-impaired community, smaller equipment greatly impacts upon usability for the speech-impaired community. If a person with a speech impairment has any collateral motor or visual impairment, their ability to set up the text terminal, to locate keys on the keyboard, to depress keys individually without touching adjacent keys, and to read small font on a small screen will be compromised. A compact device loses its advantage if it cannot be used to send accurate messages confidently and quickly. Those people with speech impairments who were interviewed expressed a preference for using voice where possible, so they will only persist with a text terminal if it

represents an advantage over using voice on a landline or mobile phone. Indeed, some in this group expressed the desire for a phone that allowed them to use combinations of voice and text: a possibility that does not seem to have been considered, perhaps because users themselves have not been closely involved in the development of the devices.

There are disadvantages to using text terminals for people with hearing impairments, in that the terminals are not as portable as mobile phones, cannot be operated with one hand, and cannot be operated while standing, walking or traveling. Equally, there are disadvantages to using text terminals for people with speech impairments, chiefly in that their very compactness makes usability challenging. The advantages would need to outweigh these disadvantages to promote purchase and use of these text terminals. The observation that the very disadvantages for one group of participants in this research turn out to be advantages perceived by the other group, indicates very clearly that all groups of people with disabilities are not seeking the same properties in a text terminal, or 'One size does not fit all,' which will be discussed in more detail below.

The second issue is that not only participants in the research, but researchers as well, who do not belong to the Deaf, hearing-impaired or speech-impaired communities, and who would not be considered visually impaired, found reading the display of the text terminals challenging. Perhaps even in the general community, it is an invalid assumption that users want increasingly compact mobile phone devices with ever more functions.

E. Matching technologies to user needs and purposes

Detailed information about the routine communications of particular disability groups reveals different patterns in the use of modes of communication for different purposes. Rather than the text terminals tested here providing the answer to all their communication needs, it became clear that the 'horses for courses' approach extended to the new equipment as well.

Situations in which the real time facility of the text terminals would be the preferred choice according to the Deaf users, were for negotiations, such as setting appointment times, conversations or discussions, so the message could be clarified immediately, and for contacting others via the National Relay Service. An important need to be met by any text terminal is that of Deaf people, particularly business people, to be able to communicate at a competitive speed to hearing people. Participants in the Deaf and hearing-impaired groups indicated they would still favor the speed and convenience of SMS messaging for passing messages, for the convenience of contacting or being contacted while walking, or traveling, and for jokes and fun. One user with a hearing impairment for whom English is a second language, would use such a text terminal at work for communicating with English speaking people, while continuing to SMS or use voice on mobile phone for contacting familiar people in her native language. They also indicated that in case of emergencies, they found SMS screen messaging information clearer, and connection faster and more reliable than the text terminals tested. One user with a hearing impairment who was not a mobile phone user felt more comfortable using the text terminal (bigger keys, one letter per key) and believed she

would use such a mobile terminal to contact family throughout the day.

For speech-impaired users, the text terminals would be suitable for 'relaxed conversations at home' (if the font were larger). One user with a speech impairment made it clear that he would probably not use the text terminal unless it made faster and more robust connections. Others indicated they would prefer to use voice than text, except in circumstances where their voice quality declined due to respiratory infection or other illness, or where the message required information to be recorded in writing during the phone call.

One Deaf user suggested the terminal would be improved by adding an email and fax facility, so that it would provide a greater range of his daily communication needs. The message is that, like the general community, phone users in the participant groups want a variety of ways to communicate with others, voice, mobile phone, SMS, text, email and fax. Ideally, one Deaf user observed that the terminal would not satisfy his communication needs until it provided a visual display of his communication partner, so they could use their preferred communication mode of signing face-to-face.

F. Providing quality connection and services

An important observation from this research is that while people with speech and hearing impairments were very interested, and initially delighted, in the technological development represented by the text terminals they tested, they were not prepared to compromise their need for speedy connection of their calls for the sake of novel devices, especially in the case of an emergency. The novelty of the text terminals soon wore off if they did not perform with the same speed and reliability as mainstream mobile phones and landlines.

Those in the Deaf community were particularly exacting with regard to the need for fast reliable calls to emergency services. They recommended that the Emergency Services be equipped with compatible text terminals, and were critical when the text terminal did not display explicit information on progress of the call connection, sometimes necessitating exiting the phone software and beginning the connection again. However, one participant with a speech impairment was also quite annoyed at the frequent disconnection, and delays in reconnecting, the O2 XDA, and was dismissive of the equipment on this basis. It should be noted here that many of these problems may be due to the dated software used rather than the functioning of the hardware. The software was not the commercial version usually used by the text terminal devices.

One participant with a hearing impairment abandoned using the O2 XDA for his interview on a stormy evening due to inability to make a connection, despite indicators of good reception on the terminal screen. Potential users will not pay a substantial price for a text terminal, only to receive a lesser service than that which they are accustomed to receiving.

G. Further uses for text terminals

Participants also raised possibilities for future use of the text terminals that were unexpected. A Deaf user saw the usefulness of text terminals for hearing people who wanted privacy while phoning on public transport or in public spaces, and also for business people who were required to send

confidential evaluations or appraisals while in the field, or in the presence of their clients.

Participants with speech impairments pointed out the great benefit to be gained from access to a text terminal immediately after laryngectomy, when a person is unable to use their voice possibly for a period of weeks. The text terminal could be used to contact others with such terminals outside hospital, to contact anyone via the National Relay Service, and to converse with friends and family in their presence using the notebook function, say, of the O2 XDA. Laryngectomees reported that the notebooks they used as auxiliary and alternative communication while in hospital, were often removed by nursing staff, leaving them totally without access to communication.

IV. DISCUSSION AND CONCLUSION

Participants with different disabilities have significantly different patterns of communication, determined largely by their ease with acquiring new communication modes. People in the group of Deaf participants are skilled at a variety of communication modes. Similarly, people with hearing impairments appear to choose a preferred mode of phone communication for most of their electronic communication, either mobile phone, landline or text terminal, depending on the extent of their hearing impairment. By contrast, participants with speech impairments in this research had acquired the disabilities later in life, due to illness or accident, and so their auxiliary and alternative communication was less well established. The members of this group are generally not part of an email network, do not use SMS messaging, rely on voice calls using landline or mobile phone despite their speech impairment, and often have protective carers acting as a filter between themselves and any caller.

Some striking contrasts are demonstrated in this research. For example, while some Deaf people are part of a fast and efficient communication SMS network and may email up to 35 contacts simultaneously in a similar fashion to email networks among hearing people, others may have experienced significant isolation due to their hearing impairment. People with speech impairments, while sometimes using mobile phones, have not taken up the SMS facility and have become relatively isolated after acquiring their disability.

This research was designed to do more than test equipment with people with a range of disabilities. It sought to understand the ways they would use the new devices in their

everyday lives and the improvements to the equipment that were needed so that the technology expanded their accessibility and provided a genuine enhancement to their communications. The text terminal equipment was enthusiastically tried by participants because they could see its possibilities even if they were sometimes frustrated by its current limitations. The results have made visible the differences between the user groups and argues for improvements and customization to gain most value from the technology.

It is hoped that this study will speed the development and production of technology to enhance the communication of those who cannot easily use phones and mobiles for their whole range of day-to-day communications.

ACKNOWLEDGEMENTS

We are very grateful to research associates Pam Danson, who interviewed by signing and videotaped the interviews and Louisa Connors who was a constant contact and kept the equipment going. The equipment loaned by ACMA was appreciated and, especially, the expertise and training by Chris Wong. The project was managed by the University of Newcastle in partnership with a Consumer Reference Group chaired by Gunela Astbrink. Their regular guidance and contacts were vital for the project's success.

V. REFERENCES

- Australian Association of the Deaf Inc. (2005) 'What is Deaf equivalent to voice telephony?' Deaf Telecommunication Access and Networking Project: Sydney
- Australian Communications Authority (2003) 'Evaluation of real-time text communication options', ACA: Melbourne
- Nguyen, T. & Garrett, R. (2005) 'New technological options for people with physical disabilities through the use of telecommunications equipment – trials results', Department of Communications Information Technology and the Arts: Canberra.
- Nguyen, T. & Hobbs, D. (2005) 'Promoting Accessible Telecommunications Options' NovitaTech: Regency Park.
- Power, M.R. & Power, D. (2004) 'Everyone here speaks TXT: Deaf people using SMS in Australia and the rest of the world', Journal of Deaf Studies and Deaf Education, 9 (3):333-343.
- TATA Working Group (2004) Report to the Department of Communications Information Technology and the Arts, Australian Communications Industry Forum: Sydney.
- Telstra (2004) 'Real Time Any-to-Any Text Connectivity – Project Test Results', Telstra: Melbourne

Analyzing the Key Distribution from Security Attacks in Wireless Sensor

Piya Techateerawat and Andrew Jennings
Electrical and Computer Engineering School
RMIT University
Melbourne, Australia
S3100474@student.rmit.edu.au, ajennings@rmit.edu.au

ABSTRACT

As wireless sensor network (WSN) has limited resource, security function and operation must be simplified. So its defense is relatively weak comparing to PC or high-power server. This paper demonstrates key distribution for sensor networks that is resistant to brute force attack, known plain text attack, replay attack, man-in-the-middle attack and denial of service attack (DoS). This paper compares a proposed solution HKD with SPINS and ARIADNE protocols which are designed for WSN and ad hoc networks. The evaluation demonstrates that ARIADNE is the strongest protocol.. HKD can minimize the power consumption while SPINS balances both energy and security.

1. INTRODUCTION

Wireless Sensor Network (WSN) offers a new approach to deploy at location without infrastructure support. Applications of WSN include monitoring space, environment, medical, mining and military [1], [2].

Advantage of WSN devices are low unit cost, small size and long life operation. With this purpose, there are strong restrictions on energy and computing resources. However, this conflicts scheme of security. That has complex computation to avoid the key cracking and exchange more data (or overhead) to guarantee the protection [3].

One of fundamental tasks in security is key distribution. It is required to set up key to communicate with base station and neighbor nodes. In PC and commercial server, this task needs a large overhead and lots of computation. There are many papers to develop protocols which are revised for WSN devices. [4], [5].

In this paper, we evaluate security attacks against the key distribution protocols which design for WSN or ad hoc. There are our proposed Hint Key Distribution (HKD), Security Protocols for Sensor Networks (SPINS)[6], A Secure On-Demand Routing Protocol for ad hoc networks (ARIADNE) [7].

Our main contributions include:

- Exploring the challenges of security in HKD, SPINS and ARIADNE.
- Evaluating consequences of attacks in these protocols. Attacks include brute force attack, known plain text attack, replay attack, man-in-the-middle attack and denial of service attack (DoS).
- To analyze the strengths and weaknesses in each protocol, it covers the resistance from key cracking and data protection.

Brute Force Attack (BFA)

This method defeats cryptography by trying every possible key. It expects to find a correct key approximately at half of key domain (e.g. if there is 2^n possible keys, BFA will average be founded correct key at 2^{n-1}). However, this theory has a limitation in real world that array processors require a large amount of energy and continuous operation for a long period [8].

Known Plain Text Attack (KPA)

KPA is attacking model where adversary has samples of plaintext (e.g. sensing data in WSN) and uses them to reveal secret key. As a result, an adversary could translate all the encrypted messages and also transmit fraudulent messages to the network [9].

Replay Attack (RPA)

RPA is an attack against the message which is repeated or delayed. It could be using as duplicated authentication or malicious data. In WSN, RPA can use for creating a new session or to bypass authentication [10].

Man-in-the-middle Attack (MITM)

MITM has the intent to read, add and modify messages between two parties. It requires intercepting messages between two parties [9].

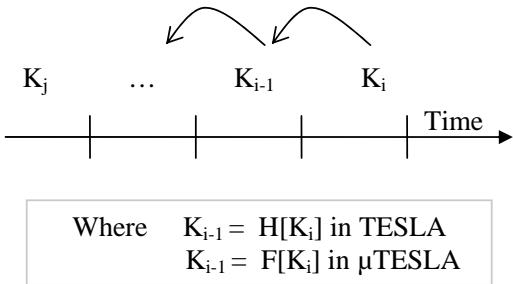


Figure 1. Key chain authentication releases the key based on time scale.

Denial of Service Attack (DoS)

DoS is an attack to disrupt computer resource or obstruct communication between user and service. DoS in WSN can be in the form of flooding network which disturbs communication between nodes, or continuous communication burns out the node battery [11].

2. NOTATION

We use the following notation to describe protocols and operations in this paper:

- A, B** are principals, such as communicating nodes
- M₁ | M₂** represents the concatenation of message M₁ and M₂
- K_{AB}** represents the symmetric key which is shared between A and B
- H[D]** represents the hash function which digests data D
- F[D]** represents the first one-way function which covert data D

3. RELATED WORK

A key attack is valuable. Since key is revealed, an adversary can interpret, modify, and create communication messages [3]. Key distribution problems in wireless network are proposed and discussed in [6].

ARIADNE

Y. Hu et. al proposes a secure on-demand routing protocol for ad hoc network (ARIADNE) [7], which uses TESLA protocol for authentication. Since it is an efficient method, authentication requires only a single broadcast message. A mechanism is set up by sharing secret keys between communicating nodes. Then it distributes one authentic public TESLA key for each node. Next, sender generates initial key K_N and one-way key chain by

```

select random number L
if this is the first time then
    load key K = master key KM
else
    load key K = saved key K0
endif
for j = L downto 0 do
    compute key K = F1[K]
endif
store key K0 = K
compute hash value S1 = H[K]
select random number N
for j = N downto 0 do
    compute key K = F2[K]
endif
compute hash value S2 = H[K]
encrypt message (S1/S2) with key KC
broadcast message KC(S1/S2)

```

Figure 2. Sender operation in HKD

repeatedly computing a one-way hash function which starts the value: K_{N-1} = H[K_N], K_{N-2} = H[K_{N-1}],... To compute previous key K_j from a key K_i, j < i can be evaluated from equation K_j = H^{i-j}[K_i] as in Fig. 1. When it receives an authenticated message, it verifies the key K_j and compute K_j. TESLA usually operates correctly except when end-to-end delay exceeds the window.

SPINS

A. Perrig et. al proposes the security protocols for sensor networks (SPINS) which uses μ TESLA instead of TESLA in authentication. This μ TESLA is developed from TESLA by replacing digital signature with symmetric mechanisms, disclosing key once per epoch instead of every packet and limiting the number of authenticated senders to minimize energy and computation [6].

HKD

We propose HKD [14] which is inspired by the use of hint messages. It uses symmetric encryption to secure transmissions. Confidentiality and simplicity are provided from encryption and decryption. When every sensor node has the secret key, it can establish secure communication without altering the routing (or tree hierarchy).

HKD authentication uses both hash and one-way function. Firstly, each WSN node has initial key K_i installed in an encrypted memory. To broadcast key, sender selects random number j which repeatedly computes a one-way function value: K_j = F^j[K_i]. Then computing hash value H[K_j] and transmitted to receiver as in Fig. 2. When it receives an authentication message, it repeatedly computes one-way function K₀ = F[K_i], K₁ = F[K₀], ... and verifies H[K₀], H[K₁], ... with hash value

```

decrypt message with standard key  $K_C$ 
extract  $S_1$  and  $S_2$  from broadcasted message
if this is the first time then
    load key  $K = \text{master key } K_M$ 
else
    load key  $K = \text{saved key } K_0$ 
endif
do
    compute key  $K = F_1[K]$ 
until  $H[K]$  equals  $S_1$ 
store key  $K_0 = K$ 
do
    compute key  $K = F_2[K]$ 
until  $H[K]$  equals  $S_2$ 
store  $K$  as secret key

```

Figure 3. Receiver operation in HKD

$H[K_j]$ until matched. Then, it keeps K_j for a secret key as in Fig. 3. An advantage of HKD is not required transmitting secret keys but requires only key signature in authentication message.

4. ASSUMPTIONS

We assume that there is end-to-end data communication between node A which is the base station of the cluster and node B which is placed at the edge of cluster. A path between A and B has transmission along the nodes in the same cluster as: $A \rightarrow n_1 \rightarrow n_2 \rightarrow \dots \rightarrow n_m \rightarrow B$. This network also has routing path set up. Each node in network has strong physical protection. Adversary cannot break the device to retrieve the key or inside data directly. Also, the length of secret key is evaluated with 40 and 128 bits. Since some applications may not require strong security that costs computation and resources. To compute key chain, we use MD5 and SHA-1.

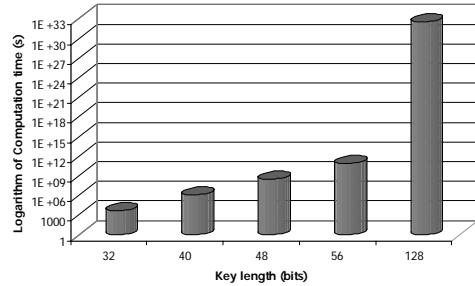
The adversary can be placed everywhere; inside and outside the network cluster. They have a server which contains Sun UltraSparc II 440 MHz Microprocessor to perform the attacks and computations. The UltraSparc is 64 bit RISC based architecture with data cache 16 KB and 2MB external cache. Their wireless antenna can reach the entire network. When adversary launch attacks, it can be initiated from anywhere along a path.

Our objective is to address only communication attack. We do not focus on physical attack and routing jamming.

5. EVALUATION

5.1 Brute Force Attack (BFA)

Since BFA can be the benchmark in comparing the security, we use it to evaluate the resistance of ARIADNE, SPINS and HKD. The evaluation is based on a pair of communications which follow the theory and algorithm. However, in real world, adversaries may

**Figure 4. Logarithm of computation time in breaking current secret key.**

reduce their computation time when they collect information from a group of nodes.

Among these protocols; ARIADNE, SPINS and HKD, they protect master key with hash or one-way function. To obtain current secret key, adversary can directly perform BFA, but it is infeasible to generate next key or master key. However, breaking current secret key requires $2^{\text{key length} - 1} \times \text{Computation Time}$. In 40 bits key length, there are 2^{40} possible keys which average half (2^{39}) must be attempted to find the correct key while 128 bits key needs 2^{127} attempts. Since UltraSparc II computes each key in 2 μs [12], in 40 bits key. It requires 1.10×10^6 s (12.7 days). To compare with 128 bits key, it requires 3.4×10^{32} s (1.08×10^{25} years). So 128 bits key can enhance security protection as shown in Fig. 4.

However, breaking master key requires more computation than current key. Since, it needs to compute for entire key chain from master key to current key. To compute key chain, MD5 and SHA-1 use the same 128 bits hash. Let maximum key chain length is N and assuming that adversary know this information. To break master key, it needs to try every key chain. In each key chain, it needs to compute hash function N_0 times. Since number of computing function N_0 depends on key chain length N (for key chain length N, it requires to compute function $N!$ times). So it must run $2^{\text{key length} - 1} \times N! \times \text{Computation Time}$. Then, let the key chain length is 10 for the worst case which actual protocols use larger number. In UltraSparc II, its execution times for MD5 and SHA-1 are 39 μs and 56 μs [12]. In MD5, BFA will find the master key for 40 bits key chain in 7.78×10^{13} s (2.47×10^6 years) and 128 bits key chain in 2.41×10^{40} s (7.64×10^{32} years). In SHA-1, it will find the master key for 40 bits key chain in 1.12×10^{14} s (3.54×10^6 years) and 128 bits key chain in 3.46×10^{40} s (1.10×10^{33} years) as in Fig. 5.

In short key length (40 bits key), it can secure data in a short period of time (less than 12 days) before renewing key. However, with sensitive information, a longer key (128 bits key) is required. To protect the system with master key, both short and long key show a secure protection from BFA. However, ARIADNE and SPINS

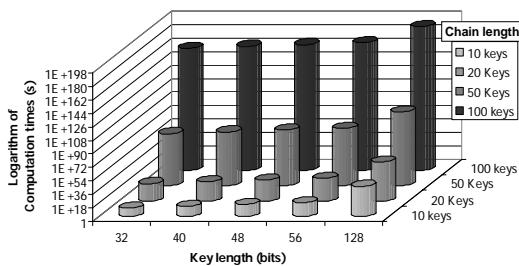


Table 2. Energy saving features in each protocol

	ARIADNE	SPINS	HKD
Not require re-organizing structure		✓	✓
Construct key from hint message	✓		✓
Not require set up secured channel			✓

mainly are energy and security. ARIADNE is the strongest protocol. HKD can minimize the power consumption while SPINS balances both energy and security as shown in table 1 and 2.

ARIADNE use TESLA to generate key chain which is the most strongest among these protocols. SPINS cuts down the operation for longer battery life. HKD focuses on minimize the energy but trade-off with secrecy of sensitive data.

BFA could be used as a benchmark to compare the strength in these protocols which demonstrates short key length (40 bits) is not sufficient to protect adversary. Although longer key (128 bits) seems to be resistant to BFA, KPA could reduce the computation significantly when sufficient information is supplied. As a consequence of revealing the key, it could be attacked from MITM which risk the network in monitoring and phishing attack. In addition, SPINS and HKD could be attack from RPA when counter value is not verified. Furthermore, DoS could not be avoided by any of these protocols and can empty the node battery in less than 10 hours.

These experiments confirm the security in WSN that ARIADNE, SPINS and HKD require a longer length key (at least 128 bits) to assure secrecy of data in general use. However, sensitive and military data could not be relied on these protocols and require message to be encrypted.

7. CONCLUSION

This paper presented an analysis of WSN security attacks in key distribution. In addition, we propose HKD to minimize energy consumption. This HKD framework is based on one way and hash function.

We evaluated ARIADNE, SPINS, and HKD from 5 attacks including BFA, KPA, RPA, MITM and DoS. According to BFA and KPA, long length key is compulsory which requires at least 128 key bits in our experiment. Major damage could result from RPA and MITM after key revealed. DoS is a major attack which affects the entire network but cannot be avoided with these protocols. It can empty the nodes battery in less than 10 hours for the worst case.

The future work is to prepare HKD to resist security attacks while maintain a minimum level of power consumption. We will also attempt to adapt a new authentication scheme to enhance efficiency in HKD. In

addition, we will do more evaluation with the other attacks which could be a greater potential risk to WSN.

8. REFERENCE

- [1] M. Ulema, "Wireless sensor networks: architectures, protocols, and management," presented at Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP, 2004.
- [2] P. Agrawal, T. S. Teck, and A. L. Ananda, "A lightweight protocol for wireless sensor networks," presented at Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE, 2003.
- [3] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks" *Commun. ACM* vol. 47 pp. 53-57 2004
- [4] Z. Yu and Y. Guan, "A key pre-distribution scheme using deployment knowledge for wireless sensor networks" in *Proceedings of the 4th international symposium on Information processing in sensor networks* Los Angeles, California IEEE Press, 2005 pp. 35
- [5] T. Ito, H. Ohta, N. Matsuda, and T. Yoneda, "A key pre-distribution scheme for secure sensor networks using probability density function of node deployment" in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* Alexandria, VA, USA ACM Press, 2005 pp. 69-75
- [6] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks" *Wirel. Netw.*, vol. 8 pp. 521-534 2002
- [7] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne:: a secure on-demand routing protocol for ad hoc networks" in *Proceedings of the 8th annual international conference on Mobile computing and networking* Atlanta, Georgia, USA ACM Press, 2002 pp. 12-23
- [8] M. Blaze, "A cryptographic file system for UNIX" in *Proceedings of the 1st ACM conference on Computer and communications security* Fairfax, Virginia, United States ACM Press, 1993 pp. 9-16
- [9] U. Meyer and S. Wetzel, "A man-in-the-middle attack on UMTS" in *Proceedings of the 2004 ACM workshop on Wireless security* Philadelphia, PA, USA ACM Press, 2004 pp. 90-97
- [10] T. Kwon and J. Song, "Clarifying straight replays and forced delays" *SIGOPS Oper. Syst. Rev.*, vol. 33 pp. 47-52 1999
- [11] J. Deng, R. Han, and S. Mishra, "Defending against path-based DoS attacks in wireless sensor networks" in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* Alexandria, VA, USA ACM Press, 2005 pp. 89-96
- [12] P. Ganeshan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes" in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications* San Diego, CA, USA ACM Press, 2003 pp. 151-159
- [13] V. Shnayder, M. Hempstead, B.-r. Chen, G. W. Allen, and M. Welsh, "Simulating the power consumption of large-scale sensor network applications" in *Proceedings of the 2nd international conference on Embedded networked sensor systems* Baltimore, MD, USA ACM Press, 2004 pp. 188-200
- [14] P. Techateerawat and A. Jennings, "Hint Key Distribution for Sensor Networks", presented at International Conference on Systems Computing Sciences and Software Engineering, 2006

Hint Key Distribution for Sensor Networks

Piya Techateerawat and Andrew Jennings

School of Electrical and Computer Engineering

RMIT University Melbourne, Australia

s3100474@student.rmit.edu.au, ajennings@rmit.edu.au

2. BACKGROUND

ABSTRACT

Many applications require authentication and confidentiality in communication (for example, military and business), but standard authentication and key distribution mechanisms involve energy expenditure. Most approaches in large group of key distributions are suitable for conventional networks. New proposals such as SPINS overcome the deficiencies, and establish the feasibility of sensor network key distribution. In this paper, we propose a new method of key distribution for sensor networks which is inspired by the use of hints in ELK. We describe in detail the operation of the method, and perform energy consumption comparisons with both ELK and SPINS.

1. INTRODUCTION

The advantages of wireless sensor network (WSN) are low unit cost, small size and long life operation. To achieve this purpose, it requires conserving energy consumption and minimizing network communication. This conflicts with the general scheme of security which has complex computation to avoid the breaking keys. It also exchanges more data (or overhead) to guarantee protection [1], [2].

Key distribution is a fundamental operation for secure communication. The objective is to deliver a secret key to receiver without leakage to a third party. Standard approaches involve several procedures in exchanging key over a network [3], [4].

This paper presents Hint Key Distribution (HKD) for WSN. A key is distributed using a hint message modified from ELK mechanisms [5]. The key is generated from a one-way function, and signature to verify the correctness. Our approach is motivated by the substitution of computation for communication. We argue that as sensor nodes improve in the sense of being capable of more computation per energy unit, then it is sensible to consider to provide more computation at the sensor node itself [6], [7], [8].

2.1 Restricted Resources

To develop any applications in WSN devices, available resources are always a significant challenge. Since WSN devices have limited power in CPU and battery (for example, 50 MHz and 2200 mAh with 1 year operation period). Therefore resources need to be reserved for other operations. So, the key distribution needs to minimize energy consumption. Message size for distributed key is also required to be minimized. Since, a larger size of message leads to more energy consumption [9], [10], [11], [12].

2.2 Security in WSN

Most security systems are designed for high power processors and energy factor is not considered. As the restriction is still critical (for example SPINS trades off the energy consumption with several steps in key set up). So, we attempt to balance the trade-off between security and energy consumption [3], [4], [13].

3. RELATED WORK

3.1 Efficient Large-group Key-distribution protocol

Efficient Large-group Key-distribution protocol (ELK) presents a new efficient key distribution. A node can join without broadcasting message. However, it needs to maintain a tree structure. Secured communication is accomplished by passing from node to node. When receiving a message, a base station can decrypt the message by searching the key in a tree map. An advantage is the key broadcasting requires only a hint message. As the hint message is received, node can perform computation by matching a signature with computed key. However, an overhead in maintaining the tree hierarchy is unsuited for sensor networks [5].

```

select random number L
if this is the first time then
    load key K = KM
else
    load key K = K0
endif
for j = L downto 0 do
    compute key K = F1[K]
endif
store key K0 = K
compute hash value S1 = H[K]
select random number N
for j = N downto 0 do
    compute key K = F2[K]
endif
compute hash value S2 = H[K]
encrypt message [S1/S2] with key KC
broadcast message KC[S1/S2]

```

Figure 1. Sender operation in HKD

3.2 Security protocol for sensor networks

A. Perrig et. al propose Security protocol for sensor networks (SPINS) that combines two existing security mechanisms: SNEP and μ TESLA. SNEP provides secured two-party data communication. μ TESLA is a small version of TESLA which set up an authentication for data broadcasting. μ TESLA generates keys from repeatedly computed one-way function. Then nodes use the keys backward: K_i, K_{i-1}, ..., K₀. Despite intruders capture the key, they cannot generate the next key. SPINS is specifically designed for sensor networks and aims to minimize energy consumption. However, it requires several steps to set up a key. To set up master key, it needs to exchange a lot of information before establishing secured communication [14].

4. NOTATION

We use the following notation to describe HKD protocol and operation in this paper:

M₁ | M₂ is the concatenation of message M₁ and M₂

H[D] is the hash function which digests data D

F₁[D] is the first one-way function which covert data D

F₂[D] is the second one-way function which covert data D

K_C is the common key to use when secret key is not set up

```

decrypt message with key KC
extract S1 and S2 from broadcasted message
if this is the first time then
    load key K = KM
else
    load key K = K0
endif
do
    compute key K = F1[K]
until H[K] equals S1
store key K0 = K
do
    compute key K = F2[K]
until H[K] equals S2
store K as secret key

```

Figure 2. Receiver operation in HKD

K_M	is the master key to generate keys for the 1 st time.
K₀	is the storing key to save previous key session
K[M]	is encryption of message M with key K
S₁	is the signature of key from F ₁
S₂	is the signature of key from F ₂
L, N	are the random numbers in the key generating

5. ASSUMPTIONS

Our objective is to address key distribution. We do not consider routing communication or physical protection of the nodes.

5.1 Physical protection

In sensor devices, physical hardware must be protected against key and program stealing. In this paper, we assume that the nodes are safe from physical tampering. If necessary, nodes can be protected by implementing Watermarking, Tamper-Proofing and Obfuscation [4].

5.2 Routing established

We assume that routing and connection are established before performing the key distribution. Despite HKD operates on top of this network layer, we include delivery features to evaluate the performance [15].

5.3 High risk area

We assume high risk environment with attackers surrounding the network. These intruders may intercept every message of transmission with unlimited computation resources. This requires keeping all messages confidential [16].

6. REQUIREMENTS

6.1 Data confidentiality

Data security is a main issue. The security is required not to be breached by a trapped message. Strong defense is necessary because WSN devices have low resources compared to intruder [13].

6.2 Simplicity

Sensor network nodes can be deployed in different topologies: tree structure, shortest-path and non-structured. The key distribution must adapt to any network topology. Also, joining and leaving nodes must not affect other parts of the network structure. Otherwise energy is wasted in adjusting hierarchy every time when structure is changed [15].

6.3 Reliability

The time interval for key updating should be minimized. The distributed mechanism must be able to operate in all scenarios: lost message, lost key, joining and battery changing [17].

7. ALGORITHM

HKD is inspired by the use of hint messages in ELK [5]. It uses symmetric encryption to secure transmissions. The confidentiality and simplicity are provided from encryption and decryption. When every sensor node has the secret key, it can establish secured communication without altering the routing (or tree hierarchy).

To construct a key, we describe two sides of operations. Sender and receiver have common key, K_C which is used as a secret key when the key is not distributed. Master key, K_M is also installed for the part of key computation.

Two one-way functions F_1 and F_2 could minimize the computation while maintain large key domain. There are more key possibilities to protect from intruders in guessing the secret key. In the long term, despite both sender and receiver remain computing in the same range (L, N). Intruders require a large set of key to attack. Since secret key is generated from previous key, this add up the

number of possible keys to $L^t \times N$ to attack (where t is number of key distribution).

7.1 Sender process

Secret key is generated from repeatedly computing one-way function F_1 and F_2 . Then, sender broadcasts encrypted message which contains signature key from both F_1 and F_2 as in Fig. 1.

7.2 Receiver process

When broadcasted message is received, receiver decrypts message and extracts signature S_1 and S_2 . Then it repeatedly computes K_M until its hash value matches with S_1 and then repeats for S_2 as in Fig 2.

7.3 Key renewing process

Sender and receiver start computing the secret key from previous key, K_0 instead of K_M . So there is no key duplication and minimize the computation.

8. EVALUATION

To evaluate, we construct HKD with selected cryptographic hash function. MD5, CRC32 and ADLER algorithm are selected. MD5 and ADLER use 32 bytes of signature while CRC32 uses 4 bytes. Although CRC32 has advantage with the smallest size among three algorithms, CRC32 and ADLER are not recommended because their signatures have potential to allow backward computing.

To simulate HKD, we use an algorithm which follows the structure of Smart Dust [20], [21]. We need to compare with SPIN, developed on Smart Dust. In this algorithm, receiving and transmitting signal are separated. Also, different amount of energy is used based on distance between nodes. To deploy nodes, they are placed in square grid. The distance between nodes is equivalent. Base station is placed in the middle. In the simulation, distance of each node is the half of maximum range to average the energy consumption. Then, we set up 10 nodes in each cluster and sampling rate 1Hz. Packet transmits every 20s with 50 Kbps bandwidth. Hardware consumes 4.8 mA on receiving and 12 mA on transmitting. In idle mode, energy consumption rate is 5 μ A. Battery supplies 2200 mAh with 3 Volts in operation.

In normal operation, HKD shows a competitive energy saving comparing to both TESLA and SPINS. However, the energy consumption increases dramatically in some scenarios, when HKD is simulated in random deployment. Since, sensor network nodes do not receive the hint message, they attempt to transmit data with the previous key. So, base station rejects the message because the key is not matched. However, the nodes continue sending data.

The problem is nodes are not noticed when messages are dropped. Hence, they need to wait until next broadcasting. In attempting to communicate, we found that a lot of energy is wasted when nodes have difficulty in transmission. In the worst case, it consumes up to 300% more.

8.1 Energy Consumption

Energy consumption is the significant issue in sensor networks. MD5 consumes 0.59 $\mu\text{J}/\text{Byte}$ when comparing to 3DES computation, 6.04 $\mu\text{J}/\text{Byte}$. So it can be assured that system has capability to operate encryption, also able to perform HKD [9], [18], [19].

Table 1 is the simulation result which shows the energy consumption in HKD, TESLA and μ TESLA (in SPINS). This simulation focuses on message size and energy consumption. This shows almost three times expected lifetime in communication comparing to TESLA. However, in set up process, TESLA in ELK consumes less energy than HKD because ELK uses tree to distributed keys comparing to traditional broadcasting in HKD.

8.2 Computational resources

According to Potlapally et. al, high power processor Strong Arm chip computes each MD5 140 μs in small wireless network device. In simulation, random number L and N are in the range of {1, 2, 3 ... 20}. In the average, MD5 requires to compute 10 times. This equals to 1.40 ms (140 μs x 10 times). To compute MD5 in low power CPU (Xscale in energy safe mode), it requires 180 μs for each computation or 1.80 ms per key distribution. So, we can be assured that computation time for this HKD would not exceed the capabilities of a sensor node [18].

8.3 Data confidentiality

In HKD security, two one-way functions have been used to compute the secret key. Comparing to SPINS, it only uses a single one-way function. HKD has an advantage in computing another one-way function. This increases a number of key possibilities which also increases complexity in key breaking. Also, hint message in HKD is encrypted with K_C to verify the base station. In SPINS, it requires negotiating before transmitting the master key. HKD has never exposed a master key in communication but transmits only their signatures. However, HKD generates keys from a single master key. So, intruder may attack on this finite set of possibilities [22].

8.4 Maintenance

In ELK, tree structure provides completed information in node connection. However, it always requires maintenance

Table 1 Energy consumption in communication

Protocols	Message size (bytes)	Operation Time (days)
TESLA	686	251
SPINS	598	277
HKD	64	715

including joining and leaving nodes. To leave without notice, several operations must be involved. This includes neighbor nodes in exchanging information and re-organizing a tree structure [5]. In SPINS, it is more dynamic structure which does not require a fixed tree structure. To distribute key, it minimizes an operation in connection establishing and master key transmitting [14]. In HKD, it requires a reliable connection to broadcast hint messages. However, in maintenance, tree structure and establishing secured connection are not required. In general situation, it is more dynamic than ELK and SPINS. However, it strongly requires a reliable connection.

9. CONCLUSION

We develop Hint Key Distribution (HKD) for sensor network. In general scenarios, this consumes little energy and provides strong security. It distributes the secret key by exchanging signatures. When sensor nodes receive hint message, they decrypt and compute the secret key. The advantages of HKD are data confidentiality, simplicity. Data confidentiality is maintained by not exposing the secret key in message. Therefore, intercepted message could not reveal the key without master key and one-way functions. Simplicity is a significant advantage in HKD which does not require maintaining tree structure. It also manages joining node to compute key without extra messages. So, the power consumption in communication is reduced. In addition, smaller broadcasting message in HKD also reduce the amount of energy.

However, HKD requires operating in reliable communication. Receivers may waste energy when hint message lost. Since it does not updated key, base station rejects the communication. Then nodes attempt to communicate until next key is broadcasted. In the worst case, it consumes energy more than TESLA and SPINS.

The future work is to implement in hardware to explore the performance. According to energy problems in unreliable connection, we expect to solve these challenging. We also consider using a set of master keys in generating key chains which is expected to improve the security in protocol. Furthermore, we attempt to implement authentication system to ensure the integrity of the data.

10. REFERENCES

- [1] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *Trans. on Embedded Computing Sys.*, vol. 3, pp. 461-491, 2004.
- [2] J. Deng, R. Han, and S. Mishra, "Security support for in-network processing in Wireless Sensor Networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*. Fairfax, Virginia: ACM Press, 2003, pp. 83-93.
- [3] S. Ravi, A. Raghunathan, and N. Potlapally, "Securing wireless data: system architecture challenges," in *Proceedings of the 15th international symposium on System Synthesis*. Kyoto, Japan: ACM Press, 2002, pp. 195-200.
- [4] C. Collberg, "Watermarking, Tamper-Proofing, and Obfuscation – Tools for Software Protection" *IEEE transactions on software engineering*, vol 28, pp 735-746, 2002
- [5] Perrig, D. Song, and D. Tygar, "ELK, a new protocol for efficient large-group key distribution," presented at Security and Privacy, 2001. S&P 2001. Proceedings. 2001 IEEE Symposium on, 2001.
- [6] W. Freeman and E. Miller, "An Experimental Analysis of Cryptographic Overhead in Performance-Critical Systems" in *Proceedings of the 7th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems* IEEE Computer Society, 1999 pp. 348
- [7] Sharaf, J. Beaver, A. Labrinidis, and K. Chrysanthis, "Balancing energy efficiency and quality of aggregate data in sensor networks," *The VLDB Journal*, vol. 13, pp. 384-403, 2004.
- [8] W. Du, R. Wang, and P. Ning, "An efficient scheme for authenticating public keys in sensor networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. Urbana-Champaign, IL, USA: ACM Press, 2005, pp. 58-67.
- [9] P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F. Mueller, and M. Sichitiu, "Analyzing and modeling encryption overhead for sensor network nodes," in *Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications*. San Diego, CA, USA: ACM Press, 2003, pp. 151-159.
- [10] S. K. Miller, "Facing the Challenge of Wireless Security," *Computer*, vol. 34, pp. 16-18, 2001.
- [11] M. Ulema, "Wireless sensor networks: architectures, protocols, and management," presented at Network Operations and Management Symposium, 2004. NOMS 2004. IEEE/IFIP, 2004.
- [12] G. Barrenechea, B. Beferrull-Lozano, and M. Vetterli, "Lattice sensor networks: capacity limits, optimal routing and robustness to failures," in *Proceedings of the third international symposium on Information processing in sensor networks*. Berkeley, California, USA: ACM Press, 2004, pp. 186-195.
- [13] Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, pp. 53-57, 2004.
- [14] Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: security protocols for sensor networks," *Wirel. Netw.*, vol. 8, pp. 521-534, 2002.
- [15] J.-H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 12, pp. 609-619, 2004.
- [16] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the 2003 ACM workshop on Wireless security*. San Diego, CA, USA: ACM Press, 2003, pp. 30-40.
- [17] S.-J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks," in *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*. Roppongi Hills, Tokyo, Japan: ACM Press, 2004, pp. 78-89.
- [18] N. R. Potlapally, S. Ravi, A. Raghunathan, and N. K. Jha, "Analyzing the energy consumption of security protocols," in *Proceedings of the 2003 international symposium on Low power electronics and design*. Seoul, Korea: ACM Press, 2003, pp. 30-35.
- [19] J. D. Touch, "Performance analysis of MD5," in *Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication*. Cambridge, Massachusetts, United States: ACM Press, 1995, pp. 77-86.
- [20] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," *SIGPLAN Not.*, vol. 35, pp. 93-104, 2000.
- [21] L. F. Perrone and D. M. Nicol, "Network modeling and simulation: a scalable simulator for TinyOS applications" in *Proceedings of the 34th conference on Winter simulation: exploring new frontiers*. San Diego, California Winter Simulation Conference, 2002 pp. 679-687
- [22] P. Techateerawat and A. Jennings, "Analyzing the Key Distribution from Security Attacks in Wireless Sensor", presented at International Conference on Systems, Computing Sciences and Software Engineering, 2006.

A Model for GSM Mobile Network Design

Plácido Rogério Pinheiro

placido@unifor.br

Alexei Barbosa de Aguiar

alexei@verde.com.br

University of Fortaleza

Av. Washington Soares, 1321, Bloco J, sala 30

Phone.: +55.85.3477.3263 Fortaleza - Ceará - Brazil

Abstract - This work shows a mathematical and computational tool to design a GSM (Global System for Mobile Communications) network, in the point of view of BSC (Base Station Controllers) allocation and dimensioning. It optimizes the total transmission cost and BSC acquisition cost. It determines how much BSC are need, in what sites they has to be allocated, what model each one must have to support the total traffic demand without wasting money with their acquisition and what BTS (Base Transceiver Station) must be linked to what BSC for transmission cost reduction. Its core is a integer programming (IP) model as presented in Wolsey *et al* [8]. The approach of data generation to the model from the real world is explained too. In this model, the BSC nodes are allocated taking account both factors: Transmission and BSC acquisition costs. The transmission cost involves distance and capacity of the E1 lines. The links between BTS and BSC are allocated, and the ones between BSC and MSC are dimensioned in number of E1 lines. The choice of the BSC model that has the best capacity to the total traffic demand gives flexibility for the mobile network design comparing with fixed capacity models. It is important since in real cases, the BSC suppliers gives configuration options from low capacity and price, until high capacity with good relative cost. This model uses the traffic demand in Erlangs instead of number of voice channels. This approach allows the links between BSC and MSC (Mobile Switching Center) dimensioning using the statistic gain of telephony switches. Otherwise, simple deterministic sum of voice channels would be very simplistic, but would oversize the links too. Other important issue in this model is the fact that it addresses the new resources allocation technique of BSC switches that rises its capacity. The traditional way of resources allocation (processors, for instance) to the radio channels was deterministic and fixed. Thus, its capacity was given by total number of voice channels (4096, for instance). Nowadays, the BSC can handle a pool of resources that are allocated on-demand. The capacity rises and is given by its total traffic in Erlang.

Key words: GSM mobile network design, cellular telephony, Integer Programming (IP), Operations Research.

1. Introduction

One GSM mobile network is composed by many kind of equipments. There are switches called MSC and BSC, HLR (Home Location Register) that act like subscriber databases, SGSN (Serving GPRS Support Node) that is the data network switch version of the MSC, and many more.

In this work, we will concentrate in the BSS (Base Station Subsystem).

The BSS is the group of equipments that goes from the BSC to the mobile phone side. It is composed mainly by BTS, BSC, MSC and transmission network to link them all.

The BTS radiates the RF (Radio Frequency) signal to the mobile phones and receive its signal back. This signal is radiated by antennas in the top of towers or buildings, creating coverage areas called cells. The geographical allocation of BTS is guided by RF coverage and traffic demand.

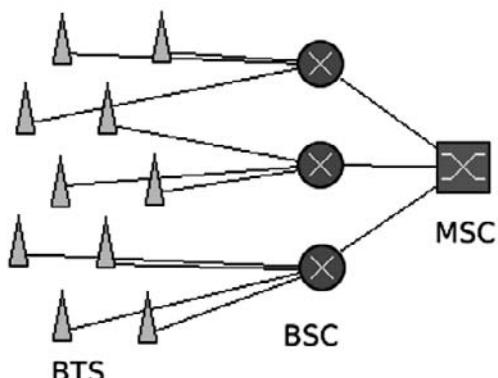


Fig 1 - Mobile Network Design

When the coverage is the goal, the RF engineering's look for high altitudes and free of obstacles sites to reach larger distances. When the goal is traffic, hot spots are focused with a BTS full equipped with radio channels in a limited and controlled RF radiation. In an urban area, the BTS proximity is limited by interference, since there is a limited number of RF channels and they are repeated on and on. The BTS sites are disposed in a triangular grid pattern, where it is possible. This disposition is due to the three cells of each BTS that are formed by the coverage of the tree groups on antennas, disposed with 120° angles between them.

Once BTS allocation is finished its time to geographically allocate the BSC.

BSC are small telephony switches that control the BTS. Its goal is to create an additional level in the network hierarchy and increase the efficiency, based on the statistical gain. It is an exclusivity of GSM system. An IS-136 and CDMA family hasn't this equipment.

Its links with BTS are E1 lines that hold voice channels slots configured deterministically in a one-to-one basis with BTS's radio channels slots. It's called Abis interface.

On the other hand, BSC's trunks with MSC are E1 lines dimensioned by the total traffic from all of its BTS. It's called A interface. These trunks are similar to trunks between two MSC, or other telephony switches. The voice channels in these cases are seized statistically and it varies with the hours. All calls must pass through the MSC, even when both subscribers are close, in the same BSC coverage.

The Erlang B formula that calculates the blocking probability (or congestion, or Grade of Service GoS) to a given number of resources (voice channel, normally) and traffic offered.

Each of the three variables in this formula can be calculated from the two others to each situation. We can calculate the percentile of calls that are lost with the number of voice channels available in some equipment and the measured traffic. We can calculate how much channels would be necessary to flow this traffic if the GoS was the desired (2%, for instance). This is used to adjust the network. We can also calculate how much traffic can we flow with a given number of channels and the desired GoS.

The Erlang B formula is shown below.

$$e_b = \frac{\frac{a^n}{n!}}{\left(\sum_{i=0}^n \frac{a^i}{i!} \right)}$$

where e_b is the probability of blocking, also known as GoS, n is the number of resources (voice channels in this case) and a is the amount of traffic offered in Erlangs.

Some BSC has a deterministic way of resources allocation. When a new radio channel is installed in a BTS, the required resources (processors, for instance) are binded with this new radio channel in a fixed way. This resources are compromised with the radio channel despite it is in a call or is idle. Thus, the BSC has a fixed maximal capacity in number of radio channels. For instance, 4096 radio voice channels (slots).

Some more modern BSC uses a pool of resources that are binded to the radio voice channel on demand, when a call is made. This feature rises the BSC capacity. Now the maximum BSC capacity in this situation can't be determined by its number of radio channels, but by its traffic capacity in Erlangs. For instance, the 4096 radio voice channel BSC would be transformed in a 4058 Erlangs (at 2% GoS) BSC, with virtually unlimited number of radio voice channels.

Therefore, there are deterministic channels in E1 lines from BTS to BSC. This lines wastes transmission resources. And there are statistical channel in E1 lines from BSC to

MSC. These lines are efficient.

The more BSC we distribute the less transmission costs, since this equipment reduces the distances of BTS to BSC links that wastes transmission lines. On the other hand, the BSC has its acquisition cost. The balance between these two costs is reached with the optimal geographical allocation of the BSC, associated with its correct choice of model that implies in its capacity and cost.

A typical GSM network has hundred or thousand BTS and tens or hundreds of BSC. The human capacity of designing efficient networks is very limited and the costs are high. The use of computational tools can reduce these costs radically.

This is this work's target.

2. The mathematical programming model

$T = \{t_1, t_2, t_3, \dots, t_m\}$ BTS nodes;

$B = \{b_1, b_2, b_3, \dots, b_n\}$ BSC nodes;

$W = \{w_1, w_2, w_3, \dots, w_o\}$ BSC models;

$C = \{c_0, c_1, c_2, \dots, c_p\}$ Link capacities;

x_{ij} Decision variables for link allocation between BTS node i and BSC node j;

y_{lc} Decision variables for choosing the capacity c of E1 (2 Mbps) lines between BSC l and MSC;

z_{lw} Decision variables for BSC l model w choice.

ct_{ij} Link cost between BTS i and BSC j nodes in an analysis time period;

cm_{lc} Link cost of capacity c between BSC l nodes and MSC in an analysis time period;

cb_w BSC model w acquisition cost, considering an analysis time period;

a_i BTS i traffic demand in Erlangs;

f_c Link capacity c in Erlangs;

e_w BSC model w traffic capacity in Erlangs.

Objective Function

The objective function (1) minimizes total cost of links between BTS and BSC, plus cost of E1 lines between BSC nodes and MSC, plus total cost of BSC's acquisition.

$$(1) \text{minimize} \sum_{i \in T} \sum_{j \in B} ct_{ij} x_{ij} + \sum_{l \in B} \sum_{c \in C} cm_{lc} y_{lc} + \sum_{d \in B} \sum_{k \in W} cb_k z_{dk}$$

Restrictions

In (2), each BTS must be connected to one and only one BSC:

$$(2) \sum_{j \in B} x_{ij} = 1, \quad \forall i \in T$$

In (3), the y_{lc} dimensioning is made. It allows all traffic from BTS assigned to one BSC to flow over its links:

$$(3) \sum_{i \in T} x_{il} a_i \leq \sum_{c \in C} f_c y_{lc}, \quad \forall l \in B$$

In (4), the BSC dimensioning is made accordingly to the given models and the total traffic demand.

$$(4) \sum_{i \in T} x_{ij} a_i \leq \sum_{k \in W} e_k p_{jk}, \quad \forall j \in B$$

Variables constraints. (4), (5) and (6) restricts the decision variables to be binary.

$$(4) x_{ij} \in \{0,1\}, \quad \forall i \in T \quad \forall j \in B$$

$$(5) y_{lc} \in \{0,1\} \quad \forall l \in B \quad \forall c \in C$$

$$(6) z_{lw} \in \{0,1\} \quad \forall l \in B \quad \forall k \in W$$

3. Model application

This model has some issues in real applications that must be observed.

The set of BTS nodes T is known previously because its design is made by RF engineers as the first step. Its geographical location is determined by coverage and traffic. Its traffic demand is known previously too by measure of other mobile network (old one that is being replaced, or by other technology such as TDMA (Time Division Multiple Access) or CDMA (Code Division Multiple Access)) or by estimation based on mean subscriber traffic and subscriber forecast based on population.

The set of BSC nodes B can be generated based on all viable sites possibilities. The sites that will have a BTS are good candidates, since its space will be already available by rental or buy. Other company buildings can be added to the set. The B set represents the possibilities, not the actual BSC

allocations. The more options this B set has, the better will be the allocation of the needed BSC.

The W set contains the possible models of BSC. Normally a BSC manufacturer offers different models. Each one has its capacity in Erlang (in our model) and price.

The C set is a table of traffic capacities for an integer number of E1 lines. Each E1 line has a number of time-slots allocated for voice from the 31 available. Other time-slots are used for signaling and data links. Thus, the first E1 line may have a different number of voice time-slots than the second E1 line, and so on. Each voice time-slot carries 4 compressed voice channels.

The elements of the C set are calculated by the reverse Erlang B formula, taking the number of voice channels and the design GoS as incoming data and the traffic as outgoing data. The first element of C set is 0 E1 lines, that has 0 Erlang. The second element of C set is 1 E1 line and has the traffic calculated for 4 times the number of time-slots allocated for voice in this E1 line. The third element of C set is 2 E1 lines and has the traffic calculated for 4 times the number of time-slots allocated for voice in all 2 E1 lines, and so on. The size of the C set is determined by the maximal capacity of the larger BSC model.

The link costs ct and cb in a given period of analysis must be determined by the transmission nature. If the transmission network belongs to the mobile company, its cost can be determined by distance bands or linearly plus an equipment fixed cost. If mobile company contracts transmission lines from other company, the costs must be calculated based on the business rules. Quantity discounts can be applied, for instance.

The model can be adapted to work with BSC that has maximum number of radio channels capacity, instead of maximum traffic capacity.

4. Computational results

Simulations were made with many network sizes. The bigger network sizes that could be solved in a reasonable time has about 40 sites. The different generated data caused big differences in the solving time. For instance: The smaller time for 40 sites, 2160 integer variables, 161 restrictions was 5 minutes and 10 seconds, while other data made the solver to spent more than 30 minutes to solve.

The data was generated using the following assumptions.

The transmission cost was linear in function of the link distance. The local market approximated cost where used. The cost of more than one E1 line in the same link was linear too.

The BTS and MSC site geographical locations where generated randomly. To each BTS site, a BSC site candidate was generated. The traffic of the BTS was generated randomly from 0 to 80 Erlangs that is the approximated value that a BTS can handle with an E1 line.

The C set was generated with 41 values, from 0 E1 lines until 40 E1 lines. For each capacity, the correspondent traffic was calculated accordingly to the exposed in the model application session (3).

Three BSC models where used in this simulations: A small model with 512 Erlangs of capacity, a medium model with

2048 Erlangs of capacity and a large model with 4096 Erlangs of capacity. Each one had an acquisition price compatible to the local market reality.

The Lingo 8.0 Schrage [5] modeling and solver tool from Lindo Systems Inc. was used in the simulations. Its license has unlimited variables and restrictions, and a full set of optional algorithms. To this model, the Branch and Bound solver was selected automatically. It runned it a 64 bits AMD Turion processor with 1.8 MHz clock and 512 MB of memory.

Despite the fact that 40 sites is very small comparing to the hundreds or even thousand sites of the real mobile networks, the simulations shown the correctness of the model. Varying the costs, more or less BSC were allocated. Its model was correctly chosen accordingly to the total traffic demanded by the BTS allocated to each BSC. The distances were minimized indirectly because of the linear cost by kilometer. The trunk between BSC and MSC was sized to flow the total traffic demand of the BSC, and its distance to MSC was took account, since the amount of E1 lines was greater than one.

TABLE 1

Characterization of the Instances Used in the Experiments

Sites	Var.	Restrict.	Non zeros	Time
10	240	41	760	00:00:00
20	680	81	2320	00:00:04
30	1320	121	4740	00:02:43
40	2160	161	7840	00:05:10

5. Correlated work

Kubat *et al* [1, 2] shows a generic model for mobile network design. This model was used as basis in Rodrigues *et al* [4]. The model had adaptations to solve the problem of electing hub nodes to group channels and reduce waste of transmission lines capacity in real scenarios. This can be seen as the first level mobile network design.

This paper extends this view to the second level hierarchy of mobile network design, since it adds new issues like Erlang probabilistic techniques and BSC model choice, for instance. The analog extension can be used to the third level of mobile network design, where the MSC would be allocated to the previously BSC allocation, to minimize the transmission and MSC model choice costs.

Each model isolated solves a specific level in the design hierarchy. The next work will merge both models in a single one to improve efficiency and give an even lower cost designs. This model is heavier than the previous one. When both models are merged, the resultant one will be much heavier and will limit the size of the network.

Experiments with new state-of-the-art parallel solvers running in 64 bits dual core processors will give extra power to help solving the real world mobile problems. The bigger is the problem, the bigger is the optimization.

To break this limitations and turn big network designs viable, some methodologies like Lagrangean relaxation in Simple Subgradient, Bundle Methods and Space

Dilatation Methods (Shor *et al* [6, 7]) must be used. Rigolon *et al* [3] shows that the use this tools in the first model extends the size of the mobile network to be designed. Other methodologies must be analyzed too in the reach of viability for bigger networks designs.

6. Conclusion

This work gave a solution to a network design problem of mobile GSM operators capturing its essence in a mathematical model. In introduction some telecommunications background was given to help understanding the model. Then, the model was presented and explained.

After the model presentation, we showed the model application that explains how to link technical details of the real world with the model's generated data.

In computational results, a size and performance simulation was described. We can see the model by itself can't be used to the real networks because of its size. Simulation with real networks can't show the optimization potential because small networks are well designed by human intuition and have small costs too. Some methodology must be applied to extend the size of the problems to achieve hundred or thousand BTS sites. Thus, the optimization gain will be very effective.

Bibliographical references

- [1] Kubat, P e Smith, J. MacGregor. "A multi-period network design problem for cellular telecommunication systems". European Journal of Operational Research, 134:439-456, 2001.
- [2] Kubat, P., Smith, J. MacGregor e Yum. C. "Design of cellular networks with diversity and capacity constraints". IEEE Transactions on Reliability, 49:165–175, 2000.
- [3] Rigolon, A. A., Pinheiro, P. R., Macambira, E. M., Ferreira, L. O. R. A. Approximate Algorithms in Mobile Telephone Network Projects. International Conference on Telecommunications and Networking, Bridgeport, Springer Verlag, 2005, v. XV, p. 234-347
- [4] Rodrigues, S. I. M. Relaxação Lagrangeana e subgradientes com dilatação de espaço aplicados a um problema de grande porte. RJ, 1993.
- [5] Schrage, L. Optimization Modeling with Lingo. Lindo Systems Inc., 1998.
- [6] Shor, N. Z. Utilization of the operation of space dilatation in the minimization of convex functions. Cybernetics, 1:7-15, 1970.
- [7] Shor, N. Z. Zhurbenko, N. G. A minimization method using the operation of extension of the space in the direction of the difference of two successive gradients. Cybernetics, 7(3):450-459, 1970.
- [8] Wolsey, L. A. Integer programming. John Wiley & Sons, 1998.

Application of LFSR with NTRU Algorithm

P.R.Suri, Priti Puri

Department of Computer Science & Application, Kurukshetra University, Kurukshetra,
pushpa.suri@yahoo.com, puri_priti@rediffmail.com, phone: 09871287130; 011-26472891

Abstract— The paper deals with stream cipher based on Linear Feedback Shift Registers (LFSR). A scheme is proposed where n-Linear Feedback Shift Registers are used for the encryption and decryption. Both the public key cryptography and the concept of linear feedback shift registers are used in this scheme. The plaintext message is encrypted by LFSRs and secret key, i.e., Initialization Vector (IV) is sent with the help of public key cryptography. The mathematical model for this scheme is described with a case study for (n=4) LFSRs.

I. INTRODUCTION

Currently, the internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce. Therefore, security becomes tremendously important issue to deal with. In security, cryptography is the art of achieving security by encoding messages to make them non readable. Plain text, the original message, codified by using a suitable scheme, is known as cipher text. The method of producing cipher text from plain text is encryption and reverse process is decryption.

Cryptography Schemes: There are two types of cryptographic schemes:

1. *Secret key (or symmetric) cryptography (SKC):* In the symmetric-key approach, both sender and receiver share a common key with a level of trust, is required to ensure that neither party divulges the key. Here, D_k is decryption and E_k is encryption and M is original message.

$$D_k(E_k(M)) = M \quad (1)$$

There are two broad categories of Symmetric algorithms, viz., block cipher and stream cipher.

Block cipher transforms a fixed length block of plaintext P_i 's into the same length of cipher text C_i 's:

$$C = E(P, k) \quad (2)$$

where the encryption function E is applied to P under the influence of a key k of length m bits. Some important block ciphers are used efficiently as DES, 3DES and AES [5].

A stream cipher converts each P_i into C_i as follows:

$$C_i = P_i \text{ XOR } k_i \quad (3)$$

Where k_i 's are generated through a key stream generator. The security of stream cipher depends entirely on the non-linear structure of the key stream generator. Stream cipher [2] encrypt individual characters (binary digits) of a plaintext message one at a time, using an encryption transformation, which varies with time as the Vernam cryptosystem or one-time-pad. The need for a key of the same size as the plaintext makes the One-Time-Pad impractical for most

applications. Instead, stream ciphers expand a given short random key into a pseudo-random key stream, which is then XOR'ed with the plaintext to generate the cipher text. The used part of the key must be discarded. A seed or initialization vector is used to build the key with a pseudo-random sequence generator. Stream ciphers are faster than block ciphers in hardware with less complex hardware circuitry and also advantageous when transmission errors are highly probable.

There are different types of stream ciphers as synchronous and self synchronising stream ciphers and LFSR based stream ciphers. Our concentration is on LFSR based stream ciphers as they can be implemented cheaply in hardware, and their properties are well-understood. Binary stream ciphers are constructed using (LFSR)s because easily implemented and readily analysed mathematically.

2. Public-key (or asymmetric) cryptography (PKC)

one key for encryption and another for decryption is used.

Hybrid Scheme is also used where message is encrypted with the help of the symmetric key cryptography and key is sent at receiver side with the help of the public key cryptography.

II. PURPOSED APPROACH

The approach utilizes different LFSRs in parallel for encryption and decryption. This approach is using hybrid scheme for security where LFSR is used to encrypt the message for sending secret key, public key cryptography is used.

The approach first converts the plaintext into binary format and LFSRs start by initialization Vector values. Here n-LFSR will work together and n-IV functions are required to start n LFSRs.

Initialization Vector of first LFSR, IV_1 , starts with one non-linear polynomial function. The variable of this polynomial is behaving like the key, which is required at both the sides. For sending the key, the concept of the public key cryptography is used.

The scheme is divided into two parts.

- Working of LFSR with Initialization Vector generation.
- Sending the key at receiver side with the help of public key cryptography.

A. For first part

- 1) Convert plaintext message into binary format
- 2) LFSRs start with their IVs.
- 3) n- LFSRs will work in parallel and for initiate these LFSRs we required n- IVs.

For Initialization Vector generation

- 1) Take some non-linear polynomial function (i.e.modulo 2) with a value of variable or

indeterminate and output of this polynomial will be IV_1 of LFSR₁.

- 2) For IV_2 , value of the variable (X_2) of non-linear polynomial function will be changed and this value will be IV_1 to get the Initialization Vector of the second LFSR and same process will be repeated for LFSR₃,LFSR₄....LFSR_n.
- 3) Generated Initialization Vectors, IVs are given to LFSRs and by primitive polynomial concept[1], XOR the different position of LFSRs and get the output of LFSRs. Then this output of LFSR will be XORed with plaintext binary format and send to receiver.
- 4) Depending on the position of the characters in the plain text file, XOR the values with the corresponding LFSR_n, (where n is between 0-3,fig.2) on the basis of modulo n value. For Example, if the position of some character is 23 then 23 modulo 4 is 3, hence the character is XOR with LFSR₄, if it is at position 40 then 40 modulo 4 is 0, hence it is XOR with LFSR₁ and so on.
- 5) After applying steps 3 and 4 on all the characters of the original file, send the new file (Cipher Text) to the other authorized user along with the value of variable of non-linear polynomial used for the determination of IV.

B. For second part

- 1) Send the value (X_1) of the variable of non-linear polynomial and this will generate IV_1 of LFSR₁ at receiving end by using the concept of public key.
- 2) The value of the variable will be encrypted with NTRU algorithm [3] of public key cryptography.
- 3) Ask for the public key of receiver and encrypt this value with receiver's public key and send it to receiver with encrypted message.

C. NTRU (Number Theorist Research Unit)

Co-founders Jeffrey Hoffstein and Joe Silverman used this name of the cryptosystem. The NTRU algorithm is based on embedding messages in a polynomial ring, R. The ring is defined such that the multiplication operation of the polynomials is wrapped around the degree ("size") of the polynomial rather than expanding the degree of the polynomial. Each coefficient of the polynomial is an integer which is reduced modulo of certain parameters, after every math operation. The notation for the ring is given as: $R = \mathbb{Z}[[X]]/(X^N - 1)$ where Z represents the set of integers and N is 1 more than the degree of the polynomial.

Key creation: Receiver A chooses two random polynomials f and g that are in the defined ring R and whose inverses exist in the ring modulo key parameters p and q. These inverses are denoted F_p and F_q respectively, and need to be computed for the chosen f. If the inverse of either does not exist another f is chosen and the process is repeated. Next receiver A generates the public key as the polynomial h:

$$h = F_q * g \bmod q \quad (4)$$

where f and g have a specific amount of coefficients that are 0, +1 and -1. The private key is the polynomial f along with the inverses F_p and F_q . N, p, and q are considered parameters of the algorithm rather than part of either key. Now plain text is described into the binary form and after that encrypted message, e is created as below. Public key, h is the inverse of private key polynomial f.

Encryption: Sender B, wishing to send a binary message X_1 to A, begins by randomly choosing a polynomial r that is in R. Sender B performs the encryption by computing

$$e = pr * h + X_1 \bmod q \quad (5)$$

integer p and r have scalar multiplication. Multiplication of r with h is wrapped around the ring size.

Decryption: Receiver A begins to decrypt the message e by multiplying it with polynomial f as given below

$$z = f * (pr * h + X_1 \bmod q) \quad (6)$$

and reducing the coefficients of z to lie between $-q/2$ to $q/2$. Now z is again multiplied with F_p to decrypt the message x, which is value of variable of polynomial, i.e. key required at both the sides,

$$= z * F_p$$

$$= \{f * (pr * h + X_1 \bmod q)\} * F_p \quad (7)$$

where F_p is part of his private key and is the multiplicative inverse of f mod p, as derived in the key generation.

D. At sending end

- 1) The value of variable of non-linear polynomial behaves as plaintext and encrypted with the receiver's public key and sent to the receiver's side.
- 2) With this encrypted value, cipher text message also sent at receiver side. This cipher text is created by XORing the plain text with the output of the LFSRs. Depending on the position of the characters in the plain text file, XOR the values with the corresponding LFSR_n, (where n is between 0-3,fig.2) on the basis of modulo n value.

Initialization Vector generation:

$P(X) = \text{Non-linear polynomial}$
 $X = X_1 \quad (\text{Secret Key})$
 $Q_1 = P(X_1)$
 $IV_1 = Q_1 \quad (\text{First Initialization Vector})$
 $X_2 = IV_1$
 $Q_2 = P(X_2)$
 $IV_2 = Q_2$
.....
.....

$$\begin{aligned} X_n &= IV_{n-1} \\ Q_n &= P(X_n) \\ IV_n &= Q_n \\ n &= \text{Number of LFSRs} \end{aligned}$$

E. At Receiving end

- 1) Receiver will see the encrypted message and encrypted key with his public key.
- 2) He will decrypt the value of the variable(X_1) of non-linear polynomial, by using his private key which is dependent on NTRU algorithm.
- 3) Then apply the value of (X_1) on non-linear polynomial function, to get the Initialization Vector of the first LFSR i.e. IV_1 .
- 4) The same procedure will be repeated on the $LFSR_2, LFSR_3, \dots, LFSR_n$ as at the encryption side.
- 5) On the other hand, change the cipher text from the file to its corresponding binary format, character by character. Now depending on the position of the character in the file, XOR the values with the corresponding $LFSR_n$, (where n is between 0-3, fig2.) on the basis of modulo n value.
- 6) The Plain text file will be obtained after applying steps 4 and 5 on all the characters of the received file.

F. Formula representation of the approach

Output of polynomial $Q_1 \leftarrow$ Value of variable(X_1) of non linear polynomial $P(X_1)$

$$\begin{aligned} IV_1 &\leftarrow Q_1 \\ IV_2 &\leftarrow Q_2, \text{output of polynomial } P(X_2) \text{ with } IV_1 \text{ as } X_2. \\ IV_3 &\leftarrow Q_3, \text{output of polynomial } P(X_3) \text{ with } IV_2 \text{ as } X_3. \\ \dots & \\ IV_n &\leftarrow Q_n, \text{output of polynomial } P(X_n) \text{ with } IV_{n-1} \text{ as } X_n. \\ \text{Binary Text} &\leftarrow \text{Plain Text} \end{aligned}$$

Check the value for state modulo n (Fig.2,n=4)

For Remainder = 1 do

$$PT_1(\text{Binary format}) \oplus LFSR_1(IV_1)$$

For Remainder = 2 do

$$PT_2(\text{Binary format}) \oplus LFSR_2(IV_2)$$

For Remainder = 3 do

$$PT_3(\text{Binary format}) \oplus LFSR_3(IV_3)$$

For Remainder = 4 do

$$PT_4(\text{Binary format}) \oplus LFSR_4(IV_4)$$

For Remainder = n do

$$PT_n(\text{Binary format}) \oplus LFSR_n(IV_n)$$

$$\text{Cipher Text} \leftarrow \text{Binary Text} \quad (8)$$

This gives the Cipher Text to be transmitted. Hence the file is transmitted over the network without any leakage of data. This prevents unauthorized access to the data and ensures security.

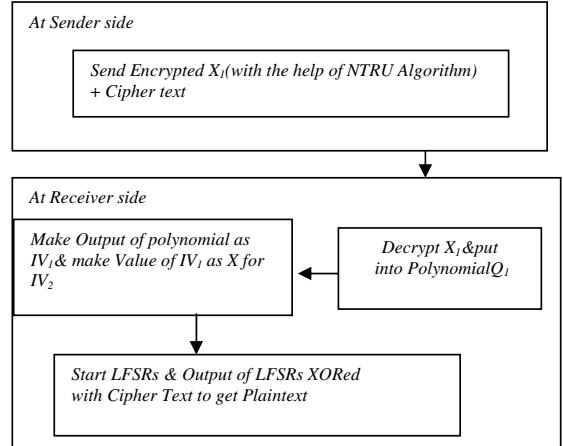


Figure1:IV generation and delivering with NTRU Algorithm

III. CONCLUSION

The paper utilizes the concept of hybrid technology where symmetric key as stream cipher is used for encryption and decryption and for sending the secret key, public key cryptography, NTRU is used. Accordingly the security will be doubled. The complexity of the algorithm will increase when different polynomials for different LFSRs are used. The values of the IV_2, \dots, IV_n are dependent on the previous values, which can be a limitation. This can be overcome by increasing the degree of the polynomials. BRUTE FORCE ATTACK can be avoided here because first it needs to find the secret key which is encrypted with public key cryptography then it has to work for Initialization vector polynomial. In this approach, the position of plain text in the file also plays the important role because XORing of plaintext with output of LFSR depends on the position of plaintext in the file and that is hidden. The number of LFSR used is also hidden, i.e. the value of n . In the end, we have illustrated a working scheme with four LFSRs and their IV generations diagrammatically.

(fig2.)

IV. MATHEMATICAL MODEL

h =public key

f, g, r =randomly chosen polynomial in ring R .

f along with the inverses F_p and F_q = private key

$N, p,$ and q = parameters of the algorithm.

e = encrypted message with help of public key, h .

$x=X_1$ = value of variable of polynomial i.e. key.

$Q_1, Q_2, Q_3, \dots, Q_n = IV_1, IV_2, IV_3, \dots, IV_n$ for

LFSR₁,LFSR₂,LFSR₃,...LFSR_n

PT=Plain Text,

CT=Cipher Text

Plaintext can be divide into parts(binary format)

Differentiation of Plain Text

$$PT = PT_1 + PT_2 + PT_3 + \dots + PT_n \quad (9)$$

Generating the public key, h, with the help of polynomials,

$$h = F_q * g \bmod q \quad (10)$$

$$e = pr^*h + X_1 \bmod q. \quad (11)$$

$Q_1 = \text{Polynomial } P(X_1)$

$Q_2 = P(Q_1)$

$Q_3 = P(Q_2)$

.....

.....

$$Q_n = P(Q_{n-1}) \quad (12)$$

$$(Q_1(LFSR_1) \oplus PT_1) + (Q_2(LFSR_2) \oplus PT_2) + (Q_3(LFSR_3) \oplus PT_3) + \dots + (Q_n(LFSR_n) \oplus PT_n) \quad (13)$$

$$CT_1 + CT_2 + CT_3 + \dots + CT_n = \sum_1^n CT_m \quad (14)$$

For sending at receiving side,

$$= \sum_1^n CT_m + e = \text{Cipher text+encrypted message} \quad (15)$$

Differentiation of $\sum_1^n CT_m + e$

$$CT_1 + CT_2 + CT_3 + \dots + CT_n + e \quad (16)$$

For decryption,at receiving side

$$z = f^*e = f^*(pr^*h + X_1 \bmod q) \quad (17)$$

$$= f^*(pr^*h + X_1 \bmod q) * F_p \quad (18)$$

$$Q_1 = P(X_1)$$

$$Q_2 = P(Q_1)$$

.....

.....

$$Q_n = P(Q_{n-1}) \quad (19)$$

$$(Q_1(LFSR_1) \oplus CT_1) + (Q_2(LFSR_2) \oplus CT_2) + (Q_3(LFSR_3) \oplus CT_3) + \dots + (Q_n(LFSR_n) \oplus CT_n) \quad (20)$$

$$= PT_1 + PT_2 + PT_3 + \dots + PT_n$$

$$PT = \int_1^n PT_m \quad (21)$$

REFERENCES

- [1] Schneider, B. *Applied Cryptography*, 2nd ed. New York: John Wiley & Sons, 1996.
- [2] Matt J. B. Robshaw, Stream Ciphers Technical Report TR-701, version 2.0, RSA Laboratories, 1995
- [3] Hoffstein, J.Pipher and J.Silverman. NTRU: A ring based public key cryptosystem, Algorithmic Number Theory (ANTS III), Portland, June 1998, Lecture Notes in Computer Science 1423, 267-288
- [4] Ferguson, N. & Schneider, B. *Practical Cryptography*. New York: John Wiley & Sons, 2003.
- [5] FIPS PUB 197: The official AES standard.

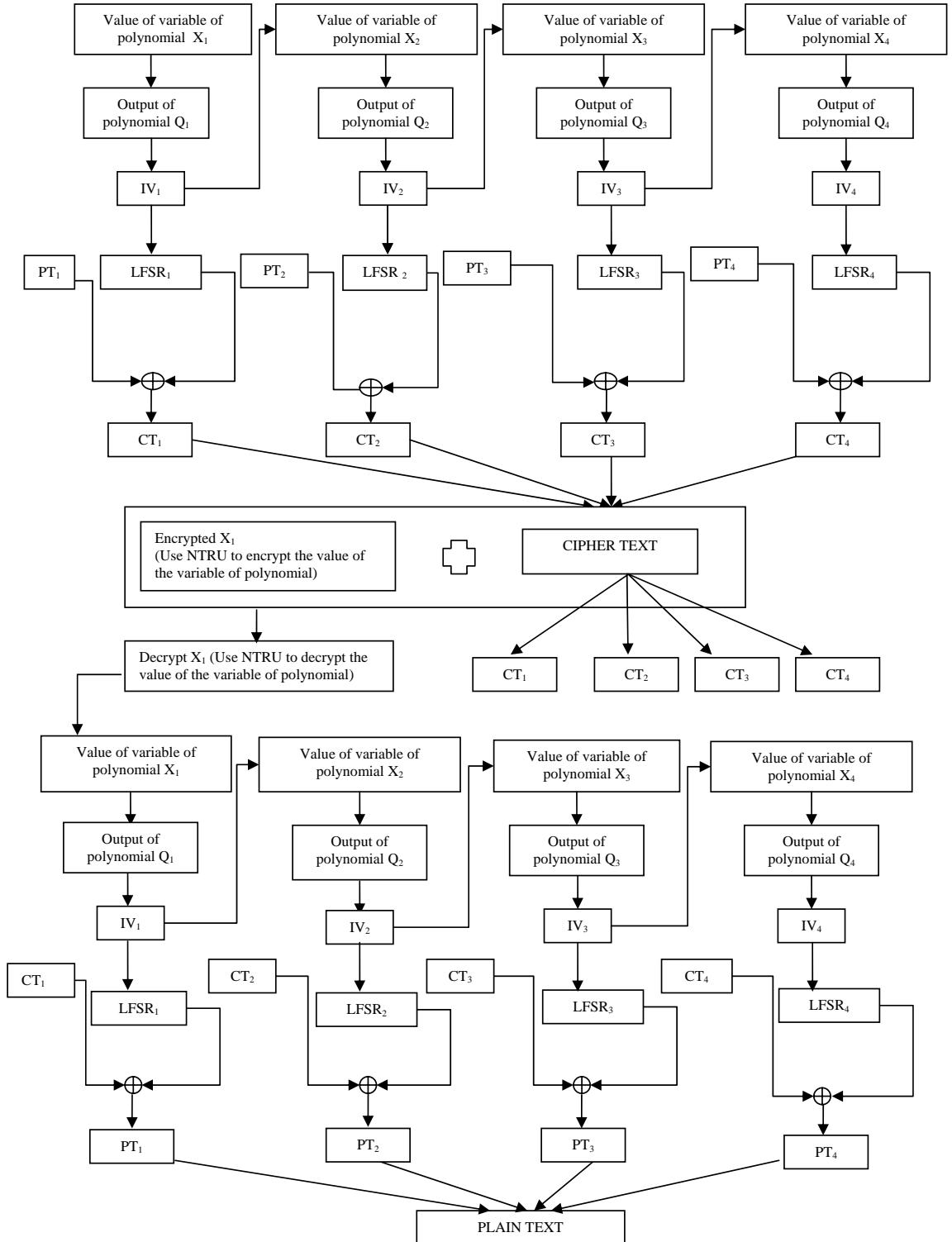


Figure2: Working scheme with four LFSRs and their IV generation

ADAPTIVE PACKET LOSS CONCEALMENT MECHANISM FOR WIRELESS VOICE OVER IP

M.Razvi Doomun
Faculty of Engineering
University of Mauritius
r.doomun@uom.ac.mu

Abstract— Various packet loss concealment (PLC) techniques exist for packet voice communication. A wireless VoIP simulation methodology is developed for analysing the tradeoff between PLC methods performance and complexity. We evaluate the quality of the reconstructed speech under different packet loss rates for various receiver-based recovery methods individually and propose an adaptive mechanism that can select the PLC method with the minimal complexity in accordance with different packet loss rates encountered. Simulation results have shown that the adaptive PLC scheme delivers acceptable speech quality across varying packet loss rates.

Keywords- *Voice over IP (VoIP); packet loss concealment; adaptive mechanism; speech quality.*

I. INTRODUCTION

With the wide availability and interest in mobile voice communications, particularly wireless technologies, it is necessary that Voice over IP (VoIP) services over wireless must provide at least similar, if not better, perceived voice quality at the user level than traditional wired VoIP. Compared with wired links, wireless channels are typically much more noisy and have both small-scale (multipath) and large-scale (shadowing) fades, making the Bit Error Rates (BER) very high. The resulting bit errors can have devastating effect on packet voice communication quality. Packet loss occurs because of congestion, interference and discarded packets arriving later than their scheduled playout times. As a real-time application, VoIP over wireless local area network (WLAN) is delay-sensitive but can tolerate a certain level of packet loss.

Different packet loss concealment (PLC) techniques have been proposed in research surveys [1][2]. These techniques are categorised as sender-based and receiver-based. They are primarily designed to improve the quality of reconstructed speech in the presence of packet loss, and to enable VoIP to be tolerable to higher packet loss rates. To achieve this objective, parameters that have to be taken into consideration are packet overhead, processing delays and computational complexity. Ideally, we aim to have an optimised system that can tolerate high packet loss rates with overhead, delay and complexity minimised.

The paper is organized as follows: In Section II, background and related work are discussed. Section III presents the adaptive PLC mechanism. In Section IV, we provide the

performance analysis and present graphical results and discussions, followed by conclusion remarks in Section V.

II. RELATED WORK

Concealment techniques at the receiver's side are insertion techniques that aim at padding the gap left by a lost packet with silence, the previous correctly received packet or Gaussian noise [3]. The lost packet can also be filled with a fill-in of zero length, so that there remains no gap caused by the lost packet. This technique is known as splicing which is a rather quick and easy way of solving the problem but leads to a disruption in the timing of the stream for the jitter buffer. The silence substitution method simply fills the lost packet with silence (i.e. zero) to maintain the speech timing sequence. The complexity is very low. The repetition method uses the correctly received packet preceding the lost packet as the substitution. Its complexity is same as that of silence substitution, but has better recovery performance than the silence substitution method. Other receiver-based techniques are interpolation techniques, subdivided into waveform substitution and pitch waveform replication and model-based recovery regeneration technique [2]. Waveform substitution works by examining audio patterns before and after the lost to find a suitable substitute whereas pitch waveform replication detects pitch on a sufficient length of speech samples kept in a history buffer. The concealment unit then places the pointer one pitch period backward and copies a speech signal with the duration of the lost packet. This pitch predicted replica is then played in the gap resulting from the missing speech segment. In model-based recovery the speech on one, or both, sides of the loss is fitted to a model in which the signal was originally created by and then used to recover from losses. A new approach, proposed by Barry Cheetham improves current error concealment strategies for voice over WLAN in converged enterprise networks by reducing the dependency on packet loss concealment [4]. As well as improving speech quality in situations where bit-errors are occurring, this approach is also intended to reduce power consumption and WLAN congestion by reducing the number of automatic packet retransmissions. Another technique called intra-flow loss recovery and control [5] is concerned with correcting the errors as the audio stream travels from the sender to the receiver. Within VoIP, this technique is known to increase the perceptual quality an end user experiences. Time-scale modification has been used for adaptive playout scheduling by scaling individual voice packets

which modifies the rate of the playout voice signal in packet voice communication [6]. It has also been used for packet loss concealment or delay concealment for internet voice applications [7].

III. ADAPTIVE PLC MECHANISMS

It is possible to reconstruct lost packets by dynamically changing the packet concealment techniques. Speech codecs for VoIP over WLAN would have to make trade-off between perceived quality, reconstruction delay and complexity. Clearly, different PLC methods involve different computational overhead. PLC algorithms having higher tolerance to packet loss, unavoidably incurs a larger computational cost. In view of this, one would like to adopt a proper recovery scheme in response to the packet loss rate, while attaining the required speech quality and minimizing the corresponding computational cost. Consequently, we deal with the development of the adaptive mechanism in this section. First, we analyse the reconstructed speech quality for various PLC methods under different packet loss rates (random loss and different burst loss), and compare the computational overhead (processing delay) among these methods. The burst loss length is determined by subtracting the sequence number of the previous lost packet from the sequence number of the current lost packet. Specifically, we propose an optimised system model to automatically recognise which recovery method should be used subject to a given packet loss rate, as shown in figure 1. According to the optimised system model, we are able to adaptively select the most adequate PLC technique that incurs the minimal computational overhead and possesses the required speech quality. Packet repetition, noise insertion, pitch replication and waveform substitution methods are used for the adaptive recovery mechanisms. The mechanism of this adaptive scheme can easily be modified to include other future PLC techniques suitable for the wireless VoIP application requirement.

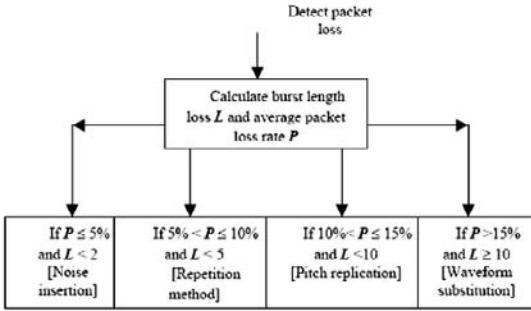


Figure 1. Adaptive PLC model.

IV. PERFORMANCE EVALUATION

The different PLC techniques were tested for several loss rates, ranging from 1% to 50%, and different burst lengths. The adaptive technique was also tested for the same loss rates. In particular, packet repetition, noise insertion, pitch replication and waveform substitution methods are used as the members of the adaptive packet loss recovery mechanism. In table I, the average PSNR results of 20 tests are given.

TABLE I. PSNR VALUES FOR ALL CONCEALMENT TECHNIQUES.

Packet loss rate /%	Packet Repetition /dB	Noise Insertion /dB	Pitch Replication /dB	Waveform Substitution /dB	Adaptive technique /dB
5	76.22	77.11	75.63	75.54	77.34
10	75.81	76.65	75.59	75.00	76.75
15	75.17	74.28	75.46	76.11	75.14
20	75.77	76.19	75.15	75.35	75.90
30	74.92	76.63	76.72	77.33	75.15
40	74.90	77.21	76.77	78.43	74.88
50	73.91	75.46	72.89	75.59	76.68

When the packet loss rate is below 5% and burst length is less than 2, the noise insertion method is applied to obtain acceptable speech quality, but white noise speech has to be generated. Between 5% and 10 % loss rate and burst length is less than 5, the repetition method is used to obtain acceptable speech quality, because of its low complexity, low delay and acceptable quality. The pitch replication method used when the packet loss rate is between 10% and 15% and burst length is less than 10. When the packet loss rate is above 15% and burst length is 10 or above, we use waveform substitution to attain the quality required.

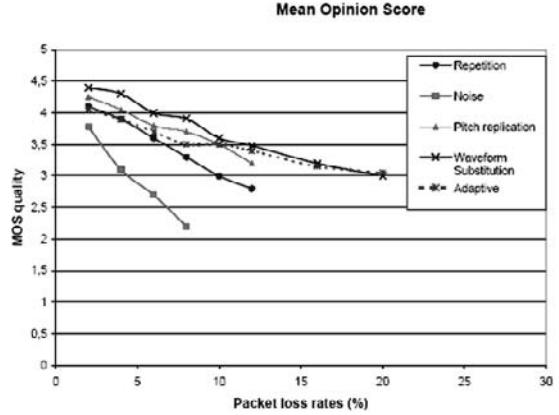


Figure 2. The MOS of PLC methods under different packet loss rates.

The subjective quality test scores under various packet loss rates for different recovery methods are shown in figure 2. Mean Opinion Score (MOS) is used as a measurement for listening test experiments.

V. CONCLUSIONS

VoIP via wireless LANs are expected to grow in importance over the next few years. The key challenge in handling voice traffic on a WLAN is that such service must be time-bounded with acceptable voice quality under lossy conditions. This can be achieved via the adaptive PLC mechanism. In this paper, we evaluated the quality of reconstructed speech using different PLC methods under different packet loss rates, and compared the computational complexity. According to our results, the adaptive PLC approach is an optimal compromise between desired speech quality and computational load. The PSNR and MOS values are more stable over packet loss rates up to 20 %. A good adaptive PLC mechanism can greatly improve the perceived quality with no bandwidth overhead.

REFERENCES

- [1] G. Carle and E.W. Biersack "Survey of Error Recovery Techniques for IP-Based Audio-Visual Multicast Applications," *IEEE Network*, vol. 11, no. 6, pp. 24–36, 1997.
- [2] C. Perkins, O. Hodson, and V. Hardman, "A Survey of Packet-Loss Recovery Techniques for Streaming Audio," *IEEE Network*, vol. 12, no. 5, pp. 40–48, 1998.
- [3] M. Hassan, A. Nayandoro, and M. Atiquzzaman, "Internet Telephony: Services, Technical Challenges, and Products," *IEEE Communications Magazine*, vol. 38, no. 4, pp. 96–103, 2000.
- [4] B. Cheetham B., "Error Concealment for Voice over WLAN in Converged Enterprise Networks", *15th IST Mobile & Wireless Communications Summit 2006*, Mykonos, 4-8 June 2006.
- [5] H. Sanneck, N. Long Lee., A. Wolisz and G. Carlie, "Intraflow Loss Recovery and Control for VoIP," *International Multimedia Conference archive Proceedings of the ninth ACM international conference on Multimedia*, Ottawa, Canada, 2001, pp. 441-454, 2001.
- [6] Y.J. Liang, N. Farber, and B. Girod, "Adaptive playout scheduling using time-scale modification in packet voice communications," *Proc. IEEE Int. Conf. on Acoustics, Speech, Signal Processing* (Utah, USA), May 2001.
- [7] Y.J. Liang, N. Farber, and B. Girod., "Adaptive playout scheduling and loss concealment for voice communications over IP networks," *IEEE Transactions on Multimedia*, Vol. 5, No. 4, pp 532-543, 2003.

Dynamic Location Privacy Mechanism in Location-Aware System

M. Razvi Doomun

Faculty of Engineering, University of Mauritius

r.doomun@uom.ac.mu

Abstract - Protecting location privacy is one of the most significant issues in location-based services because such position data include highly personal and sensitive information. An adversary can analyse location traces and try to detect patterns that can be matched to find user locations easily. In this paper, an efficient multilevel dynamic location privacy mechanism is proposed for location-aware services. A model of the knowledge of an attacker is applied to protect, anonymise and secure location information. It consists of a location prediction engine (LPE), based on modelling of user mobility pattern, for accurate future position predictions. The system frequently produces path crossing trajectories and pseudonyms exchanges between true users and dummies using the knowledge from the LPE. Level of privacy is flexible by setting the percentage of privacy and selecting sensitive or insensitive cells. Simulation experiments show that the proposed location privacy architecture dynamically protects location privacy of users. The LPE raises the level of intelligence within the privacy mechanism so that the system aggressively and effectively maintains location privacy without interrupting the service to the mobile user.

1. INTRODUCTION

Context-awareness is a key element for the development of adaptive applications in ubiquitous and mobile computing environments. However, access to context information introduces new vulnerabilities and exposures. Context information, especially location information of individuals, are very sensitive data, as it may be possible to extract information like routine activities, habits and preferences of tracked users from it. Thus, location privacy protection is a challenging task and there is still a lack of effective solutions to solve privacy problems in location-based services (LBS).

In general, LBS provide users with context-aware services related to user's location information. From the perspective of service providers, it is desirable to retrieve the target's position with low error using highly accurate positioning devices to improve their quality of service. On the other hand, users do not want to expose critical location information in order to have complete personal control of their location privacy. In fact, continuous location-based applications worsen privacy problems since individual's desired levels of privacy can be spatial and temporal dependent [1]. Moreover, the requirements for privacy depend on the application, but different users, e.g. normal person or celebrity, may want different privacy levels for

the same application.

Traditional security mechanisms and policies are generally static and context insensitive, which may not provide adequate guarantees to deal with the dynamicity of context-aware environment. Thus, there is a need to have real-time, flexible, customizable and adaptive security and privacy mechanisms to protect the location privacy of individuals in a dynamic way. This also includes different levels of security services based on system policy, context information, user preferences and quality of service. In addition, security and privacy mechanisms have to be scalable to support huge number of heterogeneous users, in terms of roles, privileges and location-based services.

In this paper, we study the problem of designing privacy-aware LBS and propose an efficient dynamic location privacy architecture. In particular the paper uses a hybrid approach using location prediction to model the adversary and adjust the overall privacy mechanism. The rest of the paper is as follows. In section II, we review related work. In section III, we describe privacy features and metrics. We present the detail dynamic privacy mechanism in section IV and then we evaluate simulation results. Finally, we assess the privacy level and conclude the paper.

II. RELATED WORK

In this section, existing related works on privacy in location-aware systems are discussed and the major privacy enhancing techniques available for protecting sensitive mobile location information are analysed. Recently, quite a few papers have been published to tackle the new security and privacy challenges in ubiquitous and pervasive computing environments [10] [2] [12] [13] [14]. However, none of them offer satisfactory privacy level without restricting the functionality and quality of the system.

In *pawS* system [2], the author focuses on implementing certain features of privacy awareness system by specifying privacy policies and data usage policies. It assumes trustworthiness in data collectors and sensors, and provides guidelines for users to keep track on how their sensitive data is stored, used and processed by the system through accountability. Another concept of personal location privacy policy, presented by Snekkenes [18], is that an individual has the power to adjust the accuracy of

his location, identity, time and speed depending on parameters such as the intended use of data and the recipient. The key idea is to degrade location information in a controlled way before releasing it. By reducing the spatial or temporal accuracy of the location data, the quality of the data is reduced for attackers as well as for the applications. However, the privacy protection level is relatively low even when choosing lower resolution data, and the method is not applicable for services which continuously need more accurate data. A similar 'position accuracy reduction' approach is proposed in [4] where a user's position data is sent with modification to service provider. The latter can only obtain vague details of the position of a user. The main problem is that low accuracy of position data causes low service quality. Moreover, another drawback is that an adversary can easily observe and figure out user displacements because the sequence of position data creates a rough trajectory.

The anonymisation of location information method [1] is suitable for the class of location-aware applications that accept pseudonyms. An anonymising proxy enables applications to communicate to pseudonymous messages from users. In this case, the middleware sensing infrastructure is assumed trusted and might help users conceal their identity. However, using long-term pseudonym for each user does not provide guaranteed privacy. So, the infrastructure delays and reorders messages within Mix Zones [5] to confuse an observer to provide a level of anonymity. The mix zone concept, tested using data from the Active Bat system [1][5], showed that even when relatively large mix zones were used, the privacy of users remained low. This system is exposed to statistical attacks; there must be enough users within the mix zone to enhance location privacy. If there is only one user, this user is fully exposed. The number of location updates and the predictability of user movements are also important.

Another proposed architecture, called Mist, that uses anonymizing techniques is described in [10]. Its main feature is to provide anonymous communication by setting a hierarchy of routers and using hop-by-hop routing to preserve privacy and hide information about original source and final destination. This is an ad hoc model for privacy preserving. Reference [6] described linking of trajectories, which infers a user's path from several individual location samples of users. Path confusion [7] is an algorithm that improves user's location privacy. The key idea of the algorithm is to exploit the proximity or meeting of two users' paths and confuse the tracks in such regions. Another technique for privacy protection is to mix the real correct location data with a certain proportion of virtual dummy data [16] so that attackers are unable to distinguish between them. A similar approach, known as trusted location cloaking proxy, provides anonymity by controlling the resolution of the location information reported to services based on the density of users in an area [3]. The proxy runs a cloaking algorithm that selects the smallest of a set of areas that includes the user and at least $k-l$ other users. So, a distrusted service receives location data of a user with $k-$

anonymity within a region that also contains $k-l$ other users. It cannot easily map the reported location back to an individual user.

An approach that appears promising for implementing privacy is location-based encryption [17]. The location position provider encrypts its information with location-dependent encryption keys and makes the encrypted information publicly available in a distributed way. Decryption keys are exchanged with users based on their current location. This scheme protects location privacy based on the assumption that a location position provider is unlikely to track all requests to the nodes that keep the distributed database. However, this approach has the usual limitations associated with the deployment of encryption-based access control. First, the decryption keys (and thus potentially the encryption keys) should expire to avoid that obtained keys can be used after moving away from a location. Second, the encryption scheme should be aware of location hierarchies. Third, the access-control scheme fails when customers expose decryption keys, which is difficult to avoid since these keys typically have no value for a customer. Fourth, the entity issuing the decryption keys has access to all the information.

Hence, the design requirements that need to be addressed for privacy in location-aware systems are total anonymity, decoupling identity and location, customizable privacy and cost effective. With respect to LBS, this means that neither a user's identity nor location can be inferred and decoupling one's identity from one's location information provides the user with a better level of privacy. In addition, it is necessary to have a system of relative privacy that allows a user to choose the level of desired privacy, which is derived from the user's interactions with the environment and the amount of personalization a user desires.

III. PROTECTING LOCATION PRIVACY

A. Privacy Attributes and Metrics

The level of location privacy of users in location-aware applications is determined by a number of factors. The identity of the owner of the location data can be an explicit identifier or a pseudonym. The latter prevents the location-aware application from linking the location data with the real-world entity. Access to location information can be controlled based on physical area. Users can restrict collection of their information to specified geographic areas, for example tracking location while only on public streets but not inside buildings. The access to location information can be limited for specific time periods also. Users can associate time bounds with preferences and impose constraints such as accessing location data during working hours only. Limiting the rate of location queries per hour minimizes the risk of pervasive tracking of all user displacements. In fact, mutual exchange of authenticated location information and notification between requester and user ensure trusted usage. Lower location resolution by spatial accuracy modification

conceals personal knowledge of user actions. Similarly, lower temporal accuracy is used to delay communication of location information in order to reduce its value when location event has already occurred. Both spatial and temporal accuracy reduction improves overall motion privacy of users.

To analyze the level of anonymity achieved, anonymity metric based on entropy proposed in [19] will be used. Two metrics commonly used for measuring location privacy are: entropy and anonymity sets. The anonymity of a system is defined as the amount of information an untrusted party or an attacker is missing to uniquely identify an actor's link to an action, e.g. uniquely identify the user or the displacement of the user. The anonymity set is the subset of \mathbf{S} that contains exactly those who could have possibly initiated the event observed by the attacker. Consider X be a discrete random variable with probability function $P_i = P_r(X=i)$, where i represents each possible value that X can take. So, X represents the pseudonym/user location under the attacker's scrutiny, and each i corresponds to an element (a user) of the anonymity set S . For each user belonging to the anonymity set S of size N , an attacker assigns a probability P_i , and the entropy $H(X)$ is given as

$$H(X) = - \sum_i P_i \log_2 P_i \quad (1)$$

Where, in the case of location privacy, the P_i describes the adversaries' probabilities for different assignments of user identity to the observed positions and N indicates the total number of such assignment hypothesis. Thus, the pseudonym/user's location maximum entropy [1] is

$$H_{max} = \log_2 N \quad (2)$$

The degree of anonymity d , is computed as

$$d = H(X) / H_{max}, \quad (3)$$

which quantifies the amount of information leakage by privacy-protection system for a given pseudonym location [1]. The higher the entropy, the more uncertain an adversary will be about the true location, and hence the higher will be the anonymity. The obvious way of increasing the entropy, $H(X)$, is to obtain lower probabilities, P_i , i.e. lower probability of distinguishing a user from a dummy. From the adversary's perspective, a path is a collection of location/time pairs that a single user has visited. More precisely, the path will contain all data from a user if the user always communicates under the same pseudonym with the service provider. When a user changes his pseudonym, the following location information appears as a different path to the adversary. In the extreme case where the user transmits every location/time pair separately and anonymously, paths will comprise of only a single point.

B. Location Prediction

Previous work in the field of mobility prediction includes the method in [10], which suggests that the mobile's

location may be determined based on its quasi-deterministic mobility behaviour represented by a set of movement patterns stored in the user profile or based on historical trajectories. In other words, it is possible to predict location of a moving object at a certain future time. In [11], an improved hierarchical location prediction algorithm is proposed for predicting the future location and speed of mobiles. Classical stochastic signal processing techniques are applied to extract user mobility by approximate pattern matching algorithm and extended self-learning Kalman filter. Location prediction is based on the belief that, at a global level, a user's mobility pattern is fairly regular and can be approximated based on past storage pattern of his movements. Hence, user mobility pattern prediction is used as a key feedback to prevent location privacy degradation in the proposed dynamic privacy mechanism.

Strong anonymity requires that a larger group of potential service users travel along the same path at the same time. But it is unlikely that many users simultaneously travel the same path. The adversary can often concatenate multiple path segments (assuming changing pseudonyms) into a longer path because most user's movements are relative predictable in small areas - they typically follow streets and often move at known speeds, e.g. walking speed or near the road speed limit. However, when the paths of multiple users meet and cross, linking segments become more difficult. On the other hand, an adversary's certainty is higher when precise position and time information is available in areas with low user density. Thus, privacy parameters must be chosen with care and adapted to the current situation.

IV. DYNAMIC PRIVACY MECHANISM

Our challenge is to provide a dynamic location privacy model that varies in the degree of restrictiveness but can be customized according to users' needs. Strong dynamic privacy protection should as far as possible maintain availability of accurate location information in all areas visited (sensitive/private or insensitive/public) in order not to degrade the quality of service. Since users request for location-aware applications, they generally do not wish to block all their location information and also do not accept poor quality of service.

A. Overall System Architecture

The dynamic privacy system model assumes that a trustworthy infrastructure exists and users can request the level of desired privacy. Figure 1 shows the relationship between entities of the general infrastructure model to support location privacy. Untrusted 3rd party and service provider request the location communication system (LCS) to retrieve location details. The LCS captures the position data, processes it and returns the location details to the service provider. The LCS is assumed trusted by users. However, users may not be prepared to trust location based service providers. In the architecture

described, the service provider acts as a man-in-the-middle between the LCS and the users with mobile devices.

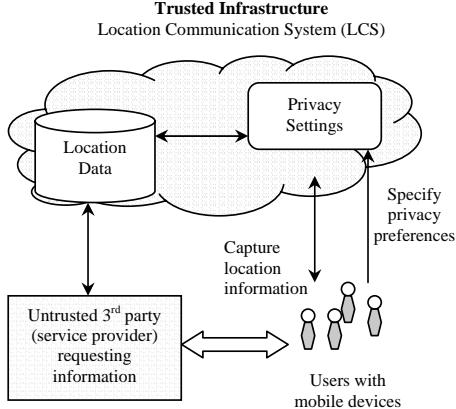


Figure 1. Overall location-based privacy system infrastructure.

We use a cellular grid that each user can categorize as sensitive and insensitive geographic areas, as shown in figure 3. Cells containing largely well-frequented public areas, such as markets and streets will normally be classified as insensitive and other areas with private buildings or residences can be tagged as sensitive cells. Each user can dynamically set the cells either sensitive or insensitive based on his daily privacy requirements.

Mix-zones on-demand, for example temporarily disables the use of the service for a number of users in the same cell area for the time sufficient to confuse the service provider. Given a specific point in space, k diverging trajectories are required (each one for a different user/dummy) that are sufficiently close to the point. The “diverging” feature captures the intuitive idea that these users/dummies, once out of the mix-zone, will take very different trajectories. Unlinking is performed by changing the pseudonyms/identifiers of the users/dummies, possibly doing it when they cross a sensitive cell in order for the service provider not to be able of binding the different pseudonyms to the same ‘user’. This prevents attackers from utilizing the predictability of user movement to correlate user locations before and after position updates. The exchange or update of pseudonyms/identifiers is performed by the system when users/dummies traverse cell areas of different sensitivities and when a change in user/dummies velocity occurs in the proximity.

B. Modeling Realistic Collaborative Dummy

The system architecture proposed is shown in figure 2. Strongly inspired by [15] [16], we improve the use of ‘pseudo-real’ collaborative dummy users to increase location privacy by controlling their motion. The displacement of each user in a fixed time is limited by speed and direction. Generally, moving users may have some degree of

regularity in their motion, e.g. home-office-home pattern. The mobility of a user is a combination of regular and random movement patterns. The privacy-protection system predicts each moving user’s location at future time on the basis of past motion patterns recorded using past location information. This deliberate location estimation, say L_j , is compared with the real user location information, L_k , to measure the level of uncertainty. If any partial user motion pattern or periodic pattern is detected within or between cell zones, then higher numbers of dummy users are generated with realistic synchronized movements to confuse attackers from finding the true position data or motion path. As shown in figure 3, the target user C has three neighbour dummies A, B and D with path crossing trajectories. After path crossing points, the user and dummies swap their pseudonyms identifiers with a probability 0.5 to maximize the anonymity set size.

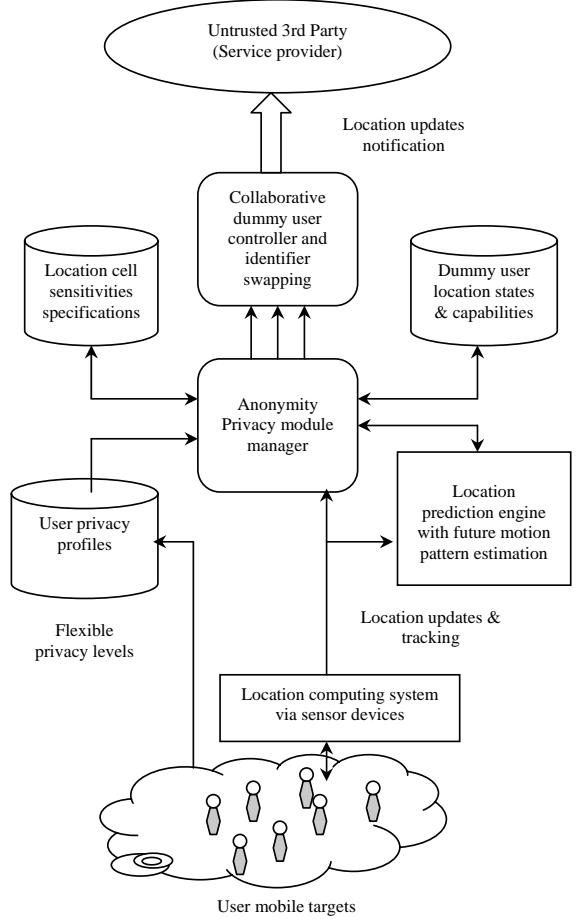


Figure 2. Dynamic location privacy with location prediction engine.

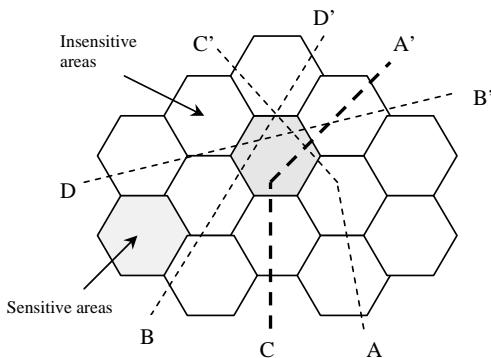


Figure 3. Sensitivity areas and exchanging pseudonyms.

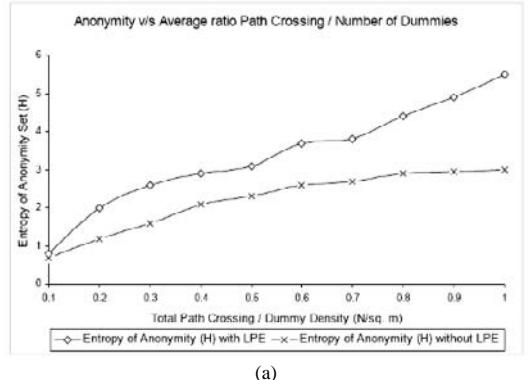
The well-known extended Kalman filter (EKF) [8][9] is used with state vector of six components, three position components (x, y, z) and three velocity components (v_x, v_y, v_z), for the location-mobility prediction engine. The EKF uses the most recent location samples and its internal state to predict an estimate of the location where the user might be in the next time-step. When the real next distance sample is obtained, the EKF first corrects its internal state based on the difference between the actual displacement and the forecasted one. The prediction and correction loop runs continuously as the location prediction engine receives more location samples.

C. LPE and Dummy Controller

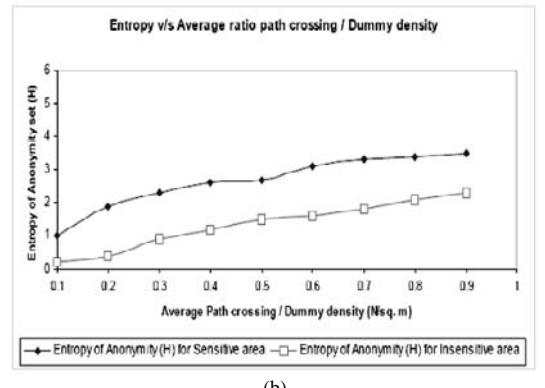
The technique we use to prevent observers or service providers from tracing a location is to perform path crossing between a user's trajectory and dummies' trajectories. We also assume that a service provider cannot distinguish a user from a dummy. The dynamic location privacy system, shown in figure 2, generates collaborative dummies moving in different valid directions based on feedback and motion control from location prediction engine (LPE) so that there are frequent path crossings to decrease user's location traceability. Each user motion behaviour is masked by a variable number of dummies that depends on sensitivity area defined by each user. If a user is in an insensitive/public area, a variable number of dummies are generated from 1 to a maximum of 5 and in other sensitive areas, a trade-off maximum of 10 dummies are produced. Furthermore, LPE gathers the positioning data history of each user to emulate attackers by making inferences about user location traceability. This enables dynamic monitoring of the privacy levels. In case, the privacy level falls below a threshold after a length of time, additional optional measures can be implemented and activated, such as temporal and spatial cloaking. This will imply suspending the location-aware application if the level of privacy degrades below a critical threshold.

V. SIMULATION RESULTS

Figure 4(a) compares the entropy provided by the dynamic location privacy mechanism using location prediction engine (LPE) and also without LPE. As illustrated, LPE provides very high level of privacy and as expected more realistic path crossings and dummy density enhances the privacy level.



(a)



(b)

Figure 4. Privacy performance (a) comparing with and without LPE. (b) Comparing within and outside sensitive area.

Every time a true user and any dummy user's paths meet, there is a chance for the adversary to confuse the tracks and follow the wrong user. In sensitive areas, the entropy values are larger, since the dynamic privacy mechanism consists of more path confusing dummies controlled by the anonymity privacy module manager and. frequent probabilistic swapping of pseudonym identifiers. As shown in figure 4(b), this naturally explains better performance compared with insensitive areas where the privacy requirements are less strict.

VI. PRIVACY LEVEL ANALYSIS

In this section, we evaluate how collaborative dummy generation with path crossing improves location privacy by comparing location anonymity with the number of collaborative dummies across sensitive and insensitive areas. The simulation results show that dynamic location privacy system performs better than traditional static dummy generation algorithm, and it has the capability to react when the measured anonymity is falling below a certain threshold. The local location prediction engine automatically identifies user mobility patterns to enable the anonymity module to control the movement and number of collaborative dummy users within a sensitive or insensitive region. Adequate level of privacy can be obtained if user density is sufficiently high. In low user density environment, the system will increase the number of dummy users and the frequency crossing paths. If it is known that few crossing segments exist in the original paths, an adversary could assume that all crossing segments have been artificially inserted. Privacy may be further compromised through advanced tracking algorithms that reject unlikely location samples. Hence, variable number collaborative dummy users and pseudonym identifiers swapping address these problems through increased realistic path confusion.

The main complication is that the genuine service provider has to deal with dummies and real users, hence the need to reply them all. The computation overhead and cost increase with large number of dummies to handle, become significant. One approach to reduce communication cost is to form cluster of dummies and users within privacy cells. Clustering saves processing time and communication cost without affecting location privacy. Finally, the propose dynamic privacy method seek to effectively protect not only the identity of visited location, but also the duration of stay in and the frequency of visits to both sensitive and insensitive regions.

VII. CONCLUSION

In wireless sensor environments with extensive use of “invisible” computing devices gathering identities, collecting locations and transaction information of users, handling user privacy is a challenging task. In this paper, we refined the anonymous communication technique and proposed a dynamic location privacy model. The scheme integrates four important elements; real dummy user behaviour, motion pattern tracking and modelling, path crossing trajectories with identifier swapping and flexible privacy level. The issue of location privacy in location-aware systems is addressed by generating variable number of dummies with realistic movement patterns having path-crossing trajectories. A user location prediction feedback based on mobility pattern is used to produce frequent valid user-dummies path crossing events, which give improved location privacy. Users have the flexibility to configure their privacy level preferences by specifying different cells as sensitive/private or insensitive/public areas. Location privacy, like security, is a multifaceted problem. In future

work, more accurate model of the knowledge of an attacker needs to be designed, with extensive historical location and movement data, to remove subtle mobility clues, thus providing higher assurance of privacy.

REFERENCES

- [1] A.R. Beresford and F. Stajano F. "Location privacy in pervasive computing," *IEEE Pervasive Computing*, vol 2, pp. 46-55, 2003.
- [2] M Langheinrich , "A Privacy awareness system for ubiquitous computing environments" UbiComp 2002, Springer Verlag, LNCS 2498, pp.237-245, 2002.
- [3] Schilit, Bill, Hong, Jason and Gruteser Marco. "Wireless location privacy protection," *Invisible Computing*, December 2003. pp. 135-137. 2003.
- [4] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proc. of the 1st International Conference on Mobile Systems, Applications and Services*, pp. 31-42,2003.
- [5] A.R. Beresford and F. Stajano. "Mix Zones: User privacy in location aware services," in *Proc. of 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshop*, pp. 127-131, 2004.
- [6] M. Gruteser and B. Hoh, "On the anonymity of periodic location samples," in *Proc. of 2nd International Conference on Security in Pervasive Computing*, pp. 179-192, 2005.
- [7] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion" in *Proc. of IEEEICreateNet International Conference on Security and Privacy for Emerging Areas in Communications Networks (SecureComm)*. 2005.
- [8] P. Pathirana, A Savkin and S. Jha, "Mobility modeling and trajectory prediction for cellular networks with mobile base stations," *MobiHoc 03*, 2003.
- [9] I.R. Petersen, A Savkin, "Robust Kalman filtering for signals and systems with large uncertainties" *Springer Verlag*, 1999.
- [10] J. Al-Muhtadi, Kapadia R., Mickunas A, Seung Yi, "Routing through Mist: Privacy preserving communication in ubiquitous computing environments," in *International Conference of Distributed Computing Systems (IDCS 2002)*, pp. 65-74,2002.
- [11] T Lui, P Bahl and I Chlarntac, "Mobility modelling, location tracking, and trajectory prediction in wireless ATM networks", *IEEE Journal on Selected Areas in Communications*, vol 16, August 1 1998.
- [12] J. Al-Muhtadi, A. Ranganathan, R. Campbell and M. Mickunas, "A flexible, privacy preserving authentication framework for ubiquitous computing environments", *ICDS Workshops 2002*; pp.771-776, 2002.
- [13] Q. He et al. "The Quest for personal control over mobile location privacy", *IEEE Communications Magazine*, pp.130-136, May 2004.
- [14] M. Wu and A. Friday, "Integrating Privacy enhancing services in ubiquitous computing environments", *Workshop on security in Ubiquitous Computing, 4th International UbiComp*, 2002
- [15] B. Hoh and M. Gruteser "Protecting Location Privacy Through Path Confusion" *First IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm)*, pp.194-205, 2005
- [16] H. Kido, Y. Yanagisawa and T. Satoh, "An Anonymous Communication Technique using Dummies for Location-based Services". *IEEE International Conference on Pervasive Services 2005 (ICPS'05) 11-14 July 2005*
- [17] J. Al-Muhtadi, R. Hill, R. Campbell, and D. Mickunas. "Context and Location-Aware Encryption for Pervasive Computing Environments". In *Proceedings of Third IEEE International Workshop on Pervasive Computing and Communications Security (PerSec 2006)*, pages 283-288, March 2006.
- [18] E. Snekkenes. "Concepts for Personal Location Privacy Policies". In *Proceedings of the 3rd ACM Conference on Electronic Commerce*, pages 48-57. ACM Press, 2001.
- [19] A. Serjantov and G. Danezis. "Towards an information theoretic metric for anonymity". In *Privacy Enhancing Technologies (PET)*, 2002.

Video Transmission Performance Using Bluetooth Technology

M. Razvi Doomun

Faculty of Engineering
University of Mauritius
r.doomun@uom.ac.mu

Abstract— Bluetooth is increasingly being used in the role of "last meter" technology for indoor wireless universal coverage. In such scenario, ad-hoc Bluetooth networks provide simple and cost-effective intercommunication of various mobile devices, and are now targeted to support multimedia traffic. However, the transmission of video over Bluetooth is a challenging problem, partly due to error and interference conditions. This paper examines the performance of Bluetooth protocol to carry streaming video in real experimental test scenarios. The impact of interference, obstruction and transmission distance on the performance of video streaming over Bluetooth link are investigated. Analysis and suggestions of how the performance of the streaming can be enhanced are discussed.

Keywords— *Bluetooth; Video transmission; Distance, Interference; Obstruction.*

I. INTRODUCTION

Bluetooth is a short-range wireless technology, which facilitates data transmission and personal communication. It provides a feasible and promising platform for low-power and low-cost multimedia applications, allowing the replacement of cables and infrared links and connecting such devices through RF links [1]. Bluetooth enabled devices operate in the Industrial Scientific Medicine (ISM) frequency band of 2.4 GHz. With its frequency hopping techniques, the radio transmission is theoretically designed to be immune to interferences in the above frequency band, attaining a maximum of 1 Mbps within operating range. Bluetooth carries communication traffic over two types of air interface links defined as Asynchronous Connection-Less (ACL) and Synchronous Connection Oriented (SCO) [2]. ACL links support symmetric and asymmetric packet-switched connections and can achieve a maximum data rate of 721 kbps. SCO links support symmetrical, circuit-switched, point-to-point connections and are therefore suitable for time-bound data transmissions. Each SCO link provides a maximum of 64 kbps data rate and there can be up to three concurrent SCO links.

A current challenge for video distribution over a wireless link, using Bluetooth-enabled devices, is the high degree of variability in the radio signal strength, meaning unreliable connections between devices. This work examines the performance of streaming video over Bluetooth using realistic experimental test scenarios. The impacts of interference,

obstruction and transmission distance on the performance of video streaming over Bluetooth link are investigated. The paper structure is as follows: Section II presents background study and related work. Section III describes the test scenarios and results obtained. Finally, section IV and V give the discussion and conclusions, respectively.

II. BACKGROUND STUDY

Bluetooth and IEEE 802.11 WLAN (also known as Wi-Fi), all share the 2.4 GHz portion of the ISM band. Bluetooth employs FHSS (Frequency Hopping Spread Spectrum) to avoid interference, where data is transmitted on a frequency that is regularly changed to another frequency in a pseudo-random pattern known to both transmitter and receiver. There are usually 79 hopping frequencies, each having a bandwidth of 1MHz. The simultaneous operation of Bluetooth and 802.11 in close proximity leads to degradation in the performance of both systems. A Wi-Fi channel is typically 17 MHz wide and is located within the 79 frequencies that Bluetooth uses. Hence, in theory 22% of the 79 frequencies used will overlap and all Bluetooth packets sent on the overlapping frequencies are subject to interference. However, the degree of interference depends on the signal to noise ratio at the receiving device. The signal strength also depends on the distance between the transmitter and receiver, the transmission power and the geography of the environment. Similarly, the noise level depends on the interferer's transmit power and distance from the affected receiver. To determine the extent of the interference problem, there has been a substantial amount of research into the coexistence of different wireless technologies in the 2.4 GHz band. However, this work focuses on real test scenarios to measure the true effects of interference on a Bluetooth link.

In the literature [3], the performance of Bluetooth in the presence of WLAN interference has been presented based on the probability of packet collision in frequency and time overlap at the Bluetooth receiver. Kamerman [4] reports on tolerable interference levels between the Bluetooth and 802.11 devices for various scenarios and device dispositions at various floor locations. The probability of an 802.11 packet error in the presence of a Bluetooth piconet has been derived by Zyren [5] and extended by Shellhammer [6].

III. PERFORMANCE TESTS

The components of the experiment are shown in figure 1. The system architecture is based on simple client-server application, using Bluetooth and multimedia support in the Nokia Series 60 Developer Platform 2.0. H.263 video is the mandatory format in 3GPP, designed for low bit-rate communication.

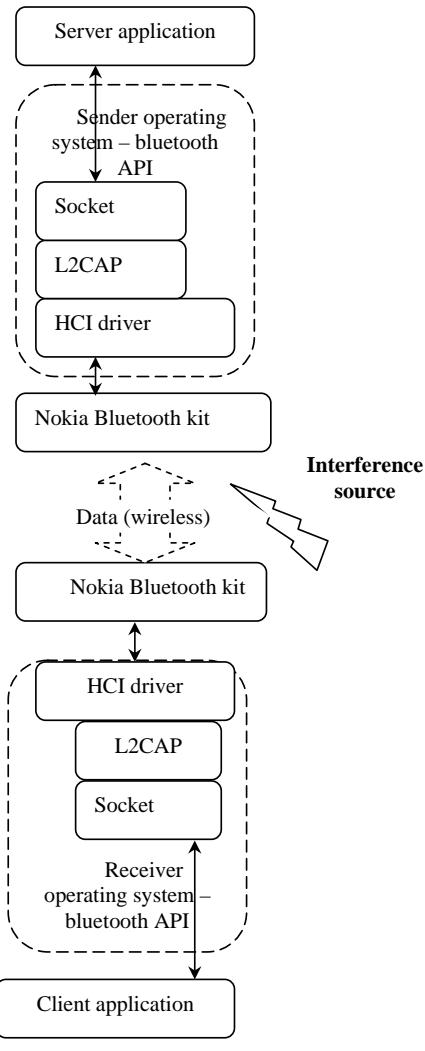


Figure 1. Interference test environment

Logical link and Control Adaptation Protocol (L2CAP) supports ACL links with packet size up to 64 Kbytes and serves as a media access control layer. Host Controller

Interface (HCI) provides uniform interface method to access hardware capabilities. A number of test scenarios are considered, as shown in table I.

TABLE I. VIDEO TRANSMISSION SCENARIO VIA BLUETOOTH LINK.

Bluetooth enable-device	Experiment Scenario
A. Mobile to Mobile	No obstruction, No interference
B. Mobile to Laptop	concrete wall obstruction
C. Mobile to Laptop	metal sheet obstruction
D. Mobile to Laptop	Wi-Fi interference
E. Mobile to Laptop	Bluetooth interference
F. Mobile to Laptop	IrDA interference

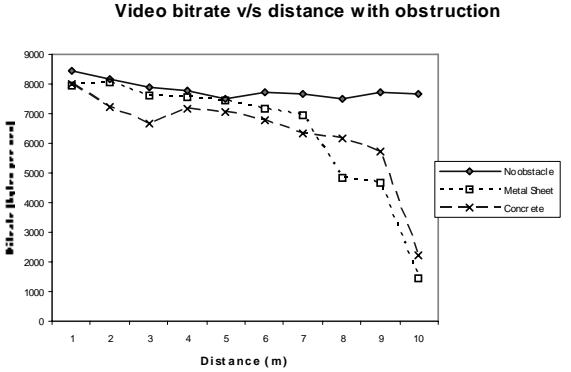


Figure 2. Performance comparison of video transmission with obstruction.

The experimental test results, in figure 2, show that over 0-10 m range, the bitrate is relatively stable when having line of sight. A slight decrease in bitrate is noticed as higher than 10 m distances, but it is not enough to affect the performance of video streaming. In the different obstruction test scenarios it is noted that the bandwidth falls drastically below acceptable level and all communications are disconnected at 10 m. Bluetooth communication degrades when the receiver is moving further away.

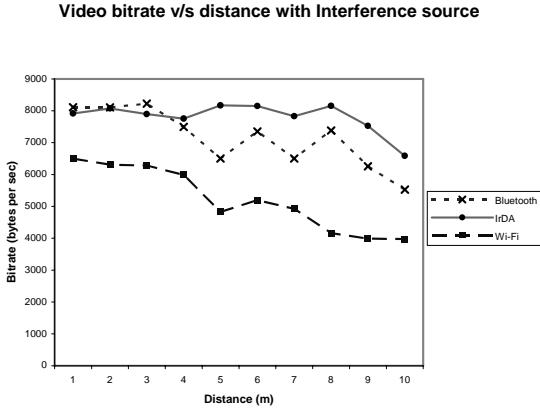


Figure 3 Performance comparison of video transmission with interference.

In interference test results, figure 3, the presence of other Bluetooth or 802.11 transmissions affect the Bluetooth piconet. With the Wi-Fi interfering source, there is an average bitrate reduction of 25-35%. With Bluetooth interference in the proximity, a decrease in bitrate of about 15-20% is observed over the whole range. However, as expected IrDA does not have any effect on the Bluetooth link, by the fact the infrared technology is clearly distinct from the ISM range.

IV. DISCUSSION

In an office environment, high Wi-Fi density with extensive use of wireless LAN channels in the same area will increase the number of frequencies that are shared with Bluetooth and may cause considerable interference. If one busy Wi-Fi channel reduces the bitrate throughput in practice up to 30%, it is possible that simultaneous use of multiple channels will prevent Bluetooth from functioning at all. The lowest performance results came from the adverse effect observed when the Wi-Fi interferer came within half a meter of the receiving Bluetooth device, the sender could not connect at all. This raises the question of whether certain critical functions in everyday life should rely on Bluetooth for their operation.

Collaborative schemes are mechanisms to enhance performance and they are based on a MAC time domain solution that alternates the transmission of Bluetooth and

WLAN packets [7]. A priority of access is given to Bluetooth for transmitting voice packets, while WLAN is given priority for transmitting data. Non-collaborative mechanisms range from adaptive frequency hopping to packet scheduling and traffic control [8]. Adaptive frequency hopping changes the Bluetooth hopping pattern and can reduce the packet loss and the impact of interference.

V. CONCLUSIONS

In this paper, experimental scenarios were tested to investigate video transfer performance over Bluetooth with obstruction or interference sources. The results obtained, when measuring video throughput while using Wi-Fi interference source, were found to be substantially worse than that in theory, i.e. above 22 % degradation. This is due to out-of-band noise that can be generated by interfering equipments. The accuracy of any results of theoretical analysis and simulation depend on assumptions, whereas the experimental measurements depend on the equipments and test environment.

REFERENCES

- [1] A. Iyer and U.B. Desai U.B, "A comparative study of video transfer over Bluetooth and 802.11 wireless MAC", *IEEE*, pp. 2053-2057. 2003.
- [2] E. Ferro and F. Potorti , "Bluetooth and Wi-Fi wireless protocols: A survey and a comparison," *IEEE Wireless Communications*, pp. 12-26, 2005.
- [3] N. Gomlie and F. Mouveaux, "Interference in the 2.4 GHz ISM band: Impact on the Bluetooth access control performance," in *Proceedings of IEEE ICC'01*, Helsinki, Finland. 2001.
- [4] A. Kamerman, "Coexistence between Bluetooth and IEEE 802.11 CCK solutions to avoid mutual interference," *IEEE 802.11-00/162, Lucent Technologies*, 2000.
- [5] J. Zyren, "Reliability of IEEE 802.11 WLANs in presence of Bluetooth radios," in *IEEE P802.11 Working Group Contribution*, IEEE P802.15-99/073r0, Santa Rosa, California, 1999.
- [6] Shellhammer, "Packet error rate of an IEEE 802.11 WLAN in the presence of Bluetooth," in *IEEE P802.15 Working Group Contribution*, IEEE P802.15-00/133r0, Seattle, Washington, 2000.
- [7] J.Lansford, R. Nevo, E. Zehavi, "MEHTA : A method for coexistence between co-located 802.11b and Bluetooth systems", *IEEE P802.15 Working Group Contribution*, IEEE P802.15-00/360r0, 2002.
- [8] N. Gomlie and N. Chevrollier, "Techniques to improve Bluetooth performance in interference environment," in *Proceedings of MILCOM'01*, McLean, Virginia, 2001.

Kelvin Effect, Mean Curvatures and Load Impedance in Surface Induction Hardening: An Analytical Approach including Magnetic Losses

Roberto Suárez-Ántola

Department of Electrical Engineering, Catholic University of Uruguay.

8 de Octubre 2738, Montevideo 11600, Uruguay.

Abstract-- Kelvin effect (Skin effect) is used in surface hardening produced by induction heating of gears, cam forms, camshafts and other work pieces of fairly complex geometries. The induction heating equipment for surface hardening of metals and alloys using LF (medium frequencies in the jargon of induction heating) is composed by a coil or coil assembly and a power semiconductor driving system up to 50 kHz. The load seen by the driving system is equivalent to a transformer. The primary corresponds to the excitation coil or coil assembly, and the work piece corresponds to a short-circuited secondary. In these and others technical applications of Kelvin effect it is often necessary to be able to relate local skin depths with local curvatures of the surface of electrically conductive bodies. It was proposed recently a closed form analytical formula that relates the local skin depth with the local mean curvature and the well known skin depth for a flat conductive but non ferromagnetic body. The purpose of this paper is threefold. First, improve and give a critical discussion of the derivation of the aforementioned analytical formula. Second, generalize it to bodies with magnetic hysteresis losses. Third, apply the above mentioned generalized formula to describe the electrical load seen by the driving system in the conditions used for surface hardening. The formulas given here could be applied to assess some characteristics of the load that may be of interest in the choice or design of the driving system, including the planning of digital simulations using complex computer codes.

Index Terms--Induction heating, Load impedance modeling, Skin effect, Mean curvature, Hysteresis losses.

I. INTRODUCTION

Induction heating is a non-contact heating method. An electrically conductive work piece is located in an alternating magnetic field of a coil or coil assembly. By electromagnetic induction, the external field produces eddy - currents in the material, which is heated as a result of Joule effect. If the material is non-ferromagnetic, this is the only heating effect. If it is ferromagnetic, there is another heating effect due to magnetic

hysteresis, albeit it is usually of less importance. Figure 1 shows an idealized representation of a work piece inside an induction coil.

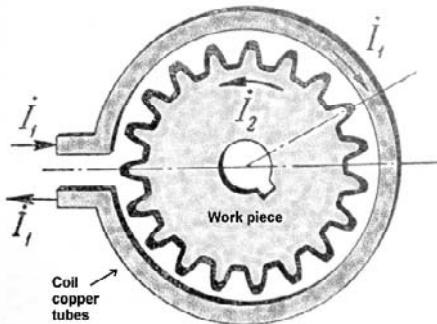


Fig.1 A simplified representation of the coil and the work piece. The total currents in the coil tube and in the work piece are sketched.

The induced current density and its heating effects are non uniform. The current density is a maximum at the surface of the work piece nearest to the coil conductors. As the local density of thermal power is proportional to the square of the local electric current density, the heating effect is also non - uniform. If the frequency of the alternating magnetic field is high enough, the induced electric currents are developed in a thin layer adjacent to the above mentioned surface of the work piece. This is the skin or Kelvin effect, which is used in engineering manufacturing industry for the hardening of bearing surfaces, for welding, for brazing, and similar heat treatment processes [1].

The depth of penetration of eddy - currents can be characterized by the so called "skin depth". It is a function of the frequency of the field, as well as the physical properties and geometry of the work piece [1]. For surface hardening, the material is heated during a few seconds. In the earlier stages of the process, the heat is

confined in a layer with the skin depth. The heated area is then cooled very fast, so that a surface hardening effect is obtained while the bulk of the material remains ductile. The distribution of heating in the body can be controlled adjusting the frequency of the alternating magnetic field. Frequencies in the range 50 Hz to 1 MHz are used for several purposes, from **through heating** at low frequencies to **surface heating** at high frequencies.

The load circuit seen by the driving system is equivalent to a short – circuited transformer. The primary corresponds to the excitation coil or coil assembly. The work piece can be considered as a short – circuited secondary. The impedance of this short circuited transformer depends on the geometry and physical properties of the work piece, the frequency of operation, and the geometry and number of turns of the coils.

A complete description of the problems posed by the method can be found in reference [2].

The practical importance of finding a relation between the local skin depth and the local curvature of the boundary of the work piece was stressed in reference [3]. Recently it was proposed a **closed form analytical formula** that relates, for **non ferromagnetic materials**, the **local skin depth** with the **local mean curvature** and with the well known **skin depth for a flat conductive body** [4].

The purpose of this paper is three fold. First, discuss and improve the theoretical foundation of this formula. Second, generalize it to the surface heating of ferromagnetic bodies, in particular to the case of steel bodies. Third, apply the above mentioned generalized formula and the mathematical tools of lumped circuit theory of transformers, to describe the **load impedance** that must be driven by the induction heating equipment in the usual conditions for **surface hardening** of gears and other work pieces of fairly complex geometries.

II. AN ANALYTICAL FORMULA THAT RELATES SKIN DEPTH WITH LOCAL MEAN CURVATURE

In order to study the Kelvin effect in low frequency alternating fields, as in the case of induction heating, displacement current may be neglected both in the air surrounding the work piece and inside the work piece itself [5], [6]. In this case if $\vec{\Pi} = \vec{E} \wedge \vec{H}$ is the Poynting vector, from Maxwell equations we obtain for the divergence of this vector $\vec{\Pi}$ (see the Appendix (a) at the end of the paper):

$$\nabla \cdot \vec{\Pi} = -\vec{E} \cdot \vec{J} - \vec{H} \cdot \frac{\partial \vec{B}}{\partial t} \quad (1)$$

Let us consider the work piece located inside the working coil. If an alternating magnetic field is produced in the coil, the electromagnetic field in the air outside the work piece but inside the coil may be described by quasi - static equations. In the surface

of the work piece the electromagnetic energy enters to the material along the normal to the considered point, due to the big difference in phase velocity between the air and the conductive body (refraction with absorption in the boundary). As a consequence, the Poynting vector in the boundary of the work piece is perpendicular to this surface and points towards the interior.

Let us consider now the lines of the field $\vec{\Pi}$ inside the work piece, and let us suppose that there is, by continuity, at least locally, a congruence of surfaces orthogonal to these lines (one of these surfaces is the boundary of the heated body). See Fig. 2.

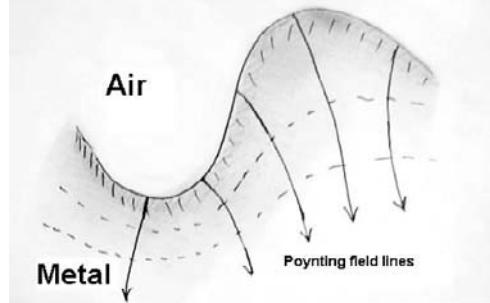


Fig.2. Vector lines corresponding to Poynting field and the associate congruence of surfaces located near the boundary of the work piece.

But $\vec{\Pi} = \Pi \vec{e}_\Pi$ being \vec{e}_Π a unit vector and Π is the norm of the Poynting vector. One surface belonging to the above mentioned congruence pass through the point in which $\vec{\Pi}$ is located, and \vec{e}_Π is the normal vector to the surface at this point. According to a result of differential geometry and classical field theory applicable to a congruence of regular surfaces, the divergence of the normal vector is twice the mean curvature of the surface φ [7].

$$\text{Then,} \quad \nabla \cdot \vec{\Pi} = \vec{e}_\Pi \cdot \nabla \Pi + \Pi (\nabla \cdot \vec{e}_\Pi) = \frac{d\Pi}{ds} + 2\Pi \varphi \quad (2)$$

Here $\frac{d\Pi}{ds}$ is the directional derivative of Π in the direction of \vec{e}_Π , and s represents the arc length along the corresponding field line. For **homogeneous** and **isotropic** bodies, from (1) and (2), substituting $\vec{J} = \sigma \vec{E}$ and taking **time averages** we obtain:

$$\frac{d\bar{\Pi}}{ds} = -2\bar{\Pi} \varphi - \sigma \bar{E}^2 - H \frac{\partial \bar{B}}{\partial t}$$

σ is the conductivity of the material. Then it follows that:

$$\frac{d(\ln \bar{\Pi})}{ds} = -2\varphi - \sigma \frac{\bar{E}^2}{\bar{\Pi}} + \frac{1}{\bar{\Pi}} H \frac{\partial \bar{B}}{\partial t} \quad (3)$$

The spatial scales that characterize the variation of the fields in a direction tangent to the boundary of the work piece are of the same

order of magnitude of a characteristic dimension of the heated body. The spatial scale of variation of the fields along the direction of the Poynting vectors is of the same order of magnitude of the skin depth δ for a flat boundary in a lossless material:

$$\delta = \sqrt{\frac{2}{\omega\mu\sigma}} \quad (4)$$

Here ω is the angular frequency of the alternating magnetic field produced by the equipment and μ is the magnetic permeability of the material, neglecting hysteresis effects.

In the case of surface hardening, the skin depth δ is several orders of magnitude less than a characteristic dimension of the heated body. As a consequence, in a first approximation, the harmonic variation of the electric and magnetic fields can be described by the formulae corresponding to a flat boundary that appear in references [3], [5] and [8]: $\Pi = E \cdot H$ E and H are the magnitudes of the electric and the magnetic field, respectively. Hysteresis can be taken into account substituting the hysteresis loop by an equivalent ellipse [3]. In this case $\hat{B} = \hat{\mu} \cdot \hat{H}$, being $\hat{\mu} = \mu \cdot e^{-j\theta_\mu}$ a suitable complex magnetic permeability and $j = \sqrt{-1}$; \hat{H}, \hat{B} complex numbers representing the magnitude and phase difference of the fields, and θ_μ is the loss angle of the material. The loss angle is

comprised between 0 and $\frac{\pi}{2}$. Then the local values of the magnetic fields are given by:

$$H = H_m \cdot \cos(\omega t) \quad (5a)$$

$$B = B_m \cdot \cos(\omega t - \theta_\mu) \quad (5b)$$

Between the electric and magnetic fields there is the relation, discussed in references [5] and [8]: $\hat{E} = \hat{\zeta} \cdot \hat{H}$

The parameter $\hat{\zeta}$ is given as the following function of the angular frequency, the permeability and the conductivity:

$$\hat{\zeta} = \sqrt{\frac{\omega\mu}{\sigma}} \cdot e^{j\left(\frac{\pi}{4} - \frac{\theta_\mu}{2}\right)}$$

Then the local values of the electric and magnetic fields are:

$$E = E_m \cdot \cos\left(\omega t + \frac{\pi}{4} - \frac{\theta_\mu}{2}\right) \quad (6a)$$

$$H = H_m \cdot \cos(\omega t) \quad (6b)$$

The following equations are verified:

$$\overline{E^2} = \langle E \rangle^2$$

(7a)

$$\langle E \rangle = \sqrt{\frac{\mu\omega}{\sigma}} \cdot \langle H \rangle \quad (7b)$$

$$\langle B \rangle = \mu \cdot \langle H \rangle \quad (7c)$$

$$\overline{\Pi} = \langle E \rangle \langle H \rangle \cdot \cos\left(\frac{\pi}{4} - \frac{\theta_\mu}{2}\right) \quad (7d)$$

$$\overline{H \frac{\partial B}{\partial t}} = \omega \langle H \rangle \langle B \rangle \sin \theta_\mu \quad (7e)$$

Here $\langle \rangle$ represents the RMS value of the magnitude that appears between parentheses. From equations (3), (4) and (7) it follows

that (see Appendix (b) at the end of the paper):

$$\frac{d(\ln \overline{\Pi})}{ds} = -2\wp - \frac{2}{\delta} \left(\sqrt{2} \cdot \cos\left(\frac{\pi}{4} - \frac{\theta_\mu}{2}\right) \right) \quad (8)$$

If the boundary is flat: $\wp = 0$ Then, from (8) it follows that:

$$\overline{\Pi}(s) = \overline{\Pi}(0) e^{-\frac{2s}{\delta} \sqrt{2} \cdot \cos\left(\frac{\pi}{4} - \frac{\theta_\mu}{2}\right)} \quad (9)$$

Equation (9) gives the vanishing of the average magnitude of the Poynting vector going towards the interior of the body from its surface, including ohmic and magnetic losses. The magnitude of the average Poynting vector in a point of the surface of the work piece is $\overline{\Pi}(0)$, and $\overline{\Pi}(s)$ is the corresponding magnitude at a point of the same field line at a distance s from the surface. This result suggests the introduction of **an equivalent skin depth δ_e that corresponds to the case of a curved surface**:

$$\wp + \frac{1}{\delta} \left(\sqrt{2} \cdot \cos\left(\frac{\pi}{4} - \frac{\theta_\mu}{2}\right) \right) = \frac{1}{\delta_e}$$

Then the magnitude of the time averaged power density would decrease along a line of the Poynting vector field approximately following an exponential function of the quotient between the arc length and a **local or equivalent skin depth δ_e** :

$$\overline{\Pi}(s) = \overline{\Pi}(0) e^{-\frac{2s}{\delta_e}} \quad \text{If } \wp \text{ is zero, } \delta_e = \frac{\delta}{\sqrt{2} \cdot \cos\left(\frac{\pi}{4} - \frac{\theta_\mu}{2}\right)} = \delta_H \quad (10)$$

δ_H is the skin depth with magnetic losses in a body with a flat boundary.

In general

$$\delta_e = \frac{\delta_H}{1 + \delta_H \wp} \quad (11)$$

This formula gives the relation between the local skin depth, the local mean curvature of the boundary and the skin depth corresponding to a flat boundary between the work piece and the surrounding air. **With it we attain the first two goals of this paper.**

If $\theta_\mu = 0$, then $\delta_H = \delta$ and formula (10) reduces to the relation

proposed in reference [4]:

$$\delta_e = \frac{\delta}{1 + \wp \delta}$$

However, if the loss angle is non zero and if the nonlinearities in the magnetization curve are taken into account using a suitable value of μ that corresponds to the magnitude of H in the surface of the work piece, (11) could be applied, as an approximation, to steel and other magnetic materials.

III. A DESCRIPTION OF THE LOAD IMPEDANCE SEEN BY THE INDUCTION HEATING POWER SOURCE

Now, let us consider the work piece as a short-circuited secondary of a transformer equivalent to the loaded coil. In the conditions prevailing during surface hardening the skin depth is much smaller than the geometric dimensions of the heated body. In this case we can consider a bar of non-circular cross section. The boundary of each cross section is given by the same curve Γ that may be described in the x-z plane of an orthogonal system of coordinates x,y,z. The y axis is parallel to the axis of the bar. It is possible to introduce a surface density of electric current integrating the volumetric density in depth following the lines of the Poynting vector field [8]. Let h be the length of the bar. If \hat{J}_s is the phasor that represents the surface density, and \hat{I}_{wp} is the phasor that represents the global current that is induced in the work piece, then

$$\hat{I}_{wp} = h\hat{J}_s \quad (12)$$

The electric currents flows parallel to the x-z plane, in each cross section of the bar.

If \hat{E}_s is the phasor that represents the electric field tangent to the boundary of the heated body (also contained in the x-z plane), the induced electromotive force is given by: $\Im = \oint \hat{E}_s dl$ (13)

In the case of a half infinite medium with a flat boundary, it is

$$\text{possible to show that [3], [5], [6], [8]: } \hat{E}_s = \frac{\sqrt{2}\epsilon}{\delta_H \sigma} \hat{J}_s$$

From Eq. (10) this may be re-written thus:

$$\hat{E}_s = \frac{1 + j \operatorname{tg} \left(\frac{\pi}{4} - \frac{\theta_\mu}{2} \right)}{\delta_H \sigma} \hat{J}_s \quad (14)$$

If the Kelvin effect is strong enough, and the curvature φ is small enough, we can suppose that (14) may be applied to the bar substituting δ_H by the local skin depth δ_e given by (11). Then multiplying and dividing by h and taking into account (12) it follows:

$$\Im = \oint \hat{E}_s dl = \left(\frac{1 + j \operatorname{tg} \left(\frac{\pi}{4} - \frac{\theta_\mu}{2} \right)}{h \sigma} \oint \frac{dl}{\delta_e} \right) \hat{I}_{wp}$$

So we obtain the following formula for the impedance of the work piece:

$$\hat{Z}_{wp} = \frac{1 + j \operatorname{tg} \left(\frac{\pi}{4} - \frac{\theta_\mu}{2} \right)}{h \sigma} \oint \frac{dl}{\delta_e} \quad (15)$$

If $l(\Gamma)$ is the length of the curve Γ , from (11) and (15) we obtain

$$\hat{Z}_{wp} = \frac{l(\Gamma)}{\sigma h \delta_e} \left(1 + j \operatorname{tg} \left(\frac{\pi}{4} - \frac{\theta_\mu}{2} \right) \right) \quad (16)$$

Here, by definition $\frac{1}{\delta_e} = \tilde{\delta} + \frac{1}{\delta_H}$ (17)

$\tilde{\delta}_e$ is an average skin depth that corresponds to an average mean curvature: $\tilde{\delta} = \frac{1}{l(\Gamma)} \oint \varphi dl$ (18)

To estimate the electrical load seen by the induction heating equipment, it is necessary to calculate the impedance of the loaded coil.

If a voltage V_c is applied to the coil terminals and if I_c is the electric current in the coil, R_c is the coil's resistance, $L_{c,i}$ is the internal coil's inductance, and Φ is the magnetic flux through the coil's interior, and N is the number of turns of the coil, then we suppose that: $V_c = R_c I_c + L_{c,i} \frac{dI_c}{dt} + N \frac{d\Phi}{dt}$ (19)

If Φ_a is the magnetic flux in the air space between the interior surface of the coil and the surface of the work piece, and Φ_{wp} is the magnetic flux that goes through the work piece, then :

$$\Phi = \Phi_a + \Phi_{wp} \quad (20)$$

If A_c is the area of the coil's cross section and A_{wp} is the area of the work piece cross section: $\Phi_a = A_c (1 - \nu) \mu_o H_o$ (21)

Here $\nu = \frac{A_{wp}}{A_c}$ is the so called filling factor of the work piece

relative to the coil interior. The mean field is $H_o = \frac{NI_c}{h}$ being h the length of the system. Now, let us work with phasors again.

Then the complex electromotive force that is induced in the work piece is given by $-\frac{d\hat{\Phi}_{wp}}{dt} = \hat{Z}_{wp} \hat{I}_{wp}$ (22)

The electromotive force reflected into the coil is:

$$-N \frac{d\hat{\Phi}_{wp}}{dt} = \hat{Z}_{wp} N \hat{I}_{wp}$$

But between the current \hat{I}_c in the coil and the current \hat{I}_{wp} there is the transformer current relation: $\hat{I}_{wp} = -N \hat{I}_c$

As a consequence, the fem reflected over the coil is:

$$-N \frac{d\hat{\Phi}_{wp}}{dt} = -\hat{Z}_{wp} N^2 \hat{I}_c \quad (23)$$

$$\text{From (21) it follows that: } N \frac{d\hat{\Phi}_a}{dt} = j\omega A_c (1-\nu) \frac{N^2}{h} \hat{I}_c \quad (24)$$

From (19), (20), (23) and (24) it follows:

$$\hat{V}_c = R_c \hat{I}_c + j\omega L_{c,i} \hat{I}_c + j\omega \frac{N^2}{h} \hat{I}_c + N^2 \hat{Z}_{wp} \hat{I}_c$$

Then, using equation (16) for the work piece impedance, we derive for the complete load impedance $Z_L = R_L + jX_L$ the equations:

$$R_L = R_c + N^2 \frac{l(\Gamma)}{\sigma h \tilde{\delta}_e} \quad (25)$$

$$X_L = \omega L_{c,i} + j\omega A_c (1-\nu) \frac{N^2}{h} + N^2 \frac{l(\Gamma) \operatorname{tg} \left(\frac{\pi}{4} - \frac{\theta_\mu}{2} \right)}{\sigma h \tilde{\delta}_e} \quad (26)$$

As $\frac{1}{\tilde{\delta}_e}$ grows like $\tilde{\varphi}$, and $\tilde{\varphi} = \frac{1}{l(\Gamma)} \oint \varphi dl$ is an average mean curvature, both the active resistance R_L and the reactance X_L of the load are growing functions of the average curvature.

The equivalent inductance $L_L = \frac{X_L}{\omega}$ has three terms.

The first is related with the self inductance of the coil, and it suffers the influence of the Kelvin effect. The second term is relatively independent of ω . The third term is the sum of two inductances. An inductance arising from δ_H , that is nearly

proportional to $\frac{1}{\sqrt{\omega}}$. Another inductance arising from the effect

of $\tilde{\varphi}$, that is proportional to $\frac{1}{\omega}$. Both inductances decrease when ω increases, but the component related with the curvature decreases faster than the component related with the skin depth δ_H of the flat body.

The coil resistance R_c also varies with the frequency of the alternating current due to the skin effect in the coil tubes.

The effective resistance of the loaded work coil, as shown in (25), is the sum of this resistance R_c and a resistance: $N^2 \frac{l(\Gamma)}{\sigma h \tilde{\delta}_e}$

This stems from the variation of the phase of the electric currents with the variation in depth from the surface of the work piece, relative to the phase of the electric field at the surface. When $\theta_\mu \neq 0$, this term is greater than the corresponding term in the effective reactance of the loaded work coil.

Equation (16) for the work piece impedance and its consequences in the active resistance (25) and in the reactance (26) allows us to attain the third goal of this paper.

IV. DISCUSSION AND CONCLUSIONS

We will consider first the simplest and more common type of gear: spur gears [10]. At the teeth level the boundary is convex. But if the boundary is convex, the mean curvature is negative. Then, the local skin depth, according to formula (11) will be greater than the skin depth of a flat boundary. If the boundary is concave, the mean curvature will be positive. Then the local skin depth will be smaller than the skin depth of a flat boundary. This is shown in Fig. 3.

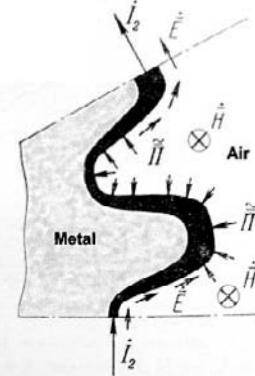


Fig.3. Variations of the local skin depths with the local curvatures of the boundary for a work piece. The arrows that point towards the material of the work piece represent the field of Poynting vectors. The arrows, tangent to the boundary, represent the electric field. The magnetic field is perpendicular to the plane of the picture.

Now, let us suppose that this toothed wheel is located inside a coil in order to be heated by induction. The induced electric current will circulate in a layer adjacent to the surface of the teeth and the notches between the teeth, vanishing towards the interior of the wheel. As the local skin depth is higher at the teeth level than at the notches level, the real part of the local value of the impedance (the so called active resistance) will be lower at the teeth level than at the notches level. However, the same electric current circulates everywhere (so that the electric current density at the teeth level will be smaller than the electric current density at the notches level). As a consequence, the material adjacent to the notches will be heated more than the material of the teeth. If the frequency of operation is high enough, the skin depth for a flat boundary δ_H will be so small that $\delta_H \varphi$ will be negligible in comparison with 1. In that case, the local skin depth $\tilde{\delta}_e$ will be equal to δ_H and the heat power produced by the induced electric current will be the same in all locations of the surface of the gear. These consequences of the analytical formulae are confirmed both by experimental results and by digital simulations of the process of surface hardening of gears by induction heating [2].

The assumptions made in order to derive (11) suggest that the formula for the local skin depth can be applied only if the product $\delta_H |\phi|$ is small enough, perhaps less than 0.3. This guess may be substantiated in a comparison between the approximate analytical formulae obtained in this paper for bars of any cross sections and the exact results obtained for the Kelvin effect in infinite circular cylinders, in two different situations. In one of them, an infinite cylindrical conductor carries an alternating current parallel to its axis. The currents produce an alternating magnetic field perpendicular to the axis of the cylinder [5] [8]. In the other situation, an infinite cylindrical conductor is located in an alternating external magnetic field, uniform and parallel to its axis. The induced currents are contained in the circular cross sections of the cylinder. This case, studied by Förster and others [9], is a simplified mathematical model that may be applied in the framework of certain electromagnetic methods for non destructive testing of metals. However, it has a close connection with the induction heating case. In both situations the comparison was successful for the case of an ohmic work piece without hysteresis losses [4].

Formula (16) gives an analytical estimate of the work piece impedance. If the line integral of the local mean curvature, taken over the curve Γ , is negative (as is the case of a predominantly convex body) both the resistive and the inductive parts of the impedance will be less than the corresponding impedance components for a flat body. If the line integral is positive (as is the case of a predominantly concave body) both the resistive and inductive parts will be greater than the corresponding impedance components of a flat body. If the frequency is high enough, these differences vanish. As the load impedance will change during the heating cycle, a re-tuning or re-matching of the loaded work coil could be indicated, so that an estimation of load impedance variations is useful. In order to calculate the impedance seen by the electronic driving system, the work piece impedance was reflected from the secondary to the primary circuit (the coil) of the equivalent transformer, using a well known procedure. Equations (25) and (26) were thus derived. They correspond to the simplest mathematical model of the electric load. End effects and leakage of fluxes were neglected in this analytical approach, as well as the variations in conductivity and magnetic permeability produced by local temperature increase and magnetic nonlinearities. These variations are produced in time scales often greater than the period of oscillation of the external magnetic field. So, the formulae obtained here could be applied substituting the conductivity, magnetic permeability and loss angle by suitable functions of time.

Anyhow, to determine the best shape and size of induction coils or coil assemblies, in order to heat by induction the work pieces of complex geometry as found in practice, the analytical approach is clearly insufficient. The complex thermal and electromagnetic processes produced in the work pieces and the interaction between

the work pieces and the coils must be simulated using computer codes. The use of these codes is not always straight forward, and sometimes wrong results can be obtained from the numerical calculations.

Nevertheless, the analytical approach affords general results that may be used as guide lines about what to expect and about what to search in relation with the results of the digital simulations.

Also the analytical approach gives us useful lower and upper bounds for the values of parameters such as the local skin depths or the impedances that may be used to select induction heat equipment and to establish some main characteristics of the heating process. All this seems to deserve further study.

V. APPENDIX

(a) Equation (1) is obtained directly from the equation

$$\nabla \cdot (\vec{E} \wedge \vec{H}) = \vec{H} \cdot \nabla \wedge \vec{E} - \vec{E} \cdot \nabla \wedge \vec{H}. \text{ In this equality: } \nabla \wedge \vec{H}, \text{ is substituted by its expression given by Ampere's law: } \nabla \wedge \vec{H} = \vec{J}; \\ \nabla \wedge \vec{E}, \text{ is substituted by } \nabla \wedge \vec{E} = -\frac{\partial \vec{B}}{\partial t}.$$

(b) The relation: $1 + \sin \theta_\mu = \left(\sqrt{2} \cdot \cos \left(\frac{\pi}{4} - \frac{\theta_\mu}{2} \right) \right)^2$ is needed to

obtain Equation (8) from Equations (3), (4), and (7).

VI. REFERENCES

- [1] M. Laughton and R. Warne (Eds.) "Electrical Engineer's Reference Handbook", Oxford: Newness, 2003, Chapter 9.
- [2] V. Rudnev, D. Loveless, R. Cook and M. Black, "Handbook of induction heating", New York: Marcel Dekker, 2003.
- [3] A. Netushil and K.Polivanov, "Principles of Electrotechnics", Vol. 3, Electromagnetic field theory, Gosenergoisdat, Moscow, 1958, Chapter 5.
- [4] R. Suárez-Ántola and Diego Suárez-Bagnasco, "A Tool for Load Modelling in Induction Hardening Equipment Driven by Power Semiconductor Systems", EPIM2005, Montevideo, Uruguay, November 23-24, 2005 (in CD) Paper N° 7.
- [5] S. Ramo, J. Whinnery, and T. van Duzer, "Fields and Waves in Communications Electronics", Wiley, N.Y., 1994, Chapter 5.
- [6] L.Landau and E.Lifchitz, "Electrodynamics of Continuous Media", Addison-Wesley, Reading, Mass., 1960, Chapter 7.
- [7] J.Eriksen, "Tensor fields", an Appendix to C.Truessdall and R.Toupin, "Classical field theories", Encyclopedia of Physics, Volume 3, Berlin: Springer, 1960.
- [8] V. Nikolski, "Electrodynamics and Propagation of Radio Waves", MIR, Moscow, 1985, Chapter 3.

- [9] R.Hochschild, "Electromagnetic methods of testing metals", in "Progress in Non Destructive Testing", Volume 1, London: Heywood, 1959, pp57-109.
- [10] W.Stadler, "Analytical Robotics and Mechatronics", New York: Mc Graw-Hill, 1995, pp380-393.

A Simple Speed Feedback System for Low Speed DC Motor Control in Robotic Applications

R. V. Sharan, G. C. Onwubolu, R. Singh, H. Reddy, and S. Kumar

School of Engineering and Physics

University of the South Pacific, Suva, Fiji.

sharan_r@usp.ac.fj

Abstract-Robots often tend to swerve in an arc when one wants it to move forward or backward in a straight line. This is because the wheels do not rotate at the same speed. This research describes the design of a PIC microcontroller-based speed feedback system for low speed DC motor control to be used for robotic applications. Such a system, integrated with an appropriate motor control circuitry, is expected to dramatically enhance the performance of a DC motor. A feature of this design is that it uses basic principles of speed measurement. The experimental results show that the speeds measured by the PIC-microcontroller are reasonably close to the values measured by the tachometer.

I. INTRODUCTION

The strategy usually used for direct current (DC) motor control in robotic motion and similar applications is pulse width modulation. This, however, uses an open loop control scheme. In open loop control, there is no feedback from the motors informing the robot's program how fast the wheels are turning. Rather, the motors are just given different commanded voltages. But depending on terrain, surface obstacles, slippage in wheel contacts, or load on the robot, the commanded voltages do not necessarily imply particular speeds [1].

In contrast to the open loop system, a closed loop system utilizes a feedback signal as a measure of the actual output response. A feedback control system tends to maintain a prescribed relationship of one system variable to another by comparing functions of these variables and using the difference as a means of control [2].

The feedback data to be obtained is the velocity of the DC motor. To implement a velocity control algorithm, the robot needs sensors on the wheels, such as shaft encoders. Such feedback enables what is known as closed loop control algorithm [3].

II. FEEDBACK SYSTEM DESIGN

An open loop control system of a DC motor normally consists of a pulse width modulator and motor control circuitry. Information about the speed of the motor is obtained by adding a feedback system, as shown in Fig 1, to form a closed loop system.

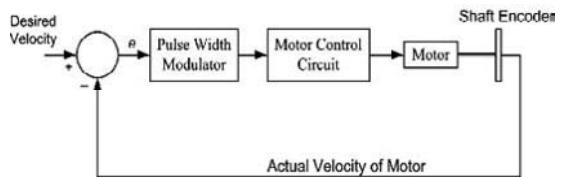


Fig. 1: A simple closed loop system for DC motor control

The basic idea of the control loop is to take in the desired velocity command, generate appropriate duty cycle (the on-time of the motor) based on the command to operate the motor, see how fast the motor actually spins, and then measure that speed and compare it to the commanded speed. The difference is referred to as the error signal and it is either positive or negative [1].

If the actual speed of the motor is less than the desired speed, the difference speed is positive, and so the duty cycle is increased to increase the actual speed of the motor to the desired speed. If the actual speed is greater than the desired speed, the error signal is negative and the duty cycle is reduced to slow the motor [4]. The amount by which the duty cycle is varied to match the actual and desired speed is purely based on the designed controller.

III. SHAFT ENCODER

The feedback transducer used for velocity is the shaft encoder. A shaft encoder is a sensor that measures the rotational rate of a shaft [5]. Typically, a shaft encoder is mounted on the output shaft of a drive motor or on an axle. The signal delivered by this sensor is a pulse train, which makes it appropriate for use in a digital system. Each time the shaft turns by a small amount, the state of its output changes from high to low or vice-versa. Thus, the rate at which pulses are produced corresponds to the rate at which the shaft turns.

Incremental shaft encoders contain a spinning disk that has slots cut in it. The disk attaches to the motor shaft and spins with it. An emitter is placed on one side of the disk's slots and a detector on the other. As the disk spins, the light passing through the disk is interrupted by the moving slots, and a signal in the form of a pulse train is produced at the

output of the detector. By using a microcontroller to count these pulses, the speed of the drive wheel is found [1].

The emitter and detector sensors used for the research reported in this paper are the infrared emitting diodes and phototransistor respectively. The device number for the diode is OP140 and it emits infrared energy at 935 (nm) [6]. The phototransistor, of OP550 series, is spectrally and mechanically matched to the OP140 series of infrared emitting diodes [7].

The output from the phototransistor is a train of pulses with period, T seconds or $T/60$ minutes. Therefore, the speed of the motor in revolutions per minute is:

$$RPM = \frac{60}{NT} \quad (1)$$

where N is the number of slots on the shaft encoder.

If the diameter of the wheel attached to the shaft of the motor is d (meters), the circumference of the wheel = πd (m) and since one revolution represents a distance of πd (m), the speed now becomes:

$$v = \frac{\pi d}{NT} \quad (2)$$

where v is the motor speed in meters per second.

The precision of the calculated speed depends on the resolution of the shaft encoder. Increasing the number of slots on the shaft encoder increases the resolution of the encoder and vice-versa. An encoder with higher resolution would however require very accurate machining and buying one would even cost more. So there is a tradeoff between resolution and costs of the encoder. The encoder designed for this research, however, has 16 slots. This implies that there will be 16 complete pulses produced in one revolution or a sum of 32 high and low signals. Therefore, the minimum angular movement that is detected by the microcontroller is $360^\circ/32 = 11.25^\circ$ and since the circumference of the wheel is πd (m), the robot has a travel resolution of:

$$r = \frac{\pi d}{2N} \quad (3)$$

If used with a wheel of diameter 0.2 m, the maximum travel resolution will be:

$$r_{(d=0.2m, N=16)} = \frac{\pi(0.2)}{32} \approx 0.0196 \text{ m.}$$

Therefore, the microcontroller will have knowledge of every 0.0196 (m) of movement of the wheel of the robot.

IV. MICROCONTROLLER

Microcontrollers are devices that have found extensive use in electronic products globally. They provide a method to learn about digital interfacing and programming, and also provide the capability to easily create applications that control real world devices [8].

The microcontroller used for the work reported in this paper is the Peripheral Interface Controller (PIC) which is developed by Microchip [9]. PIC is essentially an input/output controller and is designed to be very fast. Its program memory is made from flash technology, that is, it can be reprogrammed. The device used is PIC 16F877 which has an internal 16-bit timer. The timer is used to time a single pulse for calculating the speed.

V. EXPERIMENTATION AND RESULTS

The first phase of experimentation involved writing codes to count inputs to the PIC 16F877. Simple push button switches were used as input and the number of manual switch presses was compared to the counter value from the microcontroller.

The next phase involved modification of these codes to time a single pulse or count. The internal *timer1* of PIC was used for this purpose. Since this is a 16 bit timer, it can time a pulse up to a period of $2^{16} = 65536 \mu\text{s} = 65.536 \text{ ms}$. Firstly, various frequencies from the signal generator were measured. This is done to show the accuracy of the frequency that is measured from the motor.

The relationship between the measured frequency using PIC microcontroller and the percentage error is shown in Fig. 2. The percentage error is given as:

$$\varepsilon = \frac{F_m - F_a}{F_a} \times 100\% \quad (4)$$

where F_m and F_a denote the measured and actual frequencies. It is observed that as the frequency increases, the error in the frequency measured from PIC increases linearly, that is, there is a linear relationship between error and frequency.

Furthermore, the shaft encoder was mounted on the shaft of a DC motor and it was driven at different speeds. The speed of the motor was first measured using the PIC microcontroller, and then a tachometer was used to compare the results. The results with an average of 10 runs are shown in Table 1.

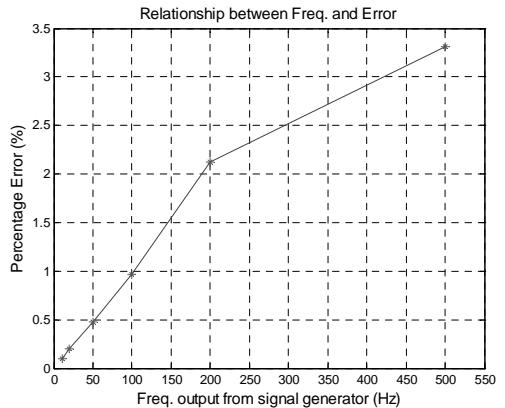


Fig. 2: Characteristics of the error associated with the frequency measured from PIC

Table 1: Measured speeds of the motor using the tachometer and PIC.

RPM (Tachometer) T_{RPM}	RPM (PIC) P_{RPM}	% Error
43**	43.5	1.16
46.6*	47.05	0.97
60.84**	61.26	0.69
73.55*	74.7	1.56

*clockwise **anticlockwise

The percentage error is defined as:

$$\varepsilon = \frac{M_{RPM} - T_{RPM}}{T_{RPM}} \times 100\% \quad (5)$$

where M_{RPM} and T_{RPM} denote the measured speed using the microcontroller and the tachometer respectively.

The speed data obtained from the two sources have some differences but can be considered constant and thus, suitable for measuring speed of DC motor in the lower speed range. Also, a tachometer is basically used to record speed data whereas the speed readings from the PIC microcontroller can be used for speed control or position control of a motor or wheel of a robot.

Some further tests were carried out to justify the need for a closed loop system. Firstly, the battery that is used to power the DC motor under test was fully charged and then the motor was run at its maximum speed. The speed of the motor was recorded at intervals of 15 minutes using the tachometer and the PIC microcontroller.

A graph of time against speed was drawn, as shown in Fig. 3, to determine the relationship between the two variables as the battery voltage drops.

For the first 90 minutes, the speed of the motor is nearly constant. But after 90 minutes, there is a proportional decrease in speed with respect to time. This experimentation shows that the speed of the motor decreases with time as the battery voltage drops. Thus, there is a need for a closed loop system to be incorporated to maintain the speed of the DC motor.

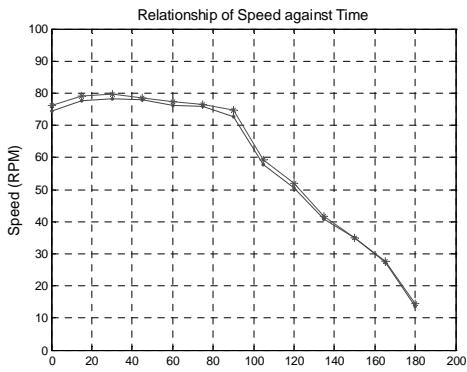


Fig. 3: Plot of speed against time

VI. CONCLUSION

A simple feedback system using a shaft encoder is incorporated in an open loop system to monitor the speed of a DC motor. This information is vital for the control of a DC motor. It can be used to vary the duty cycle of the pulse signal so that the motor speed can be controlled. To maintain desired speed, regardless of terrain, means that the robot needs to calculate the speed of the DC motor to see how fast the wheel is turning and then update the pulse width accordingly. The maximum speed that the tested DC motor had was approximately 75 revolutions per minute at a frequency of about 20 Hertz. Since the PIC microcontroller is quite accurate in measuring frequencies up to about 500 Hz, the results obtained are very close to the tachometer readings.

This is a basic speed feedback system developed for low speed DC motors. More work can be done on this to increase the speed measurement range of this feedback system. PIC microcontrollers also offer interrupt features which can be explored further as a way forward in modifying this system.

REFERENCES

- [1] J. L. Jones, and A. Flynn, *Mobile Robots-Inspiration to Implementation*, A. K. Peters, U.S.A., 1993.
- [2] C. Phillips, and R. Bishop, *Feedback Control Systems*, 4th edition, Prentice Hall, U.S.A., 2000.
- [3] J. Borenstein, and Y. Koren, 'A mobile platform for nursing robots', *IEEE Transactions on Industrial Electronics*, 32(2), 158-165, 1985.
- [4] P. Scott, *The Robotics Revolution: Complete Guide for Managers and Engineers*, Basil Blackwell, U.K., 1984.
- [5] P. Smith, *Active Sensors for Local Planning*, World Scientific Printers, Singapore, 2001.
- [6] Optek Technology, *GaAs Plastic Infrared Emitting Diodes*, Product Bulletin OP140A, May 1996. <http://www.optekinc.com/pdf/OptekOP140.pdf>
- [7] Optek Technology, *NPN Silicon Phototransistors*, Product Bulletin OP550A, June 1996. <http://www.optekinc.com/pdf/OP550A.pdf>
- [8] M. Predko, *Programming and Customizing PIC micro MCU Microcontrollers*, McGraw Hill, U.S.A., 2002.
- [9] Microchip Technology Inc. <http://www.microchip.com>

A Low Power CMOS Circuit for Generating Gaussian Pulse and its Derivatives for High Frequency Applications

Sabrieh Choobkar, Abdolreza Nabavi

Faculty of Engineering
Tarbiat modares University, Tehran, Iran

Email: choobkar_s@yahoo.com, abdoln@modares.ac.ir

Abstract-This paper presents the design of a simple programmable circuit for generating the Gaussian pulse and its derivatives. Since the circuit structure is simple, both the power consumption and the area are much lower than the existing pulse generators. The control pulses are easily programmed to obtain the desired pulse shapes. The pulses, obtained with HSPICE using 0.18 μ m CMOS technology, are in sub-nanosecond range. Therefore, this circuit structure can be employed for high frequency bands.

1. Introduction

Impulse Radio UWB systems communicate the information with a base-band signal composed of sub-nanosecond pulses [1]. Unlike the conventional narrow-band communications, UWB signaling spreads the energy as widely in frequency as possible to minimize the power spectral density [2]. By minimizing the spectrum, the FCC regulation will be met, and the potential for interference to other systems is decreased.

To keep the bandwidth as wide as possible in UWB systems, the fifth order and the seventh order derivative of the Gaussian pulse is chosen for indoor and outdoor communications, respectively [1]. Therefore, generating these derivatives of the Gaussian pulses is very critical.

Since the output of the antenna can be modeled by the first derivative of the input signal [1], the 4th and the 6th derivatives of the Gaussian pulse are desirable.

In this paper, design of a low power CMOS circuit for generating Gaussian pulse and its derivatives for high frequency applications is presented. It will be shown that by choosing the appropriate circuit structure and the correct input signals for switching, the desired output will be generated.

The remainder of this paper is organized as follows. Part 2 introduces the formulation of Gaussian pulse and its derivatives. Part 3 presents the circuit structure. Part 4 explains the circuit design for the 4th derivative of the Gaussian pulse. Part 5 illustrates the simulation results for both the 4th and the 6th derivatives of the Gaussian pulse. Finally, Part 6 provides the concluding remarks.

2. Gaussian pulse and its derivatives

A general Gaussian pulse is given by:

$$x(t) = \frac{A}{\sigma\sqrt{2\pi}} \exp\left(-\frac{t^2}{2\sigma^2}\right)$$

The nth derivative of the pulse can be determined recursively from [1]:

$$x^{(n)}(t) = -\frac{n-1}{\sigma^2} x^{(n-2)}(t) - \frac{t}{\sigma^2} x^{(n-1)}(t)$$

where the superscript ⁽ⁿ⁾ denotes the nth derivative.

In the time domain, the higher order derivatives of the Gaussian pulse resemble sinusoids modulated by a Gaussian envelop [1]. For higher order derivatives, the number of time domain zero crossing increases. More zero crossing in a certain pulse width corresponds to a Gaussian envelop modulated by higher carrier frequency. These observations lead to considering higher-order derivatives of the Gaussian pulses as candidate for UWB transmission [1].

The Fourier transform of the nth order derivative pulse is [1]:

$$X_n(f) = A(j2\pi f)^n \exp\left\{-\frac{(2\pi f\sigma)^2}{2}\right\}$$

Obviously, one important factor which affects the shape of the Gaussian pulse and its derivatives is the variance σ . This factor should be properly chosen in order to achieve desirable time and frequency domain shapes.

Note that, the maximum PSD can be controlled by changing the amplitude, A , of the pulse.

3. Circuit Structure

The idea of designing the following circuit stems from the structure used in Digital to Analog converter (DAC) circuits. The structure consists of a resistive ladder and a number of switches. Also, positive and negative voltage references are required for resistive ladder. The schematic of the circuit is shown in Fig. 1.

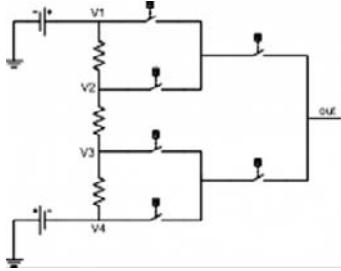


Fig 1: A general circuit for generating a pulse with 4 levels

The switches are controlled in a way that the output node connects only to a single internal voltage of the resistive ladder at a time. The most efficient design is obtained when the number of voltage levels is a power of 2, since the number of switches halves after each stage. In this case, the number of switches and the control signals are minimized.

3.1 Resistive Ladder

Each internal node of the ladder generates a certain voltage, depending on the resistor values and the voltage references.

Choosing the values of resistors is very important, since there is a trade-off between power and speed. Large resistors increase rising and falling times of the output, and small ones cause a large current to flow in the ladder.

3.2. Switches

Each switch is a transmission gate consisting of one PMOS and one NMOS transistor connected in parallel. This switch transfers a wide range of voltages with small power consumption and silicon area.

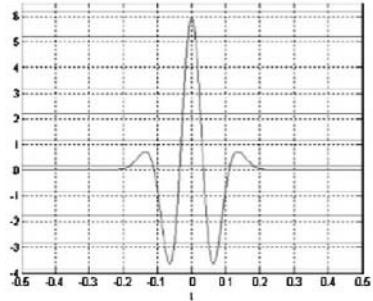
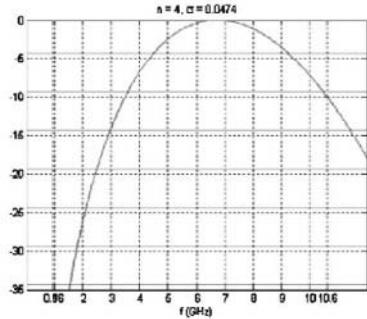
3.3. Input pulses

Each stage of switches needs a pair of complementary input control signals to generate the exact timing of the output. The output pulse width and its voltage swing directly stem from the pulse width of the control signals, since the output node needs enough time to complete the rising (falling) transition.

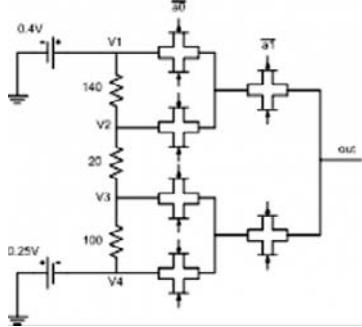
4. Circuit design

In this section, design of a circuit generating the 4th derivative of the Gaussian pulse will be explained. Similar structures can be employed for higher (or lower) order derivatives.

Fig. 2 and 3 show, respectively, the time domain and the power spectral density (PSD) of the 4th derivative of the Gaussian pulse with $\mu=0$ and $\sigma\sim 0.05$ generated by Matlab.

Fig 2: The time domain schematic of the 4th derivative of the Gaussian pulseFig 3: Power spectral density (PSD) of the 4th derivative of the Gaussian pulse (above pulse)

Based on four voltage levels in Fig. 2, the circuit is designed to have three resistors and four (two) transmission gates in the 1st (2nd) switch-stage, as illustrated in Fig. 4.

Fig 4: The designed circuit for generating the 4th derivative of the Gaussian pulse

The value of the resistors is calculated in order to build the appropriate voltage levels in Fig. 3.

Two input signals a_0 and a_1 , and their complements control the switches such that selecting a single voltage level will be possible at a time. The timing of control pulses and

their complements should follow the sequence of envelop needed for the output.

5. Simulation Results

In this section, experimental results are illustrated for generating the 4th and 6th derivatives of the Gaussian pulse. Both Matlab and HSPICE simulations using a 0.18μm CMOS technology are given.

By changing the variance to an appropriate value, the spectrum of the 4th (6th) derivative of the Gaussian pulse will meet the FCC mask. The output signals obtained with HSPICE are in sub-nanosecond range.

5.1. The 4th derivative of the Gaussian pulse

Fig. 5 shows the HSPICE simulation of the circuit in Fig. 4 for generating the 4th derivative of the Gaussian pulse. The power dissipation of this curcuit is 1.6mW.

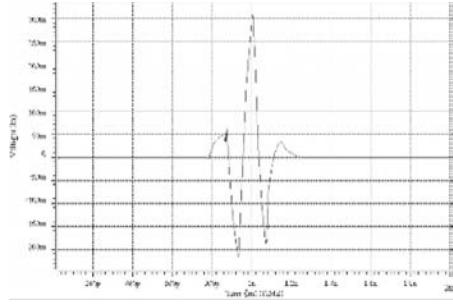


Fig 5: HSPICE simulation obtained for circuit of Fig. 4.

The PSD of this pulse derived from HSPICE file is shown in Fig. 6.

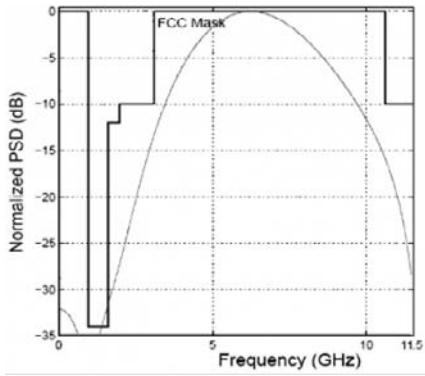


Fig 6: PSD of the 4th derivative of the Gaussian pulse

5.2. The 6th derivative of the Gaussian pulse

Fig. 7 and 8 show, respectively, the time domain and the PSD schematics of the 6th derivative of the Gaussian pulse, plotted by Matlab.

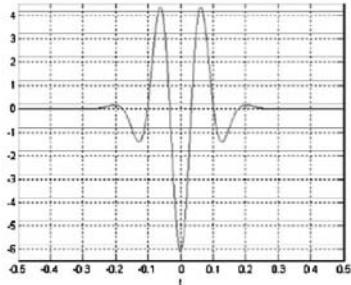


Fig 7: Time domain of the 6th derivative of the Gaussian pulse

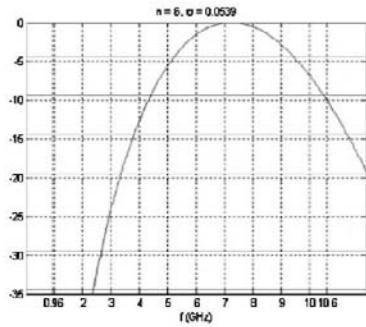


Fig 8: PSD of the 6th derivative of the Gaussian pulse of Fig. 7

The HSPICE simulation of the designed circuit for generating the 6th derivative of the Gaussian pulse is demonstrated in Fig. 9. The power dissipation is 2.3mW.

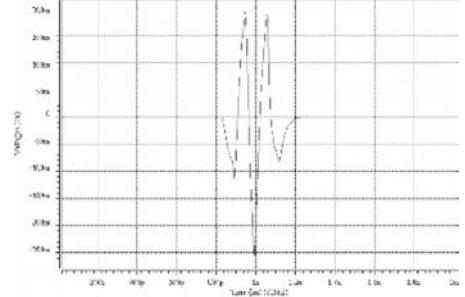


Fig 9: The HSPICE simulation result of the 6th derivative of the Gaussian pulse

Fig. 10 shows the PSD of the pulse in Fig. 9.

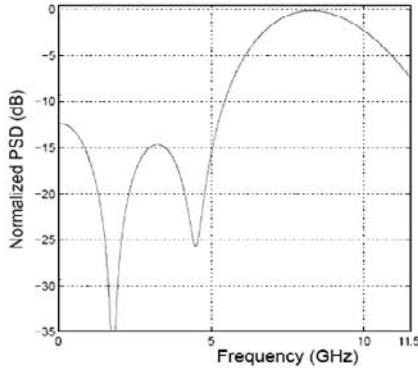


Fig 10: PSD of the 6th derivative of the Gaussian pulse of Fig. 9

6. Conclusion

A low-power programmable CMOS circuit for generating Gaussian pulse and its derivatives has been proposed. The output pulses have been simulated for the 4th and 6th derivatives of the Gaussian pulse using HSPICE. The power consumptions are 1.6mW and 2.3mW, respectively. The output signals are in sub-nanosecond range, and hence the circuit is useful for high frequency bands.

The circuit structure can be used for generating any complicated signal shapes. However, this would require more components and input pulses.

7. Acknowledgment

This research is sponsored by the Iran Telecommunication Research Centre (ITRC).

8. References

- [1] Hongsan Sheng, "Tranceiver Design and System Optimization for Ultra-WideBand Communications", A dissertation for the degree of doctor of Philosophy in Electrical Engineering, New Jersey Institute of technology, May 2005
- [2] Xiaomin Chen, Sayfe Kiaei, "Monocycle Shapes for Ultra WideBand System", IEEE, 2002

On the Efficiency and Fairness of Congestion Control Algorithms

Sachin Kumar, Department of Computer Application, KIET, Ghaziabad, India-201206.

Email: imsachingupta@rediffmai.com

M.K. Gupta, Department of Mathematics, CCS University, Meerut, India-250005.

Email: mkgupta2k1@yahoo.co.in

V.S.P. Srivastav, Computer Division, IGNOU, New Delhi, India-110068.

Email: vijaysrivastav@ignou.ac.in

Kadambri Agarwal, Department of Computer Science, IMR, Duhai, Ghaziabad, India-201206.

Email: Kadambri_agarwal@rediffmail.com

Abstract- In this paper we study various congestion control algorithms. Based on study and mathematical formulation, we present efficiency and fairness properties of congestion control algorithms. We also introduce a very important theorem namely if number of steps in equilibrium state is less, then efficiency is more.

Index Terms- Congestion control, equilibrium state, efficiency, fairness.

I. INTRODUCTION

A network is considered congested when too many packets try to access the same transmission line, router and other resources. In this case, the load exceeds the capacity of network. Congestion should be immediately control otherwise there may be a lot of chances of occurring congestion collapse [10]. During a collapse, only a fraction of bandwidth is utilized.

Several causes for congestion can be defined as:

1. Long distance and high-speed connections increase the total amount of data in the network. When the amount of data exceeds the capacity of the network, the overflow is stored in buffer. Excess utilization of the buffer leads to higher chances of packet loss.
2. Unfavorable topologies and mismatch link speed also lead to congestion.
3. The fast growth of Internet (number of clients increase very rapidly) becomes problem when supporting infrastructure is unable to carry the data.
4. Other causes of congestion may be characteristics of the underlying networks, the mechanism of transmission protocols, the level of flow contention, and functionality of the network routers etc.

Due to these reasons, congestion should be immediately control. Although there are various algorithms available, efficient one must follows efficiency, fairness, responsiveness and smoothness in effective manner. In this paper, we do not define new algorithm but we can claim that any algorithm that works on our introduced theorem will be efficient. As a result, client can get better services. To represent this theorem, a family of algorithm is studied.

In our work, we have used following concepts:

Efficiency: It is the average flows throughput, when system in equilibrium state [1].

Fairness: It characterizes the fair distribution of resources among flows in a shared network [1].

Smoothness: It is reflected by the magnitude of the oscillations during decrease operation [1].

Responsiveness: It is the number of steps to reach the system an equilibrium state [1].

Till date a lot of algorithms are available for controlling congestion. In this paper we study various algorithms based on binomial function [2]. We pass different parameters in binomial function for obtaining various algorithms like AIMD (Additive Increase and Multiplicative Decrease) [3, 7, 11], MIMD (Multiplicative Increase and Multiplicative Decrease) [3], AIAD (Additive Increase and Additive Decrease) [3] and MIAD Multiplicative Increase and Additive Decrease) [3]. We present efficiency and fairness issues of these algorithms.

II ANALYSIS

Every congestion control approach has 2 operations. These two are increasing 'I' and decreasing 'D' respectively. When traffic is congested, 'D' takes place otherwise 'I' takes place. As per our class of algorithms, these can work in additive or multiplicative manner. Binomial function is defined as:

$$'I': W = W + \frac{a}{W^k}, \text{ where } a > 0.$$

$$'D': W = W - bW^l, \text{ Where } 0 < b < 1$$

Here W means size of Window.

Step I: when $k = 0$ and $l = 1$, we get

$$'I': W = W + a$$

$$'D': W = W - bW \text{ or } W(1 - b)$$

Above steps give AIMD. Here additive and multiplicative factors are a and b respectively.

Step II: when $k = -1$ and $l = 1$, we get

$$'I': W = W + aW \text{ or } W(1 + a)$$

'D': $W = W - bW$ or $W(1 - b)$

Above steps give MIMD.

Step III: when $k = -1$ and $l = 0$, we get

'I': $W = W + aW$ or $W(1 + a)$

'D': $W = W - b$

Above Steps give MIAD.

Step IV: when $k = 0$ and $l = 0$, we get

'I': $W = W + a$

'D': $W = W - b$

Above steps give AIAD.

Using these algorithms, we take 2 flows (x and y). Initially, we assume $x < y$ and system converges in such a manner that two flows should be share same amount of bandwidth ($x = y$).

A. Fairness

We know that fairness ratio $(f_i) \frac{x}{y}$ should be 1 for equilibrium state, where i is positive integer.

In AIMD, let $f_1 = \frac{x}{y}$. After 'I' operation flows will be $x = x + a$ and $y = y + a$.

Therefore $f_2 = \frac{x+a}{y+a}$.

Clearly $f_1 < f_2$ (fairness improved).

After 'D' operation flows will be

$x = x(1 - b)$ and $y = y(1 - b)$,

Therefore $f_2 = \frac{x}{y}$.

Clearly $f_1 = f_2$ (fairness unchanged)

In MIMD, let $f_1 = \frac{x}{y}$. After 'I' operation flows will be $x = x + ax$ or $x(1 + a)$

and $y = y + ay$ or $y(1 + a)$.

Therefore $f_2 = \frac{x}{y}$.

As a result, we have $f_1 = f_2$ (fairness unchanged).

After 'D' operation flows will be $x(1 - b)$ and $y(1 - b)$.

Therefore $f_2 = \frac{x}{y}$.

As a result, we have $f_1 = f_2$ (fairness unchanged).

In MIAD, fairness is unchanged in 'I' operation because Multiplicative Increase gives no change in fairness (from 'I' operation of MIMD).

Now let $f_1 = \frac{x}{y}$, after 'D' operation flows will be

$x = x - b$ and $y = y - b$.

Therefore $f_2 = \frac{x-b}{y-b}$.

As a result, we have $f_1 > f_2$ (Fairness reduced).

In AIAD, 'I' operation improves fairness because Additive Increase from AIMD improves it and 'D' operation reduces fairness because Additive decrease from MIAD reduces it.

These observations give following results:

Additive Increase improves fairness.

Additive Decrease reduces fairness.

Multiplicative Increase unchanged fairness.

Multiplicative Decrease unchanged in fairness.

These observations recommended AIMD is better approach.

B. Theorem

Statement: If the number of steps in equilibrium state is less then efficiency is more.

Proof for AIMD: Let number of steps is t and both flow (2 flow system) share same amount of bandwidth ($x = y$ in equilibrium state). At the end of cycle the sum of flow becomes W . Therefore, complete cycle of equilibrium state is given by $x, x + a, x + 2a, \dots, x + (t-1)a$ and for 2 flows system at equilibrium state, value of each flow should be $x + (t-1)a = \frac{W}{2}$.

Therefore sum of the cycle is given by $\left(\frac{W}{2} - (t-1)a\right) + \dots + \left(\frac{W}{2} - 2a\right) + \left(\frac{W}{2} - a\right) + \frac{W}{2}$.

i.e., $\frac{tW}{2} - \frac{t}{2}(t-1)a$.

The sum of 2 flows is $tW - t(t-1)a$.

But for 100% utilization, the sum of 2 flows should be Wt .

Efficiency is given by $\frac{tW - t(t-1)a}{Wt}$.

i.e., $1 - \frac{(t-1)a}{W}$.

It is clear that efficiency is depending on number of steps.

Proof for AIAD: To find out efficiency, only increase steps of equilibrium state are studied. Therefore AIMD and AIAD give equal efficiency.

Proof for MIMD: In MIMD, equilibrium cycle for flow x is given by

$$x, (1+a)x, (1+a)^2x, \dots, (1+a)^{t-1}x.$$

The sum of equilibrium cycle for x is given by

$$x + (1+a)x + (1+a)^2x + \dots + (1+a)^{t-1}x.$$

$$= \frac{x}{a} ((1+a)^t - 1)$$

$$\approx \frac{x}{a} (1+a)^t.$$

We know that at end of the cycle x equals $\frac{W}{2}$.

$$\text{Then } (1+a)^{t-1}x = \frac{W}{2}$$

$$\text{Or, } x = \frac{W}{2(1+a)^{t-1}}.$$

Therefore sum is given by $\frac{W(1+a)}{2}$.

For both flow, sum is given by $W(1+a)$.

Thus efficiency is given by $\frac{(1+a)}{t}$.

Proof for MIAD: As we know only increase steps take place in efficiency, therefore MIAD holds same efficiency as MIMD holds.

III CONCLUSION

We have presented fairness and efficiency properties of various algorithms like AIAD, AIMD, MIAD and MIMD. In AIMD and AIAD (If system reaches equilibrium state)

efficiency is given by $1 - \frac{(t-1)a}{W}$. For MIAD and MIMD,

efficiency is given by $\frac{(1+a)}{t}$. Based on these results, we

have proved that if number of steps in equilibrium state is less, then efficiency is more. Based on these results, researchers can introduce new algorithms in order to maintain good efficiency.

REFERENCES

- [1] A.Lahans, V.Tsaoussidis, "Exploiting the efficiency and fairness potential of AIMD-based Congestion avoidance and control," Computer Networks, vol. 43, pp. 227-245, 2003.
- [2] D. Bansal and H. Balakrishnan, "Bionomal Congestion Control Algorithms", IEEE INFOCOM, April 2001.
- [3] D. Chiu, R.Jain, "Analysis of the increase and decrease algorithms for congestion avoidance in computer neworks," Computer Networks and ISDN Systems, vol. 17, pp. 1-14,1989.
- [4] J.Mahadavi, S.Floyd, "TCP-friendly unicast rate-based flow control, note sent to the end2end-interest mailing list", 1997.
- [5] Pierre G. Paulin and John P. Knight, ``Force Directed Scheduling for the behavioral synthesis of ASIC's," IEEE Trans. Computer Aided Design, Vol.8, pp. 661-679, June 1989.
- [6] R. G. Gupta, V.S.P. Srivastava "On Synthesis of Scheduling Algorithms," Information Processing Letters, Elsevier Science Publishers, vol. 19, pp. 147-150, 1984.
- [7] S.Floyd, M. Handley, J. Padhye, "Comparison of equation-based congestion control and AIMD-based congestion control," work-in-progress. Available from <http://www.aciri.org/tfrc>, 2000.
- [8] S.Floyd, M.Handley, J.Padhye, J.Widmer, "Equation-based congestion control for unicast applications," in: Proceedings of ACM SIGCOMM, September 2000.
- [9] S.Floyd, K. Fall, "Promoting the use of end- to-end congestion control in theInternet,"IEEE/ACM Transactions on Networking, vol. 7, pp. 458-472, 1999.
- [10] V.Jacobson, "Congestion avoidance and control", in: proceedings of ACM SIGCOMM 88, 1988.
- [11] V.S.P. Srivastav, M.K. Gupta, Sachin Kumar, Kadambri Agarwal, "Improved AIMD- A Mathematical Study," Journal of Computer Science, Science Publications USA, vol. 1, pp. 515-520, 2005.
- [12] Y.R. Yang, S.S. Lam, "General AIMD congestion control, on: Proceedings of the 8th IEEE International Conference on Network Protocols," Osaka, Japan, 2000.

Hopfield Neural Network as a Channel Allocator

Ahmed Emam¹ and Sarhan M. Musa²

¹Western Kentucky University

²Prairie View A&M University

Abstract- Dynamic Channel Allocation (DCA) schemes based on Artificial Neural Network (ANN) technology were seen as performing better overall than conventional statistically based DCA schemes. Furthermore, some papers report that within the ANN schemes adopted as Channel Allocators (CA), the Hopfield Neural Network (HNN) performs considerably better than the conventional non-HNN methods. The work reported in this paper is a summary of research where a new HNNCA is proposed and simulated to check the validity of the argument itself. The simulation of the project was done through non-uniform traffic to simulate extreme conditions and have a more realistic approach; the number of prerecorded patterns was also a subject of the simulation. The simulation's results recorded different correlated situations and there have been substantial conclusions that can be made from the simulation itself.

I. INTRODUCTION

Over the recent years, various techniques for channel allocation have been developed in order to face the steep augmentation of mobile communication traffic as quantity and quality. Many have been DCA schemes developed by different sources [1], [4], [6], [7], [8], [14], [16], [17], [18] where the Artificial Neural Network (ANN) part was not included. They were just pure Dynamic Channel Allocation (DCA) schemes whose structure and formulae were calculated to maximize the different aspects that composed channel allocators. Some other DCA schemes were made involving ANN [3], [11], [13], [15], [16]; these schemes were developed and studied and their performance was compared to both non-ANN-DCA and other ANN-DCA schemes, the results are that the ANN-DCA schemes appeared to perform much better as a whole. Their adaptability and flexibility resulted in having a higher response time, call handling, channel reuse and Quality of Service (QoS).

The aim of this paper is to summarize the analysis made when a new Hopfield Neural Network (HNN) CA is proposed and simulated to check the validity of the argument itself. This paper will reinforce what already has already been confirmed and it will give some more insight to the analysis conducted and will explain further certain aspects of the results.

The paper is organized as follows. Section 2 describes the input's activation function. In section 3 a summary of the simulation itself is presented with the main results of the paper discussed in section 4. A brief summary of the work and concluding remarks are presented in the final section.

II. ACTIVATION FUNCTION

As mentioned before, a unique activation function is proposed, this activation function deals with the traffic amount present and turns its value to a value between 0 and 1, also, the activation function deals with the prioritization of call types (hand-off, home calls or receiving calls) and call genres (linked to the origin of the call and the caller's plan, the importance of the caller). This activation function is as follows:

$$Af_{ij} = \frac{\left(1 - e^{\alpha x_{ij}} + \sum_{y=1}^n \Delta_y o_{ij}\right)}{\left(1 + \sum_{y=1}^n \Delta_y\right)} \quad (1)$$

This activation function (Af) has different components that are listed below:

- Af_{ij} : activation function of the neuron i,j.
- α : prioritization factor, this constant is the multiplication of α_1 and α_2 [21].
- x_{ij} : input for the neuron ij.
- $\Delta_y o_{ij}$: dampening factor linked with recurrences in the inputs, usually temporal recurrences.
- $\Sigma\Delta$ is the summation of all the fractions (Δ) used and applied for each $\Delta_y o_{ij}$.

The denominator of the function has the effect of resizing the activation function's outcome to a value between 0 and 1.

There is no need to put restraint on the number for the inputs: x can be as big as it wants the output value for that neuron after going through the activation function will always fall between the 0 and 1.

Thus a good activation function value must be chosen since there is no best value.

III. SIMULATION

The simulation itself consists of having devised a system that can replace completely the CA part of the base station.

The simulation consists of two parts connected:

1. The HNN section, this section deals on the calculating the best Fuzzy Channel Allocation (FCA) to use in that particular situation.
2. The FCA pool: this section is where, once the output is calculated, the next step for the allocator is to pick the appropriate scheme.

The system was first simulated by entering four pre made patterns, then run some tests on distorted versions of the patterns and see if they could go back to the original pattern. The second run was with completely random inputs and see if the network could locate a pre made pattern. The third part would be like the second one with the difference that the patterns were generated randomly as well and their number increased to 5, the next experiment was with 6 such randomized patterns and the last one with 7 randomized patterns.

A. Scenario situation

The scenario setting consists on an isolated single cell situation using the above mentioned Hopfield Neural Network Channel Allocator (HNNCA). This scenario, although it involves only one isolated cell, it does include hand-off calls. The simulation is made so to exclude aspects like channel interference, channel borrowing and other such problems and issues cropping up when other cells are included around the single cell.

Although the model has some missing components, it has been constructed to be the most flexible with the present ones: the model has no restriction for the number of callers that use the model, as a matter of fact, the model uses a Bernoulli distribution when generating both predetermined patterns and input patterns; also, the predetermined patterns can then be linked to a pool of any type of Division Multiplexing Access (DMA), Time, Frequency or even Code, or FCA schemes.

The only restrictions on the network that were set by the simulation included the fact that it was run with 4 to 7 predetermined patterns, the network consisted on a 3 by 18 grid of neurons in a Hopfield network structure. Also, the input generated was generated directly as a suitable value; that is bypassing the activation function calculations.

IV. RESULTS

For all simulations, patterns were linked to an FCA scheme and since there was no real need to choose a time frame to stick to, the simulations concentrate on the pure aspect of having the network learning to change direction towards choosing good patterns in an efficient way and with the minimum of energy loss. Also, all simulations are made under non-uniform traffic, which means the inputs are randomized using the Bernoulli distribution. The simulation

was conducted in different phases. The results of the experiments were confronted thoroughly and meticulously to find any possible patterns or recurrences of any kind. All possible aspects were put in comparison, and the followings were the results:

A. Pattern probability comparison

The pattern probability comparison was made between the each pattern and, as it can be noticed; there is a trend in the chance for a certain pattern to come up. Fig.(1) shows that, the higher the pattern number the lower the probability that a certain pattern can be chosen. This does not seem to be always the case, but it does happen more times than if it were a completely random case, meaning that this trend has to be taken into consideration.

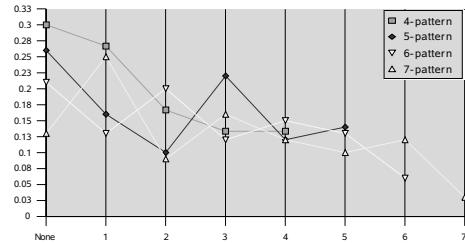


Fig. 1: Comparisons between the probabilities for each pattern to appear from completely randomly generated inputs.

B. Iteration probability

Apart from the 4-pattern simulation, the other patterns seem to show a certain trend where the bigger the number of patterns in memory the more spread is the iteration probability. Fig. (2) shows that, the comparison the number of iterations needed for the network to reach any pattern. This data is presented in a graph where the x-axis represent the number of iterations and the y-axis the probability that the network will go through that number of iterations to reach a pattern. The lines between the points have no value and should not be considered other for spotting any correlations.

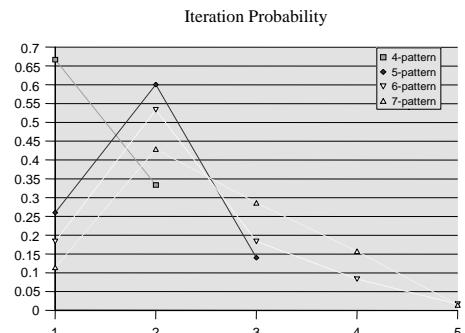


Fig. 2. Comparison between the patterns for what concerns the probability for the simulation to go through a certain number of iterations before reaching a stable pattern.

C. Error Probability

The case for error probability seems to resolve itself as the number of patterns in memory augment; this could just be a distribution case: the fact that there are more patterns to choose from. Fig. (3) shows the pure probability for an error in the evaluating the right pattern to occur without considerations for the number of patterns stored in the network's memory. As a result, there is a trend and this trend shows that the higher the patterns in memory, the lower the probability that an erroneous pattern will be chosen over a valid one. Fig. (4) shows that the probability multiplied by the number of patterns pre-stored in the network's memory, this should remove the bias situation and the result comes up to be encouraging: the trend continues to descent as the number of patterns in memory augment.

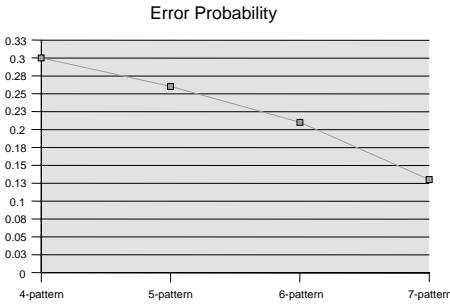


Fig. 3. Probability that a stable but undesired pattern will be chosen.

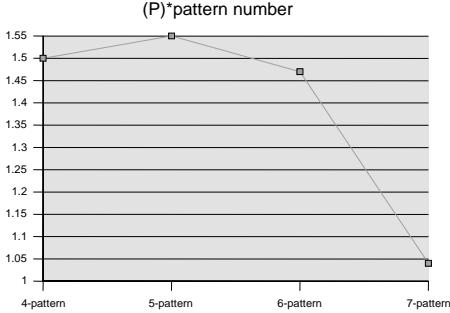


Fig. 4. Representing probability of an undesired pattern appearing multiplied by the number of patterns present.

D. Energy state vs. frequency

The last comparison is an energy comparison; a comparison is made between the energy state of each network pattern and the frequency that the given energy states is achieved by the network. The experiments showed that there is no clear trend or particular convergences among the patterns and the only distinguishable thing that is erroneous patterns have a higher energy state than valid patterns. From all the graphs (figures 5 to 7) there is a trend that can be established, this trend seems to indicate that in general, the higher the energy state of the pattern the lower the probability that the network will reach it. There are some exceptions, but those

exceptions can well be the result of a low number of samples. This is why the 4-pattern was not included in this comparison.

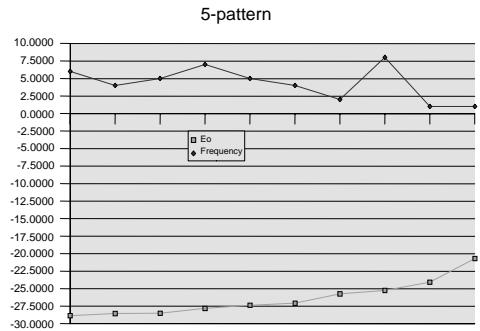


Fig. 5. Energy state-frequency that particular energy state will be picked when iterating a random input for the simulation with 5 patterns memorized.

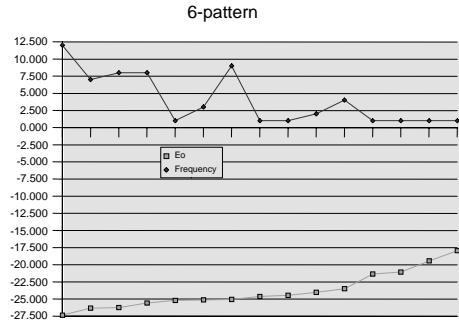


Fig. 6. Energy state – frequency that particular energy state will be picked when iterating a random input for the simulation with 6 patterns memorized.

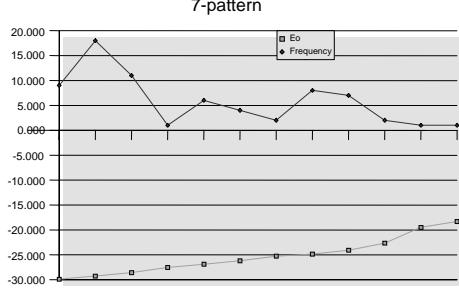


Fig. 7. Energy state- frequency that particular energy state will be picked when iterating a random input for the simulation with 7 patterns memorized.

E. Energy state vs. pattern numbers

The last comparison is between the energy state and the pattern numbers; this comparison includes also the energy state for unwanted patterns. Fig.(8) shows that there are different interesting factors that appear in comparisons: the first one is

that the pattern's number is not linked in any way to its energy state, the second one is except for what concerns unwanted patterns, these patterns seem to reside in an energy state interval that is, in average, higher than the other wanted patterns.

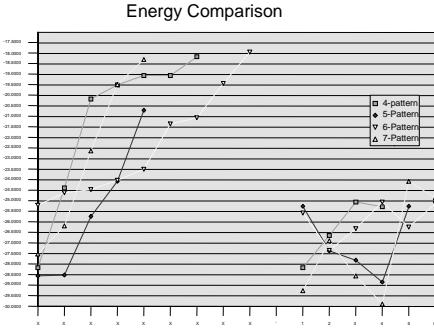


Fig. 8. Comparisons between energy state of the pattern and the number of the pattern itself, x means that the energy state corresponds to an undesired stable pattern.

V. CONCLUSION

This paper concludes by showing that there are certain factors to be considered when generating such network, these factors can go from trying to organize all patterns to a certain energy state and if it cannot be done, try and see if the energy state can be used as a further method of prioritizing patterns over others, this will give the network full customization by the user.

Also, it would be a good idea to work on a working model that takes into account all the aspects previously amiss.

This project has room for expansion and can be ameliorated, all the results from the experiment conducted show that there is potential in the program and that it could be feasible.

REFERENCES

- [1]. O. Lazaro, D. Girma, "Enhanced Formulations for Call Capacity Improvement of Distributed DCA Schemes Based on Hopfield Neural Network", European Wireless 2002, 26-28 Feb. 2002, Florence, Italy, pp. 490-495.
- [2]. Computation and Neural Systems Series Editor – Christof Koch – California Institute of Technology
- [3]. K. Murray, R. Mathur, D. Pesch, "Adaptive Policy Based Management in Heterogeneous Wireless Networks", Proc. IEEE WPMC 2003, Yokosuka, Japan, Oct. 2003
- [4]. Zukang Shen, Jeffrey G. Andrews, and Brian L. Evans, "Short Range Wireless Channel Prediction Using Local Information" in Proc. IEEE Asilomar Conf. on Signals, Systems, and Computers, vol. 1, pp. 1147-1151, Nov. 9-12, 2003, Pacific Grove, CA, USA
- [5]. An Exploration and Development of Current Artificial Neural Network Theory and Applications with Emphasis on Artificial Life – David J. Cavuto – Albert Nerken School of Engineering
- [6]. Dynamic Channel Assignment with Delay and Loss Considerations for Wireless TDMA LANs – Nikos Passas, George Lampropoulos, and Lazaros Merakos – Communication Networks Laboratory Department of Informatics, University of Athens, Greece
- [7]. Siba K Udgata and Dang Van Hung. A formal model for dynamic channel allocation as a mutual exclusion concept in a distributed mobile computing system. Presented at and published in the proceedings of the 2003 International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'03), June 23-26, 2003, Las Vegas, Nevada, USA, Hamid Arabnia and Younsong Mun (eds), CSREA Press, pp. 1464-1468.
- [8]. Reinforcement Learning for Dynamic Channel Allocation in Cellular Telephone Systems, Satinder Singh and Dimitri Bertsekas, Advances in Neural Information Processing Systems (NIPS) 1997 -Volume 9
- [9]. Neural Networks – Algorithms, Applications and Programming Techniques (Addison, Wesley) [Ebook]
- [10]. http://web.doe.carleton.ca/~qjz/ANN_Course/ANN_Structure.pdf, Qi-Jun Zhang - Department of Electronics Carleton University, Ottawa, ON, Canada
- [11]. osiris.sunderland.ac.uk/~cs0kmc/COM198_L07.ppt, Ken McGarry,
- [12]. <http://www.root.cz/>
- [13]. http://www.mdx.ac.uk/www/psychology/cog/psy3250/McPitts/09_McPitts.html
- [14]. SH Wong and IJ Wassell, "Channel allocation for broadband fixed wireless access networks", Wireless Personal Multimedia Communications , Volume: 2, PP: 626- 630, 2002
- [15]. http://openai.sourceforge.net/docs/nn_algorithms/networksarticle/re_es.html
- [16]. Reinforcement Learning for Dynamic Channel Allocation in Cellular Telephone Systems, Satinder Singh, Department of Computer Science, University of Colorado.
- [17]. Jianchang Yang, D. Manivannan and Mukesh Singhal, "A Fault-Tolerant Dynamic Channel Allocation Scheme for Enhancing QoS in Cellular Networks", IEEE Proc. 36th Hawaii Int'l Conf. System Sciences,2003
- [18]. Kwan Lawrence Yeung and Tak-Shing Peter Yum, "Phantom Cell Analysis of Dynamic Channel Assignment in Cellular Mobile Systems", Vehicular Technology, IEEE Transactions on, 1998
- [19]. Introduction to Artificial Neural Systems by Jacek M. Zurada (PWS Publishing Company, 1992) ISBN 0-534-95460-X
- [20]. Introduction to Wireless and Mobile Systems by Dharma Prakash Agrawal and Qing-An Zeng, [University of Cincinnati Brooks/Cole (Thomson Learning)] ISBN No. 0534-40851-6

Command Charging Circuit with Energy Recovery for Pulsed Power Supply of Copper Vapor Laser

Satish Kumar Singh

Jaypee Institute of Engineering & Technology,
Guna, 473 226 – India
satish.singh@jiit.ac.in

Dr. Shishir Kumar

Jaypee Institute of Engineering & Technology,
Guna, 473 226 – India
shishir.kumar@jiit.ac.in

S. V. Nakhe

Raja Ramanna Center for Advanced Technology,
Indore, 452 013 – India
nakhe@cat.gov.in

Abstract- Copper vapor laser (CVL) is the highest power laser in metal vapor laser family. The copper vapor laser has very high gain and it gives output at two wavelengths; 510.5 nm (green) and 578.2 nm (yellow). When this copper vapor laser is used in MOPA (Master Oscillator Power Amplifier) mode in laser chains for high power lasers applications then a common problem arises due to false triggering of power supply pulses to drive this master oscillator and this problem is known as “Jitter”. The conventional power supply for this laser is based on capacitor charge transfer circuit or L-C inversion circuit in which the hydrogen Thyratron is used as a pulse power switch. Thyratron has the inherent limitation of lifetime typically 1200Hrs, as it is gas filled switch. Due to this it results in higher running cost of the laser. This limitation is overcome in pulse excitation circuit based on semiconductor switches & magnetic pulse compressors. Insulated Gate Bipolar Transistor (IGBT) is comparatively recent device used as pulsed power switch in these circuits. IGBT switches offer several advantages over other power semiconductor switches like fast switching, ease of paralleling, simple control circuit, high repetition rate etc. However use of magnetic pulse compressors (MPC) introduces additional jitter in laser because of change in saturation time due to changes in input voltage.

In this paper a new design and performance of a capacitor charging power supply for IGBT based pulse power supply for copper vapor laser is reported. The new circuit scheme for the power supply uses modified command charging scheme with energy recovery. This design resulted in reduced jitter for the pulse power supplies using magnetic pulse compressors.

Key words: MPC, Command Charging Circuit, Fly Back Converter, CVL

I. INTRODUCTION

Copper vapor laser requires the fast excitation pulses with rise time less than 100ns. The optimum repetition rate for copper vapor laser depends upon laser tube, gas/gas mixture. For a typical 30 W average output power elemental copper vapor laser having 45 mm diameter of discharge tube and the Neon (Ne) as buffer gas, typical pulse power supply requirements are as Rise time: 80ns, Voltage magnitude (open circuit voltage): 25 kV, Peak current: 800 Amps, Pulse repetition rate: 6 kHz, Average output power: 5kWatt.

The charging voltage of the capacitor should be constant such that there should be no pulse-to-pulse variation in charging voltage of capacitor. It means that if the charging voltage of charging capacitor is fixed at a predefined value

then it should be charged at that value only at each and every pulse or attempt. If there is variation in charging voltage then at laser output, jitter appears because the saturation time for magnetic pulse compressor is voltage dependant. Before going into the design consideration it is very necessary to understand about the jitter. The jitter is defined as pulse-to-pulse variation in the relative position of the laser pulses with respect to trigger pulse. Jitter may be shown as in figure (1.03). As in figure the pulse is not at precisely the same position but it has shifted from pulse-to-pulse relative position.

The jitter is very severe problem for the copper vapor laser applications specially when operated in MOPA mode. There are several causes as follows when magnetic pulse compressor is used; (1) Due to variation in input line voltage there is variation in the charging voltage of capacitor and it is the cause for jitter in laser output pulses, (2) There is some reflected energy from the laser load due to mismatch in the output impedance of power supply and laser load. This reflected energy changes the initial conditions of the charging capacitor and thus the charging voltage of capacitor changes pulse to pulse. This pulse-to-pulse variation causes the jitter in output of laser pulses, (3) Jitter in other electronic circuits used for triggering IGBT switches, other ICs etc. Literature survey is carried out in this paper on pulsed power supply for CVL using semiconductor switches for pulse generation & charging circuits used in such power supplies. Semiconductor switches in CVL power supply have been reported long life as compared to Thyratron like SCR stacks found to increase the entire CVL and circuitry system life MTBF about 7000 Hrs [1]. It has been reported that maximum electric efficiency of 67% has been achieved with pulse exciters in case of CVL [2]. High energy transfer efficiency in the input power range of 2.9 kW to 6.5kW by optimizing the reset current for the saturable inductors is also reported with the above configuration, they achieved average laser power 21W at 5 kHz repetition rate. IGBT based pulsed exciter circuit operating at 6 kHz is reported [3]. It has been also reported that the energy deposition efficiency of IGBT based pulse exciter circuit is 53% at input power 6.1 kW and the laser power obtained is by the above circuit is 31W [3]. It has been reported that for IGBT based pulsar, the expected cost per hour is very less compared to Thyratron-based pulsars and the latching frequency of the switch is nil [3]. It has been reported 6.5kW average power IGBT based pulse excitation circuit for a 30W discharge heated copper vapor laser [4]. Under the optimized conditions of the reset current jitter of $\pm 2.5\text{ns}$ in laser output pulse with respect to

gate trigger pulse is reported for 25W average output power copper vapor laser^[5]. Various capacitor-charging circuits are summarized in ref.^[7]. After carrying out the literature survey it is concluded that the command charging circuit with energy recovery for solid-state pulse power supplies for copper vapor laser is very useful to achieve low jitter.

II. TOPOLOGY

Block diagram of the pulse width modulated command charging based solid-state pulse power supply designed & developed for a small bore test CVL along with pulse generator circuit is shown in figure (1.01). The circuit is designed to handle average power of 1.5kW. This block diagram shows several sub block as single phase Variac, isolation transformer, rectifier, power circuit block, energy recovery block, pulse transformer, MPC, sampling network, control block, and driver block.

Functioning of the circuit: The mains supply of 220-volt is connected to a 1-φ Variac (0-220 volts) and the o/p of Variac is fed to the isolation transformer; which isolates the circuit from the AC mains line. The isolation transformer's output is given to the MCB, which protects the circuit from the fault current. The o/p of MCB is given to a full bridge rectifier, and the o/p of which is connected a filter capacitor C_f . Operating cycle IGBT controller circuit is shown in figure (1.02). The switch S1 (IGBT) closes for time duration T1 and is stopped when the storage capacitor charges up to a predefined voltage level. After time T1 the IGBT controller circuit opens the switch S1 for time T2. T2-T1 is the delay time between charging and discharging pulses. After time T2 the S2 is switched on and the storage capacitor discharges in load.

III. RESULTS

Results with Laser Load with Two Stages MPC: The power supply along with two stages MPC has been tested on 10mm bore, 60cm long CVL. The power supply is operated at 5 kHz repetition rate.

Figure (1.04) to (1.13) shows the wave forms at different channels as given in table (1.01)

Ch1	Voltage across the storage capacitor
Ch2	Voltage at I/P side of pulse transformer
Ch3	Output voltage pulse at laser load

Table (1.01)

A-Uncontrolled Mode of Operations: Waveforms in Figure (1.04) to (1.06) show the different voltages at Ch1, Ch2, & Ch3 at input AC voltage of 198V, 220V, & 242V respectively. Waveform in figure (1.07) shows the variation in different channel voltages in infinite persistence mode of operation of oscilloscope.

From figure 1.04 to 1.06 shows the line regulation of the circuit in uncontrolled mode of operations which is $\pm 20.73\%$ across the laser load for $\pm 10\%$ change in input AC voltage and form figure 1.07 voltage stability across the laser load is $\pm 2.80\%$ when terminated on pulse transformer, two stages MPC and laser load.

B-controlled Mode of Operations: Waveforms in Figure (1.07) to (1.11) show the different voltages at Ch1, Ch2, & Ch3 at input AC voltage of 198V, 220V, & 242V respectively. Waveform in figure (1.07) shows the variation in different channel voltages in infinite persistence mode of operation of oscilloscope.

From figure 1.08 to 1.10 shows the line regulation of the circuit in uncontrolled mode of operations which is $\pm 4.89\%$ across the laser load for $\pm 10\%$ change in input AC voltage and form figure 1.11 voltage stability across the laser load is $\pm 0.91\%$ when terminated on pulse transformer, two stages MPC and laser load.

Figure (1.12) & (1.13) shows the time jitter in two cases as in uncontrolled and controlled mode respectively. From figures (1.12) and (1.13) it is clear that the time jitter in uncontrolled and controlled mode of operations are $\pm 2.75\text{ns}$ and $\pm 1.75\text{ns}$ respectively.

Comparison: The following table (1.02) & (1.03) shows the comparative results between controlled and uncontrolled mode of operations on laser load.

Input AC <i>Volts</i>	Uncontrolled			Controlled		
	V_S (Volts)	V_{Sec} (kV)	V_L (kV)	V_S (Volts)	$V_{Sec}(\text{kV})$	V_L (kV)
198	358	8.26	8.02	322	7.46	7.12
220	396	9.04	10.32	334	7.7	7.56
242	488	10.48	12.3	342	7.88	7.86

Table (1.02)

	a	b	c	d	e	f	g	h
UC	130	16.4	2.22	12.3	4.28	20.7	$\pm 2.75\text{ns}$	2.51%
C	20	2.99	0.42	2.72	0.74	4.89	$\pm 1.75\text{ns}$	0.91%

Table (1.03)

Where

UC: Uncontrolled & C: Controlled modes of operations

- a: Change in voltage across the storage capacitor ($\pm \Delta V_S$) in Volts
- b: Percentage change in voltage across the storage capacitor ($\pm \% \Delta V_S$) in volts
- c: Change in voltage across the secondary of pulse transformer($\pm \Delta V_{Sec}$) in kVolts
- d: Percentage change cange in voltage across the secondaryof pulse transformer($\pm \% \Delta V_{Sec}$) in kVolts
- e: Change in voltage across the laser load ($\pm \Delta V_L$) in kVolts
- f: Percentage change in voltage across the laser load ($\pm \% \Delta V_L$) in kVolts
- g: Time jitter in nanoseconds
- h: Voltage jitter

IV. FIGURES

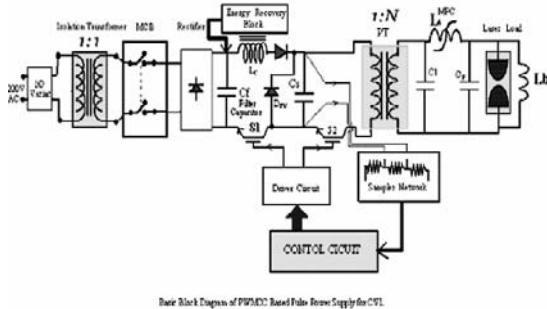


Figure (1.01)

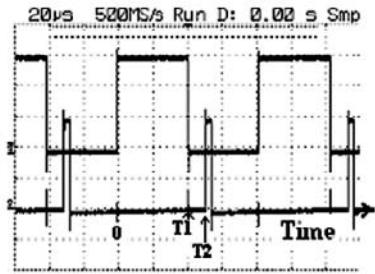


Figure (1.02)

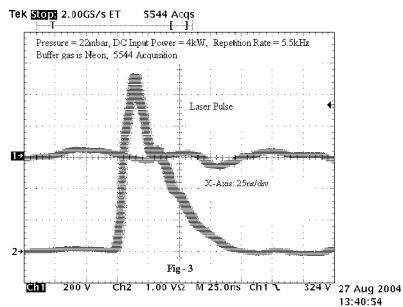


Figure (1.03)

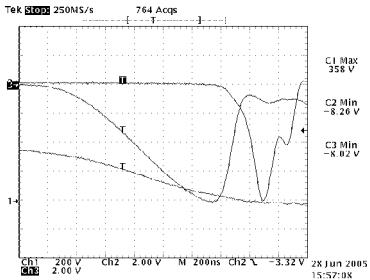


Figure (1.04)

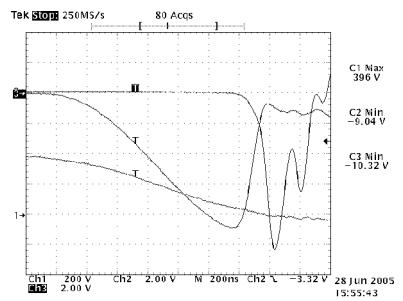


Figure (1.05)

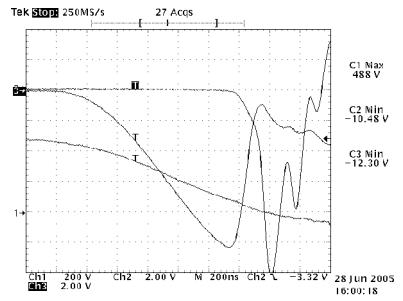


Figure (1.06)

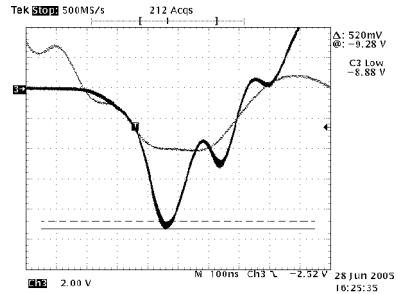


Figure (1.07)

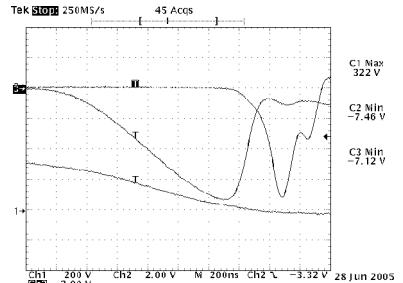


Figure (1.08)

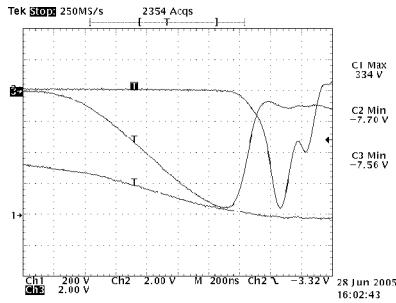


Figure (1.09)

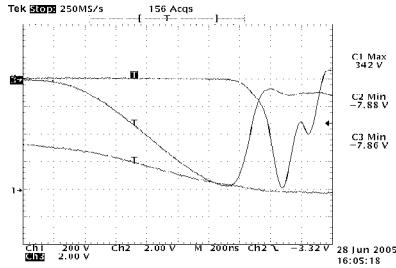


Figure (1.10)

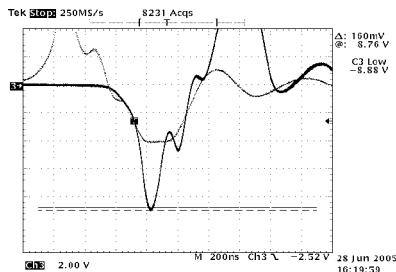


Figure (1.11)

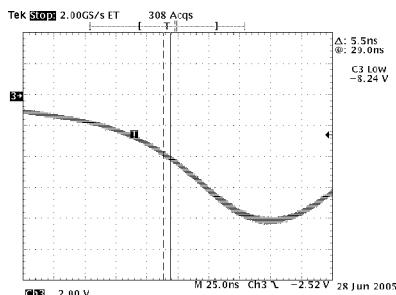


Figure (1.12)

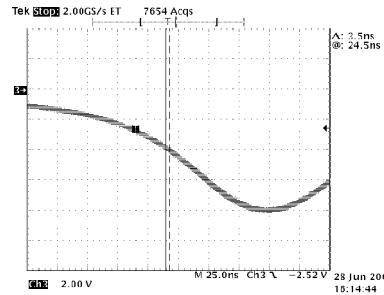


Figure (1.13)

V. CONCLUSION

IGBT based PWMCC; high voltage pulse power supply for small bore test copper vapor laser has been designed & developed. This power supply is tested and waveforms are taken at different input AC voltage and also at different load conditions i.e. only resistive load, pulse transformer plus resistive load and pulse transformer, two stages MPC and laser load. All the measurements are taken at 5 kHz frequencies. Performance of PWMCC circuit based capacitor charging power supply has been recorded in this thesis and found to be improved in comparison to SMPS (with $\pm 2\%$ ripple & regulation performance) based supply for pulse power supply of the CVL. Unlike SMPS the circuit proposed here will take care of reflected voltage from the laser load. The circuit reported here can improve the jitter performance of the CVL at reduced cost.

The performance of PWMCC high voltage pulse power supply i.e. voltage regulation, time jitter, voltage stability, can be improved by modifications involved the improvement of response time of the circuit for any feed back signal to the controller card and response time of switches. The circuit scheme then can be extended for higher power laser power supply units to extract full benefits of the scheme.

VI. ACKNOWLEDGMENT

We want to acknowledge Jayprakash Sewa Sansthan (JSS) that provided us a strong platform to present the paper in this conference. Our sincere thanks go to Prof. Y. Medury, Vice Chancellor-JUIT Wknaghat, Prof. N. J. Rao, Director-JIET Guna, Prof. K. K. Jain, Brig. S. K. Sud, Prof. R. Saxena, Prof. B. K. Mohanty, Mr. G. S. Tomar, and all our dear friends who encouraged us for the same.

REFERENCES

- [1] A Self-Consistent Model for High Repetition Rate Copper Vapor Laser by M. J. Kushner. *IEEE Journal of Quantum Electronics*. Vol. 61.1981IEEE.
- [2] Copper Vapor Operated By A Solid State Switch By E. Fujiwara; Ch Yamanaka; N. Nakashima, Institute Of Laser Engineering Osaka University Japan. E. Murata, *Kansai Electric Power Co. Inc et al. Page No 240.S11e Vol 1212 High Power Gas Lasers 1990*.

- [3] Energy Deposition Studies In A Copper Vapor Laser Under Different Pulse Excitation Schemes, by S V Nakhe et al, *MEAS Sci. technology*, 14(2003), pp607-613.
- [4] IGBT Based Pulse Excitation Circuit For Copper Vapor Laser, By S V Nakhe *NLS 2002*, PP187-188.
- [5] Magnetic Pulse Compressor For Copper Vapor Laser Using Indigenous Ferrites By R. K. Mishra, S. V. Nakhe *NLS-2004*.
- [6] 550V/20A Switch Mode Power Supply For All Solid State Switch Pulsed Power Supply For Copper Vapor Laser, By Dharmraj V Ghodke And K Muralikrishnan *NLS 2002*,Pp177-178.
- [7] Constant Power Charging Supplies For High Voltage Energy Transfer By Bruce R Hayworth, President, Capacitor Specialists, Inc., *Escodido, California Tech Note 109*.
- [8] An Algorithm Of Design Of Magnatic Pulse Compresso, By L.Druckmann; Scaboy & I Smilanski.
- [9] Fly back Converter Design; Application Note by West Cost Magnatics.
- [10] Data Sheet and Application Manual IHD 215/280/680; Concept www.igbt-driver.com.
- [11] Application Notes And Technical Information IXYS, 1998.
- [12] www.ct-concept.com

Performance Evaluation of MANET Routing Protocols Using Scenario Based Mobility Models

Shams-ul-Arfeen

Hamdard Institute of Information Technology Hamdard University Karachi, Pakistan
shams.arfeen@hamdard.edu.pk

A. W. Kazi Jan M. Memon

Department of Computer Science Isra University Hyderabad, Pakistan
{janmohd, walikazi}@isra.edu.pk

S. Irfan Hyder

College of Computer Science, Karachi Institute of Economics & Technology, Karachi, Pakistan
hyder@pafkiet.edu.pk

Abstract- MANET is a multi-hop wireless network without a fixed infrastructure. Many routing protocols have been proposed and tested under various traffic loads and speeds for MANETs. However, the simulations of such routing protocols usually do not consider the nomadic velocities of MANET participants witnessed in real-world scenarios, which may have significant impact on the performance of MANET routing protocols. In this paper, we have designed four scenario-based mobility models having various speeds of MANET participants to compare the performance of DSDV and AODV routing protocols. The simulation results indicate that DSDV protocol is suitable for HRM and HWM models under high traffic load.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of autonomous mobile nodes that communicate with each other over wireless links [1]. In MANETs, mobile nodes can communicate with each other directly if they are within the transmission range of each other or via intermediate nodes. In later case it is referred to as multihop network.

The wireless arena has been experiencing exponential growth since the past decade [1]. It has seen great advances in network infrastructures, growing availability of wireless applications; and the emergence of omnipresent wireless devices, such as portable or handheld computers, PDAs and cell phones; all getting more powerful in their capabilities. These devices are now playing an ever-increasing important role in our lives. Not only are mobile devices getting smaller in size, cheaper, more convenient and more powerful, but also they are capable to run more applications and network services.

In the past decade, a special category of wireless networks, namely, Mobile Ad Hoc Networks (MANETs) have been brought into existence. The main reason for their popularity is because of their potential to provide a widespread connectivity in areas where network services.

infrastructure is unavailable or cannot be installed in times, such as battlefields, search-and-rescue operations, disaster-stricken areas and medical camps in rural areas. The characteristics of MANETs such as dynamic topology, frequent link breakages, limited power and limited bandwidth pose challenges for design of these applications as well [2, 3].

During the past couple of years, many routing protocols have been proposed for the MANETs. Their performance under various network environments and traffic conditions have been closely studied and compared. However, the simulations of MANET routing protocol usually do not consider nomadic velocities and pause-time intervals witnessed in real-world scenarios [1, 4, 5], which may have significant impact on the performance of MANET routing protocols. Therefore, in this paper, we propose four scenario-based mobility models that mimic the movements of the nodes in the real world scenarios. The DSDV and AODV protocols will be compared with these models.

The remainder of the paper is organized as follows: section 2 briefly reviews the two distance vector routing protocols, DSDV and AODV; section 3 covers motivation and description of our designed scenario-based mobility models; Section 4 is used to describe the simulation performance; section 5 covers the discussion of simulation results; while section 6 presents conclusion and future work.

II. RELATED WORK

In our study, we have focused our simulations on two MANET routing protocols, namely, AODV and DSDV. This section briefly describes the general working principles behind both of them.

A. DSDV Routing Protocol

In DSDV [1, 6], each node maintains a routing table, which has an entry for each destination in the network. The attributes for each destination are the next hop, metric (hop counts) and a sequence number originated by

the destination node. To maintain the consistency of the routing tables, DSDV uses both periodic and triggered routing updates; triggered routing updates are used in addition to the periodic updates in order to propagate the routing information as rapidly as possible when there is any topological change. The update packets include the destinations accessible from each node and the number of hops required to reach each destination along with the sequence number associated with each route.

Upon receiving a route-update packet, each node compares it to the existing information regarding the route. Routes with old sequence numbers are simply discarded. In case of routes with equal sequence numbers, the advertised route replaces the old one if it has a better metric. The metric is then incremented by one hop since incoming packets will require one more hop to reach the destination. A newly recorded route is immediately communicated to its neighbors.

When a link to the next hop is broken, any route through that next hop is immediately assigned infinity metric and assigned an updated sequence number. This is the only case when sequence numbers are not assigned by the destination. When a node receives infinity metric and it has an equal or later sequence number with a finite metric, a route update broadcast is triggered. Therefore, routes with infinity metrics are quickly replaced by real routes propagated from the newly located destination.

One of the major advantages of DSDV is that it provides loop-free routes at all instants. It has a number of drawbacks, however. Optimal values for the parameters, such as maximum settling time, for a particular destination are difficult to determine. This might lead to route fluctuations and spurious advertisements resulting in waste of bandwidth. DSDV also uses both periodic and triggered routing updates, which could cause excessive communication overhead. In addition, in DSDV, a node has to wait until it receives the next route update originated by the destination before it can update its routing table entry for that destination. Furthermore, DSDV does not support multipath routing.

B. AODV Routing Protocol

The AODV is an on-demand or reactive MANET routing protocol [4, 7, 8]. In AODV, when a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a route discovery process to locate the intended node. It places the destination IP address and last known sequence number for that destination, as well as its own IP address and current sequence number (Broadcast-ID), into a Route Request (RREQ) message. The broadcast-ID and the nodes own IP address, uniquely identifies the RREQ which helps to suppress duplicate RREQ's to flow in the MANET when the same RREQ is received by a

mobile node again. After that it broadcasts the route request (RREQ) message to its neighbors, which then forward the request to their neighbors, and so on, until either (a) the destination or (b) an intermediate node with a “fresh enough” route to the destination is found. If neither of these conditions is met, the node rebroadcasts the RREQ.

On the reception of RREQ message, the destination node creates a Route Reply (RREP) message. It places the current sequence number of the destination as well as its distance in hops to the destination, into the RREP, and sends back a unicast message to the source. The node from which it received the RREQ is used as the next hop. When an intermediate node receives the RREP, it creates a forward route entry for the destination node in its route table, and then forwards the RREP to the source node. Once the source node receives the RREP, it can begin using the route to transmit data packets to the destination. If it later receives a RREP with a greater destination sequence number or an equivalent sequence number with smaller hop count, it updates its route table entry and begins using the new route.

In AODV, an active route is defined as a route which has recently been used to transmit data packets. Link breaks in non-active links do not trigger any protocol action. However, when a link break in an active route occurs, a link failure notification is propagated to the node upstream of the break determines whether any of its neighbors use that link to reach the destination. If so, it creates a Route Error (RERR) packet. The RERR packet contains the IP address of each destination which is now unreachable, due to the link break. The RERR also contains the sequence number of each such destination, incremented by one. The node then broadcasts the packet and invalidates those routes in its route table.

There are many advantages of AODV. The number of routing messages in the network is reduced due to its reactive approach that makes it use the bandwidth more efficiently. However, protocol overhead may increase if it is used in highly mobile and heavily loaded networks. Furthermore, due to reactive approach it is more immune to the topological changes witnessed in the MANET environment. As a result, the AODV offers quick adaptation to dynamic link conditions, low CPU processing and memory overhead, low network utilization and determines unicast routes to destinations within the MANET. It also allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. A distinguishing feature of AODV is its use of a destination sequence-number (DSN) that ensures loop freedom. Hence, AODV operates in a loop-free style.

III. SCENARIO-BASED MOBILITY MODELS

Human mobility is crucial in simulations of MANET routing protocols [9], as mostly different wireless devices are carried by humans in real-world scenarios. Therefore, to simulate a MANET protocol more realistically, it is essential to design a scenario-based mobility model that accurately represents the speed patterns of various MANET participants observed in real-world. Such models should attempt to mimic the actual movements of human and other MANET participants. It is important to create different models based on the limits of various MANET participants in which different nodes can move at maximum speed, which will be helpful in classifying protocols suitable in different conditions. Therefore, in this study, these models are entitled Scenario-Based Mobility Models which are designed to compare the performance of DSDV and AODV protocols.

Fast Car Model (FCM): FCM assumes that nodes are cars and they can move up to the speeds of 30 m/s or 108 km/h. As discussed earlier, these mobile nodes are not moving all the time as they may be stationary for a while and then move to the next specified destination. For instance, if an ambulance is moving at 100 km/h [10], it has to stop at different signals and break points. Therefore, pause-time intervals should also be considered in this model.

Slow Car Model (SCM): This is the same as FCM model with the assumption that cars / ambulances are in busy streets and may not move at higher speeds. Therefore, in this model, speed is reduced to 15 m/s or 45 km/h [10].

Human Running Model (HRM): Most of the time MANET participants are human and, therefore, it is mandatory to consider their speeds carefully. For instance, soldiers in battlefield can run or walk. On average, the running speed of a human is 8 m/s or 28.8 km/h [10]. There are various other situations in which human participants run. These scenarios include sports and rescue operations.

Human Walking Model (HWM): This is alike HRM model, but its considerations are different. For example, people usually walk in a shopping mall, campus or at a festival. Human walking speed on the average is 2 m/s or 7.2 km/h [10].

IV. PERFORMANCE EVALUATION

The simulations were conducted using NS-2 running on an Athlon-64 bit 3000+ processor, with 512MB of RAM and Windows XP operating system. Table 1 summarizes various parameters used to setup simulation environment in NS-2.

A. Simulation Results

This section describes the results achieved from the simulations. To analyze the affect of scenarios-based models, 10 mobility scenario files were generated for pause-time 0, 10, 100 and 450 for every scenario-based model, namely, FCM, SCM, HRM and HWM. Furthermore, the traffic load is fixed to 20 sources, generating 4 packets per second. Hence, the affect of scenario-based models is analyzed in an adequately loaded environment.

VARIABLES	VALUE
Transmission range	250 m
Simulation time	900 s
Topology size	1000 m x 1000 m
Total nodes	50
Mobility model	Random Waypoint
Traffic type	Constant bit rate
Packet rate	4 packets/sec
Packet size	512 bytes
Maximum Speed	2, 8, 15, 30 m/s
Number of sources	20
Pause time	0, 10, 100, 450 s
NS-2 Version	NS-2.28

TABLE 1: SIMULATION PARAMETERS

There are three performance metrics that are measured in these simulations, namely, packet delivery fraction, average end-to-end delay and normalized routing overhead.

Packet Delivery Fraction (PDF)

It can be seen in Figure 1 that under very fast speed i.e. 30m/s and high mobility with 0 pause-time interval, throughput is below 40% for both DSDV and AODV protocols. However, as the pause-time increases, the throughput for the DSDV protocol rises up to 60%. On the contrary, the throughput for the AODV remains steady.

Both the SCM and HRM models show almost identical throughput for all pause-times as depicted in Figure 2 and 3. The throughput for the pause-times 0, 10 and 100 are almost equal. However, the throughput steadily improves when the pause-time reaches 450 seconds. In Figure 4, the throughputs for both the DSDV and AODV are identical for all pause-times.

It can be seen in Figure 5 that under very fast speed i.e. 30m/s and high mobility with 0 pause-time interval, end-to-end delay varies between 200 and 250 milliseconds for AODV and DSDV respectively. However, as the pause-time increases, the end-to-end delay remains steady for AODV, whereas, for DSDV, it surpasses 250 milliseconds. Moreover, in Figure 6, 7 and 8, the DSDV protocol is consistently over 200 milliseconds which are inadequate for real time voice communication.

Normalized Routing Overhead

The packet overhead is the number of routing packets transmitted per data packet delivered at the destination. In Figure 9 that under very fast speed i.e. 30m/s and high mobility with 0 pause-time AODV generated around 12 packets only to transmit one data packet. With the change in pause-time from 0 to 450, AODV still generates around 11 routing packets to transmit one data packet. On the other hand, DSDV is more bandwidth saver; it takes around half of the packets (6 protocol packets to transmit one data packet) as compared to the AODV.

In Figure 10 which reflects the results of SCM model, AODV improves its performance by reducing number of control packets from 8 to 6 to transmit one data packet. Further improvements can be seen in Figure 11 and 12, where on all pause-time values; AODV gives almost steady performance and maintains 6 control packets fraction versus one data packet. In all cases and all models, nowhere AODV crosses or gives better performance in terms of control packets versus data packets.

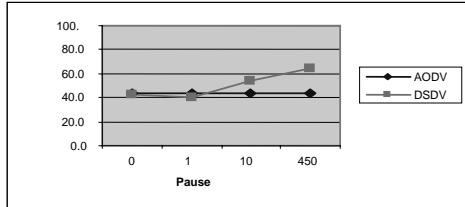


Figure 1: Throughput (FCM, Speed 30m/s)

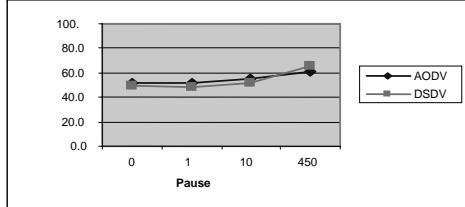


Figure 2: Throughput (SCM, Speed 15m/s)

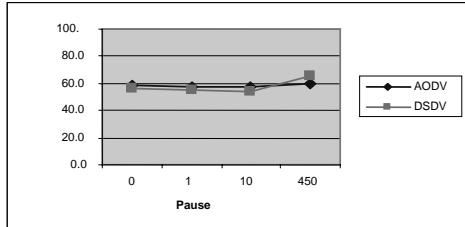


Figure 3: Throughput (HRM, Speed 8m/s)

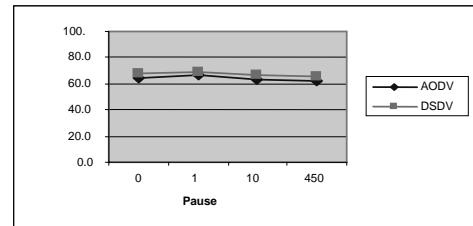


Figure 4: Throughput (HWM, Speed 2m/s)

V. DISCUSSION

It is observed that DSDV protocol has a higher average end-to-end delay than AODV protocol does in all cases, which seems to contradict to the advantages, the proactive approach has over reactive approach in the literature. This is mainly due to the implementations of the protocols in NS-2. Although both implementations apply the drop-tail approach for packet queues, AODV protocol poses a limit on the time a packet can be queued, which currently is 30 seconds, hence, the delay of any received packet is bounded. The DSDV protocol keeps packets in queues indefinitely until they are delivered to the next hop or the destination node. Therefore, it delivers the older packets rather than the newer ones, and hence there is an increase in the average end-to-end delay for the DSDV protocol.

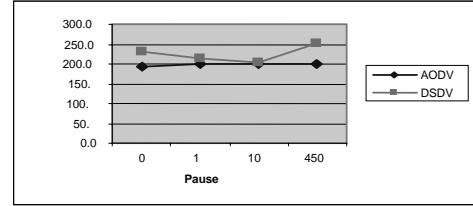


Figure 5: End-to-End Delay (FCM, Speed 30m/s)

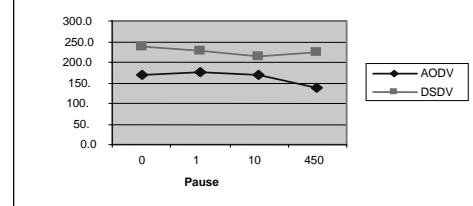


Figure 6: End-to-End Delay (SCM, Speed 15m/s)

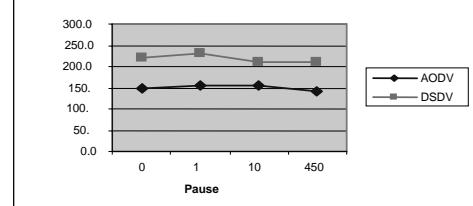


Figure 7: End-to-End Delay (HRM, Speed 8m/s)

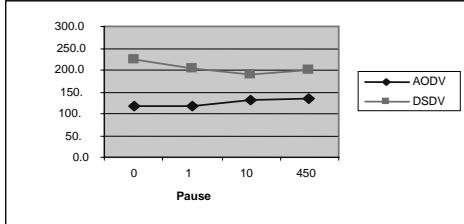


Figure 8: End-to-End Delay (HWM, Speed 2m/s)

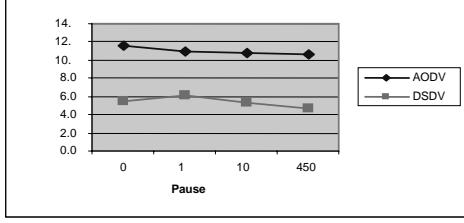


Figure 9: Protocol Overhead (FCM, Speed 30m/s)

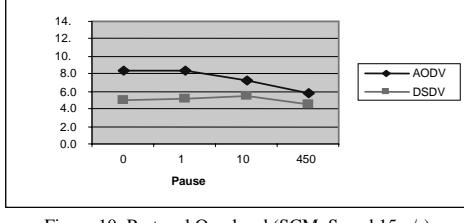


Figure 10: Protocol Overhead (SCM, Speed 15m/s)

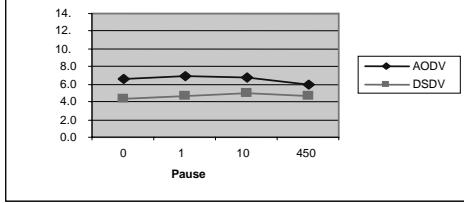


Figure 11: Protocol Overhead (HRM, Speed 8m/s)

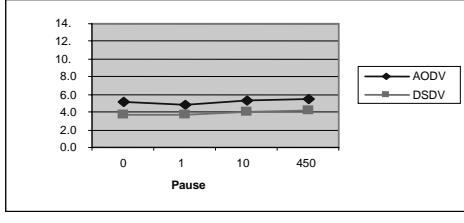


Figure 12: Protocol Overhead (HWM, Speed 2m/s)

The Figures 5 and 6 show the average end-to-end delay in FCM and SCM models respectively. It can be seen that even at very high speed i.e. 30m/s in FCM model, the results of DSDV protocol for pause-time 0, 10, 100 are almost identical. However, the SCM model for the DSDV protocol, at pause-time 450, gives a slightly better performance that is because the reduction

in speed increases the probability of validity of the paths stored in routing tables. On the other hand, the AODV protocol performs consistently for all pause time-intervals. Furthermore, the average end-to-end delay decreases with the reduction of the speed.

In Figures 3 and 4, it can be seen that throughput for HRM and HWM models has increased as compare to FCM and SCM models seen in Figure 1 and 2. The reduction in speed increases the profitability of the life time of a link. Therefore, both protocols (AODV and DSDV) give almost identical performance in both HRM and HWM models in which speed is 8m/s and 2m/s respectively. However, in Figure 1, there is an exceptional case in which under high speed and pause-time of 0 and 10 seconds, both protocols give almost identical performance but suffer in performance compared to the HRM & HWM models. This is mainly due to the fact that routes become obsolete before their utilization. However, with the increase in pause-time, the DSDV protocol increases its throughput and raises it up 62% while AODV remains unchanged. This is obvious in the case of DSDV protocol as it is proactive and gives better performance with fewer changes in network topologies.

In general, it can be seen in Figure 9, 10, 11 and 12 that the normalized routing overhead of DSDV protocol is lower as compare to AODV protocol for all cases. Furthermore, the overhead for both protocols decreases as the speed is reduced. Moreover, the difference between the DSDV and AODV overhead is almost identical for the FCM, and HWM models. However, in the FCM model (Figure 9) it can be seen that routing overhead for AODV is very high, reaching to 12 protocol packets for one data packet. In this model, pause-time does not have any significant impact on the performance of AODV protocol. Hence, when the route breaks during transmission, a route error (RERR) packet is sent to the source, which then tries to find another route by sending broadcast RREQ packet into the network. Once again a new route is found and route error may occur before the utilization of the newly found route. This is the reason there are many routing packets sent in FCM model in order to deliver one data packet. The Situation becomes worse when there is no route information available in caches on intermediate nodes. Furthermore, AODV protocol uses hello packets to maintain pointers which are necessary to maintain source-destination link on the intermediate nodes. These hello packets are also routing packets and hence are included in the protocol overhead. On the other hand, the DSDV protocol maintains routing tables regardless of source and destination pair. Whenever a route breaks or a node moves away from any node, this information is triggered and is sent to all

neighboring nodes. Therefore, normalized routing overhead is 50% lower than AODV in FCM model.

It is interesting to see that under same mobility AODV protocol has higher protocol overhead than DSDV in all cases. In Figure 10, the AODV protocol has significant reduction in terms of protocol with respect to pause-time values. At pause-time 450, the AODV protocol improves its performance and gives better result by reducing its overhead from 8 protocol packets to 6 protocol packets for delivering one data packet. This is because there are fewer link breakages than in the previous cases in which speed was 30m/s. In Figure 12, both protocols have considerably low protocol overhead. This is due to the fact that both are table driven protocols and maintain routing tables according to the network changes. The AODV protocol takes advantage of its cache facility and utilizes information stored in caches. In fact, information becomes more useful in caches when there are fewer changes or changes at slow pace in the network.

VI. CONCLUSION AND FUTURE WORK

This paper addresses the performance comparison of two table driven protocols namely DSDV and AODV specially designed for MANETs. Instead of comparing these protocols based on traffic load and number of connections, it was analyzed considering the participants in MANET and their speeds. Furthermore, importance of pause-time interval was also highlighted. As a matter of fact, mobile nodes are not always moving in MANETs, instead they move from one direction to another at their possible maximum speeds. Due to this reason four mobility models were designed, namely FCM, SCM, HRM and HWM. Each model represents a particular case in which a node moves at a particular speed. For example, if a MANET is deployed in a shopping mall then its participants are human and there is an upper limit on which they can walk or run. These eye-witnessed real-world speeds and pause-time values were used to analyze the performance of two protocols.

Finding-1: It was observed that DSDV gives same throughput as AODV does in SCM, HRM and HWM models. Even in FCM, with pause-time 100 and 450, DSDV gives better results than AODV.

Finding-2: Reactive protocols may have degradation in performance with high node density and network connections, whereas this is not an issue in reactive protocols, because already found routes are used efficiently in these kind of protocols.

Finding-3: AODV has better End-to-End delay than DSDV does, hence it can be used to provide support for real-time applications. In current implementation of DSDV, drop-tail queuing scheme is used without

bounded buffers. Therefore, DSDV can also improve this parameter with bounded buffers if implemented.

Finding-4: AODV has higher protocol overhead than DSDV, this is because reactive protocols depend on number of network connections. AODV reduces its protocol overhead in HRM and HWM models and comes closer to the performance of DSDV.

Based on these findings, it can be said that DSDV has scope in MANETs even it is rated lower in previous simulations. Especially in HRM and HWM models, it can be used because in these models nodes move slowly and may have higher delays in choosing next point.

In this paper, four pause-time values (0, 10, 100 and 450) are taken to compare DSDV and AODV protocols. For more realistic results and analysis other possible pause-time values should also be taken and considered. Other protocols such as DSR, WRP and TORA should also be compared and analyzed with respect to speeds and pause-time values studied in this paper.

REFERENCES

- [1] Ashwini K. Pandey, "Study of MANET routing protocols by GloMoSim simulator," *International Journal of Network Management*, pp. 393-410, 2005.
- [2] C. R. Dow, "A Study of Recent Research Trends and Experimental Guidelines in Mobile Ad-Hoc Networks," in *Proceedings of 19th International Conference on Advanced Information Networking and Applications, IEEE*, vol. 1, pp. 72-77 March 2005.
- [3] S. Corson and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", *IETF MANET Working Group RFC -2501*, January 1999.
- [4] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das, and Mahesh K. Marina, "Performance comparison of two on-demand routing protocols for ad hoc networks," *IEEE Personal Communications*, vol. 8, no. 1, pp. 16-28, February 2001.
- [5] A. Boukerches, "Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks," *Mobile Networks and Applications*, vol. 9, pp. 333-342, February 2004.
- [6] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," in *Proceedings of the ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications, London, UK*, pp. 234-244, September 1994.
- [7] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing". *IETF MANET Working Group RFC-3561*, July 2003.
- [8] Y. Lu, W. Wang, Y. Zhong, and B. Bhargava, "Study of distance vector routing protocols for mobile ad hoc networks," in *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications. IEEE Computer Society*, p. 187, 2003.
- [9] Nils Aschenbruck, "Human Mobility in MANET Disaster Area Simulation - A Realistic Approach," *29th Annual IEEE International Conference on Local Computer Networks*, pp. 668-675, November 2004.
- [10] Wikipedia encyclopedia, "Orders of magnitude (speed)", Available: http://en.wikipedia.org/wiki/Orders_of_magnitude_%28speed%29 [Accessed April. 12, 2006]

Analysis of small world phenomena and group mobility in ad hoc networks

Sonja Filiposka, Dimitar Trajanov and Aksentii Grnarov

Dept. of Computer Sciences

Faculty of Electrical Engineering and Information Technology

University Ss. Cyril and Methodious Skopje

Skopje, R. Macedonia

filipos@etf.ukim.edu.mk

Abstract – The main application of wireless mobile ad hoc networks is to offer services for situations wherein groups of people come together and share information. The groups of people that use the ad hoc network form some kind of social network. In this paper an analysis of the performances of mobile ad hoc networks is performed when taking into consideration its social characteristics through the small world phenomena of the application layer and usage of group-based mobility. The simulations show that the social interconnection between the network users has an extreme influence on the network performances. The results bring forth a different view on the real life deployment of ad hoc networks when compared to the poor performances of the purely randomized scenarios.

I. INTRODUCTION

Mobile hosts such as notebook computers are now easily affordable and are becoming quite common in everyday business and personal life. At the same time, network connectivity options for use with mobile hosts have increased dramatically, including support for a growing number of wireless networking products based on radio and infrared. With this type of mobile computing equipment, there is a natural desire and ability to share information between mobile users. In areas in which there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use, wireless mobile users may still be able to communicate through the formation of an ad hoc network. A few examples include: military soldiers in the field; an infrastructure-less network of notebook computers in a conference or campus setting; and temporary offices such as campaign headquarters. An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of any existing network infrastructure or centralized administration.

The people that come together and form an ad hoc network in order to share information are also part of some social network. Since most human communication takes place directly between individuals, such networks are crucially important for communications. This sociological concept is the basis for the small world research, which describes the tendency for each entity in a large system to be separated from any other entity in the system by only a few steps [1]. From this point of view, most of the communication between the entities is done inside the friends group while the necessity to communicate with a non friend is scarcely rare.

Mobile devices are usually carried by humans, so the movement of such devices is necessarily based on human decisions and socialization behavior. Please note that movement is strongly affected by the needs of humans to socialize in one form or another. Fortunately, humans are known to associate in particular ways that can be mathematically modeled, and that are likely to bias their movement patterns. Thus, it is important to model the behavior of individuals moving in groups and between groups, as is likely in the typical ad hoc networking deployment scenarios. In order to capture this type of behavior, it is necessary to define models for group mobility that are heavily dependent on the structure of the relationships among the people carrying the devices.

In this paper the small world driven communication in combination with an appropriate group mobility model is observed. The main goal is to observe the performances of the ad hoc network when the real social network formed by the network users affects both the application layer and the physical clustering of the socially aware moving nodes, i.e. campus collaboration or military campaign [6].

The remainder of this paper is organized as follows. In Section 2, the interaction between the small world concept and ad hoc network is described. Section 3 describes used simulation methodology, starting with application protocol, then the applied mobility model, scenarios' characteristics and performance metrics. In Section 4 results from simulations of various scenarios are shown. In Section 5 conclusions according to the obtained results are presented.

II. RELATED WORK

In most of the articles on ad hoc network performances traffic in a randomly connected nodes environment is considered. Johansson et al. [2] made a performance analysis by simulating three realistic scenarios that include rescue operations in remote areas, ad-hoc networks between notebook computers used to spread and share information among the participants of a conference; and short range ad-hoc network intercommunication of various mobile devices (e.g., a cellular phone or PDA).

When considering ad hoc networks and their employment, the first necessity that arises is to take into account the node's mobility features. However, because of their intrinsic nature ad

hoc networks are more than just ordinary networks with mobile nodes. Their utilization is completely dependent on the way the network is utilized by its users. In [10] and [11] the social aspects of the users of the network are imprinted in the mobility model designed for ad hoc networks.

The way the ad hoc network users interact has influence on the network performances in different ways. The user interaction defines the mobility model for the mobile nodes, but also defines the communication pattern between the mobile nodes. Thus, in [3] an application layer with clustering is used in order to investigate the performances of ad hoc networks and in [4] and [5] the effects of small world phenomena clustering on performances of ad hoc networks are observed.

II. MODELING AD HOC NETWORK USERS

Watts [7] has shown that the connection topology of some biological, technological and social networks is neither completely regular nor completely random but stays somehow in between these two extreme cases. This particular class of networks, named small worlds in analogy with the concept of the small-world phenomenon observed by Milgram more than 30 years ago in social systems [1], are in fact highly clustered like regular lattices, yet having small characteristic path lengths like random graphs.

A. Small World Communication Pattern

Small world networks are promising candidates for communication networks since data-flow patterns show a large amount of clustering with a small number of "long-distance" communications that need to be accomplished efficiently [8]. This is a result of the fact that people tend not so much to have friends as to have groups of friends, each of which is like a little cluster based on shared experience, location, or interests. These groups are joined to each other by the overlaps created when individuals in one group also belong to other groups [9]. Most of the communication between the entities is done inside the friends cluster while the necessity to communicate with a non friend is scarcely rare.

Since the people that form a communication network are interconnected in a small world fashion, this interconnection reflects in the source-drain distribution in the ad hoc network they use as a tool for their communication. As a result we can not observe the ad hoc network as a collection of randomly interconnected nodes, nor consider its features using pure random traffic generators. The coupling topology of the social network of the ad hoc users results into a different, small world, approach in the application layer modeling of the ad hoc network communication. That is, the application layer has information about the user's friends since the user communicates only with them. Thus, the user's social network is expressed on the application layer and is called logical network or application layer network.

B. Physical Proximity Modeling

The underlining ad hoc network is called physical network and may be different from the application layer network. Take

notice that in most of the cases the users from the same social network also share physical proximity in the ad hoc network. Thus, very often, the physical and logical networks are overlapping. For an example, when considering a deployment of an ad hoc network for campus students, where each student represents an ad hoc network node, we can view the established ad hoc network logical and physical grouping:

1. logical – the study groups created and interleaved via the students friends that belong to different study groups

2. physical – the movement of each student, which complies to the movement of each study group.

Since most of the communication will be between the participants of the same study group, here we have a classical example of physical and logical groups overlap. The same discussion can be done for a number of different examples of practical ad hoc network establishment.

When reviewing the physical network, it is clear that node mobility is an intrinsic characteristic of ad hoc networks. Thus, the study of ad hoc networks performances in presence of appropriate node mobility represents a fundamental stage of the designer process. In lack of available established ad hoc network, the natural approach is to use a synthetic mobility model in combination with simulations. The mobility model for ad hoc networks should respond to the real life movements of the nodes. That is, in correlation with the many possibilities for ad hoc network deployment, we need a model that will allow representation of the movement of campus students, group of tourists in an urban scenario, rescue groups on the field...

In order to simulate the group mobility behavior of the ad hoc network users, we use the group-based mobility model proposed in [10] that is aware of the social clustering of the network users [11]. In particular, the model allows collections of hosts to be grouped together in a way that is based on social relationships among the individuals. This grouping is only then mapped to a topographical space, with topography biased by the strength of social ties. Individuals move within the sphere of influence of the geographic group with which they are associated at any given point in time.

A host belonging to a group moves inside the corresponding group area towards a goal (i.e., a point randomly chosen in the group space) using the standard Random Way-Point model. It is worth noting that groups also move towards randomly chosen goals in the simulation space. Each group moves with a random speed (with a value contained in a predefined range); moreover, each host moves with a randomly generated different speed (once again, contained in a predefined range). Therefore, the movement of a host that belongs to a group is the result of the composition of these speeds. When two groups meet, each member of one of the groups may leave its group and join the other determined with a given probability.

III. SIMULATION METHODOLOGY AND PARAMETERS

For analyzing the performances of mobile ad hoc networks, NS-2 network simulator [12] was used, since it has proven to be one of the most accurate and popular network simulators [13]. At the physical layer, a radio propagation model

supporting propagation delay, omni-directional antennas, and a shared media network interface are used. The IEEE 802.11 Medium Access Protocol is employed at the Link Layer level and the transmission range is set to 250m. AODV routing protocol [14] in combination with UDP are used.

A. Parameters

The logical small world network is generated with the proposed generation algorithm in [5]. Input parameters for the proposed model are: number of groups (clusters) U , number of nodes per cluster M , average degree of node d , and percentage of in-cluster communications a . The algorithm result is an $N \times N$ connection matrix, where N is the total number of nodes (users) and $N = M * U$. The first M nodes belong to first cluster; the nodes with numbers $M + 1$ to $2M$ belong to second cluster, etc. First, in each cluster $M * d * a$ links between randomly chosen nodes are created. After that $N * d * (1-a)$ links between nodes belonging to different clusters are created. By the means of the algorithm it is possible to model a wide range of social groups i.e. from highly interconnected to strictly independent.

The values of the parameters for the logical network generation model are: number of clusters $U = 4$, number of nodes per cluster $M = 25$, average degree of node $d = 12$ and the percentage of in-cluster communications a is varied from 0% to 100%.

The mobility model employed is the group-based mobility model discussed in section II-B. The nodes are moving with speeds varying by a maximum of $\pm 0.001\text{m/s}$ from the chosen speed of the group, which is held constant at 1, 2, or 5 m/s.

B. Scenario Characteristics

In the simulations, nodes are placed in a square-shaped area of $1\text{km} \times 1\text{km}$. The four sub areas, in which the total simulation area is divided, are $0.5\text{km} \times 0.5\text{km}$ each. When physical clustering exists, the four groups of 25 nodes are placed in a different sub area each, and are allowed to move only within its borders.

When there is no physical clustering, all 100 nodes are randomly scattered in the whole area, and are free to move across the whole simulation area. On the other hand, logical clustering is achieved through our custom made application layer protocol, which makes it possible for the nodes to distinguish between nodes that belong to the same logical cluster (nodes they can communicate with), and nodes from other logical clusters.

When logical clustering is used (i.e. the network manifests small-world characteristics), nodes send messages to their friends only (nodes from the same logical cluster). In the opposite case (the random traffic scenario), destination nodes are randomly chosen from the whole population of nodes, regardless of the logical cluster they belong to.

All scenarios are tested with offered load from 0.1Mbps to 7Mbps.

C. Ad Hoc Network Performance Metrics

For ad hoc network performance measuring using the small world application layer in combination with the group mobility model, the following performance metrics are used: end-to-end throughput and clustering performance factor. The end-to-end throughput represents the total amount of bits received by all nodes per second and is measured in bits per second (bps). In order to quantify the impact of clustering to performance of the ad hoc network we use the clustering performance factor (CPF) defined as the ratio of achieved end-to-end throughput with clustering and end-to-end throughput without it (here we have random traffic on application layer and random movement on the physical layer).

IV. SIMULATION RESULTS

Several sets of simulations were made in order to investigate the behavior of mobile ad hoc networks and the impact of their small-world properties to the network performances.

A. Logical and physical clustering impact on end-to-end throughput

In the first set of scenarios, the impact of small-world phenomenon on the performance of mobile ad hoc networks was investigated. Four different scenarios were simulated:

1. Logical clustering with physical clustering (L-1 P-1), i.e. all nodes from a given logical cluster are placed in the same physical cluster;
2. Logical clustering with no physical clustering (L-1 P-0), i.e. nodes from certain logical cluster are randomly placed in the whole area;
3. No logical clustering, but physical clustering only (L-0 P-1), i.e. there are no logical clusters and nodes are placed like in the first scenario;
4. Neither logical, nor physical clustering (L-0 P-0), i.e. no logical clusters and nodes are randomly scattered in the whole simulation area.

In the scenarios with logical clustering, 83% of communications are between nodes of the same cluster and 17% are between nodes of different clusters.

Fig. 1, 2, 3 and 4 present the impact of node mobility for the four different clustering scenarios. The cases when the nodes are static, and are moving with speed of 1, 2 or 5 m/s are shown. Please take into consideration that the vertical axes are not in the same range. It can easily be concluded that the scenario where clustering exists on both logical and physical layer shows the best performances. Even more, while the other scenarios, when clustering exists in one and lacks in the other layer, show great dependence on the node mobility, the scenario for l=1 and p=1 performs very similarly for different node speeds. An interesting remark is the network performance for the case of static nodes. The performances rise for small offered load, and rapidly decrease for higher load as a result of the node immobility. For higher loads there is a significant number of packets throughout the network and it is very difficult to successfully send a packet from one to the other end of the network area. However, when the nodes are moving

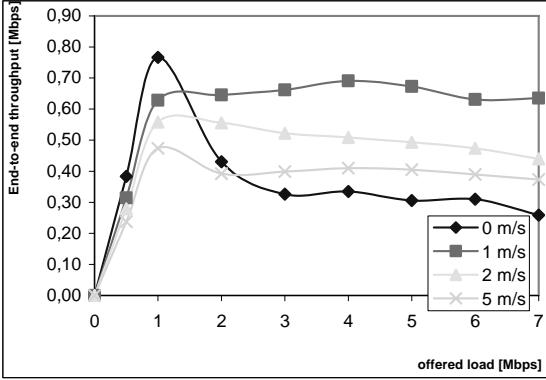


Fig. 1. Impact of the node speed on end-to-end throughput depending on the offered load for $L=1$ and $P=0$

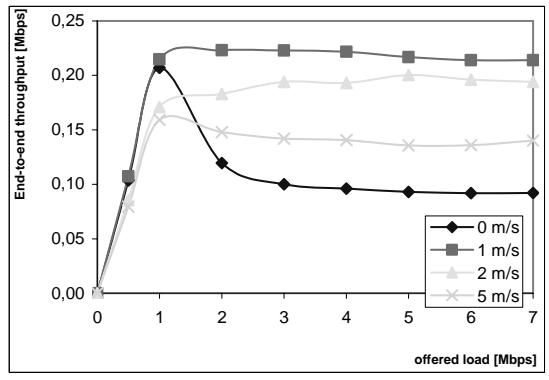


Fig. 2. Impact of the node speed on end-to-end throughput depending on the offered load for $L=0$ and $P=1$

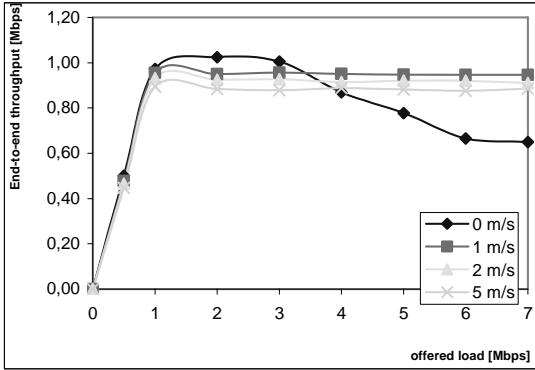


Fig. 3 Impact of the node speed on end-to-end throughput depending on the offered load for $L=1$ and $P=1$

relatively slow, the possibility that in some period of time the two nodes that communicate are going to be in range of one another, or are in a small number of hops distance, is very big, thus making the performances of the network rise.

B. Node speed impact in different clustering coefficient

In order to investigate the end-to-end throughput dependency on the in-cluster communications percentage, a second set of scenarios was created. In all scenarios, nodes are logically and physically clustered, with the in-cluster communication percentage varying from 0% to 100%.

Fig. 5 presents the impact of node speed on network performances when all of the communication takes place inside the cluster. Here, the network performance is the greatest for static nodes because of the fixed short source-destination routes.

Again for greater offered load this performance decreases because of the need for a greater number of transmissions in the group area. On Fig. 6 the clustering performance factor is represented for the case of 100% in-cluster communication,

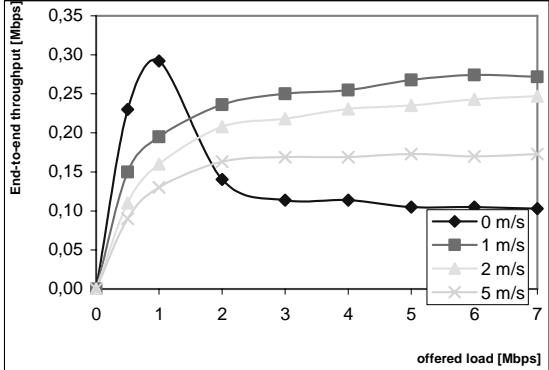


Fig. 4. Impact of the node speed on end-to-end throughput depending on the offered load for $L=0$ and $P=0$

and it can easily be concluded that the performances are around 5 times greater when compared to the random scenarios. For the static case, the performances increase up to 15 times.

Fig. 7 represents the impact of node speed on the network performances in the case of 50% in-cluster communication, while on Fig. 8 the clustering performance factor for the same scenario is shown. It is interesting to notice, that while the performances of the network rapidly decrease when considering static nodes, the performances of the network for mobile nodes increase up to 10 times when compared to the random scenarios.

Fig. 9 and Fig. 10 present the impact of node speed on the network performances for 0% of in-cluster communication. In this case, it can be observed that the network performances are very low when the nodes are static, especially when the offered load rises, since now all of the communication is being done with members of other groups and it always includes longer source-destination routes for the packets. Also, in this case the impact of the node speed is more significant.

When taking into consideration all of the phenomena shown on this group of figures it can be concluded that in the case of

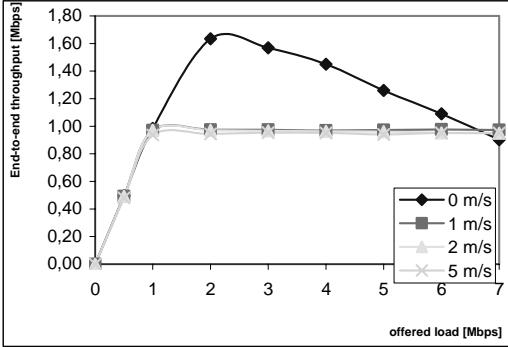


Fig. 5. Impact of node speed on end-to-end throughput depending on the offered load for 100% in-cluster communication

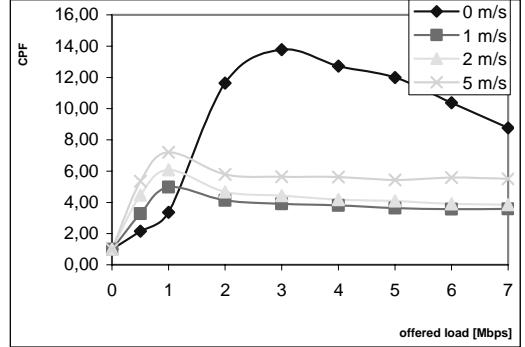


Fig. 6. Clustering performance factor for 100% in-cluster communication and various node speeds depending on the offered load

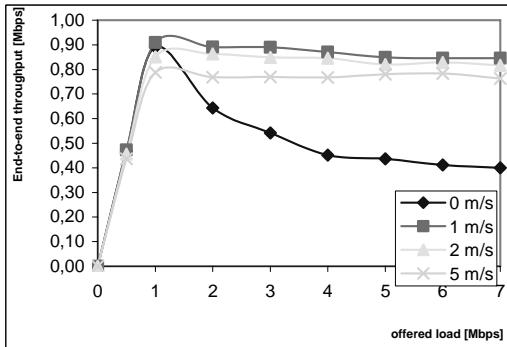


Fig. 7. Impact of node speed on end-to-end throughput depending on the offered load for 50% in-cluster communication

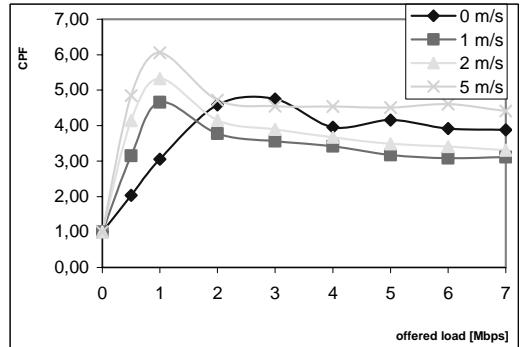


Fig. 8. Clustering performance factor for 50% in-cluster communication and various node speeds depending on the offered load

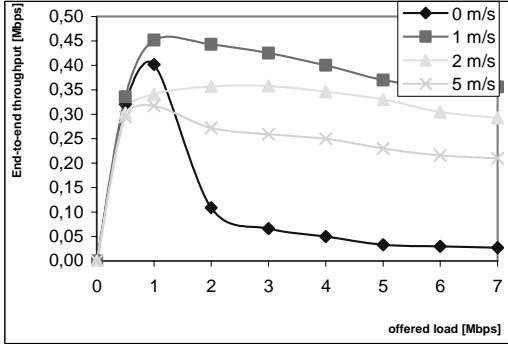


Fig. 9. Impact of node speed on end-to-end throughput depending on the offered load for 0% in-cluster communication

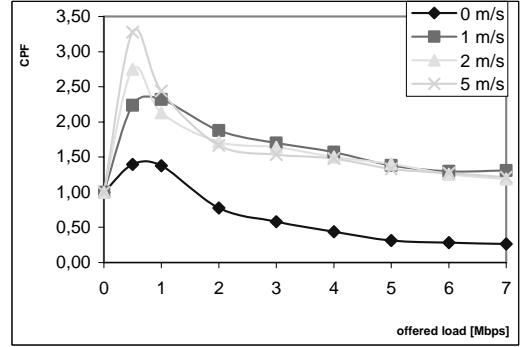


Fig. 10. Clustering performance factor for 0% in-cluster communication and various node speeds depending on the offered load

static network, where the nodes are not moving, performances of the network are rising with the in-cluster coefficient, from the worst performing network for 0% in-cluster communication, where it is better to have mobile than static nodes, to the best performing network for 100% in-cluster

communication where the results show that the static network is the one with best performances.

Also, the impact of node mobility is evidently closely connected to the in-cluster communication, from having minimum impact for the case when all of the messages are

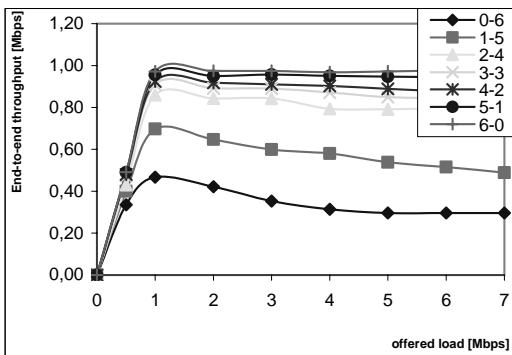


Fig. 11. End-to-end throughputs for various in-cluster communications percentage depending on the offered load

passed between the nodes from the same group, to the last example, when the node speed has significant influence on the network performances when all of the messages are passed between nodes from different groups. The example for 50% of in-cluster communication is, in a way, the break point of the above mentioned tendencies.

C. Impact of different clustering coefficient

Fig. 11 shows the impact of in-cluster communications percentage on end-to-end throughput when considering both physically and logically clustered network with nodes moving with an average speed of 1 m/s. The first scenario (100%), in which all communications are between nodes from the same logical and physical cluster, shows highest end-to-end throughput due to the decreased interference between wireless transmissions and the possibility of parallel communications in different clusters when the nodes that communicate are on distance greater than the transmission range. In the other scenarios, the end-to-end throughput decreases along with the decreasing of the percentage of communications between nodes in the same cluster. The network performances are especially improved when considering social networks with high in-cluster communication which is to be expected for the social network of the ad hoc network users.

V. CONCLUSION

Analyzing real social networks in combination with the real life possible applications of ad hoc networking it can easily be concluded that clustering appears in both application and physical level. The results in this paper show that when taking in consideration the impact of the underlining social network formed by the ad hoc users on the source-drain distribution of the network packets and on the community based node mobility, the ad hoc networks performances are significantly changed when compared to the randomized scenarios usually employed.

REFERENCES

- [1] Milgram S., "The small world problem", *Psychology today* 2, pp. 60-67, 1967
- [2] P. Johansson, T. Larsson and N. Hedman, "Scenario-based performance analysis of routing protocols for mobile ad-hoc networks", *Mobicom '99* Seattle Washington USA
- [3] D. Trajanov, S. Filiposka, J. Makraduli and A. Grnarov, "Small world application layer for ad hoc networks", *TELFOR 2003*, Serbia, 2003
- [4] D. Trajanov, S. Filiposka and A. Grnarov, "Impact of clustering in different layers on performance for ad hoc wireless networks", *ETAI VI nat. conf. 2003*, Ohrid, Macedonia, 2003, pp103-109
- [5] D. Trajanov, S. Filiposka and A. Grnarov, "Small world phenomena and performances of wireless ad hoc networks", *SETIT 2004*, Tunisia, 2004
- [6] R. Malladi and D. P. Agrawal, "Current and future applications on mobile and wireless networks", *Communications of the ACM*, Vol. 45, No. 10, October 2002
- [7] D. J. Watts, *Small Worlds: The Dynamics of Networks between Order and Randomness*, Princeton University Press, 2003
- [8] F. Comellas, J. Ozon, "Deterministic small-world communication networks", *Inform. Process. Lett.*, pp. 83-90, November 2000
- [9] D. J. Watts, *Six Degrees: The Science of a Connected Age*, W.W. Norton & Company, New York, 2003
- [10] M. Musolesi and C. Mascolo, "A community based mobility model for ad hoc network research", *REALMAN '06*, pp 31-38, Italy, 2006
- [11] M. Musolesi, S. Hailes and C. Mascolo, "Social networks based ad hoc mobility models", *Proc. of the 7th ACM int. sym. on Modeling, analysis and simulation of wireless and mobile systems*, pp 20-24, Italy, 2004
- [12] The network simulator - NS-2
Available: <http://www.isi.edu/nsnam/ns>
- [13] D. Cavin, Y. Sasson and A. Schiper, "On the accuracy of MANET simulators", *POMC'02*, October 2002
- [14] C. E. Perkins, *Ad hoc On-Demand Distance Vector (AODV) Routing Protocol*, internet draft, November 2002

Handoff Management Schemes for HCN/WLAN Interworking

Srinivas Manepalli, and Alex A. Aravind, *Member, IEEE*

(manepal, csalex)@unbc.ca

University of Northern British Columbia,
Prince George, BC, CANADA V2N 4Z9.

Abstract — Recent trends in wireless technology indicate that the future wireless networks will be the integration of two dominant evolving technologies namely cellular network and wireless local area network (WLAN) offering public wireless broadband services to end users. Wireless mobile users want high quality of service (QoS). One of the factors directly affecting QoS is the number of call drops and therefore it has to be reduced or eliminated if possible to achieve high QoS. The number of call drops experienced by a system mainly depends on its channel assignment and handoff schemes. There are two types of handoffs in such integrated networks: (i) *horizontal handoff* - handoff between the cells in the same layer; and (ii) *vertical handoff* - between the cells in different layers. Vertical handoff can be further divided into two types: *downward vertical handoff* - handover from a cell in higher layer to a cell in lower layer; and *upward vertical handoff* - handover from a cell in lower layer to a cell in higher layer. WLANs are in the lowest layer of the interworking.

In this short paper, first we propose two simple and efficient upward vertical handoff schemes for HCN/WLAN interworking. Then modifications to random walk mobility model are presented in order to closely emulate the realistic mobility in the systems. We also conducted a simulation study to observe the performance of our proposed handoff schemes. The results illustrate that these schemes reduce the number of handoffs and system overhead in HCN/WLAN interworking.

I. INTRODUCTION

A. Background

Recent trends in wireless technology indicate that the future wireless networks will be primarily hybrid resulting from the integration of two dominant evolving technologies namely cellular network and wireless local area network (WLAN) and offering public wireless broadband services to end users [3,4,5]. The characteristics of these two technologies nicely complement each other in achieving the current visions of future wireless technology.

In cellular networks, the network region is divided into smaller units called cells. Each cell has a fixed communication support node called base station (BS) at its center. These BSs are generally connected by wires. The users of the network can be either stationary or mobile. Radio frequency spectrum is used as the medium of communication and it is divided into channels for multiple users. A group of channels is assigned to each BS and the BSs are responsible for assigning channels to their users. The group of channels assigned to one cell must be different from the group of channels assigned to its neighboring cells in order to avoid channel interference. Since

the frequency spectrum available to a cellular network is limited, the channels have to be optimally assigned to its users, in order to achieve effective communication across the network. The high demand for the mobile communications in daily life has driven the cellular network technology to an extensive growth. Present day 3G cellular networks are able to provide all packet oriented services including live streaming, video conferencing, downloading, and web browsing besides its regular voice services in its larger coverage. If a mobile user moves from one cell to another cell with an active service, then the channel from the old base station is disconnected, and a channel from the new base station is required to continue the service. This process of channel reassignment is called a *handoff*.

A local area network (LAN) is a computer network covering a local area, like a home, office, or group of buildings and the nodes in the network are generally connected by wires. The main characteristics of a LAN are higher data rates, smaller geographic range, and it does not require high cost leased telecommunication lines. WLAN typically extends an existing wired local area network and they are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter.

Hierarchical cellular network (HCN) is introduced mainly to increase the system capacity, by handling the users based on their speed [1]. In HCN, group of smaller cells are overlaid by a larger cell. Smaller cells or micro cells are normally having a radius of 300 m to 1 km and larger cells or macro cells (also known as umbrella cells) are having a radius of 1 km to 3 km. Since micro cells are smaller in size, a fast user can cross more number of micro cells causing more number of handoffs. In order to reduce these handoffs, in HCN, fast users are served by macro cells and slow users are served by micro cells. There are two types of handoffs in hierarchical cellular networks: (i) *horizontal handoff* - handoff between the cells in the same layer; and (ii) *vertical handoff* - between the cells in different layers. Vertical handoff can be further divided into two types [8]: *downward vertical handoff* – handover from a cell in higher layer to a cell in lower layer; and *upward vertical handoff* - handover from a cell in lower layer to a cell in higher layer.

Though Hierarchical layers of macro-micro can support data rates up to 2Mbps, this is not generally enough to the increasing user needs. On the other hand WLANs are able to

provide high data rates up to 54 Mbps (for IEEE 802.11g, HIPER-LAN/2) at low cost. The WLAN coverage is normally 100 m in outdoor and 30 m indoor [2]. By considering WLANs smaller coverage area with high data rates and low cost, and HCN larger coverage area with low data rates and high cost, industry is concentrating increasingly on HCN/WLAN integration to benefit from each other.

This paper deals with the problem of handling upward vertical handoff in HCN/WLAN interworking. A vertical handoff in HCN/WLAN interworking occurs when a user with an active service moves from either WLAN to HCN (upward) or from HCN to WLAN (downward). As mentioned before, in HCN, fast users are served by macro layer and slow users are served by micro layer. When a user from WLAN moves into HCN, a channel has to be assigned either from macro layer or from micro layer in such a way to reduce the handoffs and system overhead.

B. Motivation

Wireless mobile users want high quality of service (QoS). One of the factors directly affecting QoS is the number of call drops and therefore it has to be reduced or eliminated if possible to achieve high QoS. The number of call drops experienced by a system mainly depends on its channel assignment and handoff schemes. Since majority of the WLANs are deployed in the areas like hotels, cafés, airports, offices, etc., the speed of the users are generally normalized within a range while entering the WLAN, and then they become either stationary or less mobile within the WLAN coverage area [14]. In HCN/WLAN interworking, a user can enter either from micro layer or from macro layer of HCN. Similarly, user can be handed over to either micro layer or macro layer of HCN based on whether slow or fast. In HCN, user speed is the primary factor to determine whether a user is fast or slow and that information is subsequently used to handle vertical handoff. Since the speed information about the users are not directly available when they are within WLAN coverage area, the vertical handoff schemes employed in hierarchical cellular networks are not directly suitable for solving vertical handoff problem in HCN/WLAN interworking. This brings us to many questions.

- Assume that the speed of each user in a WLAN coverage area is within a small threshold value. Normally, when a user is outside WLAN coverage area, the type of the user, whether fast or slow, is determined based on the user speed. How to determine the type of user, whether fast or slow, when the user is within the WLAN coverage area?
- A fast user can become slow user temporarily due to various conditions such as traffic signals, turns, etc. Does the speed alone sufficient to determine whether a user is slow or fast? If not, (i) what other parameters can be used to determine whether a user is fast or slow and (ii) how they can be obtained?
- Most simulation studies use random walk to model the users' mobility in the system, mainly for its simplicity and generality. In random walk model, since speed, direction, and distance for each leg are chosen randomly, the overall

speed of a user is also fluctuates randomly. Also, choosing random direction results in sharp turns. This behavior is not realistic in most practical cases. So, how to tune the random walk model to capture a more realistic user mobility while retaining the generality and simplicity of random walk model?

C. Contributions

In this short paper, we address the questions raised in the motivation section: (i) by presenting two simple upward vertical handoff schemes for HCN/WLAN interworking; and (ii) proposing modifications to random walk mobility model. We also conducted a simulation study to observe the performance of our proposed schemes. The results illustrate that these schemes reduce the number of handoffs and system overhead in HCN/WLAN interworking.

D. Organization

The rest of the paper is organized as follows. The proposed handoff schemes are given in section II. Section III discusses simple modifications to random walk mobility model. The simulation study is presented in section IV. Section V concludes the paper.

II. PROPOSED HANDOFF SCHEMES

This section describes the upward vertical handoff schemes proposed for HCN/WLAN interworking. That is, we propose schemes to choose proper layer in HCN for handoff when a user with an active service leaves WLAN. For our discussion, we refer the region outside WLAN coverage area as the *HCN only coverage area*. We propose two schemes to handle upward vertical handoff in HCN/WLAN interworking: one is based on the user speed in HCN only coverage area and the other is based on the speed in HCN only coverage area and the history of handoffs. In both schemes, a slow user is given to micro cell and the fast user is given to macro cell in HCN.

Scheme I: First we describe a naïve upward vertical handoff scheme which will be used later for comparison purpose. In this scheme, the current speed of the user in WLAN coverage area is used to identify whether a user is slow or fast, and then slow users are assigned to micro cells and fast users are assigned to macro cells in HCN. A predetermined threshold speed v_{th} is compared with the observed speed v_c to determine whether a user is fast or slow. As indicated earlier, since majority of the WLANs are deployed in the areas like hotels, cafés, airports, offices, etc., their speed is normally below a small threshold value and therefore most or all users are identified as slow users.

Scheme II: The motivation for speed based upward vertical handoff scheme comes from the observation that the speeds of a user in HCN coverage area before and after spending time in WLAN would be normally similar. So the expected future speed of a user in HCN coverage area can be inferred from the speed of the user before entering WLAN. Since the speed of a

user in the surrounding area of WLAN is generally normalized, it would be better to observe the speed beyond that surrounding area. We propose to use the speed of the user well before entering WLAN coverage area. Then, when a vertical upward handoff is needed, this speed is used to determine whether the user is fast or slow. For example, the speed of the leg before entering the WLAN coverage area can be used. If the speed of a user before entering WLAN is not available, the user is categorized as fast or slow based on the current speed.

Scheme III: For many reasons, a fast user can become slow user temporarily. Therefore, it is possible that a fast user can be incorrectly categorized as slow user if the speed is determined during this temporary slow down periods. In order to alleviate this problem, we propose to use the history of actual handoffs (h_{ac}) and the estimated handoffs (h_{ex}) of a user. The expected number of handoffs is computed, based on a threshold speed and a mean cell residence time, for a given period. For each user, if $h_{ac} > h_{ex}$, then the user is identified as fast user irrespective of the speed. If $h_{ac} < h_{ex}$, then user speed (determined in scheme II) is used to categorize whether the user is fast or slow. In summary, a user is identified as either slow or fast as follows.

- If $h_{ac} > h_{ex}$, and $v_c > v_{th}$ ----- user is fast
- If $h_{ac} < h_{ex}$, and $v_c > v_{th}$ ----- user is fast
- If $h_{ac} > h_{ex}$, and $v_c < v_{th}$ ----- user is fast
- If $h_{ac} < h_{ex}$, and $v_c < v_{th}$ ----- user is slow

Basically, as mentioned in [7], mostly there will be a similarity in a users' daily routine and behavior, like daily going to work, mostly traveling in vehicle, have a habit of less talk, etc. With the help of users' regular behavior, one can categorize a user as either fast or slow with respect to a given threshold value. In this paper, we use the number of handoffs incurred in the past as the history information. There are two interesting cases: (i) history of handoffs in the current call up to the recent downward vertical handoff and (ii) history of handoffs in previous calls in a fixed period of time. We deal with the case (i) in this paper.

Now the question is how to estimate the expected number of handoffs in the current call for each user. For this we adopt and tune the estimation scheme proposed in [9] to compute the expected handoffs for a call. Since the estimation is required in the middle of the call in our case, that is when the user is in WLAN coverage area, we consider the current call up to the recent downward vertical handoff in HCN/WLAN interworking as a logical call and compute the expected handoffs for this logical call. We introduce the following definitions.

- **Logical call duration** is the time between the initiation of current call and the time of most recent

downward vertical handoff in HCN/WLAN interworking.

- **Cell residence time** for a call is the sum of cell residence time in HCN only coverage area and cell residence time in WLAN coverage area.

We list the notations used to derive the expected number of handoffs in TABLE 1.

TABLE I
NOTATIONS

Parameter	Description
t_l	Logical call duration
t_c	Complete call duration
t_r	Cell residence time for a call
t_{COA}	Cell residence time in HCN only coverage area
t_{WA}	Cell residence time in WLAN area
t_{WAI}	Cell residence time in ith WLAN
t_{vh}	Time at HCN to WLAN vertical handoff
t_{st}	Start time of a call
D_c	Mean travel distance per cell
V_{th}	Threshold speed
h_{ex}	Expected handoffs for a call

The handoffs are estimated as follows. According to [9],

$$h_{ex} = \frac{t_c}{t_r} \quad (1)$$

We are interested in handoffs only during the logical call duration $t_l = t_{vh} - t_{st}$.

Replacing the complete call duration t_c with logical call duration t_l , we get the expected number of handoffs as follows.

$$h_{ex} = \frac{t_{vh} - t_{st}}{t_r} \quad (2)$$

To compute the cell residence time, we first compute the cell residence times for HCN only coverage area and the cell residence time in WLAN coverage area separately and then combine them to get the total cell residence time.

$$t_r = t_{COA} + t_{WA} \quad (3)$$

The cell residence time in HCN only coverage area is computed as follows.

$$t_{COA} = \frac{D_c}{V_{th}} \quad (4)$$

The WLAN residence time for a call is the average of all the WLAN residence times the user has traveled and it is computed as follows.

$$t_{WA} = \frac{\sum_{i=1}^n t_{WAI}}{n} \quad (5)$$

Substituting (4) and (5) in (3), we get the following equation.

$$t_r = \frac{D_c}{V_{th}} + \frac{\sum_{i=1}^n t_{WAI}}{n} \quad (6)$$

Substituting (6) in (2), we get the following equation for expected number of handoffs for a logical call duration with threshold speed.

$$h_{ex} = \frac{\frac{t_{vh} - t_{st}}{V_{th}}}{\frac{D_c}{V_{th}} + \frac{\sum_{i=1}^n t_{WAI}}{n}} \quad (7)$$

This expected number of handoffs along with the observed user speed can be used to determine whether a user is slow or fast.

III. CONTROLLED RANDOM WALK MOBILITY MODEL

To address the last question regarding unrealistic speed and direction fluctuations in random walk model, posed in the motivation section, we propose simple modifications to random walk mobility model, and we refer it as *controlled random walk mobility model*. In random walk mobility model, each user makes a sequence of *leg* travels. For each leg, distance, direction, and speed are chosen randomly from given distributions. In our speed controlled random walk model:

- To reduce the speed variation, a small offset within a range $(-\delta, \delta)$ is chosen and added to the current speed. Then this new speed is used for the next leg.
- To avoid sharp turns, an offset within a range $(-0, \theta)$ is chosen and added to the current direction. Then this new direction is used for the next leg.
- When a user is within a threshold distance to a WLAN, then the probability of user to enter the WLAN is set high.

An example snapshot of user mobility using controlled random walk is given in Fig. 2.

IV. SIMULATION STUDY

We conducted a simulation study to observe the performance of our proposed schemes. We are primarily interested in studying the number of handoffs. We conducted experiments by varying call arrival rate and number of calls.

A. Simulation Setup

We assume that a macro cell overlays seven micro cells and each micro cell has a WLAN in its center. Also, we assume that all the users in WLAN are completely stationary or low mobile. Total numbers of calls are uniformly distributed in all

the micro cells at the time of call arrival.

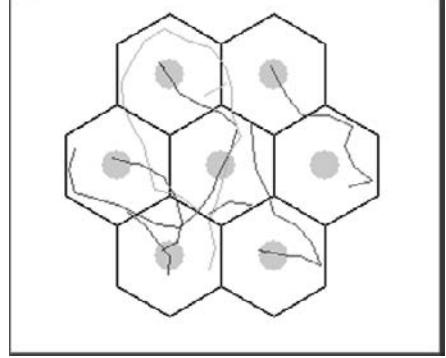


Fig. 2 Snapshot of user Mobility

We have considered 1000 users in our system. The user mobility is modeled based on controlled random walk mobility model proposed in Section III. We chose $\delta = 2$ for slow users and $\delta = 4$ for fast users, and $\theta = 45^\circ$. The mean speed of the fast user and slow user, respectively, are 15 m/sec and 5 m/sec. Each user is assigned to one of the following categories:

Category 1: Probability of being a fast user is 80%, and probability of being a slow user is 20%.

Category 2: Probability of being a fast user is 20%, and probability of being a slow user is 80%.

Category 3: Probability of being a fast user is 50%, and probability of being a slow user is 50%.

The set of parameters used in our simulation are given in TABLE II.

TABLE II
SIMULATION PARAMETERS

parameter	Description	Values
<i>mr</i>	Micro cell radius	400 m
<i>WR</i>	WLAN radius	100 m
λ_{da}	Mean of call duration	300 sec
λ_{wr}	Mean WLAN residence time	120 sec
λ_a	Call arrival rate	1 – 10sec
λ_{leg}	Mean distance of each leg	135 m
v_{th}	Threshold speed	10 m/sec

We used the following distributions.

- Poisson distribution with mean λ_a for call arrival times.
- Exponential distributions, with mean λ_{da} for call durations, with mean λ_{leg} for leg distance, and with mean λ_{wr} for WLAN cell residence time.
- Uniform distribution with given ranges for leg direction and user speed.

C. Simulation Experiments and Observations

We conducted two experiments for the schemes given in section II. The results obtained below are the average of each parameter for 100 simulation runs.

Experiment 1: In this experiment we have computed the average number of handoffs generated for a set of calls with different call arrival rates. The obtained results for three schemes are shown in Fig. 3.

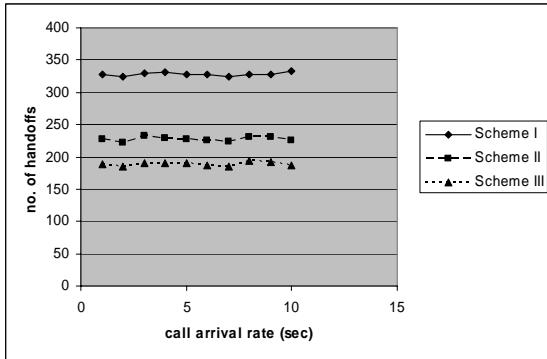


Fig. 3

Observation: From Fig.3, we can observe that the number of handoffs in Scheme II is significantly low compared to Scheme I. Using the additional information of the history of handoffs in Scheme III further reduces the future handoffs as evidenced from its performance.

Experiment 2: In this experiment, we computed the average number of handoffs for different set of calls. Fig. 4 shows the performance of the three schemes.

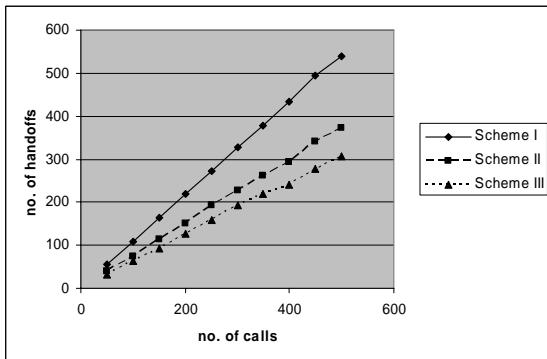


Fig. 4

Observation: As the number of calls increases, the number of handoffs also increases. However, the rate of increase for Schemes II and III are consistently low compared to the rate of increase in Scheme I. Also, this experiment combined with experiment I confirms that Schemes II and III reduces the handoff significantly in HCN/WLAN interworking.

V. CONCLUSION

Handoff is a fundamental problem in wireless communication systems. In [15], the authors considered network resources in addition to users' speed for vertical handoff in CN-WLAN interworking. In [13], authors considered threshold speed for each layer (Pico, micro, macro, and satellite). Based on the current speed of the user, the call is allocated to the proper layer. Vertical handoff schemes for HCN can be found in [10, 11, 12, 16].

In this short paper, first we proposed two simple and efficient upward vertical handoff schemes for HCN/WLAN interworking. Then modifications to random walk mobility model are presented in order to closely emulate the realistic mobility in the systems. We also conducted a simulation study to observe the performance of our proposed schemes. The results illustrate that these schemes reduce the number of handoffs and system overhead in HCN/WLAN interworking significantly. Such reduction in the number of handoffs has the advantage of both reducing the overall system overhead and increasing the quality of service.

REFERENCES

- [1] Yang Xiao and Guizani M., "Paging load balance in hierarchical cellular networks," *Proc. of the IEEE Globecom*, vol. 5, Dec. 2005.
- [2] Axiotis D.I, Al-Gizawi T., Peppas K., Protonotarios E.N, Lazarakis F.I, Papadias C, and Philippopoulos P.I, "Services in interworking 3G and WLAN environments," *IEEE Wireless Communications*, vol. 11, no.5, pp. 14 – 20, Oct. 2004.
- [3] Salkintzis A. K and Fors C. Pazhyannur R, "WLAN-GPRS integration for next-generation mobile data networks," *IEEE Wireless Communications*, vol. 9, no. 5, pp. 112 – 124, Oct. 2002
- [4] Falowo E. O and Chan A, "AAA and Mobility Management in UMTS-WLAN Interworking," *Proc. of the 12th International conference on telecommunications*, ICT, May 2005.
- [5] Seongsu Park, Donghahk Lee, Sunggun Kim, Jongtae Ihm, and Sehyun Oh, "A Performance Evaluation of Handoff Method between WLAN and cdma2000 1x Ev-DO System," *Proc. of IEEE ICNICONSMCL*, 2006.
- [6] Stevens-Navarro E., Wong V.W.S., "Comparison between Vertical Handoff Decision Algorithms for Heterogeneous Wireless Networks," *IEEE vehicular technology conference*, vol. 2, pp. 947 – 951, 2006.
- [7] Eun Kyung Paik and Yanghee Choi, "Prediction-based fast handoff for mobile WLANs," *IEEE 10th international conference on telecommunications*, ICT, vol. 1, pp. 748 – 753, March 2003.
- [8] Tansu F. and Salamah M., "On the vertical handoff decision for wireless overlay networks," *Proc. Of 7th IEEE International Symposium on Computer Networks*, ISCN, pp. 111 – 115, June 2006.
- [9] Nanda S., "Teletraffic models for urban and suburban microcells: cell sizes and handoff rates," *IEEE Transactions on Vehicular Technology*, vol. 42, no. 4, pp. 673 – 682, Nov. 1993.
- [10] Jabbari B and Fuhrmann W.F, "Teletraffic modeling and analysis of flexible hierarchical cellular networks with speed-sensitive handoff strategy," *IEEE Journal on selected areas in communications*, vol. 15, no. 8, pp. 1539 – 1548, Oct. 1997.
- [11] Lagrange X. and Godlewski P., "Performance of a hierarchical cellular network with mobility-dependent hand-over strategies," *IEEE 46th vehicular technology conference*, vol. 3, pp. 1868 – 1872, 1996.
- [12] Valois F. and Veque V., "QoS-oriented channel assignment strategy for hierarchical cellular networks," *11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, PIMRC, vol. 2, pp. 1599 – 1603, 2000.
- [13] Ying-Hong Wang, Hui-Min Huang, Chih-Peng Hsu, "Handoff strategy for multi-tier IP-based wireless network," *IEEE 17th International Conference on Advanced Information Networking and Applications*, AINA, pp. 790 – 793, 2003.

- [14] Wei Song, Hai Jiang, Weihua Zhuang, and Xuemin Shen, "Resource management for QoS support in cellular/WLAN interworking," *IEEE Network*, vol. 19, no. 5, pp. 12 – 18, 2005.
- [15] Hasswa A., Nasser N., and Hossanein H., "Generic vertical handoff decision function for heterogeneous wireless," *IEEE Second International Conference on Wireless and Optical Communications Networks*, IFIP, pp. 239-243, 2005.
- [16] Nasif Ekiz, Tara Salih, Sibel Küçüköner, and Kermal Fidanboyulu, "An Overview of Handoff Techniques in Cellular Networks", International Journal of Information Technology, Vol. 2, No. 3, 2005.

Cross-Layer Fast and Seamless Handoff Scheme for 3GPP-WLAN Interworking

SungMin Yoon

Dept. of Computer Science
Yonsei University
Seoul, KOREA
smyoon@emerald.yonsei.ac.kr

SuJung Yu

Dept. of Computer Science
Yonsei University
Seoul, KOREA
sues@emerald.yonsei.ac.kr

JooSeok Song

Dept. of Computer Science
Yonsei University
Seoul, KOREA
jssong@emerald.yonsei.ac.kr

Abstract— In this paper, we present new handoff scheme using a cross-layer design. We focus on 3GPP-WLAN Interworking architecture for mobile IPv6. Using new L2 trigger, the network layer can prepare for the L3 handoff. As results of performance analysis, the proposed handoff operation performs well with respect to handoff delay and packet loss compared with the conventional schemes. Therefore, our scheme can guarantee fast and seamless handoff for the 3GPP-WLAN Interworking.

I. INTRODUCTION

A variety of telecommunication access technologies have been developed continuously, and recently they have been integrated. A research on integrated wireless network among them is achieving widely. Most active research is the integration of Wireless Wide Area Networks (WWAN) which have sufficient infrastructure and Wireless Local Area Networks (WLANs) that needs increase continuously.

The third generation wireless communication technology like W-CDMA and CDMA2000 1X EV-DO support high mobility and seamless handoff, but the data transmission rate is relatively low. On the other hand, WLAN technology like IEEE 802.11a/b/g service high transmission rate, but the coverage is very restricted.

moves across over different types of wire/wireless networks are researched widely.

One of these interworking issues, the 3rd Generation Partnership Project (3GPP) [1], discusses interworking architectures that use a Mobile Internet Protocol (MIP) to provide seamless handoff between the Universal Mobile Telecommunication System (UTMS) and WLAN [1][2].

Another issue is a cross-layer approach. Each OSI 7 layer operates independently. However, today there are a lot of cross-layer researches which propose coordination of layers to operate efficiently, such as optimization between PHY and MAC [3], L3 handoff scheme using L2 trigger information [4][5].

Therefore, in this paper, we survey current standard techniques of interworking architectures for vertical handoff, and propose a cross-layer fast and seamless handoff scheme between 3GPP and WLAN Interworking architecture.

The remaining part of this paper is organized as follows. In section 2, we present related works. Our integrated network architecture and proposed handoff procedures in 3GPP-WLAN interworking are described in Section 3. Performance analysis and simulation results are presented in Section 4. Finally conclusions and future work are given in Section 5.

TABLE I. FEATURES OF WWAN AND WLAN

	WWAN		WLAN
	<i>Cdma2000 1X EV-DO</i>	<i>UMTS</i>	<i>IEEE 802.11 a/b/g</i>
Max. Transmission Rate (bps)	144K	2M	11~54M
Coverage Area (Km)	1~10	1~10	0.05~0.1
Transmission Direction	Duplex	Duplex	Duplex

Each technology has limitations, such as mobility and data transmission rate. In order to solve these problems, the seamless vertical handoff schemes which cannot only provide the same service but also maintain active connection as they

II. RELATED WORKS

A. Mobile IPv6

In MIPv6 (Mobile IPv6) is Internet protocol that enable MN (Mobile Node) to communicate with correspondent nodes out of home network. To communicate in new subnet, MN must get new CoA (Care-of-Address) and register HA (Home Agent) and CN (Correspondent Node) via BU (Binding Update) [6]. However, handoff delay is pretty big. To reduce such a handoff delay, the Internet Engineering Task Force (IETF)'s mobile IP workgroup suggest Fast Handovers for Mobile IPv6 [4].

"This work has been supported by the BK21 Research Program for the Next Generation Mobile Software at Yonsei University in Korea"

B. Fast Mobile IPv6

Fast Mobile IPv6 (FMIPv6) is classified into predictive mode and reactive mode. The difference is time when PAR recognizes NAR. The former recognize NAR information before L2 handoff and the latter know NAR after L2 handoff [4].

Figure 1 shows FMIPv6 predictive mode stage. We will use this scheme.

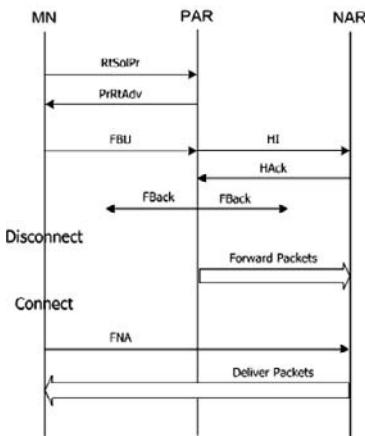


Figure 1. Predictive mode for FMIPv6

- 1) *RtSolPr / PrRtAdv* : MN send RtSolPr to PAR to get router information and PAR reply to MN with PrRtAdv (Proxy Router Advertisement) which contain at least one router information.
- 2) *FBU* : MN send PAR FBU (Fast Binding Update) to request handoff.
- 3) *HI / HAck* : PAR send HI(Handoff Initiate) to NAR as exchange message and receive HAck (Handoff Acknowledgement) as reply message.
- 4) *FBack* : PAR send FBack (Fast Binding Acknowledgement) to MN and NAR for acknowledgement.
- 5) *FNA* : MN send NAR FNA (Fast Neighbor Advertisement) to complete handoff.

C. Cross-Layer Optimization (MIPv6 using L2 information)

To change connection between heterogeneous network, MAC layer (L2) layer handoff which change actual access point and Network layer (L3) layer handoff which change data connection are required. During this time, the MN can't receive IP packet until completion of handoff. To reduce handoff delay, [7] and [8] use L3 information using L2 information additionally by cross-layer approach.

III. PROPOSED SCHEME

In this section, we introduce 3GPP specification based interworking architecture for our proposal, and describe our proposed elements. Then we propose the novel handoff scheme. It uses enhanced FMIPv6 using link layer information for the 3GPP-WLAN Interworking.

A. System Architecture

Our proposed 3GPP-WLAN interworking architecture is based on interworking network models of 3GPP standards documents [2]. After consideration of 3GPP-WLAN interworking reference models presented in [1], we were able to design the network architecture, as in Figure 2.

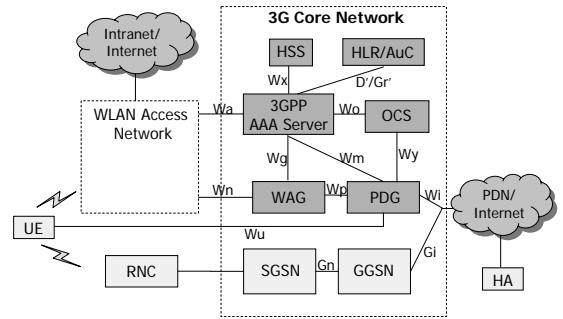


Figure 2. 3GPP-WLAN Interworking Architecture

The next is a brief description of Figure 2's components:

- *User Equipment (UE)* : The User Equipment (UE) is a mobile node that can communicate with both a WLAN access network and a 3GPP network.
- *WLAN Access Network (WLAN AN)* : The WLAN Access Network (WLAN AN) provides WLAN access services for the UE. It is not limited to any specific WLAN technology and may consist of several WLAN entities, such as Access Point (AP) and Access Point Controller (APC) [2]. The WLAN AN is connected to the 3GPP network via the WLAN Access Gateway (WAG) and to the 3GPP Authentication, Authorization, Accounting (AAA) server for the WLAN authentication process.
- *WLAN Access Gateway (WAG)* : The WAG is a gateway through which the data to/from the WLAN AN is routed.
- *Authentication, Authorization, Accounting (AAA) Server* : The 3GPP AAA server is located within the 3GPP network. There should be only one 3GPP AAA Server for a WLAN attached subscriber.

- **3GPP Core Network :** The 3GPP Core Network contains the Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Packet Data Gateway (PDG), AAA server, Home Subscriber Server (HSS), and Home Location Register/Authentication Center (HLR/AuC).
- **Gateway GPRS Support Node (GGSN) :** The GGSN serves as a gateway between the SGSN and the public data network (PDN).
- **Serving GPRS Support Node (SGSN) :** The SGSN performs the 3GPP authentication and interacts with the HSS/HLR.
- **Packet Data Gateway (PDG) :** The PDG routes the packet data received from/sent to the PDN and allows allocation of the WLAN UE's IP address.
- **HLR/HSS :** The HLR/HSS located within the 3GPP subscriber's home network is the entity containing authentication and subscription data required for the 3GPP subscriber to access the WLAN interworking service.

B. Link layer(L2) Information

A L2 trigger is information from the Link Layer used by the Network Layer. It allows L3 to quickly know information such as a sign of L2 connections. In our scheme, we use new L2 trigger called 'Link-To-Be-Down' besides 'Link-UP' and 'Link-Down' trigger. As using these L2 triggers by cross-layer approach, we propose more efficient handoff scheme than original handoff schemes.

- 1) **Link-Up trigger :** This event corresponds to the establishment of a new L2 link, which allows IP communication over it. This is typically a new connection between the MN and an AP.
- 2) **Link-To-Be-Down trigger :** This is a hint that the L2 link is about to go down. This information can be sent to the IP layer for example because the mobile may be receiving poor signal from its serving Access Point as a consequence of the node moving outside the coverage of that AP.
- 3) **Link-Down trigger :** This event corresponds to a L2 link that has been broken down. This typically happens when a current connection between the MN and an Access Point has been terminated.

C. The 3GPP-WLAN Mobile IPv6 Handoff Procedure

1) 3GPP to WLAN handoff

The detailed operation depicted in Figure 3, the handoff procedure from 3GPP to WLAN, may be explained by dividing the process into four parts as follows.

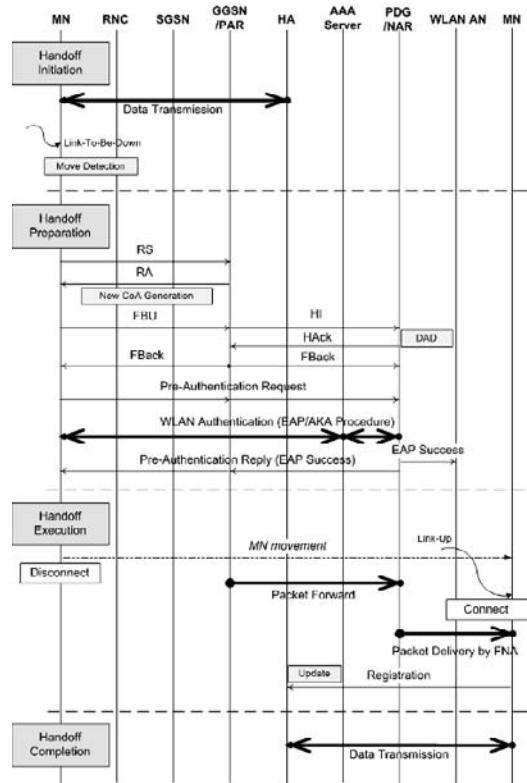


Figure 3. 3GPP to WLAN Handoff Procedure

a) Step1 : Handoff Initiation Phase

At the beginning, the MN communicates with the 3GPP network. So, a packet transmission route is formed between the HA and the MN through the 3GPP network entities. If the Link-To-Be-Down trigger occurs, it decides the acceptance or rejection of the handoff attempt into the WLAN AN.

b) Step2 : Handoff Preparation Phase

This step includes two parts. One part is an address configuration for fast handoff process, another is pre-authentication process prior to L2 handoff.

• Address configuration for fast handoff

Once occurred movement detection by Link-To-Be-Down trigger, the MN sends the RS message to the GGSN in order to fast handoff. Thereafter, it receives the RA message from the GGSN. This address configuration phase is the same to the FMIPv6 operations that are described in section 2.

• Pre-authentication

If the address configuration for fast handoff completed successfully, the MN transmits the pre-authentication request message to the GGSN and the GGSN relays it to the PDG of the WLAN in order to request WLAN authentication. The GGSN can deliver the request message to the PDG without error. This message contains the MN authentication information that is required for standard WLAN authentication [9]. If the PDG receives a pre-authentication request message, it begins the standard Extensible Authentication Protocol/Authentication and Key Agreement (EAP/AKA) procedure for WLAN authentication among the MN, PDG and AAA server [10]. At this point, instead of the WLAN AN, the PDG relays WLAN authentication messages between the MN and AAA server although the original WLAN authentication is performed through the WLAN AN [10]. If pre-authentication phase is completed successfully according to the standard authentication process, the EAP success is transmitted to the WLAN AN with authentication keying material. This WLAN AN memorizes the received EAP success information that corresponds to the pre-authenticated MN, in order to use it after the MN is attached to itself. The EAP success is also delivered to the MN via the pre-authentication reply message.

c) Step3 : Handoff Execution Phase

If both address configuration for fast handoff and pre-authentication phase are finished, the MN moves from 3GPP to the WLAN, and then the MN disconnects from the 3GPP network by using the L2 detachment process based on the 3GPP standard. Thereafter, it performs the WLAN attachment process by using standard WLAN association procedures. Namely, the L2 handoff is carried out from the 3GPP to the WLAN. During this attachment process, the WLAN AN can confirm that the MN is the pre-authenticated user from the previously received EAP success message. Therefore, the MN is able to communicate via WLAN AN immediately, without a further WLAN authentication process [9]. Once the MN disconnects from 3GPP network, the GGSN forwards the packets to PDG. Then the PDG delivers the packets to MN by FNA. If the packets are delivered successfully, the MN registers own location information to HA.

d) Step4 : Handoff Completion Phase

If the handoff execution phase completes successfully, then the entire handoff procedures are completed and the packet transmission route is formed through the WLAN AN. Now the MN communicates with the HA again, and can transfer data packets.

2) WLAN to 3GPP handoff

The handoff procedure that the MN uses to move from WLAN to 3GPP is depicted in Figure 4. This handoff procedure is also divided into four parts, and also it has similar

procedure as in the case of handoff from 3GPP to WLAN, except for the pre-authentication phase. When the MN handoffs from WLAN to 3GPP, pre-authentication is performed among the MN, SGSN and AAA Server based on the 3GPP authentication procedure. Because the 3GPP authentication is issued by the SGSN, the pre-authentication request message must be sent to the SGSN, and so the SGSN must process the 3GPP authentication and transmit the pre-authentication reply message to the MN following successful authentication. The remaining handoff procedure is the same to when the MN moves from 3GPP to WLAN described before.

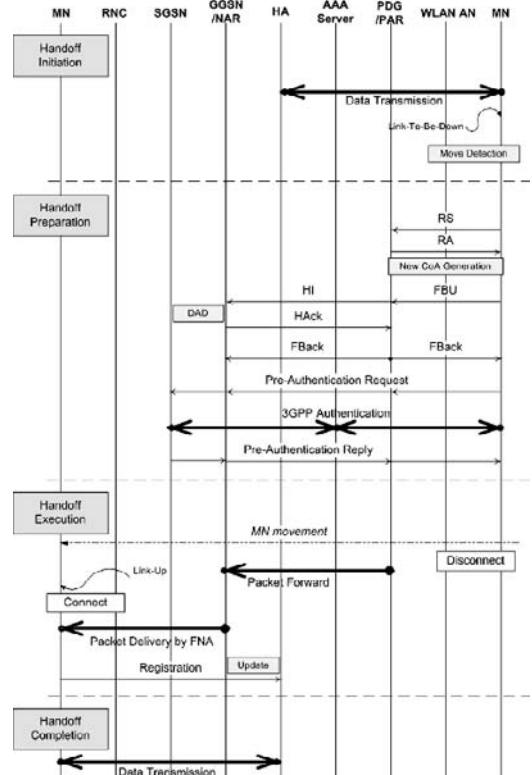


Figure 4. WLAN to 3GPP Handoff Procedure

IV. PERFORMANCE ANALYSIS

Due to real system performance depends on a lot of factors, such as network topology and location of entities, we must consider many factors to measure accurately handoff performance. Therefore, we investigate the overall performance with respect to handoff delay by using a simple analytic calculation.

A Figure 5 shows total handoff delays in each handoff scheme.

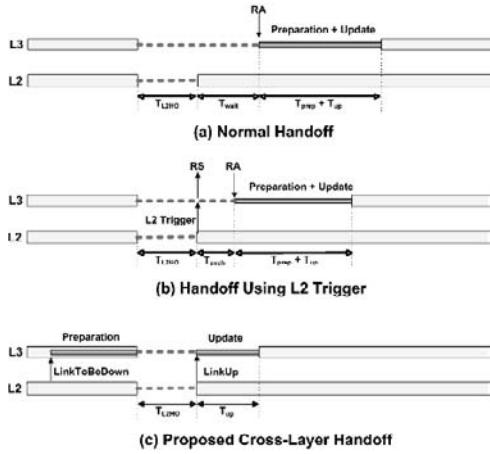


Figure 5. Handoff Schemes

We use a simple analytic calculation in order to evaluate the handoff delay under the following assumptions.

TABLE II. PARAMETERS FOR HANDOFF DELAY EVALUATION

D _{scheme}	Average total delay of each scheme
T _{L2HO}	Average delay needed for L2 handoff
T _{auth}	Average delay needed for 3GPP or WLAN authentication
T _{wait}	Average delay needed until L3 receives the RA message
T _{exch}	Average delay between RS and RA message exchange
T _{prep}	Average delay needed for preparation phase
T _{up}	Average delay needed for update phase

Figure 5.(a) shows the normal handoff scheme such as MIPv6. In the figure, "L2" and "L3" mean the link layer and the network layer in an MN, respectively. First, the L2 handoff occurs. However, the network layer can not detect the L2 handoff. In a short time, the MN receives the RA (Router Advertisement) message. The network layer starts L3 handoff. As shown in this figure, there is a delay between the time when the L2 handoff ends and the time when the network layer receives the RA message. In this case, average total delay is as follows:

$$D_{MIP} = T_{L2HO} + T_{auth} + T_{wait} + T_{prep} + T_{up}$$

Figure 5.(b) shows the handoff scheme using L2 information such as FMIPv6. In this figure, the link layer notifies the network layer of the end of the L2 handoff just after

the L2 handoff finishes. By receiving this notification, the network layer sends the RS message and receives the RA message. In this case, average total delay is as follows:

$$D_{FMIP} = T_{L2HO} + T_{auth} + T_{exch} + T_{prep} + T_{up}$$

Figure 5.(c) shows our scheme. The link layer notifies the network layer of a sign of the L2 handoff when the link layer detects that the link quality goes down below the threshold. Receiving this notification, the network layer executes the preparation phase, and then it requests the link layer to do the L2 handoff. The link layer notifies the network layer of the end of the L2 handoff just after the L2 handoff finishes. Receiving this notification, the network layer executes the signaling phase. As shown in the figure, it is possible to reduce the gap time caused by a handoff to the L2 handoff time plus the RTT between the MN and the HA. In this case, average total delay is as follows:

$$D_{Prop} = T_{L2HO} + T_{auth} + T_{up}$$

To evaluate the performance of the proposed scheme, we performed simulation using the Network Simulator 2 (NS-2) [11] and Mobiwan [12]. Using the analyzed total delay, we could obtain the packet loss performance during handoff. Table 3 shows our simulation parameters.

TABLE III. SIMULATION PARAMETERS AND VALUES

Parameters	Values
Simulation Time	250 sec
Velocity of Nodes	20 m/s
Number of Nodes	20
Capacity of WLAN	100 Mbps
Capacity of 3GPP	2 Mbps
Boundary	670 m X 670 m

Figure 6 shows the packet drop rates during simulation time. In this simulation, we assumed that twenty nodes moves with velocity of 20 meters per second from WLAN to 3GPP. Packet drop rate in MIPv6 is the highest among three handoff schemes because MIPv6 has the longest duration of packet loss during handoff. The proposed cross-layer handoff scheme shows the best performance because its duration of packet loss is shorter than that of the others. Therefore, the proposed scheme can guarantee a low packet drop rate.

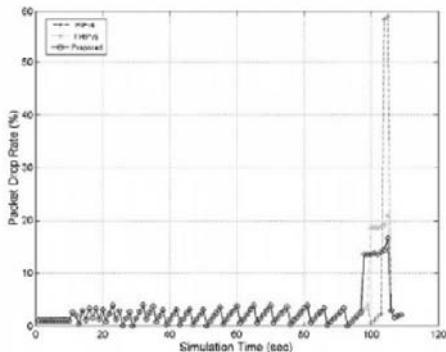


Figure 6. Simulation – Packet Drop Rate

V. CONCLUSIONS

To achieve a fast and seamless handoff in the 3GPP-WLAN interworking, this paper proposed new handoff scheme using a cross-layer design. In our scheme, the network layer can quickly know a sign of the L2 handoff by receiving an indication from the link layer in terms of a cross-layer approach, and then the network layer can prepare for the L3 handoff. After the pre-authentication and the preparation phase, the network layer can start the L2 handoff. Because the end of the L2 handoff is also notified to the network layer, the network layer can start the update immediately after the L2 handoff. As results of performance analysis, the proposed

handoff operation performs well with respect to handoff delay and packet loss compared with the conventional schemes. Therefore, the proposed handoff scheme is able to guarantee fast and seamless handoff supporting QoS and service continuity for the 3GPP-WLAN interworking.

In the future, we will work more simulations about signaling cost or other factors.

REFERENCES

- [1] 3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 7), 3GPP TS 23.234 v7.1.0, 2006-03.
- [2] www.3gpp.org
- [3] Luis Alonso, Ramón Ferrús, Ramón Agustí, "MAC-PHY Enhancement for 802.11b WLAN Systems via Cross-layering", IEEE 2003.
- [4] R. Koodli, Ed., "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.
- [5] Vineet Srivastava, "Cross-Layer Design: A Survey and the Road Ahead", IEEE Communications Magazine, December 2005.
- [6] P. McCann, "Mobile IPv6 Fast Handovers for 802.11 Networks", RFC 4260, November 2005.
- [7] Fang Zhu and Janise McNair, "Cross Layer Design for Mobile IP Handoff", IEEE 2005.
- [8] Nicolas Montavont and Thomas Noel, "Handover Management for Mobile Nodes in IPv6 Networks", IEEE Communications Magazine, August 2002.
- [9] G. M. Koien and T. Haslestad, "Security aspects of 3G-WLAN interworking," IEEE Commun. Magazine, vol. 41, no. 11, pp. 82-88, Nov.2003.
- [10] Yan Zhang and Masayuki Fujise, "Security Management in the Next Generation Wireless Networks", IJNS, vol.3, No.1, PP1-7, July 2006.
- [11] The VINT Project, "The Network Simulator - ns-2," available at <http://www.isi.edu/nsnam>.
- [12] <http://www.ti-wmc.nl/mobiwan2/>

Minimizing the Null Message Exchange in Conservative Distributed Simulation

Syed S. Rizvi, K. M. Elleithy

Computer Science and Engineering Department
University of Bridgeport
Bridgeport, CT 06605
{srizvi, elleithy}@bridgeport.edu

Asia Riasat

Department of Computer Science
Old Dominion University
Norfolk, VA 23529
ariast@cs.odu.edu

Abstract— The performance of a conservative time management algorithm in a distributed simulation system degrades significantly if a large number of null messages are exchanged across the logical processes in order to avoid deadlock. This situation gets more severe when the exchange of null messages is increased due to the poor selection of key parameters such as lookahead values. However, with a mathematical model that can approximate the optimal values of parameters that are directly involved in the performance of a time management algorithm, we can limit the exchange of null messages. The reduction in the exchange of null messages greatly improves the performance of the time management algorithm by both minimizing the transmission overhead and maintaining a consistent parallelization. This paper presents a generic mathematical model that can be effectively used to evaluate the performance of a conservative distributed simulation system that uses null messages to avoid deadlock. Since the proposed mathematical model is generic, the performance of any conservative synchronization algorithm can be approximated. In addition, we develop a performance model that demonstrates that how a conservative distributed simulation system performs with the null message algorithm (NMA). The simulation results show that the performance of a conservative distributed system degrades if the NMA generates an excessive number of null messages due to the improper selection of parameters. In addition, the proposed mathematical model presents the critical role of lookahead which may increase or decrease the amount of null messages across the logical processes. Furthermore, the proposed mathematical model is not limited to NMA. It can also be used with any conservative synchronization algorithm to approximate the optimal values of parameters.

Keywords— conservative distributed simulation, Lookahead, logical processes null messages, null message algorithm.

I. INTRODUCTION

This paper presents a mathematical model for a conservative distributed simulation system that uses null messages to avoid deadlock. The term distributed refers to distributing the execution of a single run of a simulation program across

multiple processors [1]. By distributing the execution of a computation across N processors, one can finish the computation up to N times faster than if it were executed on a single processor. Therefore, the main reason behind the use of distributed simulation is to reduce the overall simulation execution time.

One of the main problems associated with distributed simulation is the synchronization of distributed execution. If not properly handled, synchronization problems may degrade the performance of a distributed simulation environment [2]. Time management algorithms are, therefore, required to ensure that the execution of the distributed simulation is properly synchronized. Two main classes of time management algorithms are *conservative* and *optimistic*. This paper focuses on the performance issues related to the conservative null message algorithm (NMA) that uses null messages to avoid deadlock and provide synchronization among the logical processes (LPs). The selection of values for several critical parameters such as lookahead, null message ratio (NMR), and frequency of transmission plays an important role in the generation of null messages. If these values are not properly chosen by a simulation designer, the result will be an excessive number of null messages across each LP. This situation gets more severe when the NMA needs to run to perform a detailed logistics simulation in a distributed environment to simulate a huge amount of data as specified in “in press” [9]. This paper provides a quantitative criterion to limit an excessive number of null messages exchanged by predicting the optimal values of the critical parameters. The reduction in the null message exchange minimizes the transmission overhead and hence improves the overall system performance. In addition, we show that the performance of a conservative distributed simulation system degrades if the NMA generates an excessive number of null messages.

The rest of the paper is organized as follows. In section II, we provide an overview of the conservative protocols, focusing on the null message protocol (NMP) and its related problems. In section III, we derive the proposed mathematical model that approximates the optimal values of the key parameters. Section IV provides a comprehensive discussion on various optimizations that we have incorporated in our

proposed mathematical model. In addition, section IV gives a brief discussion on the numerical and simulation results. Finally, we conclude in section V.

II. RELATED WORK

Event synchronization is an essential part of parallel simulation. In general, synchronization protocols can be categorized into two different families: conservative and optimistic. Conservative protocols fundamentally maintain causality in event execution by strictly disallowing the processing of events out of timestamp order. The main problems faced in conservative algorithms are overcoming deadlock and guaranteeing the steady progress of simulation time.

Examples of conservative mechanisms include Chandy, Misra and Bryant's NMP [6], and Peacock, Manning, and Wong [11] avoided deadlock through null messages. The primary problem associated with null messages is that if their timestamps are chosen inappropriately, the simulation becomes choked with null messages and performance suffers. Some intelligent approaches to null message generation include generation on demand [8], and generation after a timeout [5]. Some earlier research on discrete event simulation has focused on variants of NMP, with the objective of reducing the high null message overhead. For instance, Bain and Scott [4] attempt to simplify the communication topology to resolve the problem of transmitting redundant null messages due to low lookahead cycles. Other recent developments [10] have focused on incorporating knowledge about the LP into the synchronization algorithms. Cota and Sargent [7] focused on the skew in simulation time between different LPs by exploiting knowledge about the LPs and the topology of the interconnections.

Although earlier work has aimed to optimize the performance of the NMA by proposing the variants of the NMP [3, 4, 8, 10], it has not addressed reducing the exchange of null messages that is caused by improper selection of the parameters. This paper provides a mathematical model that approximates the optimal values of parameters in order to minimize the null message exchange across the LPs, while still maintaining a consistent parallelization.

The principal problem is that the NMA uses only the current simulation time of each LP and the lookahead value to predict the minimum time stamp of messages it can generate in the future. These messages with the minimum time stamp are then used to avoid deadlock. As a result, if one of the important parameters such as the lookahead value is chosen poorly, the performance will degrade significantly due to an excessive number of null messages. However, the prediction of minimum time stamps of messages can be improved by understanding the relationship between the time stamp and the lookahead value. The proposed mathematical model helps designers to choose appropriate values for lookahead to intelligently generate the null messages.

III. MATHEMATICAL MODEL

A conservative distributed simulation environment involves synchronization overhead which is added due to the distributed nature of simulation. With NMA, this overhead is mainly associated with the transmission of null messages. Therefore, when comparing the performance of a conservative distributed simulation environment using NMA with the performance of sequential execution, the message overhead can make a significant performance difference between the two approaches. Before developing the mathematical model, it is worth mentioning some of our key assumptions.

A. Key Assumptions

- For NMA, we assume that the value of lookahead may change during the execution of a lookahead period. This assumption makes it easier to analyze the variation in null message overhead with respect to different values of lookahead.
- We assume that each LP is initialized with a constant event arrival or job intensity rate (i.e., a uniform distribution of event-messages). This assumption will be used to analyze the relationship of event arrival rate with the lookahead values.
- For the frequency of message transmission, we assume that all messages are equally distributed among the LPs. Unless otherwise stated, we use the term all messages to refer to both null and event messages.
- Finally, we assume that a fixed size message is transmitted between LPs.

B. Definition of System Parameters

All model variables, along with their definition, are listed in Table I. Based on NMA, we assume that each LP maintains two clock times, one for each of its input and output neighbors. One is the minimum receiving time (*MRT*) for the input neighbor LP and the second is the minimum sending time (*MST*) for the output neighbor LP. The *MRT* contains the minimum simulation time the LP can receive an event from an input neighbor LP, whereas the *MST* contains the minimum simulation time the LP might send a message to its output neighbor LP. These times play an important part in computing the timestamp for a null message. The performance (*P*) of a conservative distributed simulation environment mainly depends on the amount of computation required for processing an event per second. In addition, the event arrival rate (ρ) represents the number of events that occur per second (in practice, events occur per simulation second). Unlike performance, the parameter ρ mainly depends on the model. Lookahead (*L*) is measured in seconds. As mentioned earlier, the value of *L* changes over the execution of lookahead period. Frequency of transmission (F_T) is the frequency of sending a message from one LP to another. T_{Null}

represents the timestamp of a null message sent from one LP to another. T_{Null} is the sum of the current simulation time and the lookahead value. In other words, one may consider T_{Null} as an equivalent of MST for an LP (i.e., the value of T_{Null} is always updated by the sender LP to its current MST). This relationship can be expressed as: $T_{Null} = MRT + L$.

In order to measure the performance, it is imperative to consider one parameter that can compute simulation time advancement. As mentioned earlier, the performance is determined by the processing of a number of events per second whereas the event arrival rate is characterized by the number of events that occur per second. Taking these facts into account, the simulation time advancement can be defined as a ratio of performance to event arrival rate. This can be expressed mathematically as:

$$\text{Simulation Time Advancement} = STA = P/\rho \quad (1)$$

MRT represents the earliest time an LP can receive an event from its input neighbor. MRT is analogous to the clock associated with each incoming link of an LP. The value of MRT is updated through a null message coming from other LPs on the output link of a receiving LP. MST , on the other hand, represents the minimum time of an LP that may send a message to its output neighbor LP. A sender LP sends null messages to other LPs to avoid a deadlock situation. The timestamp for these null messages is determined by the current MST of that LP.

Each LP maintains a simulation time clock that indicates the timestamp of the most recent event processed by the LP. Any event scheduled by an LP must have a timestamp at least as large as the LP's simulation time clock when the event was scheduled [1]. This requirement is also referred as the local causality constraint. To strictly follow this requirement, a large number of null messages can be transmitted by LPs before the non null-messages can be processed. This large message overhead may degrade the performance of a conservative distributed simulation. It is, therefore, worth computing the ratio of null messages to the total messages transmitted among LPs. The null message ratio can be simply defined as the ratio of total number of null messages to total messages where total messages include both null and event messages. Mathematically, it can be expressed as follows:

$$\text{Null Message Ratio (NMR)} = \frac{\text{Total Number of Null Messages}}{\text{Total Messages}} \quad (2)$$

IV. OPTIMIZATION OF CRITICAL PARAMETERS VIA THE PROPOSED MATHEMATICAL MODEL

This section provides an analysis of the proposed mathematical model for a conservative distributed simulation environment. The numerical analysis provides several

TABLE I
System Parameter Definition

Parameter	Definition
P	Computation required for processing an event per second
ρ	Event arrival rate (events per second)
MRT	Minimum receiving time
MST	Minimum sending time
L	Lookahead
STA	Simulation time advancement
F_T	Frequency of transmission
T_{Null}	Timestamp of a null message
T_S	Current simulation of a LP
T_{Total}	Total simulation time in seconds

examples of parameters-optimization which are based on the mathematical equations and properties discussed above.

A. Impact of Null Messages On the Distributed Simulation Environment performance

Null messages are used to avoid deadlock in distributed simulation environment. As mentioned earlier, the computation of a null message involves the current simulation time of an LP and a lookahead value. The NMA performs well as a deadlock avoidance mechanism and gives good performance as long as the message overhead is not sufficiently high. The message overhead depends on the frequency of null message transmissions. Ignoring the fact that the transmission of null messages becomes essential when deadlock approaches in a distributed simulation environment, the value of lookahead also plays a critical role in increasing or decreasing the amount of null messages across the LPs. In other words, the value of lookahead is a design choice which should be appropriately chosen with respect to other system parameters.

For instance, consider the following simulation example that demonstrates the impact of lookahead on the overall performance of a system. Let a single LP process an event in 0.1 seconds and the rate at which events arrive be 0.25 events per second (i.e., events arrive for processing once every 4 seconds). In addition we compute event arrival rate by dividing the total number of event message to the simulation time. Mathematically, this can be expressed as:

$$\rho = \text{Total number of event messages}/T_{Total} \quad (3)$$

Using (1), one can easily approximate the STA . The value of STA can tell us how many null messages an LP needs to transmit to break a deadlock situation. For the above system parameters, the result would be $P/\rho = 40$. Thus this implies that 40 null messages are required to advance the simulation time to the next event. However, if we assume that the lookahead value is 10 times greater than the processing time value (i.e., $L = 0.1 \times 10 = 1\text{sec}$), then only approximately 4 null messages must be transmitted to avoid deadlock. In other

words, a lookahead of one second yields an increase in *MRT* of one simulation second per step as shown in Fig. 1. Similarly, a lookahead value, which approaches the processing time, may significantly degrade the overall performance of a conservative distributed simulation environment. This degradation in performance is evident in Fig. 1. It can be concluded from the simulation results shown in Fig. 1 that a large number of null messages must be transmitted in order to advance the simulation time of each LP if the value of lookahead is quite small compared to the mean simulation time. Note that the purpose of this example is to demonstrate the behavior of null message algorithm for different values of lookahead.

B. Characteristics of Event Arrival Rate and Lookahead

Observing the simulation results of Fig. 1, one can compute an ideal value of lookahead that minimizes the null message overhead while at the same time maintains an acceptable performance for a conservative distributed simulation environment. It can be seen that the number of null messages approaches 1 as the value of lookahead approaches the inverse of the event arrival rate. Thus, this leads us to the following hypothesis that the ideal value of lookahead should be at least equal to or greater than the inverse of the event arrival rate. Mathematically, this relationship can be expressed as follows:

$$\text{Lookahead}(L) \geq \text{inverse of } \rho \Rightarrow L\rho \geq 1 \quad \text{Property (1)}$$

For instance, if we assume that L is equal to 4 seconds and the event arrival rate is 0.25 events per second, then the result will be the transmission of only one null message and, thus improved performance.

C. Null Message Ratio

Another important relationship to be analyzed is the ratio of total number of null messages to the total messages per LP. Consider the following simulation example which shows the

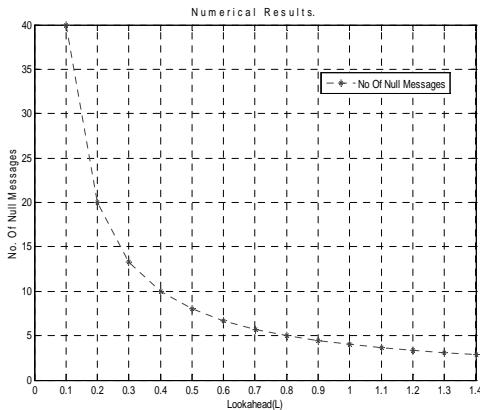


Fig.1. L versus number of null messages

variations in null message overhead with respect to event arrival rate, processing time, and the lookahead values. Let the processing rate of a single LP be 50 event messages per second (i.e., $P=50$ event messages per second = 0.02 second per event) and let the event arrival rate be 10 events per second computed using (3) (i.e., $\rho=0.1$ seconds between each event).

Using the lookahead value from the previous example (i.e., initially it is 10 times the processing time required by a single event), then the ratio of null messages to total messages can be computed using (2) as follows: When $L = 10$, $P = 10 \times 0.02 = 0.2$ seconds, the number of null messages that need to be transmitted is 50. We can interpret this numerical result as a lower bound for null message overhead as shown in Fig. 2. It should be noted that the value of L in this example is much less than the inverse of event arrival rate and this can be considered as one of the main reasons for the large number of null messages (a 50% null message ratio) and a lower bound of message overhead.

In other words, property (1) shows that the product of L and ρ should be greater than or equal to 1 in order to achieve better performance. Since for the above example, $STA = P/\rho = 0.2$ seconds per step (i.e., the value of *MRT* increases by 0.2 second in each transmission of a null message), the product of L and ρ is about 2, which conforms the characteristic of property (1). If the value of L linearly decreases during the execution of a lookahead period, the resultant performance will be degraded due to the increase in null message traffic as shown in both Table II and Fig. 2. The numerical results of Table II imply that in order to achieve good performance, the parameter L should not only satisfy property (1) but also remain stable (ideally growing with respect to simulation time).

D. Processing Rate and Null Message Overhead

In order to understand the relationship between processing rate and message overhead, consider the following example where we reduce the processing rate in the previous example by 50% (i.e., now a single LP can process 25 events per second). Furthermore, we use the same event arrival rate from the previous example using (3) (10 events per second). Given these changes, the new computation of null messages yields a reduction in null message overhead by 50% as shown in Fig. 3. This is because of the increase in the lookahead value that increases the *MRT* by 0.4 seconds per null message transmission instead of 0.2. Fig. 3 illustrates that the product of lookahead and the event arrival rate has significantly increased due to the reduction in the processing power of an LP. Thus, the increase in $L\rho$ ensures a better performance for a conservative distributed simulation environment.

E. Effects of Multiple LPs on the Performance

This section presents a brief discussion on the use of multiple LPs and its corresponding effect on the null message

overhead as well as on the overall system performance. Consider an example where four LPs are interacting together to perform tasks. If each LP processes 25 event messages, then four LP should process $25/4$ messages (recall one of our assumptions about uniform event message distribution) where each of them has an equal computing power (i.e., one event processing in every 0.04 seconds). This implies that an average of 6.25 events per second will be processed by each LP. In addition, as we have already seen in the previous example that a single LP processes one event message in 0.04 seconds, four LPs approximately accomplish the same job in 0.01 seconds. If we use the event arrival rate of 10 events per second, then the resultant STA will be approximately 0.1 seconds and consequently the required null message transmission will tend toward 100 messages. This numerical result demonstrates that the null message overhead grows as the number of LPs grows in the system. Mathematically this relationship can be expressed as:

$$(Null\ Message\ Overhead) \propto (Number\ of\ Neighbor\ LPs) \quad \text{Property (2)}$$

Where ' \propto ' represents the sign of proportionality.

In this example, although the number of null messages is increased significantly, the required execution time for the same number of events is also reduced 4 times. This numerical result is achieved since we distribute the execution of events across four LPs that complete the required processing up to four times faster than if it were executed on a single LP.

F. Frequency of Transmission and the Computational Power of an LP

Another important relationship that we should analyze in our analysis is the variation in the computational power of an LP with respect to the frequency of transmission of null messages. If we increase the message transmission between two LPs, the result will be reduced computing power for each LP (i.e., the number of event-messages processed per second per LP will be reduced). This is due to the fact that an increase in the message transmission between LPs forces the LPs to spend more time dealing with these messages instead of processing the real event-messages. Thus, this leads us to the following mathematical hypothesis:

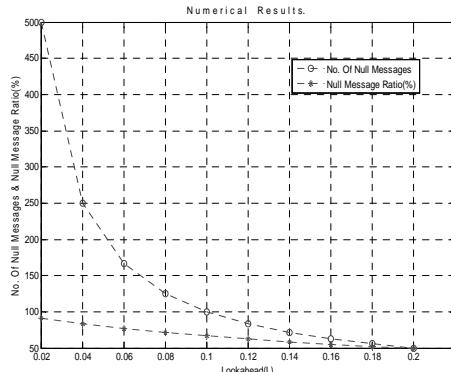


Fig.2. Frequency of transmission versus performance.

TABLE II
L Versus Null Messages and NMR (%)

Lookahead (L)	Null Messages	NMR (%)
0.020	500.000	90.900
0.040	250.000	83.330
0.060	166.660	76.920
0.080	125.000	71.420
0.120	83.330	62.400
0.160	62.500	55.000
0.180	55.550	52.000
2.00	50.000	50.000

$$\text{frequency of transmission} \propto \frac{1}{\text{computing power}} \Rightarrow F_T \propto \frac{1}{P} \quad \text{Property (3)}$$

Recalling (1), if we substitute the value of P , property (3) becomes,

$$F_T \propto 1/P \Rightarrow F_T \propto \frac{1}{STA} \rho \Leftrightarrow \frac{\rho STA}{P} \propto F_T \quad \text{Property (4)}$$

Or equivalently, property (4) can be written for performance such as:

$$P \propto \frac{\rho STA}{F_T} \quad \text{Property (5)}$$

If we assume that we have an average value for L (note that the value of L is considered to be poor if it is very small compared to STA), then it can be approximated as STA (i.e., $L \approx STA$ for an average case). Property (5) can now be written as:

$$P \propto \rho L / F_T \quad \text{Property (6)}$$

For instance, if we consider a large value of lookahead, for example, 10 seconds, and let the event arrival rate be 1000 events per second, then the number of events processed per seconds for a range of F_T can be computed using property (6), as shown in Fig. 4.

G. System Behavior with a Dormant LP

Distributed simulation that uses the null message algorithm assumes that the simulation environment consists of a collection of LPs that communicate with each other by sending and receiving time stamped messages. Each LP in distributed simulation environment maintains local state information and a list of time stamped events that have been scheduled for the LP. This list of scheduled events contains both internal and external events. The internal and external scheduled events are handled by separate queues. In addition, the LP never blocks on the internal queue containing messages it schedules for itself. However, if any of the external queues that have the smallest clock (i.e., MRT) are empty, the LP blocks. Thus, this implies that the system behavior that has a dormant LP is only

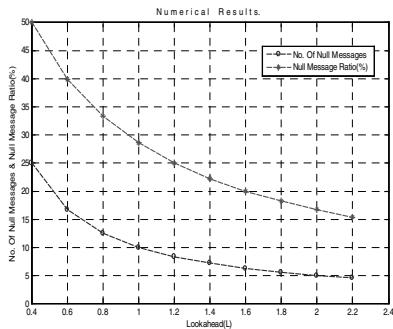


Fig.3. L versus null messages and NMR (%)

vulnerable to external events. In other words, the system remains stable and works smoothly if a single LP stops generating internal events as shown by the characteristics of the derived properties. However, the overall performance of the system may degrade slightly due to the passive state of an LP for internal events generation. On the other hand, in the presence of deadlock, the termination of external event generation by an LP can put the whole system in a non-continuous null message transmission cycle. Consequently, the whole system remains in the deadlock situation. This is because a finite cycle of null message transmission is required to avoid a deadlock situation. If this cycle does not go through, all the LPs, the deadlock situation will not be resolved. Finally, we believe that a single dormant LP does not have any severe effects on the performance if a system is working without a deadlock. But once a deadlock is reached, the dormant LP causes the cycle of null messages to stop.

V. CONCLUSION

We have proposed a mathematical model to predict the optimum values of critical parameters that have great impact on the performance of NMA. The derived properties of the proposed mathematical model account for the cases when the NMA would send too many null messages. The proposed mathematical model provides a quick and practical way for simulation designers to predict whether a simulation model has potential to perform well under NMA in a given simulation

environment by giving the approximate optimal values of the critical parameters. We have experimentally verified that if critical parameters, specifically the lookahead value, are chosen intelligently, we can limit the transmission of null messages among the LPs and consequently improve the performance of NMA in a distributed simulation environment. It is left to further studies to experimentally verify the implementation of the proposed mathematical model on other conservative synchronization algorithms.

REFERENCES

- [1] R. M. Fujimoto, "Distributed Simulation system," *preceding of the 2003 winter simulation conference*. College of Computing, Georgia Institute of Technology, Atlanta.
- [2] Y.M. Teo, Y.K. Ng and B.S.S. Onggo, "Conservative Simulation using Distributed Shared Memory," *Proceedings of the 16th Workshop on Parallel and Distributed Simulation (PADS-02)*, IEEE Computer Society, 2002.
- [3] B. R. Preiss, W. M. Loucks, J. D. MacIntyre, J. A. Field, "Null Message Cancellation in Conservative Distributed Simulation," *Distributed Simulation 91 Proceedings of the SCS Multiconference on Advances in Parallel and Distributed Simulation*, 1991.
- [4] W. L. Bain, and D. S. Scott, "An Algorithm for Time Synchronization in Distributed Discrete Event Simulation", *Proceedings of the SCS Multiconference on Distributed Simulation*, 19, 3 (February), pp. 30-33, 1988.
- [5] N. J. Davis, D. L. Mannix, W. H. Shaw, and Hartrum, T. C., "Distributed Discrete-Event Simulation using Null Message Algorithms on Hypercube Architectures," *Journal of Parallel and Distributed Computing*, Vol. 8, No. 4, pp. 349-357, April 1990.
- [6] K. M. Chandy and J. Misra, "Distributed Simulation: A case study in design and verification of distributed programs", *IEEE Transactions on Software Engineering*, SE-5:5, pp. 440-452, 1979.
- [7] B. A. Cota and R. G. Sargent, "An Algorithm for Parallel Discrete Event Simulation using Common Memory," *Proc. 22nd Ann. Simulation Symp.*, pp. 23-31, March 1989.
- [8] J. K. Peacock, J. W. Wong, and E. Manning, "Synchronization of Distributed Simulation using Broadcast Algorithms," *Computer Networks*, Vol. 4, pp. 3-10, 1980.
- [9] L. A. Belfiore, S. Mazumdar, and S. S. Rizvi et al., "Integrating the joint operation feasibility tool with JFAST," *Proceedings of the Fall 2006 Simulation Interoperability Workshop*, Orlando Fl, September 10-15 2006.
- [10] D. M. Nicol and P. F. Reynolds, "Problem Oriented Protocol Design," *Proc. 1984 Winter Simulation Conf.*, pp. 471-474, Nov. 1984.
- [11] J. K. Peacock, J. W. Wong, and E. Manning, "A Distributed Approach to Queuing Network Simulation," *Proc. 1979 Winter Simulation Conf.*, pp. 39 9-406, Dec. 1979.

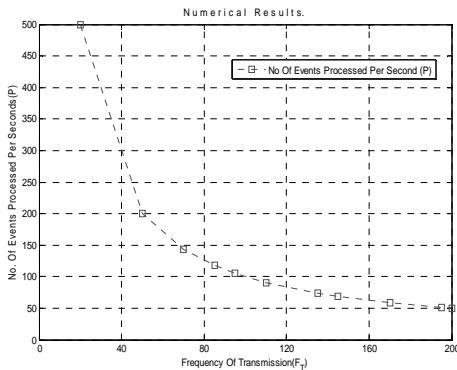


Fig.4. Frequency of transmission versus performance.

An Analog Computer To Solve Any Second Order Linear Differential Equation With Arbitrary Coefficients

T. ElAli, S. Jones, F. Arammash, C. Eason, A. Sopeju, A. Fapohunda, O. Olorode

Department of Physics and Engineering

Benedict College

1600 Harden Street

Columbia, SC 29204

Abstract

An analog computer was designed and tested to solve any second order constant-coefficients and linear differential equation. The analog computer was built using operational amplifiers, resistors and capacitors. Using the Multisim simulator, various input types were tested across the input terminals of the analog computer and the results were recorded.

I. INTRODUCTION

Our goal is to build a generic Operational Amplifier circuit to solve a generic 2nd order differential equation with any input. Consider the generic differential equation to be solved

$$a \frac{d^2}{dt^2} y(t) + b \frac{d}{dt} y(t) + c y(t) = x(t) \quad (1)$$

$x(t)$ is the forcing function (the input to the system represented by this differential equation) and $y(t)$ is the solution (the output of the same system). The variables a , b , and c are some real constant numbers. [1]

In the last equation, (assuming zero initial conditions) let $y_1(t) = y(t)$ and $y_2(t) = \frac{d}{dt} y(t)$. Thus we have the set of two first order differential equations

$$\begin{cases} \frac{d}{dt} y_1(t) = y_2(t) \\ \frac{d}{dt} y_2(t) = -\frac{c}{a} y_1(t) - \frac{b}{a} y_2(t) + \frac{1}{a} x(t) \end{cases} \quad (2)$$

II. METHODS

Consider the Operational amplifier circuit shown in Figure 1. The input-output relationship is given as

$$y(t) = -A \frac{1}{RC} \int x_1(t) dt - B \frac{1}{RC} \int x_2(t) dt \quad (3)$$

In Figure 1, the output $y(t)$ is the integral of the input arriving at the negative terminal of the Operational Amplifier. Thus the negative of the derivative of $y(t)$ is located at the negative terminal of the Operational Amplifier. [2]

If we set $RC=1$ in equation (3) we will have

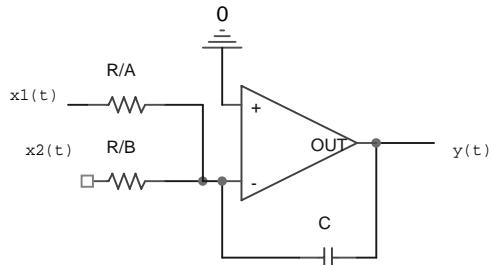


Fig. 1. Operational Amplifier Circuit

$$y(t) = -A \int x_1(t) dt - B \int x_2(t) dt \quad (4)$$

One final step before we attempt to implement Equation (4), the solution of a generic 1st order linear constant coefficient differential equation. Consider the circuit given in Figure 2. The input-output relationship is

$$y(t) = -\frac{R_f}{R} x(t) \quad (5)$$

You also can see that if $R_f = R$ then we have pure inversion (unity gain). The circuit containing an inverter and an integrator connected in series can solve the differential equation given in (6). Figure 3 is a typical example of such a circuit.

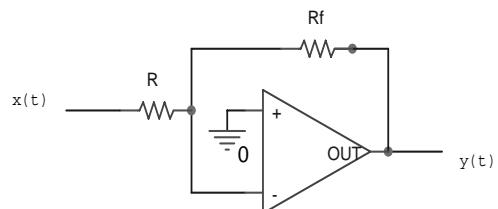


Fig. 2. Inverter

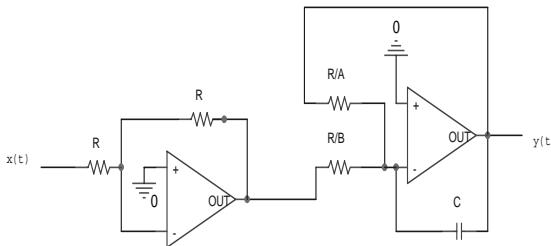


Fig. 3. A Circuit to Solve Equation 6

The circuit in Figure 3 would solve any first order differential equation of the form

$$y'(t) + Ay(t) = Bx(t) \quad (6)$$

Knowing how to solve equation (6) is helpful in solving the set of the two coupled equations in (2).

In building a circuit to solve the given differential equation in (1) we will use the set of equations in (2). We have tried step input, impulse input, and sinusoidal input. All worked nicely. In particular, we will consider the case when $x(t)$ is a unit step and pick two sets of values for a , b , and c in equation (1). One set will give us a system with real modes and the other will result in complex modes.

CASE I

If $a=1$, $b=4$, and $c=3$, the transfer function of the system will be

$$\frac{Y(s)}{X(s)} = \frac{1}{s^2 + 4s + 3} = \frac{1}{(s+3)(s+1)} \quad (7)$$

The modes are at -1 and -3 respectively. When the input is unit step of amplitude 3, the initial value of the output $y(t)$ should be zero and the final value should be 1. The circuit to solve this case is shown below in Figure 4 and the result is shown in Figure 5.

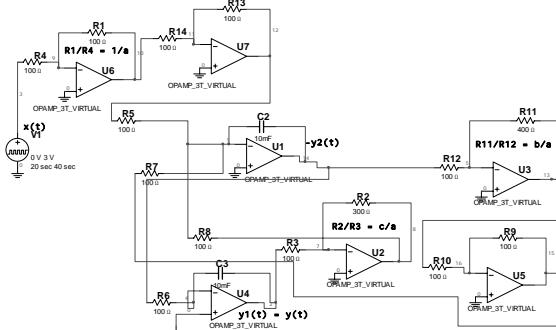
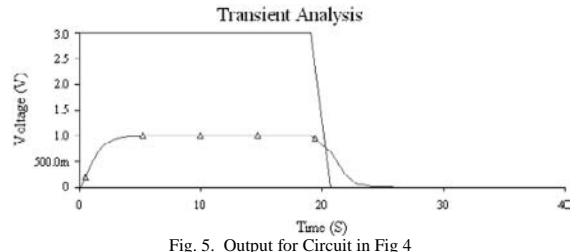
Fig. 4. Circuit to Solve: $\frac{d^2}{dt^2} y(t) + 4 \frac{d}{dt} y(t) + 3y(t) = x(t)$ 

Fig. 5. Output for Circuit in Fig 4

CASE II

If $a=1$, $b=1$, and $c=1$, the transfer function of the system will be

$$\frac{Y(s)}{X(s)} = \frac{1}{s^2 + s + 1} \quad (8)$$

The modes are complex and we will see overshoot. When the input is unit step of amplitude 1, the initial value of the output $y(t)$ should be zero and the final value should be 1 with oscillations in between. The circuit to solve this case is shown below in Figure 6 and the result is shown in Figure 7.

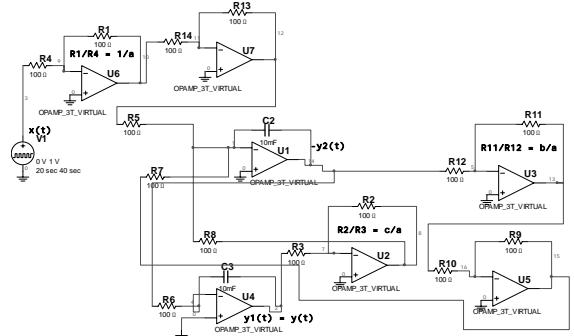
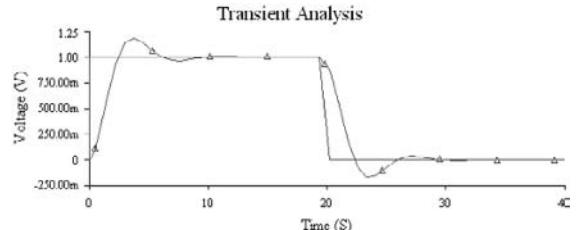
Fig. 6. Circuit to Solve: $\frac{d^2}{dt^2} y(t) + \frac{d}{dt} y(t) + y(t) = x(t)$ 

Fig. 7. Output for Circuit in Fig. 6

IV CONCLUSION

It would be discovered by looking at the graphs and also by comparing these results with what was derived analytically that the circuits worked as desired. The differential equation was solved and its outputs were a solution to the given input. In the future we will attempt to solve higher order differential equations. Practically, to solve any second order differential equation with any arbitrary coefficients requires a huge set of resistive values. However, since the constant values of a, b, and c can be translated to ratios of resistor values, that makes things easier. Issues related to amplifier saturation should also be studied. [5]

V REFERENCES

- [1] Henry Edward, "Elementary Differential Equations", 4th edition, *Prentice Hall*, 2000.
- [2] Robert Boylestad, "Electronic Devices and Circuit Theory", 8th edition, *Prentice Hall*, 2002.
- [3] J. W. Nilson, "Electric Circuits", 7th edition, *Prentice Hall*, 2005.
- [4] J. W. Nilson, "Introduction to Pspice Manual using Orcad", 7th edition, *Prentice Hall*, 2005.
- [5] C. Chen, "Analog & Digital Control System Design", 1st edition, *Saunders*, 1993.

QoS Provisioning in WCDMA 3G Networks using Mobility Prediction

T. Rachidi, M. Benkirane, and H. Bouzekri

Al Akhawayn University in Ifrane

Ifrane 53000, Morocco

Abstract-This paper proposes a mobility prediction (MP) based system for Quality of Service (QoS) provisioning in 3G Wideband Code Division Multiple Access (WCDMA) cellular networks. The proposed system uses digital road maps in a Geographical Information System (GIS) and real-time user mobility prediction information to maintain QoS, while maximizing utilization in an environment where resources (Cell Power) and cell geometry are intrinsically fluctuating. A QoS-aware congestion control mechanisms supersedes the traditional closed loop power control, while the handoff combines both mobility prediction and Signal to Interference and Noise Ration (SINR) level for dynamic power reservation and release. Both network-wide probabilities for forced terminations (P_f) and call blocking (P_{cb}) have been measured for a variety of power reservation and adaptation strategies. The evaluation testbed uses realistic values for physical layer parameters specified for Terrestrial Radio Access in Universal Mobile Telecommunication System (UMTS). Results show that, a fair dropping strategy i.e., dropping solely based on cost (power/bit), after adaptation, to resolve congestion, combined with mobility prediction and SINR based handoff strategy offer the best handoff prioritization.

I. INTRODCUTION

Wireless 3G Telecommunication Systems are being rolled out, and integrated to the global Telecommunication infrastructure with the aim of delivering multimedia services, such as video telephone calls, that are characterized by stringent real time interactivity requirements, great sensitivity to delivery delay, and the need for considerable wireless resources. UMTS, for instance, stipulates support for such services through four (4) classes of service [1]. Each class imposes different QoS requirement on the 3G network, which must be maintained during the lifetime of the connection.

Unfortunately, provisioning QoS over WCDMA-based air interface (the prevalent access method for UMTS) is hindered by serious reliability challenges. This is due, on the one hand, to the inherent characteristics of the wireless link [3], that is, user mobility and fading channel [4], high error rates, inherent interference-limited characteristics of WCDMA [5], and low and varying bandwidth (2Mbps at most); and on the other hand, to the unexpected Soft Handoffs (SHOs) resulting from user mobility. Both phenomena, if not catered for, yield inevitably an over-load on the wireless system causing increased forced terminations, call blocking, and QoS degradation, affecting seriously the reliability of the cellular network, as well as low network utilization.

In previous works [8,15], we have addressed the inherent characteristics of the link in an integrated approach, where physical layer radio and interference constraints, and user QoS requirement in user connection requests have been

brought together. That is, contrary to existing works [6,7], we augmented the closed loop power control mechanism with valuable information present in QoS profile such as Class of service, and more importantly user willingness to be gracefully degraded to lower QoS –say from color to monochrome video during a call, rather than having their call terminated-, showing significant improvement in QoS contract upholding.

On the other hand, driven by strict safety regulations and the huge market for location based services brought by initiatives such as the European Geostationary Navigation Overlay Service (EGNOS) [14], User Equipments (UEs) are being manufactured with accurate location tracking subsystems, delivering user position up to 5m, opening up the door for the use of mobility prediction techniques for efficient SHOs handling necessary to maximize network utilization. Real-time mobility prediction based on road topology information obtained from GIS, are naturally expected to yield significant improvement in resource reservation and handoff management as demonstrated in [9]. However, the techniques presented so far either assume regular geometry of cells, or do not link the geometry to power (the fundamental resource in WCDMA) available to the cell/system, implicitly basing the works on unrealistic models for WCDMA networks. For instance, in WCDMA, due to interference, low SINR and high load at a particular cell, handoffs may occur at the centre of a cell and not at the edge. Such occurrences, although rare, have to be catered for if QoS provisioning in such networks is to reach the level of provisioning in wirefull networks. More still, these works do not consider fluctuating resources as is the case for WCDMA.

In this work, we seek to demonstrate that: **1.** mobility prediction for power reservation techniques using road topology information yield significant performance improvement in WCDMA environment, **2.** the combined SINR and MP driven SHO yields better performance than MP-only driven techniques, that is, it maximizes wireless resource utilization, by minimizing forced terminations and call blocking.

Section II describes the testbed used for evaluation, while section III presents the experimental results obtained for performance evaluation.

II. THE TESTBED

The testbed is made of many modules out of which five (5) are of direct interest to the current study. Those are: Physical Layer, Admission Control, Power Control, QoS adapter, and Soft Handoff modules. The latter comprises both a mobility prediction and Power reservation sub-modules.

A. System Physical layer

Each connection request (i) by the User Equipment (UE) includes a QoS profile. The profile comprises the required bit rate R_i , the traffic class CL_i , and the SDD_i which will be used for graceful degradation. The power¹ P_i required to provide the bit rate R_i for a connection (i) at a given time t is computed according to the following formula [11]:

$$P_i(t) = C_i(t) \cdot R_i(t) \quad (1)$$

Where $C_i(t)$ is the current cost of the connection, and is given by:

$$C_i(t) = \frac{Eb}{W} \cdot \frac{1}{H_i(t)} \cdot I_i(t) \quad (2)$$

Each connection (i) experiences continuous real-time update of its cost $C_i(t)$ and $P_i(t)$ given that its channel gain $H_i(t)$, interference $I_i(t)$ and position $X_i(t)$ change over time.

The chip rate (W) is set to 3.84 Mchips, and Energy to Noise Ratio Eb/No is set by default to 5dB [16]. It can also be set to a different value to account for quality of User Equipment. Currently, we do not take into account co-channel interference from other clusters.

The interference at a given time $I_i(t)$ is the sum of interference exerted by all the existing users of the cluster on the target user. The central limit theorem is used to model $I_i(t)$ as a Gaussian process with mean 500 mW and a given variance $\sigma^2 = (N-1)/4$ [18], where N is the number of active users. The σ^2 was initially set to 0.5 to reflect urban region. However, it can be set to otherwise to account for multi-path. The channel gain at a given time $H_i(t)$ follows a Rayleigh distribution with 0 mean and variance 0.5; this was modeled using random process in the frequency domain [19]. The maximum power available at a cell is P_{max} :

$$P_{max} = N/CS * P_{max-battery} \quad (3)$$

Where N=256 is the spreading factor, i.e., the number of bits in the spreading sequence, and CS=7 is the number of cells per cluster. $P_{max-battery}$ the maximum power available at the UE is taken to be 1000 mW. So $P_{max} = 36.5$ W, and the maximum number of users per cell is N/CS is therefore 36.

For simplicity reasons, each user is allowed to request one connection at a time. The scheduler is assumed to operate close to optimum in meeting all delay requirements. The Time-shift scheduler is one such scheduler.

The dwelling time of a connection is set according to the it's QoS profile, namely its bandwidth and class.

UE position $X_i(t)$ changes over time according to the speed assigned to the corresponding connection. The speed of each connection is set according to its bandwidth. Users are assumed to move with a constant velocity $V_i(t)$.

The Active Set AS_i(t) of every existing connection also changes over time. This Set holds the cells that can serve the user at any time. The Active Set of a user (i) changes according to SINR_i. This Ratio (in dBm) is continuously monitored by each cell for all active connections of that cell:

$$SINR_i(t) = 10 * \log P_i(t) - 10 * \log [-80 + \sum_j \log P_j(t)] \quad (4)$$

where $P_i(t)$ is the required power (in mW) for the connection i and $P_j(t)$ is the power consumed by an active connection (j ≠ i) in the system/cluster. -80dB represents the acceptable noise power in dB.

B. Admission control

New connection requests are queued at the Call Admission controller, where the decision takes place based on the available power at the base station and the requested QoS profile. There are two types of admissions strategies:

Strict Admission Strategy: In this strategy, a connection is accepted in the system at instant t only if: $P_{max} - (\sum P_x(t)) + P_{new} > P_{target}$ where P_{max} is the maximum power available at the Node B, $\sum P_x(t)$ is the power used by the existing connections , P_{new} is the power required by the new connection and P_{target} is the reservation target that is used only by incoming handoffs. P_{target} changes real-time with system conditions.

NRT Overload admission Strategy: In this strategy, the system is allowed to accept connections even if the total power required by all connections exceeds the available power. In this case, NRT connections will be delayed by the scheduler. A new connection will be accepted in the system at instant t if the two conditions apply:

- (1) $P_{max} - (\sum P_{x/RT}(t)) > P_{target}$ where $\sum P_{x/RT}(t)$ is the power required by existing real time connections (Class 1 and Class 2) in the system. P_{max} is the maximum power available at the cell.
- (2) $(\sum P_{x/RT} + \sum P_{x/NRT}) < (1 + \alpha)(P_{max} - P_{target})$ where α belongs to the interval [0,1] and indicate the maximum overload allowed for NRT connections.

Soft handoff requests are treated differently than new connection requests: A handoff request is accepted as long as there are sufficient remaining resources to accommodate it regardless of the value of P_{target} :

$P_{max} - \sum P_x(t) > P_{handoff}$ where $P_{handoff}$ is the power requirement of the handoff request.

C. QOS profile power control

In WCDMA based 3G networks, Base stations implement closed loop power control at the level of the Radio Resource Manager (RRM) [12] on which we are trying to improve by taking into account QoS profile as an extra parameter for power control. In effect, by proposing our QoS profile driven power control (QPC), we are superseding to the basic closed loop control in RRM. Indeed, a traditional RRM only takes into account the received power at the base station when making a decision to control base transmit power. In implementing power control, we, however, take into account not , but also the negotiated QoS requirements of existing users, namely the bit rate, the willingness to be degraded, and the class of service.

When, due to the problems cited above, congestion occurs at a cell, QPC is triggered to address the overload in power requirements. It is this entity that copes with the link degradation in WCDMA based 3G wireless networks, by using QoS profiles of the active mobile users. Fig. 1 shows the processes triggered to handle congestion and SHOs.

¹ Power is considered to be the only limiting resource. Other system resources such spreading codes [5] and buffering capacity are considered to be available in sufficient quantities.

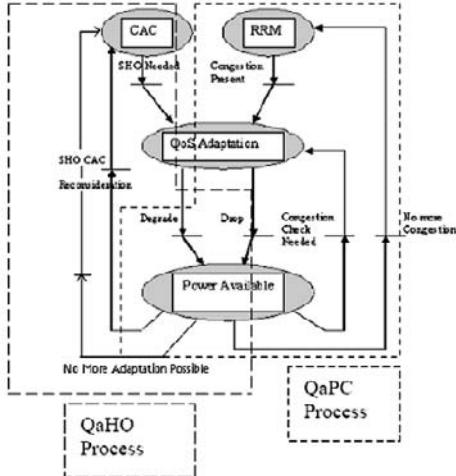


Fig. 1.. Processes triggered to handle congestion and SHOs are based on a core QPC which uses SDD descriptor, as well as class of service and bit rate.

Congestion is triggered after a congestion indication persists for a predefined duration (set to two unit time by default). Congestion is indicated at instant t if $\sum P_i(t) > P_{\max}$ where $P_i(t)$ is the power required by connection i , and P_{\max} is the maximum power available at the base/system. When NRT overload is switched on, congestion indication is set when $\sum_{i \in RT} P_i(t) > P_{\max}$, that is NRT traffic is not accounted for. It is worth mentioning that both modes are supported in the simulation model used for the evaluation, and that congestion is declared after 2 unit time (ut) persistence of congestion symptoms (lack of power). This confers to the congestion handling process stability with respect to temporary short fades.

The rationale behind our approach is to provide a basis for:

1. Handling the channel degradation in the WCDMA radio access network by dynamically triggering a QoS Adaptation Algorithm, that supercedes to the power control loop
2. Providing the incoming SHO requests which would be rejected by the Call Admission Controller (CAC) due to lack of resources, with the necessary resources by triggering the same QoS Power Control (QPC).

QPC is at the heart of our integrated system, and is triggered to make room for an incoming SHO, and in the presence of congestion. QPC resolves congestion in two phases. The two phases are applied differently in case of congestion and in case of SHO admission. In many ways, it is an improvement of the algorithm presented in [8]. In accordance with the QoS framework defined in [10].

The Degradation Phase: this phase is solely based on the SDD. Iteratively, the active connection that has the highest SDD is the connection that gets degraded in term of its bandwidth requirements as follow: 384Kbps \rightarrow 144Kbps; 144Kbps \rightarrow 64Kbps; 64Kbps \rightarrow 16Kbps. 2Mbps nad 16Kbps are not subject to degradation.

The Dropping Phase: this phase is invoked only after all willing connections were degraded, but congestion still persists. In this phase dropping is based on:

$$F_i(t) = SDD_i \cdot C_i(t) \quad (5)$$

$F_i(t)$ is high for connections requiring much cost and at the same time more willing to be degraded. Connections with high $F_i(t)$ are dropped until congestion disappears.

The profile comprises the required bit rate R_i , the traffic class CL_i and the Service Degradation Descriptor SDD_i . The latter takes values between 0 and 5. The larger the SDD is, the more willing is a mobile user to get degraded/dropped.

SDD is a number between 0 and 5. it describes how much the user is willing to get a degraded quality of service. The larger the SDD is, the more willing is the user to accept a degraded service and less the user is charged. A typical video telephony service can be degraded/adapted to current network conditions by using color/grey scale or by reducing the resolution of the image. Connection request that do not set a value for SDD, will have this value automatically set to a default service value by the network provider.

D. SHO

1. Mobility prediction

Finding the location of a mobile phone is one of the important features of the 3G mobile communication system because it will facilitate the prediction of its trajectory so as to perform resource reservation in advance. One approach is the integration of GPS receiver in each MT. According to [17], none of the previous work took into consideration that in real life the cell boundary is normally fuzzy and irregular due to terrain characteristics and the existence of obstacles that may interfere with radio wave propagation. Instead previous work assumed that the cell boundary is either circular or hexagonal for simplicity. Moreover, the previous schemes did not integrate road topology information into their prediction algorithms. QoS in cellular networks can be enhanced by the design of efficient mobility prediction schemes that make use of real-time positioning information. Those schemes could yield to better accuracy, efficient dynamic resource reservation and greater adaptability to time since MTs that are carried in vehicles are the ones that would probably encounter the most frequent handoffs.

In this Section, we will present the GIS Based (GB) scheme based resource reservation for handoff prioritization which is based on the work done by [17]. It uses a Road Topology Based (RTB) scheme which performs the road database update for each Node B and predictions for each mobile terminal (MT). Contrary to the RTB scheme, our scheme uses a real digital map designed for GPS tracking services, a spatial database, real coordinates and a map matching algorithm that translates the MT's position into the correct road segment. It is assumed that the serving BS will receive regular updates about each active MT's position every database period Δt (1s). The positioning data of the MTs will be used to predict handoff times and their target handoff cells as to make dynamic resource reservations.

As mentioned before, the road topology is incorporated into the mobility predictions. Each base station needs to maintain a spatial database of roads within its coverage area. We consider that each road is composed of segments; each segment S_{ab} is defined by a junction pair (j_a, j_b) . The coordinates of the junctions could easily be extracted from

existing digital maps designed for GPS tracking services. Usually, digital maps are not updated very often since new roads are not constructed very often.

The spatial database update is a probabilistic model that uses first and second Markov process to compute transition and conditional probabilities [17]. The spatial database is updated periodically each T_{DB} and is based on the history of MTs that have traveled the segments within each BS' coverage area. It stores some important information about Each segment S_{ab} : the segment ID, the cell ID to which the segment belongs, the length of the segment, the average time taken to transit the segment and statistical data about each possible handoff along the segment: Probability of handoff, remaining time and distance in the current segment before handoff, handoff positions, and the target handoff cell.

The Spatial database is updated periodically each T_{DB} because its elements depend on current and previous traffic conditions. The first and second elements (i.e., the segment ID, and the cell ID) are not updated, however the others elements will vary with time and traffic conditions. For a stochastic process whose statistics vary slowly with time, it is often appropriate to treat the problem as a succession of stationary problems. The transition between road segments is modeled as a Markov process [17]. Based on this model, the conditional probabilities of an MT choosing a neighboring segment given all its past segments depends only on the current and immediate previous segment.

For a new call, the previous segment of the MT is unknown; therefore the transition probability is modeled as a 1st order Markov process. For ongoing calls, the immediate previous segment is known and the transition probability is modeled a 2nd order Markov Process [17]. A Handoff Probable Segment (HPS) is a segment in which a handoff occurred. For each HPS segment, a probability of handoff is calculated and updated. In case a MT requests a handoff in the HPS segment, the target handoff cell, remaining time and distance, position of handoff and the target cell are recorded in the database. Using the model above, we could estimate the conditional probabilities using the chain rule of reaching and handing off at each of the HPS segments from segments that are several segment away [17]. We could also estimate the average time required to reach them using the current position and speed information, the target cell corresponding to each HPS is also available from the spatial database.

The prediction algorithm performs predictions for MTs that are currently traveling in segments in which MTs may make reservations. Each prediction consists of 4-tuple made up of: *The MT's predicted target handoff cell, Prediction Weight, Lower prediction limit, Upper prediction limit*. The prediction limits provide statistical bounds for the MT's remaining time from handoff. We have to mention that this scheme may return several 4-tuple predictions per MT because for each MT we can predict several paths from its current positions that may lead to a handoff with a predicted time $T_{threshold}$.

2. Power Reservation

In this section, we will present a dynamic resource reservation scheme for handoff prioritization that uses mobility predictions that were generated per MT in the prediction algorithm described in the previous section.

Previous work in the field of handoff prioritization proposed the static scheme in which a fixed part of the wireless resources are reserved specifically for incoming handoffs [20]. This scheme has many drawbacks; it can underutilize wireless resource and does not take into account the dynamic nature of traffic load and mobile users.

The Dynamic Resource Reservation (DRR) scheme is based on the work done by Soh [17], and takes into consideration both incoming and outgoing handoffs. However, our scheme is more accurate since it does not assign constant bandwidth units to the connection, instead each connection is assigned realistic power values and hence we have a Power Target P_{Target} reserved for incoming handoffs in each Node B. Moreover, the power of the handoff connection which will be used to adjust P_{Target} is calculated using physical layer characteristics of the target cell allowing Node B to have a real time knowledge of the channel conditions, the user requirement will allow for a more efficient management of the scarce radio resources in particular in high load areas.

DRR will achieve more efficient and a better tradeoff between the forced termination probability P_{FT} and call blocking probability P_{CB} because the BS will have first to look in its own list of outgoing handoff to check if enough resources will be released to accommodate the incoming handoffs, therefore over-reservation of resources and unnecessary blocking of new call calls will be limited. Next we will describe the algorithms that are used in the DRR scheme: the first algorithm relates to how prediction period $T_{threshold}$ is adjusted in each BS, the second algorithm presents how the Power Target P_{Target} is updated in each BS.

Each BS adjusts dynamically a power target P_{Target} that is updated periodically each T_{RSV} according the predicted demanded of handoffs from the switching center. We have to mention that P_{Target} is just a target not the amount of resources actually available at the target cell. P_{Target} will be satisfied in case the outgoing handoffs release their resource at their appropriate times. In the opposite case, P_{target} will not be met and some of the incoming handoffs will be dropped despite the fact that we have prior knowledge about them.

The problem can be solved in case the BS is given more time to try to meet the target. Therefore the predicted time $T_{threshold}$ can be viewed as the time given to the BS to set aside the required target to avoid forced termination of handoffs. We can conclude that it is possible to reduce forced terminations by increasing $T_{threshold}$ as to adjust the tradeoff between P_{FT} and P_{CB} . Increasing or fixing an optimal value for $T_{threshold}$ can lead again to an over-reservation of resources since it can fluctuate due to user mobility, traffic load in the target cell [17]. An adaptive algorithm is therefore needed to approximate the value of $T_{threshold}$ for any given P_{FT} .

3. PSHO

In our integrated system every NodeB monitors the SINR of all its active connections continuously. This value should be kept above a threshold value ($SINR_{Target}$) to guarantee a good quality (the $SINR_{Target}$ is set to the default value 21dB).

In our scheme, we can decide that a connection request should be handed off based on three methods:

GB strategy: When a MT is between $0.9R$ and $1.1R$ from the BS in the current cell (R is the radius of the cell), we

assume that a handoff will occur during its transit through this region. The target BS is assumed to be the nearest neighboring BS at the time when the handoff occurs. The segment that is between $0.9R$ and $1.1R$ is considered a Handoff Probable Segment (HPS), i.e. all MT that will pass through this segment have a large probability of making a handoff request. As mentioned before; the predicted Incoming/Outgoing handoff will be used to update P_{Target} in each cell.

SINR strategy: if the SINR of a connection go below a certain threshold (-121dB), the connection will handoff. We first find the neighboring cells of the current cell in which the MT is passing, then the SINR of the connection is computed to each of this neighboring cells and finally the target cell is the one with the largest SINR ratio (not necessarily the nearest neighboring BS).

Combined Strategy (Use SINR and RTB strategy): In this scheme we check both the SINR of the connection and the proximity of the user equipment to the HPS (handoff probable segment), if one of the conditions occurs, the connection is handed off to the nearest neighboring BS. In case the connection (i) has a low SINR (less than a threshold value), the NodeB will look in the Active Set of the connection AS_i(t) to find the cell with the highest SINR for that connection and send the SHO request to that cell.

III. SIMULATION DETAILS AND RESULTS

To evaluate the strategies, we augmented the testbed of [13] with distributed capabilities and used it to analyze the different QoS adaptation strategies, namely the Fair_DQAA, and the Basic Algorithm (BA) that is a blind non-QoS aware strategy with no SHO prioritization. To resolve congestion, BA uses a 1-phase process where connections with highest power are dropped first, while Fair_DQAA undergoes a two-phase process with a degradation phase and dropping phase. They both undertake the same degradation phase, but a different dropping phase as explained earlier.

TABLE I

BANDWIDTH REQUIREMENTS FOR EACH CLASS OF SERVICE	
Class	Data rate
Class 1	14.4 kbps (typical voice call), 128kbps (typical video call), 384kbps (Codec H263)
Class 2	2 Mbps (MPEG), 384 Kbps, 128kbps
Class 3	14.4 kbps, 128kbps, 384 Kbps
Class 4	14.4 kbps, 128kbps

TABLE II
DWELLING TIME AND SPEED SETTINGS

Bandwidth	Dwelling Times	Speed
2Mbps	80 min (1h video on demand stream)	0 Km/h.
384Kbps	30 min (videophone call)	60 Km/h.
128Kbps	30 min	80 Km/h.
14.4 Kbps	4 min (typical voice call)	100 Km/h.

Connections are generated according to a Poisson distribution with rate lambda (connections/sec/cell) in each cell. The initial position of an MT and its destination can be on any road segment with equal probability. The path chosen by the MT (approximately 20 segments) is assumed to follow

the shortest path between its origin and its destination. Each user is allowed to request one connection at a time.

Qos profiles are assigned randomly to each connection. Each profile comprises the required bit rate, the traffic class and the SDD, as well as Traffic parameters such as speed and dwelling time are set according to the class and bandwidth of the connection (see Table I & II).

The simulation network consists of 21 cells (3 clusters, 7 cells per cluster). Simulation does not assume that handoffs occur at the hexagonal boundary. The hexagonal model is merely used to determine where the BSs should be placed (at the center of each hexagon).

We used a digital map of Washington DC designed for GPS based tracking services (See Fig. 2), it is composed of 1330 road segments with varying lengths 0.2-0.5km. The initial 1st and 2nd transition probabilities and the probabilities of handoff are generated randomly and are updated during the database updates. R=1Km is the cell radius. We assume that a handoff will occur when an MT is between 0.9R and 1.1R from the BS. The target BS is assumed to be the nearest BS.

QoS adaptation is triggered after congestion persists for 2 unit times (default). Congestion is indicated if $\sum P_i(t) > 1.1 * P_{\text{max}}$ where $P_i(t)$ is the power required by connection i, and P_{max} is the maximum power available at the NodeB.

MT position at a given time $X_i(t)$ changes over real time according to the speed assigned to the MT. The speed of each connection is set according to its bandwidth as in Table II. We assume that a GPS device within the MT returns position information to the BS: {X, Y, and V}.

Simulations consisted in launching the testbed for 10 50 (ut) runs, with different loads and collecting the results. Before sampling starts, the system is initiated with N number of connections of different QoS profiles to bring it to a steady state. Afterward, connections are generated and thrown in the system according to the arrival patterns. We defined the normalized load per cell as:

$$L = \sum P_i / P_{\text{max}} \quad (6)$$

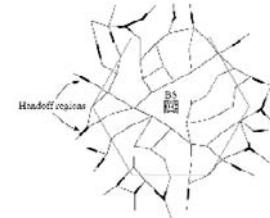


Fig. 2. Handoff regions

The min T_{thresh} ($T_{\text{thresh_min}}$), the max T_{thresh} ($T_{\text{thresh_max}}$), the Prediction Interval (T_{RSV}), and Hop limit used in GB are set respectively to 1s, 120s, 5s, and 2.

Fig. 4 shows the probability of forced termination of handoffs P_{FT} for different loads. Therein the GB-SINR scheme is more efficient than the other schemes. The SINR scheme does not update the resource target dynamically nor does it take into consideration incoming/outgoing handoffs or the real time mobile positioning method. This results in under/over use of power, hence an increase in P_{FT} . Combined SINR-GB scheme yields larger target Power in each target cell than GB scheme, because the set of HPS is updated

dynamically and takes into account the SINR threshold, real time positioning information, and finally incoming/outgoing handoffs comparing with the GB scheme.

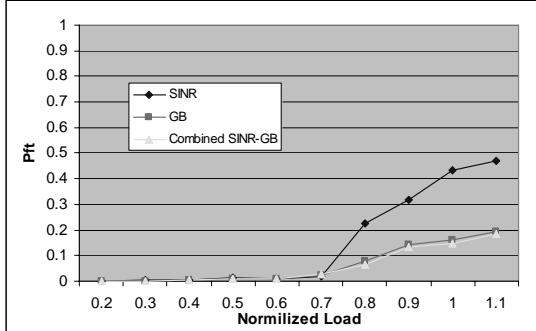


Fig. 4. Load vs. Pft (CAC :NRT overload, QoS adaptation: Fair DQAA)

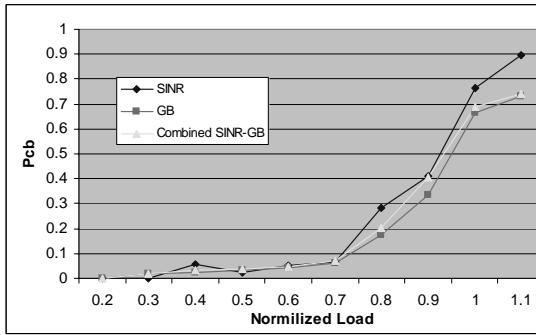


Fig. 5. Load vs. Pcb (CAC: NRT overload, QoS adaptation: Fair DQAA)

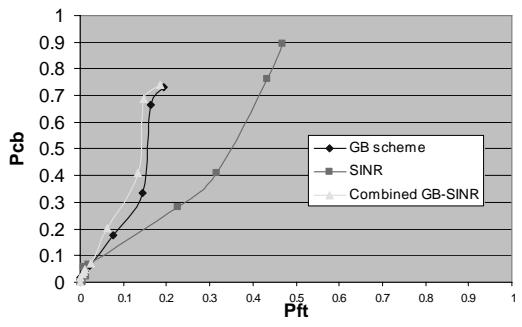


Fig. 6. Pcb vs. Pft (CAC: NRT overload, QoS adaptation: Fair DQAA)

Fig. 5 shows the probability of call blocking (new calls) P_{CB} for different loads. Therein, the GIS based (GB) scheme is more efficient than the other schemes. The power target in the combined SINR-GB scheme on average is larger than in the GB scheme, hence the wireless resources reserved for the new calls are decreased and the probability of call blocking is increased. The SINR scheme does not update dynamically the resource target, which results in an under/over use of power.

Fig. 6 shows that SINR is the least efficient scheme since under heavy load, P_{CB} and P_{FT} increase severely. As mentioned before, the Combined GB-SINR is more efficient in limiting the forced termination and less efficient in decreasing P_{CB} compared to the RTB scheme.

IV. CONCLUSIONS AND FUTURE WORK

We presented an integrated Power-based model that uses real cell boundaries and mobility information for QoS provisioning in 3G WCDMA cellular networks. Our current efforts are directed towards the use of Bit Error Rate (BER) parameter as another key element in the QoS profile for optimal resource utilization, as well as the handling of co-channel interference from other clusters.

REFERENCES

- [1] 3GPP “QoS Concept and Architecture”, <http://www.3gpp.org>, ETSI 23.107 v5.5.0 (2002-2006).
- [2] Ericsson Radio System, “Basic concepts of WCDMA radio access network”, http://www.ericsson.com/technology/whitepapers/e207_whitepaper_ny_k1.pdf, 2001.
- [3] E. Dahlman and P. Bening “WCDMA –the radio interface for future mobile multimedia communications”, IEEE Trans. on Vehicular Technology, Vol 47, No 4, Nov 1998.
- [4] G. H. Forman, and J. Zahorjan, “The challenges of mobile computing,” IEEE Comp., vol. 27, no. 4, pp. 38-47, April 1994.
- [5] G. L. Stuber, “Principles of mobile communications”, Kluwer Academic Publishers; 2nd edition, 2001.
- [6] M.Xiao, and N.Shroff “Distributed admission control for power-controlled cellular wireless systems” IEEE/ACM Transactions on Networking, Vol. 9, NO.6, December 2001.
- [7] Z. Choukri and S.Sfar, “Run Time Adaptation of UMTS Services to Available Resources”, Proc. 17th IEEE Int. Conf. on Adv. Information Net. and Applications, 2003.
- [8] T. Rachidi, A. Y. El Batji, M. Sebbane, and H. Bouzekri, “QoS-aware Power Control and Handoff prioritization in 3G WCDMA Networks”, in Proc. of IEEE WCNC04, March 21-25. 2004
- [9] Wee-Seng and Hyong S. Kim, “QoS Provisioning in Cellular Networks Based on Mobility Prediction Techniques”, IEEE Comm. Mag., Jan, Vol. 41, N°1, pp.86-92. 2003
- [10] O. Lataoui, T. Rachidi, L. G. Samuel, S. Gruhl, and Ran Hong Yan, “A QoS management architecture for packet switched 3rd generation mobile systems”, in proceedings of INTEROP00, May 17, Las Vegas, p. 365. 2000
- [11] J. Mueckenheim, and S. Gruhl “Quality of service scheduling method for UMTS downlink”, Lucent Technologies. Personal communication, 2000.
- [12] “Radio Resource Control,” UMTS.v100.50.120.601. Ed. Urs Bernhard. 2000.
- [13] A. Y. ElBatji, T. Rachidi, and H. Bouzekri, “A Testbed for the Evaluation of QoS Provisioning in WCDMA based 3G Wireless Networks”, in Proc. of the Int. Conf. on Com. Sys. and Networks, IASTED, CSN, Sept 8-10, , pp.31-36, 2003.
- [14] ESA navigation : EGNOS, <http://www.esa.int/esaNA/egnos.html>
- [15] T. Rachidi, A. Y. El Batji, M. Sebbane, and H. Bouzekri, “An Integrated System for QoS Provisioning in 3G WCDMA Cellular Networks”, in Proc. of MWCN05, 2005
- [16] UMTS World, <http://www.umtsworld.com/technology/>
- [17] W. Soh, “Mobility Prediction Based Resource Reservation and restorability enhancement in cellular Networks”, PhD thesis, Carnegie Mellon University, Pennsylvania, 2003.
- [18] R. Wang and D.C. Cox, “Doppler Spread in Ad hoc Mobile Networks” Stanford University, Stanford, CA 94305, 2002.
- [19] M.R.Abid, T. Rachidi, A. Bensaid, S. Gruhl, and M.Soellner “Adaptive Fuzzy Call Admission Controller for UMTS”, 5th world multi-conference on Systemics, Cybernetics and Informatics, Vol. xvi, Orlando July 22-25, 2001,pp. 93-99.
- [20] T. S. Rappaport “Wireless Communications: Principles and Practice”, by Prentice Hall, 1996.

Patent-Free Authenticated-Encryption As Fast As OCB

Ted Krovetz

Computer Science Department
California State University
Sacramento, California, 95819 USA
tdk@acm.org

Abstract—This paper presents an efficient authenticated encryption construction based on a universal hash function and block cipher. Encryption is achieved via counter-mode while authentication uses the Wegman-Carter paradigm. A single block-cipher key is used for both operations. The construction is instantiated using the hash functions of UMAC and VMAC, resulting in authenticated encryption with peak performance about ten percent slower than encryption alone.

Keywords—Authenticated encryption, block-cipher mode-of operation, AEAD, UMAC, VMAC.

I. INTRODUCTION

Traditionally when one wanted to both encrypt and authenticate communications, one would encrypt the message under one key and authenticate the resulting ciphertext under a separate key. Encryption in such a scenario would often use a block-cipher mode of operation, while authentication would usually use another mode or HMAC [6]. If the block cipher encrypted blocks at a rate of x processor cycles per byte (cpb), then the combined process of encryption plus authentication would require at least $2x$ cpb and the management of two separate keys.

Recently proposed modes of operation combine encryption and authentication under a single key. Some of the modes also switch to faster Wegman-Carter authentication based on universal hashing [8,9]. This switch can bring authenticated encryption down to nearly x cpb because recent Wegman-Carter schemes are as fast as 0.5 cpb—much faster than any known block cipher. One other method of authenticated encryption, typified by OCB mode, authenticates a message as a byproduct of its encryption. These modes are very efficient, but are proprietary, require licenses and cannot be used until patent disputes are resolved. With the exception of OCB, all algorithms examined in this paper are patent-free and can be used freely without securing any license.

This paper examines a general method for converting a universal hash function into an authenticated encryption scheme that uses a single key for both encryption and authentication. The resulting construction is provably secure and has peak efficiency close to the sum of counter-mode encryption and the peak speed of the chosen universal hash function. As an example, the construction is applied to the AES block cipher and

VHASH hash family [4]. The resulting authenticated encryption scheme peaks at 12.8 cpb, while OCB peaks at 13.9 cpb in our experiments. The paper closes with a performance comparison of several well-known authenticated encryption algorithms [6].

II. SECURITY DEFINITIONS

We adopt the notions of security from [7], and summarize them less formally here. An authenticated encryption with associated data (AEAD) scheme is a triple $S = (K, E, D)$, where K is a set of keys, and E and D are encryption and decryption functions. Encryption occurs by computing $E(k, n, h, p, f)$, which returns (c, t) , for key k , nonce n , header h , plaintext m and footer f . Ciphertext c is the encryption of p , and tag t authenticates h , c and f . Decryption occurs by computing $D(k, n, h, c, f, t)$, which returns p only if (c, t) is a legitimate result for $E(k, n, h, p, f)$ and “invalid” otherwise.

AEAD scheme S is secure if $\text{Adv}(S, \text{PRIV})$ and $\text{Adv}(S, \text{AUTH})$ are both small given an adversary with reasonably limited resources. $\text{Adv}(S, \text{PRIV})$ is defined to be the maximum probability that an adversary could distinguish whether an oracle O has been instantiated as $E(k, -, -, -, -)$ for a randomly chosen k or if O simply returns (an appropriate number of) random bits instead of a legitimate (c, t) pair. For the definition of $\text{Adv}(S, \text{AUTH})$, let the adversary have an oracle O instantiated as $E(k, -, -, -, -)$ for a randomly chosen k . A forgery occurs if the adversary can produce an (n, h, c, t) for which $D(k, n, h, c, f, t)$ is valid, and c was never returned by the oracle. $\text{Adv}(S, \text{AUTH})$ is the maximum probability an adversary is able to create a forgery. In both the encryption and authentication cases, it is assumed the adversary never repeats a nonce to its oracle.

III. WC-AE CONSTRUCTION

Let H be an ϵ -almost-delta-universal hash family with all member functions having the domain of arbitrary strings and co-domain of L -bit strings. We will not describe delta-universal hash families in this paper, except to say that they can be used in Wegman-Carter authentication schemes [8,9]. Assume that a random j -bit string can be used to select a random element of H , and that the function indicated by string b is H_b . Let $\langle i \rangle_n$ represent the n -bit binary encoding of integer i , and $b[a \dots c]$ repre-

sent the substring of b including bit indices a through c . Let \parallel be string concatenation and $|b|$ the bit-length of string b .

We now define AEAD scheme WC-AE. Let K be the set of all functions from L bits to L bits. Choosing a random g from K then defines the following functions (where n is an $L/2$ -bit string and h, p and f are arbitrary strings):

$$\begin{aligned} E_g(n, h, p, f) : \\ b &= g(\langle 1 \rangle_1 \parallel \langle 0 \rangle_{L-1}) \parallel g(\langle 1 \rangle_1 \parallel \langle 1 \rangle_{L-1}) \parallel \\ &\quad g(\langle 1 \rangle_1 \parallel \langle 2 \rangle_{L-1}) \parallel \dots [1 \dots j] \\ epad &= g(n \parallel \langle 1 \rangle_{L/2}) \parallel g(n \parallel \langle 2 \rangle_{L/2}) \parallel g(n \parallel \langle 3 \rangle_{L/2}) \parallel \dots [1 \dots |p|] \\ c &= p \oplus epad \\ tpad &= g(n \parallel \langle 0 \rangle_{L/2}) \\ t &= H_b(h \parallel c \parallel f \parallel \langle |h| \rangle_{64} \parallel \langle |c| \rangle_{64}) + tpad \bmod 2^L \\ &\text{return } (c, t) \\ \\ D_g(n, h, f, c, t) : \\ b &= g(\langle 1 \rangle_1 \parallel \langle 0 \rangle_{L-1}) \parallel g(\langle 1 \rangle_1 \parallel \langle 1 \rangle_{L-1}) \parallel \\ &\quad g(\langle 1 \rangle_1 \parallel \langle 2 \rangle_{L-1}) \parallel \dots [1 \dots j] \\ tpad &= g(n \parallel \langle 0 \rangle_{L/2}) \\ t' &= H_b(h \parallel c \parallel f \parallel \langle |h| \rangle_{64} \parallel \langle |c| \rangle_{64}) + tpad \bmod 2^L \\ &\text{if } t \neq t' \text{ return "invalid"} \\ epad &= g(n \parallel \langle 1 \rangle_{L/2}) \parallel g(n \parallel \langle 2 \rangle_{L/2}) \parallel g(n \parallel \langle 3 \rangle_{L/2}) \parallel \dots [1 \dots |p|] \\ p &= c \oplus epad \\ &\text{return } p \end{aligned}$$

Theorem: $\text{Adv}(\text{WC-AE}, \text{PRIV}) = 0$ and $\text{Adv}(\text{WC-AE}, \text{AUTH}) \leq \varepsilon$ when all nonces begin with a zero bit.

Proof: Because g is chosen from all possible L -bit functions, each invocation on different inputs returns a uniformly distributed L -bit string. This means b , and thus the choice H_b , is uniformly distributed. All other inputs to g are distinct over all invocations of E so long as n is unique for each and always begins with a zero bit. This means $tpad$ and $epad$ will be independent uniformly distributed strings for each invocation of E . This results in both c and t being uniformly distributed, and so $\text{Adv}(\text{WC-AE}, \text{PRIV}) = 0$. The value t is computed using a standard Wegman-Carter MAC construction, and so $\text{Adv}(\text{WC-AE}, \text{AUTH}) \leq \varepsilon$. ♦

For a more thorough examination of counter-based encryption and Wegman-Carter message authentication see [1,8,9].

The set of all L -bit functions is not a practical key set, so instead we use a block cipher in a realization of WC-AE. Block ciphers are designed to resemble random permutations, which in turn can be used in the place of a random function. Let B be a block cipher from L bits to L bits. We use standard notions of block-cipher security. We say that B is (α, q, t) -secure if no adversary can distinguish an oracle instantiated as B_k , with random block-cipher key k , from an oracle instantiated as a random L -bit permutation with probability greater than α , given q oracle queries and t computational steps. We assume, for the remainder of the paper that every adversary is limited to no more than t steps. Using B instead of g in WC-AE is accomplished by defining the key set K of WC-AE to be the set of all block cipher B keys and replacing all occurrences of g with B_k . We call this version WC-AE[B]. An advantage WC-AE[B] has

over other AEAD schemes is its use of a single block-cipher key for both authentication and encryption. As one can see in the definition and proof of WC-AE, a single function is carefully used for both authentication and encryption, ensuring that g never is computing on the same input twice. When we move from using a random function g to a block cipher, this careful avoidance of repeated inputs allows for the use of a single block-cipher key.

Proposition: $\text{Adv}(\text{WC-AE}[B], \text{PRIV}) \leq ((1 - q/2^L)^{-q/2} - 1) + \alpha$ and $\text{Adv}(\text{WC-AE}[B], \text{AUTH}) \leq \varepsilon(1 - q/2^L)^{-q/2} + \alpha$ when all nonces begin with a zero bit and B is invoked no more than q times.

The term $(1 - q/2^L)^{-q/2}$ comes from the perceptible difference between a random L -bit function and random L -bit permutation over q points [2]. If an adversary existed that achieved greater than either advantage in the proposition, standard reduction techniques would allow us to construct an adversary that could distinguish between B_k (for random k) and a random permutation with greater than α probability using q queries.

As an example, consider the use of WC-AE[AES] to encrypt and authenticate some combination of messages requiring 2^{50} block-cipher invocations. Then $\text{Adv}(\text{WC-AE[AES]}, \text{PRIV}) < 1/2^{28} + \alpha$ and $\text{Adv}(\text{WC-AE[AES]}, \text{AUTH}) < \varepsilon(1 + 1/2^{28}) + \alpha$ where α represents the maximum probability AES under a random key can be distinguished from a random permutation over 2^{50} invocations. Since ε and α are typically very small (think $1/2^{64}$ or smaller), this is significant security over so many AES invocations. If fewer block-cipher invocations are needed, say 2^{30} , then $\text{Adv}(\text{WC-AE[AES]}, \text{PRIV}) < 1/2^{68} + \alpha$ and $\text{Adv}(\text{WC-AE[AES]}, \text{AUTH}) < \varepsilon(1 + 1/2^{68}) + \alpha$.

IV. VMAC-AE, UMAC-AE

Highly efficient realizations of WC-AE can be made using VHASH and UHASH, the hash functions of VMAC and UMAC [4,5]. UMAC was developed as a Wegman-Carter MAC with exceptional speed on processors that multiply 32-bit operands efficiently, while VMAC was later developed following the same principles as UMAC, but focused on 64-bit architectures. VHASH achieves ε values as low as $1/2^{59.9}$ and $1/2^{118}$ using 0.5 and 1.0 cpb, respectively. UHASH achieves ε values of about $1/2^{30.7}$ using $i/2$ cpb on both 32- and 64-bit architectures (depending on one's choice of $1 \leq i \leq 4$). Additional information and implementations are found at fastcrypto.org [4].

To compare performance of VMAC-AE and UMAC-AE with other authenticated encryption schemes, a commonly cited public implementation of each was used. Gladman's implementations were used for OMAC, CCM, CWC and EAX, and a reference implementation of OCB was retrieved from the OCB author's website. All implementations are written in C with OCB, UMAC-AE and VMAC-AE using small amounts of inline assembly. Implementations use Gladman's AES assembly code and a similar test setup. Tests were run on two processor architectures: A 2GHz AMD Athlon 64 "Manchester" in 64-bit mode and a 2.8 GHz Intel Xeon "Ncona" in 32-bit mode. The examination intends only to give a sense of relative performance.

TABLE I. PERFORMANCE ON TWO ARCHITECTURES

	64-bit Athlon 64			32-bit Pentium 4		
	64B	256B	2KB	64B	256B	2KB
CTR	11.9	11.9	11.9	21.6	21.6	21.4
OMAC	23.8	16.7	14.3	36.6	25.8	22.3
CCM	38.2	28.3	25.0	74.9	54.9	48.5
CWC	52.4	41.1	37.4	106*	79*	65*
EAX	41.7	28.9	24.7	76.6	52.4	44.5
GCM	51.3	38.2	34.4	106.5	82.0	74.5
OCB	21.5	15.8	13.9	46.6	32.5	28.1
UMAC-AE-64	22.6	15.8	13.7	41.6	27.5	23.3
UMAC-AE-128	26.8	17.6	14.9	52.4	30.0	25.0
VMAC-AE-64	17.9	14.0	12.8	52.0	36.6	29.1
VMAC-AE-128	19.7	14.9	13.1	58.7	46.6	36.6

Table I shows performances of the various algorithms over short, medium and long message lengths using AES with 128-bit keys as the block cipher. For comparison, CTR-mode encryption and OMAC authentication (a NIST-approved block-cipher based CBC-MAC variant) are listed. All timings are generated using GCC 4.0 under similar conditions except (*) which is taken from Gladman's AES webpage [3].

Table II shows memory and code sizes on Athlon 64 using GCC 4.0. Memory is per encryption key and determined by the C sizeof function. Code size is the sum of the algorithm specific object files generated by GCC, after executing gnu strip -s (sum excludes the AES code).

One solution to authenticating encryption is to encrypt a message and authenticate the ciphertext, using separate keys for each operation. Such a solution using CTR and OMAC would perform approximately at the rate of the sum of the rates of the two algorithms, but at the cost of managing two separate keys. CCM and EAX do away with the need for two keys, but without any speed improvement. OCB integrates authentication operations into the encryption process very efficiently, at a cost slightly higher than encryption alone. The remaining algorithms in the table all encrypt in CTR mode and apply a Wegman-Carter scheme for authentication. Those using the fastest hash functions come out on top—VMAC-AE and UMAC-AE—at roughly the same speeds as OCB.

V. CONCLUSION AND FUTURE WORK

The schemes presented here represent the fastest patent-free AEAD schemes currently known to the author. The schemes, however, are tailored to specific architectures with fast multipliers. This makes them appropriate for computational environments

from laptops to servers and workstations, but less so for constrained environments such as cell phones, PDAs and inexpensive networking hardware. Also, custom hardware becomes much more expensive in terms of latency and die area when large multiplications are required. Future work could investigate the use of smaller moduli for multiplication, perhaps as little as just a few bits, and increasing parallelism. At the practical level, implementations could be developed that integrate VHASH and UHASH calculations more closely, reducing the register-to-memory overhead that a loosely coupled implementation may have.

TABLE II. MEMORY REQUIREMENTS

	Memory per key (bytes)	Code size (kilobytes)
CTR	248	—
OMAC	272	2.5
CCM	360	6.7
CWC	424	5.7
EAX	384	5.5
GCM	8552	13.0
OCB	516	4.6
UMAC-AE-64	1552	11.3
UMAC-AE-128	1704	11.8
VMAC-AE-64	624	7.2
VMAC-AE-128	608	8.1

REFERENCES

- [1] Bellare M, Desai A, Jokipii E, Rogaway P. A concrete security treatment of symmetric encryption. In Proceedings of the 38th Symposium on Foundations of Computer Science, IEEE, 1997.
- [2] Bernstein D. Stronger security bounds for Wegman-Carter-Shoup authenticators. In Advances in Cryptology – EUROCRYPT 2005. Springer-Verlag, 2005.
- [3] Gladman B. AES and Combined Encryption/Authentication Modes. Webpage: <http://fp.gladman.plus.com/AES/>.
- [4] Krovetz T. Fast cryptography. Webpage: <http://fastcrypto.org/>.
- [5] Krovetz T. Message authentication on 64-bit architectures. In Selected Areas in Cryptography: 13th International Workshop, SAC 2006. Springer-Verlag, 2006.
- [6] NIST. Modes of operation. Webpage: <http://www.nist.gov/modes/>.
- [7] Rogaway P. Authenticated-encryption with associated-data. In ACM Conference on Computer and Communications Security 2002 (CCS'02), ACM Press, 2002.
- [8] Stinson D. Universal hashing and authentication codes. Designs, Codes and Cryptography 4, 1994.
- [9] Wegman M, Carter L. New hash functions and their use in authentication and set equality. J. of Computer and System Sciences, 1979

Application of least squares support vector machines in modeling of the top-oil temperature

T. C. B. N. Assunção

Department of Electric Engineering, Federal University of São João del-Rei (UFSJ), Brazil
(e-mail: bessa@ufs.edu.br).

J. L. Silvino and P. Resende

Department of Electronics Engineering, Federal University of Minas Gerais (UFMG), Brazil
(e-mail: {silvino, pr}@cpdee.ufmg.br).

Abstract— Least squares support vector machines, a nonlinear kernel based machine was employed in modeling and simulation of the top-oil temperature of the transformers. The top-oil temperature can be estimated by using the ambient temperature and transformer loading measured data. The estimated top-oil temperature is compared with measured data of a power transformer in operation. The results are also compared with methods based on the IEEE Standard C57.91-1995/2000 and Artificial Neural Networks. It is shown that the trained Least Squares Support Vector Machines with a radial basis function kernel presents better performance than the methods based in the IEEE Standard C57.91-1995/2000 and artificial neural networks.

I. INTRODUCTION

Power transformers are high cost important equipment used in the transmission and distribution of the electric energy.

Its right performance is important for the electric systems operation, since the loss of a critical unit can generate great impact in safety, reliability and cost of the electric energy supply. One of the main factors adopted for monitoring transformers operation conditions are its internal temperatures, specially the winding hot-spot temperature (HST) and the top-oil temperature (TOT), which affect the isolation aging and, consequently, the useful life of the equipment. The thermal modeling is considered as one of most important aspects for monitoring of the power transformer operation conditions. Calculated values of TOT and HST can be used to provide a diagnostic of the equipment conditions, and to indicate possible abnormalities, reducing the risk of defects, and avoiding the problems generated by the emergency operations. There are several methods used for calculation of the transformer internal temperatures. According to Jardini [1], the method of the IEEE Standard C57.91-1995/2000 [2] is the more widely used, and it provides reliable results over transformers in operation. In the IEEE Standard C57.91-1995/2000, the thermal behavior of the transformers is represented by means of a first order model. In the G Annex of the IEEE Standard C57.91-1995/2000 [2] the TOT and HST are determined the characteristic data of the transformer. In addition to this technique, the estimation of HST and TOT can be obtained by means of other methods [3], [4], [5]. For this purpose

Artificial Neural Networks (ANN) can be used, due to its learning capacity in the modeling complex and nonlinear relations [6]. ANN is submitted to a training process from real cases, and then handling appropriately new supplied data. The most popular ANN configuration is the multi-layer feedforward network that have been applied successfully to solve some difficult and assorted problems including nonlinear system identification and control, financial market analysis, signal modeling, power load forecasting etc. Several ANN structures have been proposed by researchers that can be classified as static (SNN), dynamic temporal processing (TPNN) and recurrent (RNN). As an alternative as to the multi-layer feedforward network there has been considerable interest in a particular class of artificial neural networks denominated radial basis function network (RBFN), primarily because of its simpler structure. Its fast learning procedures and its great generalization capability have promoted the use these networks in the areas of non-linear identification, approximation and interpolation theory. In its most basic form RBFN involves three layers with entirely different roles. The input layer is made up of source nodes that connect the network to its environment. The second layer, the only hidden layer, applies a nonlinear transformation from the input space to the hidden space. The output layer is linear, supplying the response of the network to the activation pattern applied to the input layer [7]. Recently, the Support Vector Machine (SVM) has been proposed as a new and promising technique for classification and regression of the linear and nonlinear systems. The LS-SVM is a learning machine proposed in [8] corresponding a modified version of the SVM. Like the SVM, LS-SVM can be used in classification problems and approximation functions [9], [10]. The standard SVM is solved using complicated quadratic programming methods, which are often time consuming and difficult to implement adaptively, while LS-SVM is solved by a set of linear equations, without loss in the quality of the solutions. In this paper, the TOT will be estimated using the ANN and LS-SVM, and also it will be calculated by Annex G of the IEEE Standard C57.91-1995/2000 [2].

II. ARTIFICIAL NEURAL NETWORK

ANN has been established as a useful tool for regression problems, mainly for pattern recognitions and function approximations. An important characteristic of the ANN is

that is not necessary to obtain a complete knowledge about the relations among the variables involved in the problem.

The static neural network (SNN) is implemented as one nonlinear function of the following form:

$$\hat{y}_k = f_{snn}(x_k) \quad (1)$$

The temporal neural networks are classified in two basic types: non recurrent neural network (TPNN) and recurrent neural network (RNN). The inputs and outputs relationships of TPNN and RNN can be written as nonlinear functions given by (2) and (3), respectively:

$$\hat{y}_{k+1} = f_{rnn}(x_k, x_{k-1}, x_{k-2}, \dots, x_{k-d}) \quad (2)$$

$$\hat{y}_{k+1} = (x_k, x_{k-1}, x_{k-2}, \dots, x_{k-d}, y_k, y_{k-1}, y_{k-2}, \dots, y_{k-q}) \quad (3)$$

where \hat{y}_{k+1} = (k+1)th output, y_k = kth training output vector, x_k = kth training input vector, d and q are the number of input and output temporal delay lines.

The RBFN model is written as:

$$\hat{y}_k = f(x_k) = \sum_{j=1}^m w_j \phi(x_k) = \sum_{j=1}^m \phi\left(\frac{\|x_k - u_j\|}{\sigma_j}\right) \quad (4)$$

where k $\phi(\cdot)$ = radial basis function, w = weights, u = centers of the radial basis function, σ = width of radial basis function, m = number of radial basis function.

RBFN was also trained as recurrent and non recurrent, as the function given by (3), combining temporal delay lines $d = 1, 2, 3, 4$ and $q = 1, 2, 3, 4$.

III. LEAST SQUARES SUPPORT VECTOR MACHINES

Least Squares Support Vector Machines (LS-SVM) is a method used for solving non-linear classification or modeling problems and has been applied to classification, function estimation and nonlinear system optimal control problems. The basis of the method is the mapping of all available data points to a feature space, thus transforming the problem into a simple linear problem. LS-SVM expresses the training in terms of solving a linear set of equations.

A. Estimation Function

Given a training set of N points $\{x_K, y_K\}_{K=1}^N$, with input data $x_K \in R^n$, and output data $y_K \in R$, the LS-SVM model

for estimation function has the following representation in feature space:

$$y(x) = w^T \varphi(x) + b \quad (5)$$

The nonlinear function $\varphi(\cdot) : R^n \rightarrow R^{n_K}$ maps the input space to a higher dimension feature space. The dimension n_K of this space is only defined in an implicit way; b is a bias term; $w \in R^{n_K}$ is weight vector; $e_K \in R$ is error vector; γ is the regularization parameter. The optimization problem is defined as:

$$\min_{w,b,e} J(w, e) = \frac{1}{2} w^T w + \gamma \frac{1}{2} \sum_{i=1}^N e_i^2 \quad (6)$$

subject to the equality constraints:

$$y_i = w^T \varphi(x_k) + b + e_k \quad k = 1, \dots, N \quad (7)$$

The solution is obtained after constructing the Lagrangian,

$$(w, b, e, \alpha) = J(w, e) - \sum_{k=1}^N \alpha_k \{w^T \varphi(x_k) + b + e_k - y_k\} \quad (8)$$

where α_k are Lagrangian multipliers. Application of the conditions for optimality yields the following linear system:

$$\begin{bmatrix} 0 & 1^T \\ 1 & \Omega + \gamma^{-1} I \end{bmatrix} \begin{bmatrix} b \\ \alpha \end{bmatrix} = \begin{bmatrix} 0 \\ y \end{bmatrix} \quad (9)$$

where $y = [y_1, \dots, y_N]$, $1 = [1, \dots, 1]$, $\alpha = [\alpha_1, \dots, \alpha_N]$, and Mercer's condition is applied in the Ω matrix

$$\Omega_{i,l} = \psi(x_k, x_l) = \varphi(x_k)^T \varphi(x_l) \quad k, l = 1, \dots, N \quad (10)$$

The LS-SVM model for estimation function becomes:

$$\hat{y}(x) = \sum_{K=1}^N \alpha_K K(x, x_K) + b \quad (11)$$

where α_k are positive real constants and b is a real constant and comprise the solution to the linear system. $K(\cdot, \cdot)$ is called the kernel function that is used for the realization of an implicit mapping of the input data into a high-dimension feature space. In this paper the Radial Basis Function (RBF) kernel has been chosen since it tends to give good performance

under general smoothness assumptions. The RBF function Kernel is given by:

$$K(x, x_k) = \exp\left(-\frac{\|x - x_k\|^2}{2\sigma^2}\right) \quad (6)$$

where σ is a parameter specifying the width of the kernel.

In order to make an LS-SVM model with the RBF Kernel, it is necessary to calculate the γ regularization parameter in the algorithm, determining the trade-off between the fitting error minimization and smoothness of the estimated function, and also to calculate the σ kernel function parameter.

The temporal LS-SVM model is:

$$\hat{y}_{k+1} = f_{lssvm}(x_k, x_{k-1}, x_{k-2}, \dots, x_{k-d}) \quad (7)$$

The recurrent LS-SVM model is:

$$\hat{y}_{k+1} = f_{lssvm}\left(x_k, x_{k-1}, x_{k-2}, \dots, x_{k-d}, \hat{y}_k, \hat{y}_{k-1}, \dots, \hat{y}_{k-q}\right) \quad (8)$$

where the outputs (estimated values) are reinserted in the input vector.

IV. SIMULATION RESULTS

This section presents the estimation results of TOT using ANN, LS-SVM and the IEEE method.

In order to implement the methods it was used the experimental data set illustrated in fig. 1, and the transformer data presented in the Table I. The experimental data illustrated in fig. 1 corresponds to the measured values for thirty days operation of the transformer.

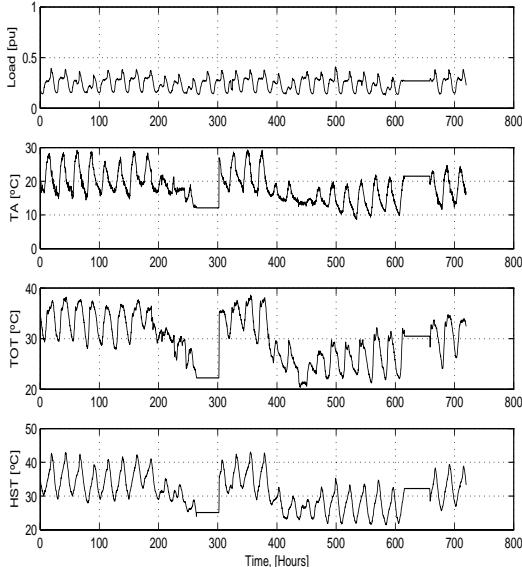


Fig. 1 Experimental Data: Load pu, Ambient Temperature °C, Top-oil Temperature °C, Hot-spot Temperature °C.

TABLE I
CHARACTERISTICS OF THE TRANSFORMER

Nameplate	30/40 MVA
Rating	
$V_{\text{primary}}/V_{\text{secondary}}$	138/13.8 kV
Iron Losses	17.8 kW
Cooper Losses	244.9 kW
Type of Cooling	ONAN/ONAF

A. TOT Calculation using G Annex of the IEEE Standard

In fig. 2, it is illustrated estimated values of TOT calculated from the IEEE model with the actual values of TOT and the testing errors (that is defined as the difference between the estimated and actual values of TOT). Where MSE = mean square error and Emax = maximum difference between estimated and measured temperatures in Celsius degrees.

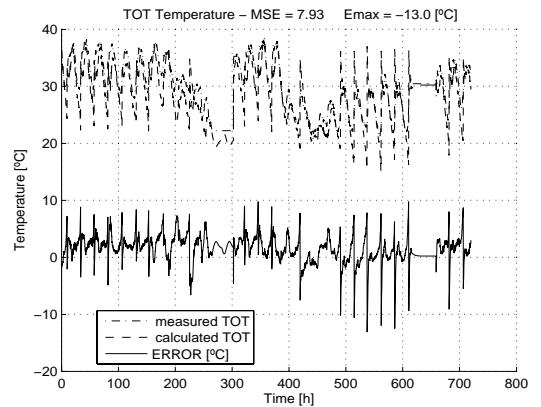


Fig. 2 Actual and estimated values of TOT using IEEE model with prediction error.

B. TOT calculation using ANN

In this section, it is used a two layers feedforward structure for the SNN, TPNN, and RNN using the ambient temperature and the loading as the input while TOT is considered as output. The hyperbolic tangent function is used as activation function for both layers. The algorithm used for SNN, TPNN and RNN training is the Levenberg-Marquardt (LM), considering 100 epochs and assuming a MSE goal as 0.01. The Levenberg-Marquardt algorithm was chosen since it takes less CPU time and it is more stable in all the training tasks when compared to other algorithms. The number of hidden nodes (n_h) is varied from 2 to 20, choosing the result that provides better training and testing errors. To eliminate the random effects of arbitrary initialization of network weights, ten training process were executed, and therefore the error performance was averaged over ten runs for a given network. The data was normalized into the range of [-1, +1]. The experimental data were separated in two groups, first 40% data samples for model building/training and the remaining 60% samples for testing.

The RBFN was trained using the same data presented previously. The number of hidden nodes (n_h) was varied and

choosing the result that provides better training and testing errors. It was assumed a MSE goal as 0.01.

Because designing an innovative ANN learning procedure is beyond the scope of this paper, routines in the Neural Toolbox of Matlab [11] are used for the estimate of TOT.

The best results for TOT obtained from the ANN are summarized in Table II.

TABLE II

MSE AND EMAX OF THE TOT FOR THE ANN

ANN	MSE	EMAX
SNN ($n_h = 2$)	6.62	- 6.60
SNN ($n_h = 3$)	6.60	6.90
SNN ($n_h = 4$)	5.34	6.40
SNN ($n_h = 5$)	5.24	6.10
SNN ($n_h = 6$)	5.62	- 6.50
TPNN ($d = 1, n_h = 5$)	4.91	6.50
TPNN ($d = 2, n_h = 4$)	4.41	6.30
TPNN ($d = 3, n_h = 3$)	3.87	- 7.80
RNN ($d = q = 1, n_h = 5$)	2.76	- 4.70
RNN ($d = q = 2, n_h = 2$)	3.58	- 5.90
RNN ($d = q = 3, n_h = 6$)	2.96	- 5.00
RNN ($d = q = 4, n_h = 4$)	3.83	- 5.10
RBFN ($d = 1, q = 4, n_h = 19$)	2.62	4.70
RBFN ($d = 2, q = 1, n_h = 20$)	2.59	5.40
RBFN ($d = 2, q = 3, n_h = 28$)	2.14	- 3.90
RBFN ($d = 3, q = 4, n_h = 40$)	2.54	- 4.10
RBFN ($d = 3, q = 2, n_h = 30$)	-2.20	4.20

For SNN it was observed that better training and testing performance with 5 hidden nodes, obtaining $MSE = 5.24$ and $Emax = 6.10$ °C. For TPNN it was compared the results by using the numbers of tapped delay lines as $d = 1, 2, 3$. It was verified that the MSE error decreases reasonably compared to that obtained by SNN. It was observed better training and testing performance with 3 hidden nodes and $d = 3$, obtaining $MSE = 3.87$ and $Emax = - 7.80$ °C. For RNN the results was also compared by using the numbers of tapped delay lines as $q = 1, 2, 3, 4$. The results indicate that the better training and testing performance was obtained with 5 hidden nodes and

$q = 1$, resulting in $MSE = 2.76$ and $Emax = - 4.70$ °C. For RBFN it was compared the results by using the numbers of tapped delay lines as $d = 1, 2, 3, 4$ and $q = 1, 2, 3, 4$. It was verified that the MSE error decreases just a little compared to that obtained by RNN. It was observed better training and testing performance with 28 hidden nodes and $d = 2, q = 3$, obtaining $MSE = 2.14$ and $Emax = - 3.90$ °C.

Table III presents the results of the implemented ANN, showing that RBFN gives better results than SNN, TPNN, and RNN.

TABLE III
COMPARISON BETWEEN THE MSE AND EMAX OF THE BETTER
RESULTS FOR THE IMPLEMENTED ANN

ANN	MSE	EMAX
SNN ($n_h = 5$)	5.24	6.10
TPNN ($d = 3, n_h = 3$)	3.87	- 7.80
RNN ($d = q = 1, n_h = 5$)	2.76	- 4.70
RBFN ($d = 2, q = 3, n_h = 28$)	2.14	- 3.90

Fig. 3 shows performance of the RBFN with 28 hidden nodes, $d = 2, q = 3$ and the prediction error.

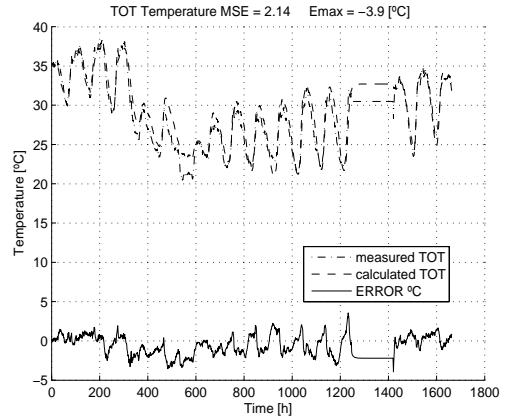


Fig. 3 Actual and estimated TOT with prediction error using RBFN.

C. TOT calculation using LS-SVM

The implementation of LS-SVM is performed by routines of the LS-SVMLab Toolbox version 1.5 [12]. In this toolbox is used an optimization algorithm for tuning the hyperparameters σ and γ of the model with respect to the given performance measure. Using the default values the optimization algorithm was shown efficient but, relatively slow. Then, the design of LS-SVM model of the transformer consists of the following steps:

- As adopted by ANN the experimental data were separate in two groups, first 40% samples will be used for model building/training and remaining 60% samples will be reserved for testing.
- The regularization parameter γ and the parameter σ specifying the width of the kernel are determined using 96 points (24 hours of operation of the transformer), reducing the computational time and avoiding the overfitting of the network. In the simulations was noticed, that a larger number of points in the determination of the hiperparameters results in overfitting of the network, and besides the optimization algorithm used is slow.
- The LS-SVM model is trained maintaining the hiperparameters γ and σ , determined previously. For training it was used 1152 points, corresponding to 288 hours of the transformer operation (first 40% samples). The LS-SVM recurrent is trained as one feedforward network as follows:

$$\hat{y}_{k+1} = f_{ls-svm} \begin{pmatrix} x_k, x_{k-1}, x_{k-2}, \dots, x_{k-d}, y_k, \\ y_{k-1}, y_{k-2}, \dots, y_{k-q} \end{pmatrix} \quad (9)$$

To calculate the p-step ahead prediction, it is used:

$$\hat{y}_{k+p} = f_{ls-svm} \left(\begin{array}{c} x_k, x_{k-1}, x_{k-2}, \dots, x_{k-d}, \\ \hat{y}_{k+p-1}, \hat{y}_{k+p-2}, \dots, \hat{y}_{k+p-q} \end{array} \right) \quad (10)$$

and gradually has to include more previous estimates for the output \hat{y} , until arrives at the p-th sample prediction \hat{y}_{k+p} . In fact the LS-SVM is used as a recurrent model to generate the prediction.

- The LS-VM model can be retrained using the same data set, but with the new estimated outputs shifted through the input vector and old inputs are discarded. The retrained model is simulated using one validation algorithm until small testing error is reached. The retraining was used to improve the result; it is not fundamental.

The better results of the performance of the LS-SVM are summarized in Table IV.

TABLE IV
MSE AND EMAX OF THE TOT BY LS-SVM

LS-SVM	MSE	EMAX [°C]
Recurrent (d = 1, q = 1)	3.93	- 5.60
Recurrent (d = 1, q = 2)	3.58	- 4.50
Recurrent (d = 1, q = 4)	2.36	5.40
Recurrent (d = 2, q = 2)	3.30	- 5.20
Recurrent (d = 2, q = 5)	3.52	5.80
Recurrent (d = 3, q = 3)	2.81	- 4.90
Recurrent (d = 4, q = 2)	1.96	- 4.80
Recurrent (d = 4, q = 3)	2.52	- 4.70
Recurrent (d = 4, q = 4)	1.50	3.70
Recurrent (d = 4, q = 5)	1.97	4.40

It is observed that better testing performance is obtained with $d = q = 4$.

Fig. 4 shows the performed by the recurrent LS-SVM.

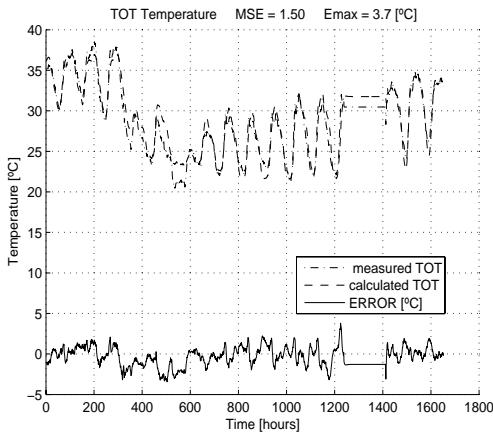


Fig. 4 Actual and estimated TOT with prediction error using recurrent LS-SVM.

D. Comments on the results

Better results of the TOT estimation for each implemented method is summarized in Table V with tabulated the performance values of MSE and Emax.

TABLE V
MSE AND EMAX OF THE MODELS

METHOD	MSE	EMAX
G ANNEX	7.93	- 13.0
SNN ($n_h = 5$)	5.24	6.10
TPNN ($d = 3, n_h = 3$)	3.87	- 7.80
RNN ($d = q = 1, n_h = 5$)	2.76	- 4.70
RBFN ($d = 2, q = 3, n_h = 28$)	2.14	- 3.90
Recurrent LS-SVM ($d = q = 4$)	1.50	3.70

It is important to remark that Recurrent LS-SVM outperforms the other five models considering MSE and Emax. It is also observed that the result achieved with the recurrent LS-SVM was done with one only training of the network.

VI. CONCLUSIONS

The IEEE model, ANN and recurrent LS-SVM are used to estimate TOT of power transformers. Of the six models, the recurrent LS-SVM provided the best performance in terms the MSE and Emax. The superior results obtained with LS-SVM justify its application in the estimate of TOT. It is also recognized that LS-SVM holds a high generalization capability in relation to multilayer feedforward network such as multilayer perceptron trained com backpropagation or other more efficient variation of this algorithm. This is due to the fact that the LS-SVM network is more robust and efficient in identification of complex dynamic plants [8]. Since the LS-SVM training is equivalent to solving a set of linear equations, the solution of the LS-SVM is always unique and globally optimal [8]. A difference with the RBFN is that no center parameters vectors of the Gaussians have to be specified and no number of hidden units has to be defined because of Mercer's condition. For the implementation of the networks it was used the Neural Toolbox [11] and LS-SVMlab Toolbox version 1.5 [12], both of MATLAB, and it was verified that with the default parameters of the respective algorithms the implementation of the LS-VM model is easier than the ANN model. ANN involves more experience for modeling and training of the network, mainly for the definition of the number of hidden layers. Therefore, recurrent LS-SVM can be used as an important alternative to ANN and IEEE method in the estimate of the TOT. We intend to continue the studies on the application of LS-SVM in modeling and simulation transformer internal temperatures using larger dataset obtained from different sites.

ACKNOWLEDGMENT

The authors acknowledge Mr. José Luis Pereira Brittes of the Companhia Paulista de Força e Luz (CPFL) – Brazil, for the experimental data set used in this paper.

REFERENCES

- [1] J. A. Jardini, J. L. P. Brittes, L. C. Magrini, M. A. Bini, and J. Yasuoka, "Power transformer temperature evaluation for overloading conditions," *IEEE Transactions on Power Delivery*, vol. 20, no. 1, pp. 179–184, January 2005.
- [2] IEEE, *Guide for Loading Mineral-Oil-Immersed Transformers*, June 2002.
- [3] V. Galdi, L. Ippolito, A. Piccolo, and A. Vaccaro, "Neural diagnostic system for transformer thermal overload protection," *IEE Proceedings Electric Power Applications*, vol. 147, pp. 415–421, September 2000.
- [4] W. H. Tang, K. Spurgeon, Q. H. Wu, and Z. Richardson, "Modeling equivalent thermal dynamics of power using genetic algorithms," in *Proceedings of the IEEE*, 2002, pp. 1396–1400.
- [5] Q. He, J. Si, and D. J. Tylavsky, "Prediction of top-oil temperature for transformers using neural networks," *IEEE Transactions on PowerDelivery*, vol. 15, pp. 1205–1211, October 2000.
- [6] K. Narendra and K. Parthasarathy, "Adaptive identification and control of dynamical systems using neural networks," in *Proceedings of the 28th IEEE Conference on Decision and Control*, 1990, pp. 1737–1738.
- [7] S. Haykin, *Neural Networks a comprehensive foundation*, Prentice-Hall, 1999.
- [8] V. Vapnik, *The Nature of Statistical Learning Theory*, 1995.
- [9] J. A. Suykens and J. Vandewalle, "Multiclass least squares support vector machines," in *International Joint Conference on Neural Networks*, 1999.
- [10] T. V. Gestel, J. K. Suykens, D. Baestaens, A. Lambrechts, G. Lanckriet, B. Vandaele, B. D. Moor, and J. Vandewalle, "Financial time series prediction using least squares support vector machines within the evidence framework," *IEEE Transactions on Neural Networks*, vol. 12, no. 4, pp. 809–821, 2001.
- [11] H. Demuth, M. Beale, and M. Hagan, *Neural Network Toolbox User's Guide for Use with Matlab*.
- [12] K. Pelckmans, J. Suykens, T. V. Gestel, J. D. Brabanter, B. Hamers, B. Moor, and J. Vanderwalle, *LS-SVMlab Toolbox, Version 1.5*, Katholieke Universiteit Leuven, Department of Electrical Engineering - ESAT-SCDSISTA, February 2003.

OPTIMAL ROUTING WITH QOS GUARANTEES IN THE WIRELESS NETWORKS

P. Venkata Krishna and N.Ch. S. N. Iyengar

School of Computing Sciences

VIT University, Vellore

ABSTRACT.

In the Advanced communication systems, there will be a mixture of different traffic classes each having its own transmission rate characteristics and QOS (quality of service) requirements. In this paper, a QOS oriented optimal routing for wireless networks is proposed. The QOS parameters under the consideration are peak cell rate (PCR), sustained cell rate (SCR) and minimum cell rate (MCR). A call can impose different QOS requirement. A connection admission control (CAC) is required to decide whether a new connection requirement can be accepted or not. Call is admitted on a path if QOS characterization of the path meets the users QOS requirements QOS routing algorithms are based on a "link state approach" where each node maintains the state information on the entire topology. The different type of traffic that may be considered is voice, video and data. The basic idea is to pre- compute the paths in advance of call routing and find the optimize path on turn and which guarantees the calls QOS requirements.

Keywords: Wireless mobile networks, Quality of service (QOS), connection admission control (CAC) etc

INTRODUCTION

Wireless communication service is sweeping the world. Its goal is to establish a mass network for mobile communications and provide a competitive alternative to the conventional wired public switched Tele communication network.

Voice communication over wireless links using cell voice phones has returned and become a significant feature of communications today.

It can be predicted that the next generation of traffic in high – speed wireless networks will be mostly generated by personal multimedia applications providing fax, news on demand, vide on demand, www browsing. For multimedia traffic (voice, video and data) to be supported successfully, it is necessary to provide quality of service (QOS) guarantees between the end -systems.

The QOS provisioning means that the multimedia traffic should get predictable service from the available resources in the communication system. Typical resources are CPU time and network bandwidth. The communication software must also guarantee an acceptable end to end delay and maximum delay jitter qos requirements are specified delay reliability's.

There are two major differences between wire line and wireless networks are due to "link

characterises" and "mobility". The board and links are characterised by high transmission rates (in gbps) and very low error rates.

In contrast wireless links have a much small transmission rate (kbps – mbps) and a much higher error rate. Additionally wireless links experience losses due to multi path dispersion and ray high fielding the second major difference between the two networks is the user mobility.

In wire line networks (UNI) remains fixed through out the duration of a connection needs the UNI in a wireless environment keeps connection. Therefore, it is the usual qos provisioning techniques for wireless networks.

RELATED NETWORK

Recently, some work has been proposed to guarantee QoS for multimedia traffic in wireless networks. Rappport and pursyski have developed any analytical models for a cell mobile environment consisting of mixed platform types with different classes of channel and resource requirements. Prioritizing hand off calls over ordinary ones and incorporating quotas for each type of resources, various performance measures like carried traffic, blocking and forced termination probabilities for each platform and call type are numerically computed from the analytical models.

Based on the minimum resource requirement criteria provided by the users, oliceia proposed a bandwidth reservation algorithm for guaranteeing QOS to multimedia traffic. For real time traffic, the call is admitted only if the requested band width can be reserved in the call originating cell and all its neighbours. For a non real time cell, the requested bandwidth is reserved only in the originating cell. Although this scheme guarantees QOS the main defects are

1. Bandwidth is reserved feudality since the user moves only to one of the six neighbouring cells consuming hexagonal cell geometry, and
2. The stringent call admission procedure might not admit many real time requests in a highly overload system.

The carried traffic in a wireless network can be increased by the "Graceful delegation" of some or all of the existing services in the system seal and sign identified two QoS parameters, namely graceful defalcation of service with the help of user supplied "loss profiles" bandwidth usage of application that can sustain loss is degraded in situations where user demands

OPTIMAL ROUTING WITH QOS GUARANTEES IN THE WIRELESS NETWORKS

exceed the networks capacity to satisfy them. A new transport supplies is proposed to implement loss profiles by selectively discarding data from special applications like a compressed vide stream.

Guillermo Barrenetxea et. Al [4] proposes an optimal routing based limited queuing stuructures for various types of networks.

1.2) CONTRIBUTIONS OF THIS WORK :-

Most of the existing literature deals separately with resource reservation approaches and call admission control in wireless multimedia networks. The most important contribution of this work is the development of an integrated frame work for QOS provisioning. Combining call admission control, peak cell rate (PCR), sustained cell rate (SCR) and minimum cell rate (MCR) using a different technique called " Dijkstras algorithm" the dynamic, error phone behaviour of wireless physical link necessitates such a QOS control scheme.

One of the important motivations behind our QOS frame work is to provide different treatment to the two important classes of wireless multimedia traffic – those generated respectively by real time (delay sensitive) and non real time (delay tolerant) applications. Our paper deals with links real time traffic of course.

The performance of this QOS provisioning frame work is captured through various analytical models and simulation experiments. Analytical models show our reservation and call admission procedures significant improvement is predicated which is also validated with simulation experiments.

The rest of the paper is organised as follows :-

The general principles for QOS provisioning are described. we develop some models based on Dijkstras algorithm with the details of the simulation experiments and concludes the paper.

2. GENERAL PRINCIPLES FOR QOS PROVISIONING :-

The contract between the customers and the network has three plats.

1. The traffic to be offered
2. The service agreed upon
3. The compliance requirement

The first fact of the contract is "traffic descriptor" It characterizes the load to be offered second plat of the contract specifies the quality of service described by the customer and accepted by the carrier. Both the load and service must be formulated in terms of measurable quantities.

PCR is the maximum rate at which sender is planning to send cells. SCR is the expected or required cell rate averaged over a long time interval. MCR is the minimum number of cells per second that the customer considers acceptable. If the carrier is unable to guarantee to provide this much bandwidth, it must reject the connection.

This paper makes use of MCR as the quality of service parameter in finding the optimal route between the source and the destination, guarantees the users specified QOS before the call is being routed. To ensure that the application required QOS parameter namely PCR, SCR, MCR jitter are satisfied, admission and congestion control mechanism is enforced at the medium aces control (MAC) layer.

SOURCE CHARACTERIZATION

DATA TRAFFIC

Generation of data from a single source is characterised by Poisson arrival process because the packet inter arrivals match a constant plus exponential arrival.

Interactive data transmission generates a single cell where as a bulk data transmission (file transfer) generates number of cell at once. In wireless networks, since the packet size is fixed and is small compared to data packet size, each data packet is broken down into multiple cells.

VOICE TRAFFIC:-

Human speech has been transmitted on a real conversational basis primarily using circuit switched network where a circuiting dedicated to each conversation for the duration of the conversation.

PARAMETERS OF VOICE TRANSMISSION:-

One major QOS parameter is the probability that a call attempt will succeed. Alternatively, blocking probability can be used, which is one's complement of the former.

Another important parameter is the quality of telephone conversation, perceived speech quality (PSQM), of the mean opinion score (MOS). This is obtained by subjective listening tools, where a group of listeners with different linguistic back grounds evaluate a series of speech samples by a score from one (unintelligible) to five (perfect).

The boundary between unacceptable speech quality and a lost call is quite subjective and arbitrary, and depends on many factors, including the cost / minute of the call, level of interactively, status of the column.

Voice traffic can be modelled as an alternating burst of talk spurts and silences. During each burst, voice calls are generated periodically and during silent periods no cells are generated. The burst of the voice packets is represented by the ON state and silence period by the OFF state.

**B**

Each voice source is modelled as an ON / OFF process. $E[\lambda_N]$ is the mean arrival rate, $\text{Var}[N]$ is the variance and a is a constant from the OFF state to the ON state (birth rate) is given by

$$\alpha = P F_p / (1 - P) L_B$$

Death rate is given by $\beta = F_p / L_B$ cell emission rate in the ON state

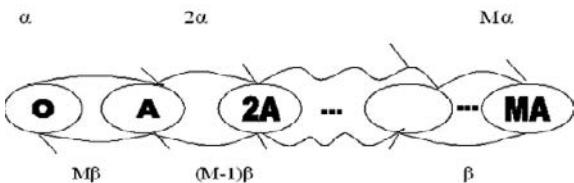
$$A = F_p / L_1$$

Where

- ❖ L_1 is the length of cell pay load
- ❖ F_p is the peak bit rate
- ❖ P , the activity factor is the ratio of bit rate and F_p
- ❖ L_B is the mean burst length

VIDEO TRAFFIC

Applications supporting video requires large bandwidth and need to meet the quality constraints of both cell fitter and cell loss probability. Even though video traffic generates correlated cell arrivals as in voice, its statistical nature is different from voice source. It is produced by encoding subsequent video frames that are generated at a rate of 30 frames per second for full motion video. Video signal exhibits spatial as well as temporal correlation.



To model the video traffic, a quantized bit rate process is assumed, the arrivals will take values which are integral multiples of a "Quantization step" – A . The continuous rate will be sampled at Poisson points and the bit rate becomes a continuous time process.

The rate assignments are based on the assumption that a process in the low activity state is

more likely to transit to a higher activity state than to an ever lower activity state and vice versa, one quantization step at a time.

For the given bimodal α , β and A are given by,

$$\beta = a / \{ (1 + N * E^2 [\lambda_N]) / (M * \text{Var}[N]) \}$$

$$a = \alpha - \beta$$

$$A = \{ \text{Var}[N] / E[\lambda_N] \} + \{ E[\lambda_N] / M \}$$

Where $E[\lambda_N]$ is the mean arrival rate, $\text{Var}[N]$ is the variance and a is a constant which is determined by the proper tuning of the parameters.

3. ANALYSIS MODELS:-

PROBLEM STATEMENT

To provide optimal path wire path cost for a call between a source and destination that assures a guaranteed to end QOS before its routing.

OVERALL FRAMEWORK :

A Network that supports both packets and packets with QOS guarantees is considered.

QOS capable router in such network is able to dedicate some of its resources to satisfy the requirements of QOS packets. Such routers are also assumed to identify and advertise their resources that remain available for additional QOS flows in order to maximise the throughput.

A call can impose requirements on 4 metrics which include delay bandwidth, jitter and loss.

A Connection Admission Control (CAC) function is required to decide whether a new connection request can be accepted or not. A call can be admitted on a path if the QOS characterization of the path needs the users QOS requirements.

On processing a request, a path that seems to be most suitable for the given flow requirements is returned. On-demand algorithm addresses bandwidth and delay requirements by first pruning unsatisfactory links and then computing the paths that satisfy the user's QOS requirements. Determining what type of paths to pre-compute is one of the key design issues in QOS routing.

Once a suitable path has been identified, the flow is assigned to it (pinning) and remains assigned to it until it either releases the path (unpinning) or has become unsuitable because of some link failure. Another issue arises when several pre-computed paths satisfy the requirements of a call. The solution is to order the pre-computed paths according to a policy

OPTIMAL ROUTING WITH QOS GUARANTEES IN THE WIRELESS NETWORKS

(from maximum to minimum bandwidth). When a call request arrives the list of pre-computed paths are traversed to find a feasible path. Two options are available:

1) The feasible path is to be assigned to the incoming call. This speeds up the call set up time.

However this may raise the blocking probability since it does not consider needs of the future calls.

2) The path whose QoS guarantees are closest to QoS requirements of the call are to be assigned. If a call with large delay arrives it is preferable to assign a large delay path in order to save the paths with smaller delay for the future calls.

On-demand algorithm only needs to find paths to a single destination since it is executed after the call request has arrived and thus the destination is specified. The requirements of pre-computed paths algorithm need not be strict since they are run in the background, but that of on-demand algorithm are strict since this is run while the call is waiting to be routed.

SIMPLIFYING ASSUMPTIONS:

The path selection algorithm should select a path that satisfies the bandwidth requirements and minimizes the network resources and possible computing overhead. The path selection algorithms are based on trade-offs between accuracy, computational complexity and ease of implementation, metrics on which the algorithm operates and link state advertisements.

Metrics:

The network prefers to select the cheapest among all the paths suitable for a new flow. It may not accept a new flow whose identified feasible path has a too high cost of path.

Link available bandwidth:

Associated with each link there is a maximal bandwidth value. For a link to accept a new flow with a given bandwidth requirements, at least that much bandwidth must be still available on the link.

Path cost:

It is used as a measure of path cost to the network. A path with lesser cost is preferable.

Policy:

The policies are used to prune from the network links that are incompatible (performance / character wise) with the requirements of the flow. A special policy is the elimination of high latency links when considering a path selection for delay sensitive flows.

Advertisement of link state information:

Router maintains an updated database of the network topology including current state of each link, so that it can make the most accurate decision on which path to select. This causes very frequent updates. Another alternative is frequent updates, where the period of updates is based on the tolerable load on the network and the routers. The main disadvantage is that the major changes in the bandwidth available on a link could remain unknown for a full period and therefore may result in incorrect routing decision.

Path selection algorithms:

The aspects to path selection algorithms includes the optimization criteria it relies on, the exact topology on which it is run, and when it is invoked. The invocation of the algorithm can be per flow or when warranted by changes in the link states. The topology is a two way directed graph with routers and nodes as vertices connected with weighted edges or links. The optimization criteria is reflected in the costs associated with each interface in the topology.

This cost is a function of link-cost and amount of bandwidth that remains available on this interface. It is combined with link-cost information to provide a cost value. It picks up a path with minimum cost that can support requested bandwidth. The proposed algorithm is a double objective path optimization because of specific nature of two objectives being optimized (bandwidth, path-cost) in contrast to single objective optimization of standard routing algorithm.

Computation of k-shortest paths:

Given a graph $G=(V,E)$ a weighing function on the arcs $I:E \rightarrow R$, a source node s , a target(destination) node t , and an integer k , find the k - different paths between s and t whose total weight is minimum in order of increasing weight.

When $k=1$, the shortest path problem can be stated as the resolution of well-known Bellman equations. If the graph does not contain the cycles, the Bellman equations can be solved in $O(|E|)$ time by visiting the node in topological order. If the graph contains cycles but no negative arcs, then the Dijkstra algorithm solves the equations in $O(|E| + |V| \log |V|)$ time.

Otherwise they can be solved by means of Bellman Ford algorithm, iterative procedure requiring $O(|V|^*|E|)$ time. Bellman and kabala generalized the Bellman equations for the case $k=2$. The algorithm proposed by these authors consisted of first finding the shortest path from s to all other nodes and, then, of computing their respective second shortest paths by an iterative procedure similar to the Bellman Ford algorithm.

Dreyfus extended the Bellman Kabala equations to the general case and proposed important improvements to the method of resolution. The time complexity of the Dreyfus algorithm is $O(A+K^*|V| \log d)$, where d is the maximum input degree, A is the asymptotic time complexity of computing the shortest path from s to all nodes in V . This algorithm computes the k -shortest paths from s to all the nodes in V even if K -shortest paths are of interest. Therefore its best-case time complexity is $O(A + K^* |V|)$. Sheir proposed several methods for the computation of the k -shortest paths.

In practice, the so-called label setting algorithm was shown to be the most efficient one. It can be seen as generalization of Dijkstra's shortest path algorithm and works only in graphs with non-negative arcs.

The time complexity of this algorithm is $O(k^2 |E| + k^*|V|^* \log |V|)$. It generates all paths starting at s and

ending at any other node of v whose length smaller than the length of k -shortest path from s to t .

Simulation results:

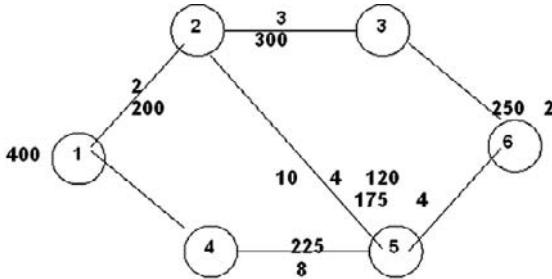


FIG. D.1 SIMULATION GRAPH

Sample Data:

```

Enter the number of nodes:6
Enter the two nodes, linkwt, link capacity(Mbps): 1 2 2 200
Any links left 1/0: 1
Enter the two nodes, linkwt, link capacity(Mbps): 1 4 4 120
Any links left 1/0: 1
Enter the two nodes, linkwt, link capacity(Mbps): 2 3 3 300
Any links left 1/0: 1
Enter the two nodes, linkwt, link capacity(Mbps): 2 5 10 400
Any links left 1/0: 1
Enter the two nodes, linkwt, link capacity(Mbps): 4 5 8 225
Any links left 1/0: 1
Enter the two nodes, linkwt, link capacity(Mbps): 3 6 2 250
Any links left 1/0: 1
Enter the two nodes, linkwt, link capacity(Mbps): 5 6 4 175
Any links left 1/0: 0
Network details stored in the file:
6 1 2 3 4 5 6
1 2 2 200
1 4 4 120
2 3 3 300
2 5 10 400
4 5 8 225
3 6 2 250
5 6 4 175

```

OUTPUT

```

Enter Source, Destination, MCR(Mbps): 1 5 200
Available Paths are:
Path 1: 1 → 3 → 6 → 5 →
Min flow (Mbps): 175 Path cost: 11
Path 2: 1 → 5 →
Min flow (Mbps): 200 Path cost: 12
Path 3: 1 → 4 → 5 →
Min flow (Mbps): 120 Path cost: 12
Path 2 is suitable
Link capacities are updated
Enter Source, Destination, MCR (Mbps): 2 6 100
Available Paths are:
Path 1: 2 → 3 → 5 →
Min flow (Mbps): 250 Path cost: 5
Path 2: 2 → 5 → 6 →

```

Min flow (Mbps): 175 Path cost: 14

Path 2 is suitable

Link capacities are updated

Conclusions

In this paper, an efficient, dynamic call routing methodology is being proposed which is suitable for real time application in wireless networks. This algorithm during its first phase finds all the possible paths between a source and destination and also finds the minimum bandwidth offered by each of the paths. During its first phase, finds all the possible paths between a source and destination and also finds the minimum bandwidth offered by each of the paths. During its second phase, the user's QoS requirement (MCR) is checked against the above results. The path that guarantees the user's QoS is selected that has the best path cost (optimal route). The amount of bandwidth required by the users call is dedicated and the remaining bandwidth is made available for the future calls in order to maximize the throughput. If none of the paths is suitable then the call is rejected and will be considered when ever the required bandwidth is available. Limiting the pre computation of paths between a source and destination can extend this project, so that the call can be routed within users setup time. Also a number of other QoS can be enforced on a particular call for it's routing

References:

- [1]. Guerin, and Orda,"QoS-Based Routing in Networks with Inaccurate Information: Theory and Algorithms", IBM Research Report, 1996.
- [2]David Eppstein , "Finding the k shortest paths" ,5th Workshop.Algorithms& Data Structures,Lecture Notes in Computer Science.1272,pp.234-247,March 31,1997.
- [3] Cheng Tang,Shree Murthy,Darrell and D.E.Lang, "Performance Guarantees on ATM Networks."IEEE,78(1):pp204-221,1990.
- [4]Guillermo Barrenetxea, Baltasar Berfull-Lozano and Martin Vetterli, "Lattice Networks: Capacity Limits, Optimal Routing and Queueing Behavior" IEEE/ACM Trans. On Networking Vol. 14, No. 3, June 2006 pp 492-505.
- [5] Victor Marques, Rui L. Aguiar, Carlos Garcia, Jose Ignacio, Chirstophe Beaujean, Eric Melin and Marco Liebsch, " An IP Based QoS Architecture for 4G Operator Scenarios", IEEE Wireless Communications, June 2003 pp 54-61
- [6] Xiaoyan Hong, Kaixin and Mario Geria, " Scalable Routing Protocols for Mobile Adhoc Networks" IEEE Trans. on Network July/August 2002 pp11-20

RFID IN AUTOMOTIVE SUPPLY CHAIN PROCESSES - THERE IS A CASE

Viacheslav Moskvich, PhD, Assoc.prof. Vladimir Modrak, PhD

Technical University of Kosice, Faculty of Manufacturing Technologies

Department of Manufacturing Management

Bayerova 1, 080 01, Presov , Slovak Republik

Abstract: Presented article is focused on analysis of RFID system implementation influence on automotive supply chain. Mathematical model of supply chain structure and function was created to analyze the impacts. Case study was conducted to prove economical feasibility of RFID implementation at automotive OEM and its 1-tier supplier.

I. INTRODUCTION

Product proliferation and customization leads to greater fulfillment of customer demands and growth of company's market share. However such hi-tech product as automobile is not easy to customize for individual requirements of a client. Customization of products adds greater complexity to product identification and company logistics by increasing assortment [1]. Competitive market environment also force companies to cut their costs and thus reduce their prices. With increasing assortment a cost reduction becomes a difficult task to accomplish. For last decade main philosophy for cost reduction for OEMs was a lean manufacturing [2]. The key to lean manufacturing is to compress time by eliminating waste and thus continually improve processes inside the company [3]. Waste can be defined as any element of production that only increase cost without adding value the customer is willing to purchase [4].

There are seven basic wastes in manufacturing process:

- overproduction
- excess inventory
- idle machine or operator time
- manipulation
- non-value added material flow
- defects
- extra processing

To eliminate excess inventory, manipulation and non-value added processes Just-In-Time (JIT) deliveries were applied in conjunction with lean manufacturing philosophy. In reality JIT deliveries were conducted in small batches several times a day. Basically JIT system moved a stock from OEMs to their suppliers. Consequently, to resolve the problem, Just-In-Sequence (JIS) system was introduced [5]. Philosophy behind Just-In-Sequence supply means deliveries of the products directly to the assembly line of OEM not only at exact amount and time (like in JIT) but also at right configuration and right order - sequence. If part or module is not delivered in right sequence and time, it cannot be assembled on the individually configured product, coming to the assembly line in certain sequence and therefore it will cause an assembly line to stop. Interruption of the assembly process will induce a considerable financial loss not only for OEM but also for all elements in supply chain [6]. This means that 100% on time, right sequenced deliveries for elimination of excess inventory; manipulation and non-value processes should have a highest priority for the management of OEM [5].

Securing right sequenced deliveries also means securing the correct information on material flow. Without such an information managing a growing assortment of products through the whole supply chain becomes increasingly difficult task for logistic departments. Following information are required at different stages of supply chain for managing the material flow:

- type of item
- individual identification number
- manufacturer/ supplier
- date of manufacturing
- current location
- item path
- batch details

- package details

Providing such an information to the logistic departments manually requiers additional staff and financial investments [7]. With the aim of cost reduction the companies have to find a solution for automatic information collection to keep the expences low.

Introduction of Just-In-Sequence system with automatic information collection into the supply chain meets considerable obstacles of strategic, tactical and operational character. The major one is a purchase and implementation costs. The major market players as WalMart or U.S. Department of Defence pursued their suppliers to introduce RFID technology to track and trace their supplies trough the whole supply chain [8] and therefore make initial investment to withstand the growing competitive pressure. But would it be econnomically sensible for suppliers to introduce such a system without a pressure from their market leading clients?

II. THE WAY TO FIND A PROVE

To prove that there is a case for intermediate suppliers to introduce RFID system for tracking and tracing of products it would be necessary to conduct a preliminary feasibility study. Nevertheless feasibility study requiers not only a prove of functionality of such a system trough the whole supply chain but also an economical feasibility and future profit promise. To gain such a prove it would be necessary to literarily build up this system. The other way is to create a mathematical model of supply chain structure and functions to analyze the impact of RFID system implementation. As it was mentioned the cost reduction is the main goal for every manufacturing company so this parameter would be a good starting point to analyze the impact.

Economical problems are best described by means of linear programming [9]. A *Linear Programming* problem is a special case of a *Mathematical Programming* problem. From an analytical perspective, a mathematical program tries to identify an *extreme* (i.e., minimum or maximum) point of a function, which furthermore satisfies a set of constraints. Linear programming is the specialization of mathematical programming to the case where both, function f - to be called the *objective function* - and the problem constraints are *linear*

[10]. For Linear Programming problems, the *Simplex* algorithm, provides a powerful computational tool, able to provide fast solutions to very large-scale applications, sometimes including hundreds of thousands of variables (i.e., decision factors). Although this algorithm is quite efficient in practice, and can be guaranteed to find the global optimum if certain precautions against *cycling* are taken, it has poor worst-case behavior [9]. Therefore for finding a solution for every condition of mathematical model of supply chain structure and functions with an aim of cost reduction a parallel push-pull method will be used.

III. MATHEMATICAL MODEL

Mathematical model of the automotive supply chain have to describe a structure and functions precisely. The overall structure of automotive supply chain is characterized by single OEM factory with certain amount of first and second tier suppliers and clients (see Fig.1). Clients are mainly represented by a distribution centers. Mathematical modelling of complete structure of automotive supply chain is a complex problem since the functional dependence of individual parts of a structure grows rapidly when moving up or down the supply chain from the OEM position. To find a prove whether implementation of RFID system has a positive economical impact on the supply chin costs it would be reasonable to calculate only with certain parts of the supply chain with their complete functions and relations. Following scheme depicts a part of automotive supply chain which would be modelled by means of linear programming.

Mathematical model functions could be described as follows:

An order from a client enters the distribution center (DC) at a time $t = 0$. It is distributed to the OEM factory and 1st and 2nd tier suppliers by means of RFID information system at a time nearly equal to $t= 0$. Order is included into the production plan of OEM factory to be completed in certain period of time T. To satisfy all customer orders and avoid bulding up a stock OEM factory have to supply exact amount of final products equal to amount of customer orders in Just-In-Sequence manner. That means that OEM factory will not be using the stock of final products from a warehouse but it has to

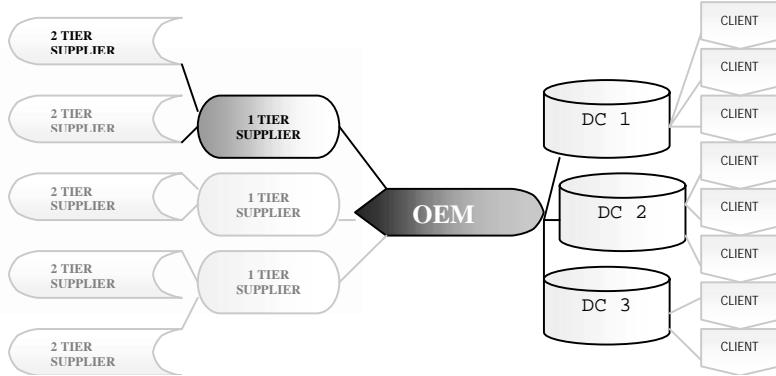


Fig. 1 Scheme of automotive supply chain structure for mathematical modelling

manufacture all the product to be delivered to DC during the time period T. Let the $x_{i,t}$ be the number of products manufactured by OEM during the time period $t = 0 \dots T$. For manufacturing of $x_{i,t}$ products OEM has to secure appropriate amount of subassemblies by ordering them from a 1st tier suppliers. Just-In-Sequence system of deliveries means that OEM can not use the subassembly warehouse. In reality current transportation restrictions and the fact that not all the 1st tier suppliers are located inside the joint industrial park (for providing < 30min. deliveries) with OEM. Therefore OEM factory is forced to have in-bound subassembly warehouse. Nevertheless JIS system allows factory to cut their security stock of subassemblies to 0 units. Mathematical model will calculate with existance of in-bound warehouse. That means that an overall amount of subassemblies form manufacturing the $x_{i,t}$ products during the time period $t = 0 \dots T$ will be $z_{p,t} + q_{p,t}$ where $z_{p,t}$ is an amount of p-subassemblies located at the in-bound warehouse and $q_{p,t}$ je is amount of p-subassemblies that have to be ordered from a 1st tier suppliers. 1st tier supplier has to satisfy the request from OEM factory by manufacturing of appropriate amount of p-subassemblies without having the completed subassemblies in out-bound warehouse. Amount of subassemblies manufactured at factory of 1st tier supplier „j“ would be $a_{p,i,t}$. 1st tier supplier „j“ can use a material from stock in in-bound warehouse or order the material from 2nd tier suppliers. Then the overall amount of material required by 1st tier supplier „j“ to manufacture the $a_{p,i,t}$ number of subassemblies would be $c_{l,i,t} + f_{l,i,t}$ where $c_{l,i,t}$ is amount of material „l“ in warehouse and $f_{l,i,t}$ je is amount of material to be ordered from 2nd tier suppliers during the time period $t = 0 \dots T$.

system requiers higher periodicity of deliveries during the time period $t = 0 \dots T$. The amount of subassemblies delivered to OEM factory will be equal to amount of purchased subassemblies $q_{p,t}$. Number of final products of i-type to be delivered to DC „k“ during the time period $t = 0 \dots T$ would be $u_{i,k,t}$.

Mathematical model has to find a optimum of overall expences and therefore it has to calculate with following costs:

- $VN_{i,t}$ – manufacturing and assembly costs of i-type final product at OEM
- $MN_{p,t}$ – warehousing costs of p-type subassembly at OEM
- $LN_{p,t}$ – purchase costs of p-type subassembly
- $HN_{i,k,t}$ – warehousing costs of i-type final product at „k“ DC
- $FN_{p,j,t}$ – manufacturing costs of p-type subassembly at „j“ 1st tier supplier
- $KN_{l,n,t}$ – warehousing costs of l-type material at „j“ 1st tier supplier
- $WN_{l,j,t}$ – purchase costs of l-type material from 2nd tier supplier
- $T_{p,j,t}$ – transportation costs of p-type subassembly to OEM factory
- $TC_{i,k,t}$ – transportation costs of i-type final product to DC

All mentioned costs will represent the constants of mathematical model and will be calculated for a time period $t = 0 \dots T$. Variables of mathematical model will be represented by individual quantities of material, subassemblies and final products which a modelled supply chain will need to meet customer demands with lowest possible costs.

Variables to be included into the model:

- $x_{i,t}$ – amount of i-type final products to be manufactured at OEM
- $z_{p,t}$ – amount of p-type subassemblies at warehouse of OEM
- $q_{p,t}$ – amount of p-type subassembly OEM has to order from 1st tier supplier
- $d_{i,k,t}$ – amount of i-type final products stocked at DC
- $a_{p,j,t}$ – amount of p-type subassembly manufactured at „j“ 1st tier supplier
- $c_{l,j,t}$ – amount of l-type material at warehouse at „j“ 1st tier supplier
- $f_{l,j,t}$ – amount of l-type material „j“ 1st tier supplier has to order from 2nd tier supplier
- $u_{i,k,t}$ – amount of i-type final products to be delivered to DC

All costs are calculated for a time period $t = 0 \dots T$. Mathematical model for calculation of optimal overall expences of automotive supply chain will have a following form:

$$\begin{aligned} & \min \sum_{i=1}^n \sum_{t=1}^T VN_i x_{i,t} + \sum_{p=1}^P \sum_{t=1}^T MN_p z_{p,t} + \sum_{p=1}^P \sum_{t=1}^T LN_p q_{p,t} + \sum_{p=1}^P \sum_{j=1}^J \sum_{t=1}^T FN_{p,j,t} a_{p,j,t} \\ & + \sum_{l=1}^L \sum_{j=1}^J \sum_{t=1}^T KN_{l,j,t} c_{l,j,t} + \sum_{l=1}^L \sum_{j=1}^J \sum_{t=1}^T WN_{l,j,t} f_{l,j,t} + \sum_{i=1}^n \sum_{k=1}^K \sum_{t=1}^T HN_{i,k,t} d_{i,k,t} \\ & + \sum_{p=1}^P \sum_{j=1}^J \sum_{t=1}^T T_{p,j,t} q_{p,j,t} + \sum_{i=1}^n \sum_{k=1}^K \sum_{t=1}^T TC_{i,k,t} u_{i,k,t} \end{aligned}$$

Restrictions to mathematical model:

$$\begin{aligned} & \sum_{i=1}^n \sum_{k=1}^K \sum_{t=1}^T CAP_{i,k,t} \geq \sum_{i=1}^n \sum_{k=1}^K \sum_{t=1}^T d_{i,k,t} \geq \sum_{i=1}^n \sum_{k=1}^K \sum_{t=1}^T \delta_{i,k,t} \\ & \sum_{i=1}^n \sum_{k=1}^K \sum_{t=1}^T u_{i,k,t} \geq \sum_{i=1}^n \sum_{k=1}^K \sum_{t=1}^T d_{i,k,t} \end{aligned} \quad (3)$$

$$\sum_{i=1}^n \sum_{t=1}^T x_{i,t} = \sum_{i=1}^n \sum_{k=1}^K \sum_{t=1}^T u_{i,k,t} \quad (4)$$

$$\sum_{i=1}^n r_{i,p} x_{i,t} = z_{p,t} + q_{p,t} \quad (5)$$

$$\sum_{p=1}^P \sum_{t=1}^T o_{p,t} \geq z_{p,t} \quad (6)$$

$$\sum_{p=1}^P \sum_{t=1}^T q_{p,t} = a_{p,j,t} \quad (7)$$

$$\sum_{p=1}^P m_{p,l} a_{p,j,t} = c_{l,j,t} + f_{l,j,t} \quad (8)$$

$$\sum_{l=1}^L \sum_{j=1}^J \sum_{t=1}^T o_{l,j,t} \geq \sum_{l=1}^L \sum_{j=1}^J \sum_{t=1}^T c_{l,j,t} \quad (9)$$

$$d_{i,k,t} = T \cdot u_{i,k,t} \quad (10)$$

$$z_{p,t} = T \cdot q_{p,t} \quad (11)$$

$$x_{i,t} \geq 0 \text{ and integer} \quad (12)$$

$$b_{p,j,t} \geq 0 \text{ and integer} \quad (13)$$

$$y_{i,t} \geq 0 \text{ and integer} \quad (14)$$

$$c_{l,j,t} \geq 0 \quad (15)$$

$$z_{p,t} \geq 0 \text{ and integer} \quad (16)$$

$$f_{l,j,t} \geq 0 \quad (17)$$

$$q_{p,t} \geq 0 \text{ and integer} \quad (18)$$

$$d_{i,k,t} \geq 0 \text{ and integer} \quad (19)$$

$$a_{p,j,t} \geq 0 \text{ and integer} \quad (20)$$

$$u_{i,k,t} \geq 0 \text{ and integer} \quad (21)$$

$$i=1..n; \quad j=1..J; \quad p=1..P; \quad k=1..K; \quad l=1..L; \quad t=1..T \quad (22)$$

where

δ - amount of customer orders entering the supply chain to be satisfied

d - amount of final products at DC

CAP – storage capacity of DC

u – amount of final products transported to DC

x – amount of final products manufactured at OEM

r – is amount of p-type subassemblies required for manufacturing of one final product x

z – amount of subassemblies OEM will use from a warehouse

q – amount of subassemblies OEM will purchase from 1st tier supplier

o – capacity of subassembly warehouse of OEM

a – amount of p-type subassemblies manufactured at 1st tier supplier

m – is amount of l-type material required for manufacturing of one subassembly

z – amount of subassemblies OEM will use from a warehouse

q – amount of subassemblies OEM will purchase from 1st tier supplier

o_l – capacity of material warehouse of j 1st tier supplier

If Little's law is applied then amount of final products delivered to DC could be described as

$$d_{i,k,t} = T \cdot u_{i,k,t} \quad (23)$$

and also amount of subassemblies delivered to OEM could be described as

$$z_{p,t} = T \cdot q_{p,t} \quad (24)$$

IV. CASE STUDY

To prove that RFID technology could be a solution for cost reduction in supply chain a case study was conducted on the ground of international automotive OEM and his 1st tier supplier. Due to the fact that all experiments required confidential economical information the OEM and supplier would not be named. Special mathematical model solver was developed using the Visual Basic. First the impact of RFID technology implementation on manufacturing process of OEM was analyzed. Figure 2 depicts the behaviour of final product production quantity curve depending on amount of customer orders. As it is evident implementation of RFID technology leads to linearization of mentioned dependence.

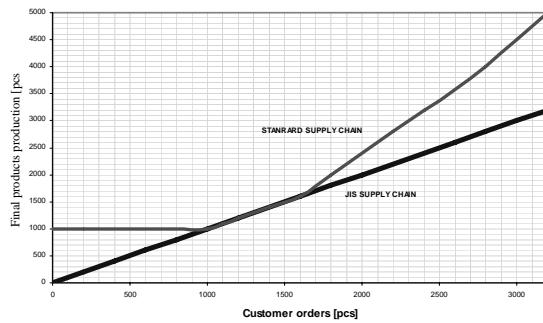


Fig. 2 Final product production quantity dependence on customer orders.

Next an impact on overall supply chain costs was analyzed. Depending on customer orders a behaviour of overall costs was constructed comparing two types of supply chain – standard and RFID one.

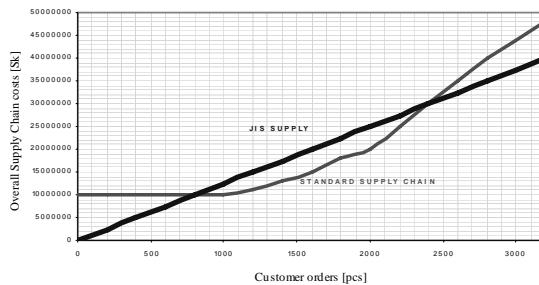


Fig. 3 Overall supply chain costs dependence on customer orders.

Analysis proved that use of RFID technology in supply chain can lead to overall costs reduction at certain conditions. Major restrictions to unconditional cost reduction is an amount of customer orders since in case of medium demand the cost savings would not cover the rising transportation expences. It is also necessary to understand that behaviour of mentioned overall costs curve is strongly individual for this case study and depending on many factors such as level of automation, production rates, product type etc.

Since the implementation of RFID technology did not lead to unconditional overall costs reduction it was necessary to analyze how it will influence storage and transportation quantities and costs. Comparison of this expences could be a way to a solution of optimal manufacturing rates and transportation quantities. Following figure 4 shows the influence of RFID technology implementation on overall supply chain costs depenting on amount of customer order and storage quantities.

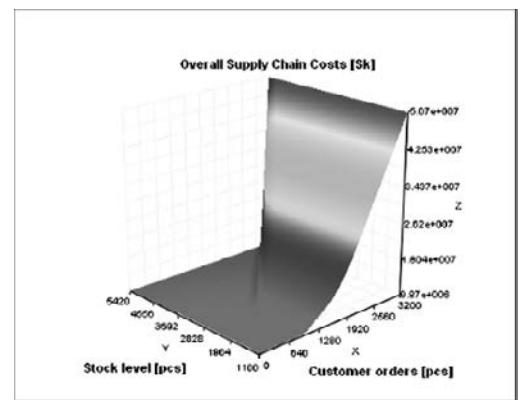


Fig.4a Overall supply chain costs dependence on customer orders and stock level before RFID implementation

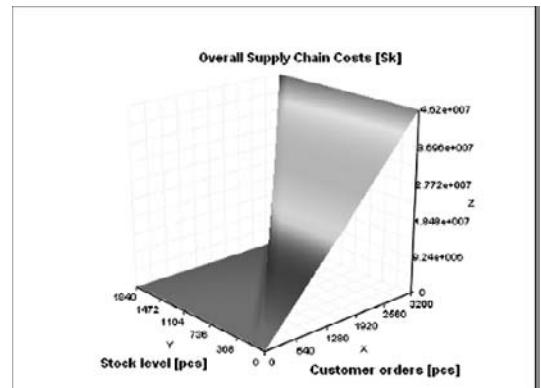


Fig.4b Overall supply chain costs dependence on customer orders and stock level after RFID implementation

Figure shows that RFID technology implementation reduced stock up to 294% with overall supply chain costs reduced by up to 9%.

Finally the transportation quantities through the supply chain had to be analysed because it was evident that implementation of RFID technology would lead to the growth of transportation requirements. Figure 5 shows the dependence of material and subassemblies transportation quantities depending on customer orders.

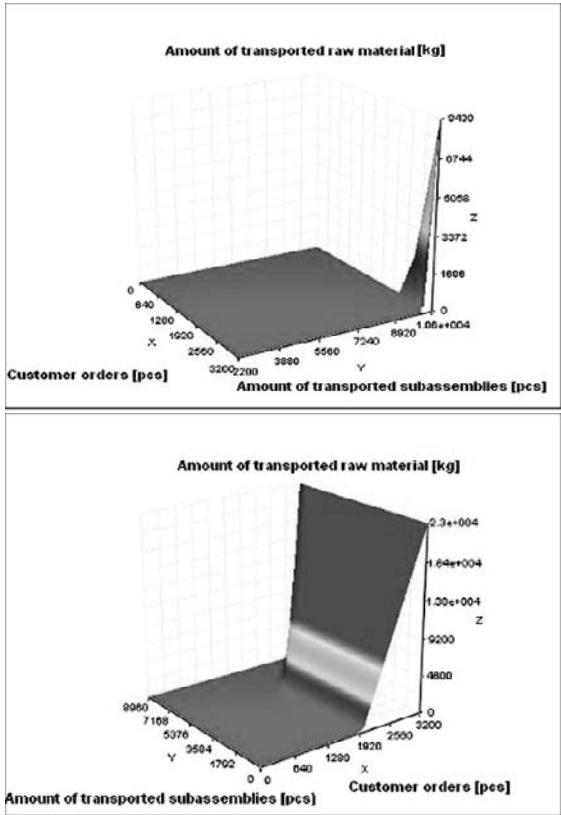


Fig.5 Transported raw material and subassemblies dependence on customer orders before and after the RFID implementation

As it is evident the transportation quantities raised by up to 228% after the implementation of RFID technology comparing to standard supply chain. Nevertheless overall supply chain costs did not increase.

V. CONCLUSION

Case study conducted for automotive supply chain proved that implementation of JIS system with RFID technology influence overall supply

chain costs but considerable reduction of expences and cost savings are not automatically caused by simple implementation of RFID. As it was proved the balance should be found between rising transportation rates and expences and costs saving from elimination of stock and warehousing operations. Therefore feasibility studies have to be conducted for every single case of RFID implementation into the supply chain. Mathematical modelling is reasonable tool to conduct such studies since it does not require any „hardware“ investments and can give an answer on most of the important economical feasibility questions. Without a prove of economical sensibility individual supply chain participants would not face initial RFID technology implementation costs by their own will and would be simply pushed by their market leading customers. Nevertheless with appropriate functional model of RFID integration into their supply chain operations companies could achieve considerable cost reduction and therefore became more competitive on the market.

REFERENCE

- [1] Viswanadham,N., 2002. Past, present and future of Supply chain automation. In *IEEE Robotics and automation magazine*
- [2] Taylor,D. ,Brunt,D., 2000. *Manufacturing Operations and Supply Chain Management The LEAN Approach*"
- [3] Czarnecki, H., Loyd, N., 2000. *Simulation of Lean Assembly Line for High Volume Manufacturing*. Center for Automation and Robotics, University of Alabama
- [4] Ohno, T., 1988. *Toyota Production System*, Productivity Press
- [5] ALTA A/S,2003. *White paper, Strategies for in sequence supply*, Copenhagen
- [6] Chappell, G., Ginsburg, L., Schmidt, P.,Smith, J., Tobolski, J., 2003. *Auto-ID on the Line: The Value of Auto-ID Technology in Manufacturing*, Auto-ID Center, Massachusetts Institute of Technology, Cambridge
- [7] Modrak, V. 2005. Functionalities and Position of Manufacturing Execution Systems. In *Encyclopedia of Information Science and Technology*, Volume 1-5. Idea Group Reference, Hershey, PA, USA
- [8] DoD suppliers passive RFID information guide,2005, Version 6.0, January 17
- [9] Schrijver A.: "Theory of Linear and Integer Programming". John Wiley and Sons, 1998
- [10] Reveliotis S.A., *The "prototype" Web-based electronic text project: An Introduction to Linear Programming and the Simplex Algorithm* , School of Industrial & Systems Eng., Georgia Institute of Technology, 1997

Reduced – Order Controller Design in Discrete Time Domain

Vivek Kumar Sehgal

Department of Electronics and Communication Engineering

Jaypee University of Information Technology,

Waknaghat, Solan– 173215, HP, INDIA

E-mail: vivekhseh@gmail.com

Abstract- The complexities of physical systems make their analysis rather difficult and possibly a non desirable task, mainly due to difficult economical and computational considerations involved. This makes the use of reduced-order controller in physical system, which constitutes a good approximation of full order control system. In this paper we developed a method which preserves time domain as well as the frequency domain characteristics of original discrete time systems with higher order controller and their application for the control of discrete-time systems. A new mixed method, improved Routh stability method using p-domain transformation have been proposed which patches up the short comings of bilinear transformation and yields stable system with reduced order controller. It provides comparatively favorable results in comparison of other existing methods.

I. INTRODUCTION

In the modern process control dynamics, controller designing frequently results in high order controllers. On one hand this may be the consequence of the complexity of the model used for the design; on other hand controller design often results in complex high order controllers even if the design model is of reasonable size. Controller order reduction is a very important issue in many control applications. Controller order reduction should aim to preserve the required loop properties as far as possible. The reasons which prompt to have reduced order controller of a control system could be:

1) To have better understanding of the system:

A system with the high order controller poses difficulty in its analysis, synthesis, or identification. An obvious method of dealing with such system with higher order controller is to approximate them by low-order controller which reflect the characteristics of original system such as time constant, damping ratio, natural frequency etc.

2) To reduce computational complexity:

When the order of the controller is high, special numerical techniques are required to permit the calculations to be done at the reasonable cost on fast digital computers. This saves both time and memory required by computer.

3) To reduce hardware complexity:

A control system design for a high order system is likely to be very complicated and of a higher order it self. This is particularly true for controller based on optimal control theory. Controller design on the basis of lower order model will become more reliable. Reduced order controller also permits to use less hardware in controller designing.

A. Related Work

Al-Saggaf, U.M. and Franklin, G.F. [3] stated that there

are two approaches for reduced order controller design. In the first approach, the order of the plant is reduced and then a controller is designed for the reduced order plant. In the second approach, a controller is design for full order plant and then reduced order controller is obtained. And these both approaches are indirect approaches used to design a reduced order controller.

Duncan M., K., Glover, M. Vidyasagar [9] studied the reduced order controller design using coprime factor model reduction technique he gave the two procedure for reduced order controller design which incorporate coprime factor. Loan Dore Landau, Alireza Karimi [8] suggested the direct approach for reduced order controller design by the identification in closed loop addresses the problem of directly estimating the parameters of a reduced order digital controller using a closed loop type identification algorithm.

Fassi, M., Warwick, K. and Guilandoust M. [7] proposed a technique which provides stable reduced order models for discrete time systems. In this method Routh stability approach is employed to reduce the order of discrete time systems. Transfer function which employs a new transformation approach i.e. p-domain. If gives a stable reduced order model if the original system is stable. Shi, J. and Gibbard, M.J. [5], studied a second order discrete transfer function, with a pair of complex poles and one real zero, is assumed to be a model which characterized the dynamic behavior of a higher order discrete system. Hwang, C., and Shih, Y.P. [2] emphasized Routh approximation for reducing order of discrete systems, where it employs the Bilinear Transformation explicitly.

Zhang, W.D., Sun, Y.X. and Xu, X.M. [6], proposed the Dahlin controller is studied in the complex - frequency domain in terms of performance and robust stability.

II. METHODS OF REDUCED ORDER CONTROLLER DESIGN

Design of digital controller for the discrete time systems has been attempted by number of researchers. Main objective is “*given a process whose performance is unsatisfactory and reference model having desired performance, drive a suitable controller such that performance of the augmented process matches that of the model*” Basically there are two approaches to design the reduced order controller in discrete time system.

1) Indirect approach:

Obtain a reduced order model which will capture the essential characteristics of the nominal model in the critical frequency region for design

2) Direct approach:

Obtain an approximate reduced order controller which will preserve the nominal closed loop properties.

In this paper, indirect approach is adopted for controller design which helps to match the desired closed loop response with the designed closed loop response. This approach is subjected to a number of criticisms. First of all, use of a reduced order model does not necessarily guarantee that the resulting controller will be of a sufficient order. Secondly, the errors caused by model approximation will spread to the subsequent design steps. The direct approach to the controller reduction seems more appropriate because the approximation is carried out in the final step of controller design and the result can be easily understood. It should be noted that the controller resulting from an indirect reduction procedure can be further reduced, if necessary, by application in the last step of a direct reduction approach.

In the indirect approach of controller order reduction, there are several methods such as bilinear Routh approximation, Pade approximation, and Routh stability and time moments matching. But these methods do not reflect the frequency-domain and time-domain characteristics of original system. So a new method called *Improved Routh Stability* using p-domain to design the reduced order digital controller, as it preserves all the frequency-domain and time-domain characteristics of the original system, which is a closed loop system with plant and full order

III. PROPOSED METHOD FOR REDUCED ORDER CONTROLLER DESIGN

In this paper Improved Routh stability method in p-domain is used to design the reduced order controller. The design of digital controllers has frequently been based on determining the discrete equivalent of an analogue controller for which the closed-loop performance specifications are satisfied. On the other hand, amongst other methods, digital controller designs have been based on graphical design methods adopted from continuous system synthesis techniques such as Bode and Nyquist plots. In this paper, second approach is adopted for the controller design, with improved Routh stability method and MATLAB designing tool.

A. The Designing Procedure

It is assumed that the controller reduction algorithm can be implemented once the coefficients in the realizable discrete transfer function are determined.

$$D_c(z) = \frac{x_0 z^m + x_1 z^{m-1} + \dots + x_m}{z^n + y_1 z^{n-1} + \dots + y_n}, m \leq n \quad (1)$$

This controller transfer function contains m no. of zeros and n no. of poles. The purpose of method is to design the reduced order controller, to meet certain desire specifications by closed-loop system configuration. The over all designing aspects cover following steps:

STEP 1: A reference model $M(z)$ is obtained by table given in Shi, J. and Gibbard, M.J. [4] which incorporates

desire time-domain and frequency-domain specifications where contribution of dead time is added additionally in the reference model as well as in plant z-transfer function

STEP 2: Open loop model $M_o(z)$ is obtained from reference model $M(z)$ in this manner:

$$M_o(z) = \frac{M(z)}{1-M(z)} \quad (2)$$

Where $M(z)$ is the desire reference model with unity feedback.

STEP 3: In the actual model, $D_c(z)$, $G_h(z)$ are the transfer functions of controller and plant with zero order hold respectively. Here $G_h(z)$ is given and $D_c(z)$ is to calculate. The open loop transfer function of reference model and for actual model should have same time and frequency characteristics. Hence by equating them we can calculate the full order controller $D_c(z)$ from Fig. 1.

$$\begin{aligned} M_o(z) &= D_c(z)G_h(z) \\ D_c(z) &= \frac{M_o(z)}{G_h(z)} \end{aligned} \quad (3)$$

STEP 4: Here $D_c(z)$ is the full order controller whose order is to reduce. There are number of methods which can be used for order reduction, but in this paper the *Improved Routh stability* method is used so the original characteristics of the system are preserved

$$\begin{aligned} D_c(z) &= \frac{D(z)}{E(z)} \\ &= \frac{d_{11}z^{n-1} + d_{21}z^{n-2} + d_{12}z^{n-3} + d_{22}z^{n-4} + \dots}{e_{11}z^{n-1} + e_{21}z^{n-2} + e_{12}z^{n-3} + e_{22}z^{n-4} + \dots} \end{aligned} \quad (4)$$

Where d and e coefficients are the numerator and denominator scalar constants. Respectively, also the numerator order is given as being one less than the denominator for explanation purposes only. Assume that a reduced-order controller $D_r(z)$ of order k ($k < n$) is to be constructed in a process dynamic system.

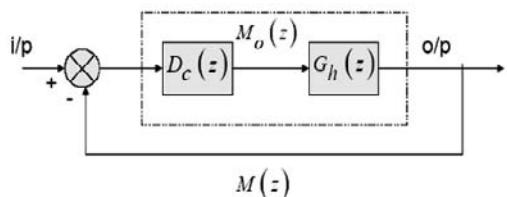


Fig. 1. Reference model with full order controller

Let it be of the form

$$D_r(z) = \frac{B(z)}{A(z)}$$

$$= \frac{b_{k-1}z^{k-1} + b_{k-2}z^{k-2} + b_{k-3}z^{k-3} + \dots + b_0}{a_k z^k + a_{k-1}z^{k-1} + a_{k-2}z^{k-2} + \dots + a_0} \quad (5)$$

STEP 5: Full order controller transfer function $D_c(z)$ is transferred in to $D_c(p)$ which is governed by $(z = p + m)$ where m is a scalar quantity equal to the distance from the furthest pole (zero) to the centre of the unit circle. This is easily performed by substituting $(z = p + m)$ in to (4). The transfer function in the z -domain is converted in to p -domain with the help of Pascal's triangle, e.g., $n = 4$ in (4). The e' and d' coefficients of denominators and numerators are then found as follows:

$$e'_{11} = e_{13} + me_{22} + m^2 e_{12} + m^3 e_{21} + m^4 e_{11}$$

$$e'_{21} = e_{22} + 2me_{12} + 3m^2 e_{21} + 4m^3 e_{11}$$

$$e'_{12} = e_{12} + 3me_{21} + 6m^2 e_{11}$$

$$e'_{22} = e_{21} + 4me_{11}$$

$$e'_{13} = e_{11}$$

The numerator $D(z)$ may also be transferred in similar fashion and numerator coefficients can be obtained:

$$d'_{11} = d_{13} + md_{22} + m^2 d_{12} + m^3 d_{21} + m^4 d_{11}$$

$$d'_{21} = d_{22} + 2md_{12} + 3m^2 d_{21} + 4m^3 d_{11}$$

$$d'_{12} = d_{12} + 3md_{21} + 6m^2 d_{11}$$

$$d'_{22} = d_{21} + 4md_{11}$$

$$d'_{13} = d_{11}$$

From these coefficients the transformer function $D_c(p)$ is obtained as follows:

$$D_c(p) = \frac{d'_{11} + d'_{21}p + d'_{12}p^2 + d'_{22}p^3 + \dots}{e'_{11} + e'_{21}p + e'_{12}p^2 + e'_{22}p^3 + \dots} \quad (6)$$

STEP 6: The Routh array for the numerator and denominator are constructed by arrangement of the parameters contained in the modified system described by (6)

The table 1. and 2. gives the Routh's stability criteria. Routh array for denominators and numerator of $D_c(p)$ is constructed by the arrangement of coefficients of denominators and numerator appearing in the transfer function of $D_c(p)$ of modified system. From these arrays we can check the stability of modified system. Any variation in the sign of coefficients in the first column gives the behavior of the system. The system may be stable, unstable or oscillatory.

TABLE I.
ROUTH ARRAY FOR E (P)

e'_{11}	e'_{12}	e'_{13}	e'_{14}	\dots
e'_{21}	e'_{22}	e'_{23}	e'_{24}	\dots
e'_{31}	e'_{32}	e'_{33}	\dots	\dots
\vdots				
e'_{n1}			\dots	\dots
$e'_{(n+1)1}$			\dots	\dots

$$e'_{(i,j)} = e'_{(i-2),(j+1)} - [e'_{(i-2),1} e'_{(i-1),(j+1)}] / [e'_{(i-1),1}] \quad (7)$$

TABLE II.
ROUTH ARRAY FOR D (P)

d'_{11}	d'_{12}	d'_{13}	d'_{14}	\dots
d'_{21}	d'_{22}	d'_{23}	d'_{24}	\dots
d'_{31}	d'_{32}	d'_{33}	\dots	\dots
\vdots				
d'_{n1}			\dots	\dots
$d'_{(n+1)1}$			\dots	\dots

$$d'_{(i,j)} = d'_{(i-2),(j+1)} - [d'_{(i-2),1} d'_{(i-1),(j+1)}] / [d'_{(i-1),1}] \quad (8)$$

STEP 7: Desired values of α_i, β_i and γ can be calculated by using:

$$\alpha_i = \frac{e'_{i,1}}{e'_{(k+1),1}} \quad (9)$$

$$\beta_i = \frac{d'_{i,1}}{d'_{k,1}} \quad (10)$$

$$\gamma = \frac{d'_{k,1}}{e'_{(k+1),1}} \quad (11)$$

Where k is the desired reduced order of controller and γ is the gain correction factor.

STEP 8: The model denominator and numerator are calculated using (12) and (13) which gives the values of numerator $B(z)$ and denominator $A(z)$.

$$A(z) = \sum_{i=0}^k \alpha_{i+1} (z-m)^i \begin{cases} i = 0, 1, 2, \dots, k \\ \alpha_{k+1} = 1 \end{cases} \quad (12)$$

$$B(z) = \sum_{i=0}^{k-1} \beta_{i+1} (z-m)^i \begin{cases} i = 0, 1, 2, \dots, k-1 \\ \beta_k = 1 \end{cases} \quad (13)$$

STEP 9: Desire reduced order controller assumes following form:

$$D_r(z) = \frac{\gamma B(z)}{A(z)} \quad (14)$$

STEP 10: Compute the closed loop system with reduced order controller.

$$M_r(z) = \frac{D_r(z) G_h(z)}{1 + D_r(z) G_h(z)} \quad (15)$$

$M_r(z)$ is the model with plant and reduced order controller with unity feedback. As shown in Fig. 2.

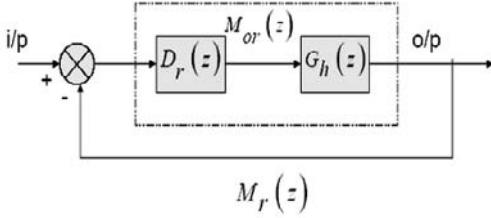


Fig. 2. Model with reduced order controller.

IV. NUMERICAL EXAMPLE

By using the Improved Routh Stability method, M. Farsi, B.S., K. Warwick, and M. Guilandoust [7] The following example give the brief idea of design of the reduced order controller. The reference model with desire time and frequency response is $M(z)$ with sampling time 0.01 sec is:

$$M(z) = \frac{0.001241z + 0.001233}{z^2 - 1.977z + 0.9802}$$

Using (2) the open loop transfer function $M_o(z)$ of reference model is:

$$M_o(z) = \frac{0.001241z + 0.001233}{z^2 - 1.979z + 0.979}$$

Sampling time = 0.01 sec. The transfer function of plant with zero order hold $G_h(z)$ is given below

$$G_h(z) = \frac{(z^2 - 1.4z + 0.53)}{(z-0.75)(z-0.6953)(z^2 - 1.979z + 0.979)} = \frac{(z^2 - 1.517z + 0.6271)}$$

Using (3), the transfer function $D_c(z)$ of full order controller is:

$$D_c(z) = \frac{3z^4 - 8.886z^3 + 10.0221z^2 - 5.091975z + 0.9811125}{z^5 - 3.7z^4 + 5.47z^3 - 4.037z^2 + 1.4856z - 0.2173}$$

The furthest pole is approximately at 1; hence the value of m is 1 using the Pascal triangle, the full order controller in p-domain is:

$$D_c(p) = \frac{3p^4 + 3.114p^3 + 1.3641p^2 + 0.294225p + 0.0252375}{p^5 + 1.3p^4 + 0.67p^3 + 0.173p^2 + 0.021p + 0.0013}$$

Routh array for numerator polynomials is obtained by using Table II and (8).

0.0252375	1.3641	3
0.294225	3.114	
1.096993	3	

Routh array for denominator polynomial is obtained by using Table I and (7).

0.0013	0.173	1.3
0.0216	0.67	1
0.1326759	1.2398148	0
0.4681547	1	0

A. Reduced Order Controller (2nd order)

Using equations. (9), (10) and (11)

$$\begin{aligned} \alpha_1 &= 0.009798313 & \alpha_2 &= 0.1628027 & \alpha_3 &= 1 \\ \beta_1 &= 0.0857762 & \beta_2 &= 1 \\ \gamma &= 2.217622 \end{aligned}$$

Numerator of the 2nd order reduced controller would be based on equation (13).

$$B(z) = (z - 0.9142238)$$

Denominator of the second order reduced controller would be based on equation (12).

$$A(z) = z^2 - 1.8371973z + 0.8469956$$

After incorporating gain correction factor γ which is described by equation (14).

$$D_r(z) = \frac{2.217622(z - 0.9142238)}{z^2 - 1.8371973z + 0.8469956}$$

The closed loop transfer function using reduced order controller will be assuming the following form. After incorporating equation (15).

$$M_r(z) = \frac{0.0009177z^7 - 0.003323z^6 + 0.003917z^5 - 0.0002235z^4 - 0.003489z^3 + 0.003273z^2 - 0.001254z + 0.0001811}{z^8 - 6.778z^7 + 20.1z^6 - 34.1z^5 + 36.18z^4 - 24.59z^3 + 10.46z^2 - 2.545z + 0.2713}$$

In the modern process control system, the desire response of a control loop i.e. $M(z)$, frequently results in high order controller $D_c(z)$. The order of full order controller $D_c(z)$ can be reduced to any desire order. When this reduced order controller $D_r(z)$ is used in the loop, the model with the reduced order controller $M_r(z)$ preserve time domain as well as the frequency domain characteristics of original systems $M(z)$ as shown in Fig. 3.

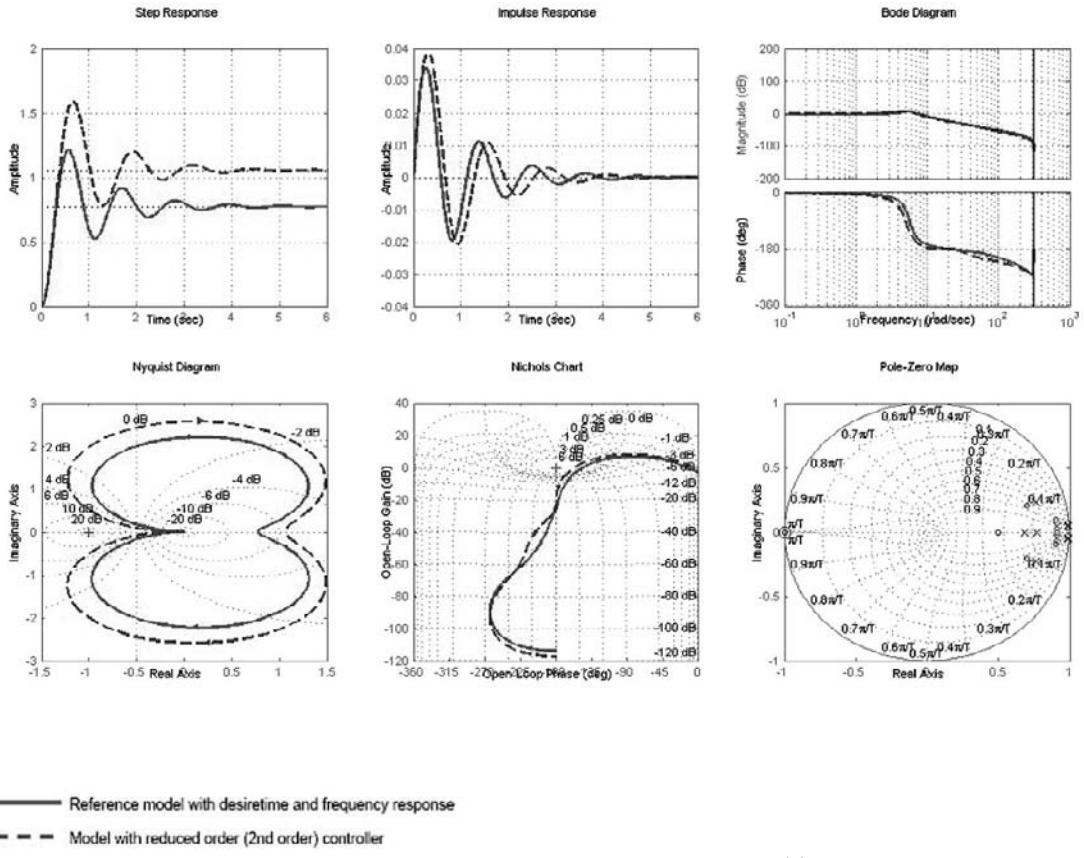


Fig. 3. Time and frequency responses of reference model with desire transient and frequency characteristics $M(z)$ and model with reduced order (2nd order) controller $M_r(z)$

V. APPLICATIONS OF REDUCED ORDER CONTROLLER

Reduced-order controller and reduction techniques have been widely used for the analysis and synthesis of the higher order systems. Some of the typical applications are listed below:

- 1) Prediction of the transient response sensitivity of a closed loop system with the full order controller using low-order controller.
- 2) Prediction of dynamic errors of a closed loop system with the full order controller.
- 3) Prediction of the frequency-domain and time-domain characteristics of closed loop system.
- 4) Control-system design.
- 5) Adaptive control using low-order models.
- 6) Designing of reduced order estimators.
- 7) Sub optimal control derived by simplified models.

VI. CONCLUSION AND FUTURE WORK

This paper contains the results of the investigations carried out by the author in the area of reduced order controller design in discrete time systems. Improved Routh stability method using p-domains transformations for stable and unstable system has been proposed in this paper. Improved Routh stability method which employs a Routh

array for reduction of linear time invariant discrete time system. Yield stable reduced order controller. If original is stable, this method is easy to employ and relates simply control engineering problem.

The main advantages of improved Routh stability method in key domain used to reduce the order of controller gives the following benefits:

- 1) It provides high accuracy i.e., it reflects the original characteristics of the system.
- 2) The reduced order controller is reliable in high frequency range.
- 3) In case of optimal control controller order reduction is essential because high order is not used in optimal control systems.

However, another objective for controller order reduction can be to minimize the closed loop error between the plant output generated in the nominal simulated closed loop and the plant output generated by the closed loop using the reduced order controller.

This work has good scope in future in the area of VLSI on chip interconnects order estimation and delay calculation. The RC or RLC trees are consist of energy storage elements which define the order of on chip interconnects. We can approximate this high order in to low order by order

reduction techniques and estimate the delay across the RLC tree nodes.

REFERENCES

- [1] Hwang, C. and Shih, Y.P., "Routh approximation for reducing order of discrete systems," *Transactions of the ASME Journal of Dynamic Systems, Measurement, and Control*, Vol. 104, pp. 107-109, March 1982.
- [2] Hwang, C. Shih, Y.P. and Hwang, RY., "A combined time and frequency domain method for model reduction of discrete systems," *Journal of Franklin Institute*, Vol. 311, No. 6, 391402, June 1981.
- [3] Al-Saggaf, U.M. and Franklin, G.F., "Reduced order controller design for discrete-time systems," *Int... J. Syst. Sci.*, Vol. 22, No. 10, pp. 1743-1756, 1991.
- [4] Shi, J. and Gibbard, MJ., "A frequency response matching method for the digital controller with constraints on Pole – Zero locations," *Int. J. Control.*, Vol. 42, No. 2, pp. 529-538, 1985.
- [5] Shi, J. and Gibbard, MJ., "Discrete system models based on simple performance specifications in the time, frequency or complex Z-domains," *Int. J. Control.*, Vol. 42, No. 2, pp. 517-527, 1985.
- [6] Zhang, W.D., Sun, Y.X., and Xu, X M, "Robust digital controller design for Processes with dead times New results," *IEE Proc-Control theory appl.* Vol. 145, NO. 2, pp. 159-164, March 1998.
- [7] Farsi, M., Warwick, K., Guilandoust, M., "Stable reduced - order models for discrete-times, *IEE Proceedings.*" Vol.133, Pt. D, No. 3, pp. 137 - 141, May 1986.
- [8] LD.Landau.A.Karimi I., "Direct controller order reduction by identification in closed loop," *Automatica* 37, pp. 1689-1702, April 2001.
- [9] Duncan M., K., Glover..M. Vidyasagar, "Reduced order controller Design using coprime factor model reduction," *IEEE Tran.* Vol. 35, pp. 369-373, 1990.
- [10] C.-S. Hsieh, PhD Prof. C. Hwang, PhD , "Model reduction of continuous-time systems using a modified Routh approximation method," *IEE Proceedings*, Vol. 136, Pt. D, No. 4, July 1989.
- [11] Younseok Choo., "Improvement to modified Routh approximation method," *Electronics Letters* Vol. 35 No. 7, 1st April 1999.
- [12] A. S. Rao, , "On Routh Approximation," *Proceedings of the IEEE*, Vol. 71, No. 2, Feb. 1983.

Simple Intrusion Detection in an 802.15.4 Sensor Cluster

Vojislav B. Mišić and Jobaida Begum

University of Manitoba, Winnipeg, MB, Canada R3T 2N2

{vmisic, tjobaida}@cs.umanitoba.ca}

Abstract

In this paper, we investigate the feasibility of a simple, traffic volume-based intrusion detection for an IEEE 802.15.4 compliant sensor cluster operating in beacon-enabled, slotted CSMA-CA mode. We have used simple exponential averaging to filter out some of the inherent variability in individual device arrival rate, and introduced a small hysteresis in the decision process in order to avoid false alarms due to dithering. Initial results demonstrate that the intrusion detection implemented in this manner may indeed operate quickly and efficiently.

I. INTRODUCTION

Security is quickly becoming one of the overwhelming concerns in all kinds of networks, including wireless sensor networks [1]. However, the implementation of security measures and policies in a wireless sensor network environment is complicated due to the many constraints present in such networks. First, wireless communication means that intruders can listen to network traffic without physical presence, and they are free to launch attacks from a distance with relative impunity. Wireless sensors are small, often battery-operated, and hence their computational and communication capabilities are severely limited. Furthermore, sensors are expected to operate for prolonged periods of time with little human intervention, or (preferably) without such intervention at all. As a result, many traditional security policies are simply inapplicable in the wireless sensor network environment, and new policies which take all the constraints into account are needed [3][13]. Among the techniques that need to be adapted is the technique that is to be used for intrusion detection, as no security measure (or even all of them together) cannot guarantee that an attack will not eventually succeed; in that case, we must be ready to detect the attack and take active steps to minimize its impact.

In this paper, we consider a single sensor cluster built using the recently introduced IEEE 802.15.4 communication standard [7]. We describe a simple intrusion detection technique which is based on traffic monitoring and averaging, and performed by the cluster coordinator. In this manner, reasonably quick detection and recovery can be accomplished despite relative simplicity and low computational requirements. We discuss the choice of parameters and

present some simulation results that demonstrate the feasibility of our approach.

The remaining part of the paper is organized as follows. In Section 2 we briefly introduce the 802.15.4 MAC and discuss possible attacks at the MAC layer. Section 3 discusses the approach we have adopted for monitoring and averaging, as well as some of its practical implications. Section 4 presents our simulation setup and demonstrates our main results. Section 5 concludes the paper and outlines some promising avenues for future research.

II. IEEE 802.15.4 OPERATION AND ATTACKS

Recently, IEEE has adopted the 802.15.4 standard for low rate Wireless Personal Area Networks (WPANs) [7]. As 802.15.4-compliant WPANs use small, cheap, energy-efficient devices operating on battery power that require little infrastructure to operate, or none at all, they appear particularly well suited for building wireless sensor networks [2].

In an IEEE 802.15.4-compliant network or cluster, a central controller device (commonly referred to as the coordinator) builds the cluster with other devices within a small physical space known as the personal operating space. Two topologies are supported: the star topology network, in which all communications, even those between the devices themselves, must go through the coordinator, and the peer-to-peer topology, in which the devices can communicate with one another directly as long as they are within the physical range, but the coordinator must still be present.

Apparently, the star topology appears better suited to sensor networks, where all ordinary nodes will report the sensed data to the cluster coordinator, to be delivered to the network sink. In this mode, the 802.15.4 network operates in a beacon enabled, slotted CSMA-CA mode, similar to 802.11 standard.

If 802.15.4 networks are to enjoy widespread use, all aspects of network operation and performance, including security, should be investigated and analyzed. A preliminary classification of malicious attacks was presented in [9], where a number of possible threats at different layers of the ISO/OSI model were identified [2].

Routing layer attacks include spoofed, altered, or replayed routing information spread by an adversary, selective forwarding of packets, sinkhole attacks that attract traffic from a specific area to a compromised node (or nodes), Sybil attacks in which a compromised node assumes many identities,

acknowledgement spoofing, injecting corrupted packets, neglecting routing information, or forward messages along wrong paths [10].

MAC layer attacks typically focus on disrupting channel access for regular nodes, thus disrupting the information flow both to and from the sensor node; this leads to a DoS condition at the MAC layer [16]. Security at the MAC layer has been mostly studied in the context of 802.11 MAC layer [10] but sometimes also in the more general context of different types of attacks [16].

Finally, **physical layer** (jamming) attacks consist of the attacker sending signals that disrupt the information flow through radio frequency interference. Jamming at the MAC level may be accomplished through sending large size packets with useless information.

Subsequent analysis focused on the impact of various attacks on the performance of a simple 802.15.4 cluster [10]. This paper focuses on the logical next step, i.e., on the design of a simple intrusion detection technique to allow the cluster coordinator to quickly identify a possible attack so that appropriate steps can be taken [13][17]. (We note that a recent paper [2] contains a preliminary classification of various intrusion detection techniques in the wireless sensor network environment.)

III. WHEN AVERAGES DIFFER

Our chosen scenario is a rather simple case of a small number of intruder devices that follow the 802.15.4 MAC protocol to the letter, and try to launch a denial-of-service attack by simply sending a large number of essentially meaningless packets in the uplink direction to the cluster coordinator. Such a scenario might occur if a malicious attacker deploys a number of sensor devices of its own within the area covered by a legitimate sensor network. Another possibility is for the attacker to capture and subvert a number of regular devices, which may occur in surveillance or military applications. Since the performance of an 802.15.4 cluster is fairly sensitive to high traffic loads [10], even moderate increases in packet arrival rate are likely to lead to substantial reductions in throughput originating from the legitimate nodes [10].

In order to detect such an attack, the coordinator of the cluster under attack would have to monitor the traffic in the cluster, and use its knowledge of short- and long-term averages for each node to decide whether an attack is under way. This decision is complicated by the essentially random character of sensor-generated traffic, where wide fluctuations in arrival rates are a rule, rather than an exception. In order to smooth those fluctuations, we have decided to apply a simple transformation known as exponentially weighted moving average, or EWMA [4]. In this approach, a moving average is maintained for packet inter-arrival times, and updated with each new packet using the formula

$$\bar{\tau}_{i+1} = \alpha t_{i+1} + (1 - \alpha)\bar{\tau}_i$$

where t_{i+1} denotes the measured inter-arrival time between i -th and $i+1$ -st packet, and $\bar{\tau}_i$ denotes the EWMA up to and including i -th packet. The level of smoothing depends primarily on the smoothing constant α ; this dependency is shown in Fig. 1 as a function of packet arrival rate λ , expressed in packet per device per minute.

Device 45 (Standard Deviation of the EWMA's)

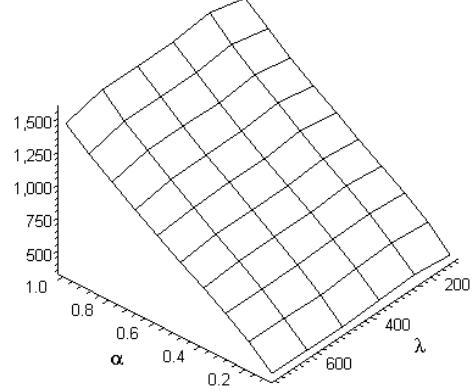


Figure 1. Standard deviation of inter-arrival times (expressed in backoff periods) as the function of the packet arrival rate λ , after exponential smoothing with the constant α .

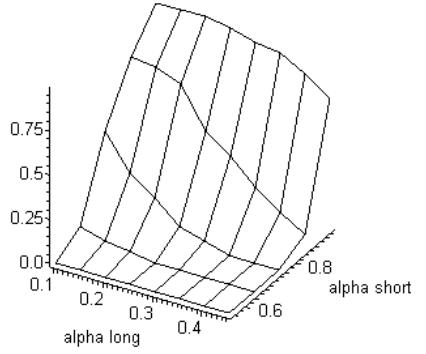
Note that all times (in this diagram, as well as in others) are expressed in backoff periods, the duration of which is prescribed by the IEEE 802.15.4 standard [7] to be 312.5usec.

In order to be able to uniquely identify the attacking device, the coordinator must maintain two separate EWMA values for each one of the sensor devices in its cluster. One of these is a long-term EWMA with a very low value for α , while the other is a short-term EWMA where α has a higher value (i.e., closer to 1). The detection algorithm, then, simply compares the two EWMA values: when their ratio drops below a predefined threshold A:

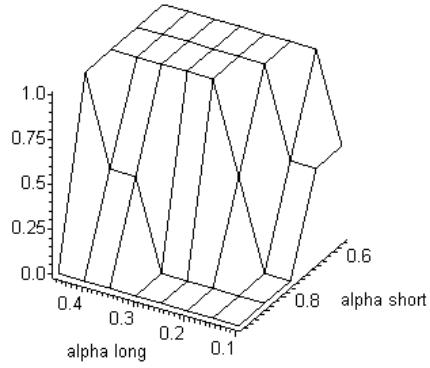
$$\frac{\tau_{short}}{\tau_{long}} < A,$$

the coordinator decides that there is an ongoing attack by the device in question. In this case, there are two options for further action. First, the coordinator may decide to switch to a different channel in order to alleviate the attack, and inform all the non-compromised devices accordingly. This procedure assumes that there is a secure communication channel, possibly with separate encryption, to each of those devices. (It should be noted that the 802.15.4 standard does provide the required security primitives to perform such an action.)

Alternatively, the coordinator may simply inform the network sink and, ultimately, the sensing application that this particular cluster has been compromised; the application may then decide to shut down the cluster, alert the human operator, or take some other action, as appropriate. However, these actions are beyond the scope of this paper.



a) Probability of false positives.



b) Probability of false negatives.

Figure 2. Pertaining to the choice of smoothing constants for long- and short-term EWMA. Note the different orientation of the axis describing the long-term smoothing coefficient α_{long} , introduced to improve clarity.

The next step is to determine the suitable values for the smoothing coefficients and the decision threshold. We have conducted an extensive set of experiments using an in-house built simulator of the 802.15.4 cluster; we have used the Artifex object-oriented Petri Net simulation engine by RSoftDesign, Inc. [13]. Unless otherwise specified, the cluster was assumed to operate in the beacon enabled, slotted CSMA-CA mode in the 2.4GHz (ISM) band with the maximum data rate of 250kbps. The cluster had 50 devices, each of which generated Poisson traffic with an arrival rate of 120 packets per minute.

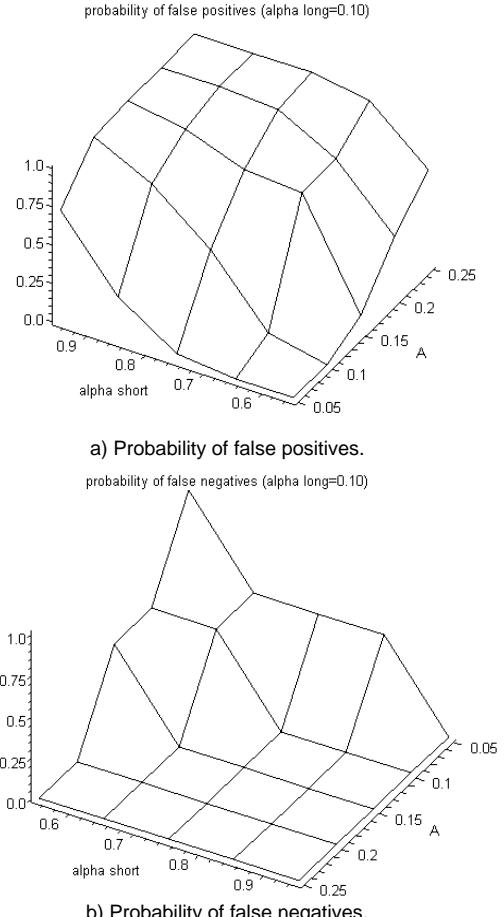


Figure 3. Probability of false alarms and detection delay (in backoff periods) as functions of the threshold A and the smoothing coefficient for short term EWMA. Note the different orientation of the axes.

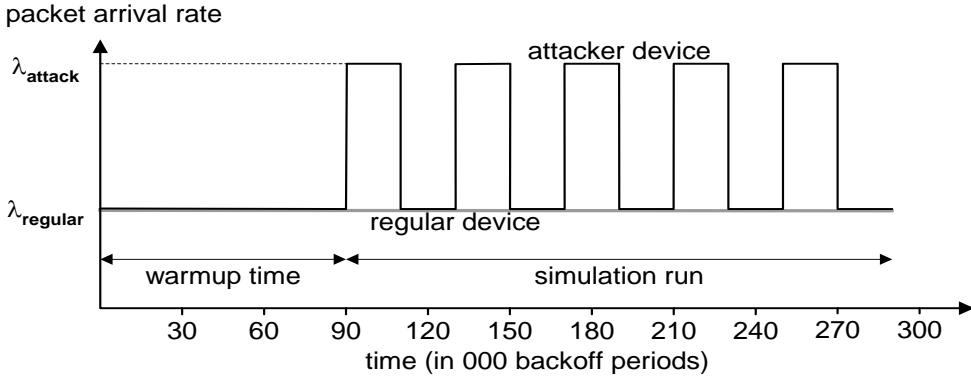


Figure 4. Attack pattern used in simulations.

As is well known, in any detection process there are two kinds of possible errors: false positives, when a non-event is recognized as an event, and false negatives, when a real event is missed. The main objective of the first set of experiments was to determine the values of smoothing coefficients α for long- and short-term EWMA's, as well as the threshold A , that will minimize the probabilities of false positives and false negatives. Again, it is well known (and unfortunate) that both probabilities can't be minimized simultaneously, as minimizing one of them invariably leads to an increase in the other. The diagrams in Fig. 2 show the probabilities of false positives and false negatives, respectively, as functions of smoothing coefficients for the long- and short-term EWMA; the threshold value was set at 0.1 unless otherwise specified. As expected, the two probabilities of false detection behave in different ways (note the different orientation of the axes!), and an optimum value that will provide low values for both probability of detecting false positives and probability of detecting false negatives must be found.

Similar results have been obtained when the smoothing coefficient for the long term average has been held constant at 0.1 while the threshold and the smoothing coefficient for the short term average were varied, as can be seen from Fig. 3.

A similar set of experiments was repeated with the value of the smoothing coefficient for the short term average held constant.

Through these measurements, we have decided to use the following values:

- 0.1 for the smoothing coefficient of the long-term EWMA;
- 0.85 for the smoothing coefficient of the short-term EWMA; and
- 0.1 for the threshold A .

IV. PERFORMANCE OF INTRUSION DETECTION

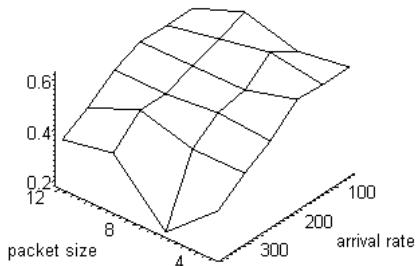
With all the parameters chosen as described above, we have focused on the actual intrusion detection experiment. The attack pattern used for the experiment consisted of a number of periods in which the 48 regular devices generated Poisson traffic with a constant arrival rate of 120 packets per minute, while two attacker devices periodically switched between two different packet arrival rates: the lower rate was fixed and equal to the packet arrival rate of regular devices; the other rate was higher and variable. This pattern is shown in Fig. 4. Moreover, a warm-up time was used in order to allow the cluster to reach a steady state before the actual attacks were launched.

The measured results, including probability of false positives (i.e., a non-attack being detected as an attack), the probability of false negatives (i.e., an actual attack missed), and the delay in detecting the actual attack (expressed in backoff periods), are shown in Fig. 5 below. As can be seen, the simple intrusion detection mechanism described above provides reasonably accurate results, in particular the low probability of false alarms. We want to stress that the computational and memory requirements of the intrusion detection mechanism are kept at an absolute minimum, through the use of exponentially weighted moving averages, which means that the proposed mechanism is feasible for use in a wireless sensor network environment where individual devices have severe resource constraints.

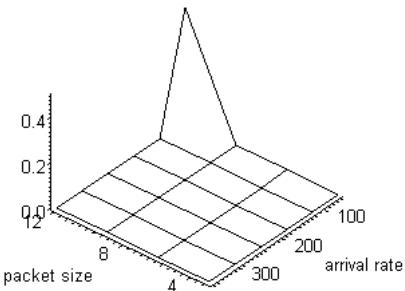
V. CONCLUSION

We have described a simple, traffic-based intrusion detection system with modest resource requirements. We have experimentally found parameter values that give a reasonable tradeoff between the probabilities of false positives and false negatives.

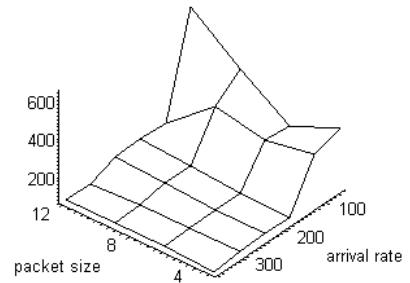
We are currently investigating ways in which the algorithm could be modified in order to improve its sensitivity and accuracy, as well as more meaningful ways to express those parameters. We are also looking into the options to take corrective actions once an attack is detected; these might include renewing the keys with the devices known to be uncompromised, instructing the uncompromised devices to switch to another RF channel, and/or informing the application and (ultimately) the human operators about the attack.



a) Probability of false positives



b) Probability of false negatives.



c) Delay in detecting an attack.

Figure 5. Performance indicators as functions of attacker arrival rate (in packets per minute) and packet size (in backoff periods).

REFERENCES

- [1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks: a survey. *IEEE Communications*, **40**(8):102–114, August 2002
- [2] F. Amini, V. B. Mišić, and J. Mišić. “Intrusion Detection in Wireless Sensor Networks”, in *Security in Distributed, Grid, and Pervasive Computing*, Yang Xiao (editor), Boca Raton, FL: CRC Press, 2006
- [3] H. Chan and A. Perrig. Security and privacy in sensor networks. *IEEE Computer*, **36**(10):103–105, Oct. 2003
- [4] S. Delurgio. *Forecasting – Principles and Application*, McGraw-Hill/Irwin, New York, 1998
- [5] V. Gupta, S. Krishnamurthy, and M. Faloutsos. Denial of service attacks at the MAC layer in wireless ad hoc networks. *Proc. MILCOM 2002*, Anaheim, CA, July 2002
- [6] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. *IEEE Security & Privacy*, **2**(3):28–39, May-June 2004
- [7] Standard for part 15.4: Wireless MAC and PHY specifications for low rate WPAN. *IEEE Std 802.15.4*, IEEE, New York, NY, Oct. 2003

- [8] C. Karlof, N. Sastry, and D. Wagner. TinySec: A link layer security architecture for wireless sensor networks. *Proc. ACM SenSys 2004*, pp. 162–175, Baltimore, MD, Nov. 2004
- [9] V. B. Mišić, J. Begum, and J. Mišić. “MAC Layer Security Issues in 802.15.4 Sensor Networks”, *Proc WiNCS'05*, pp. 550-555, Philadelphia, PA, July 2005
- [10] J. Mišić, S. Shafi, and V. B. Mišić. “Avoiding the Bottlenecks in the MAC Layer in 802.15.4 Low Rate WPAN”, *Proc. HWISE2005*, vol. 2, pp. 363-367, Fukuoka, Japan, July 2005
- [11] V. B. Mišić, J. Fung, and J. Mišić. “MAC Layer Security of 802.15.4-Compliant Networks”, *Proc. WSNS'05*, pp. 847-854, Washington, DC, Nov. 2005
- [12] Q. Ren and Q. Liang. Secure media access control (MAC) in wireless sensor networks: Intrusion detections and countermeasures. *Proc. IEEE PIMRC 2004*, volume 4, pages 3025–3029, Barcelona, Spain, Sep. 2004
- [13] Artifex v.4.4.2, RSoft Design, Inc., San Jose, CA, 2003.
- [14] E. Shi and A. Perrig. Designing secure sensor network. *IEEE Wireless Communications*, **11**(6):38–43, Dec. 2004
- [15] W. Stallings. *Cryptography and Network Security – Principles and Practice*. Prentice Hall, Upper Saddle River, NJ, 3rd edition, 2003
- [16] A. D. Wood and J. A. Stankovic. Denial of service in sensor networks. *IEEE Computer*, **35**(10):54–62, Oct. 2002
- [17] Y. Zhou, S. Wu, and S. M. Nettles. Analyzing and preventing MAC-layer denial of service attacks for stock 802.11 systems. *Proc. BroadWise2004*, pp. 22–88, San Jose, CA, Oct. 2004

Dim Target Detection in Infrared Image Sequences Using Accumulated Information

Wei He, Li Zhang

Department of Electronic Engineering
Tsinghua University
Beijing, 100084 P.R.China

Abstract-The targets in infrared images are usually dim and small, buried under heavy clutter and noise. Recognition of such targets is a challenging task, especially in detecting in real-time and low false rate. In this paper, we present a new target detection scheme based on accumulated information, and a neural network structure to realize this method is also introduced. Computer simulation was carried out and the satisfactory result showed substantial reduction in computational complexity.

I. INTRODUCTION

Automatic Target Recognition (ATR) is a specific field of study within the general scope of image processing. A detailed survey of the application of neural networks on various aspects of ATR problem is provided by Roth [1]. The main difficulties of detecting target in infrared images are,

The SNR is very low and hence impossible to detect target from a single frame.

There is little prior information about target features like shapes, textures. Because the target is usually small size in image due to the distance, these features can hardly be observed.

Only helpful information for the detection is that target has an unknown moving velocity.

This paper presents a new method for detecting the small SNR moving target. The new scheme is based on accumulated information from the image sequences, which carries the probabilities of the pixels to be a target. Represented in an iterative image, this accumulated information is generated using a modified correlation method. This paper has four major sections, the iterative method to accumulate the information is presented in section II, then we introduce an neural network structure to realize this target detection method. In section IV we present computer simulations which show the validity of the scheme. Finally we summarize our conclusion in section V.

II. ITERATIVE METHOD TO ACCUMULATE INFORMATION

A. Detection Problem and Modeling

The infrared image sequences yields a 3-D digital image in

the Cartisian coordinates (x, y, t_n) , where (x, y) are the spatial variables and t_n represents the frame number. Given a 3-D image described above, the problem of target detection from the image sequences is to identify the target within the background clutter as accurately as possible. The following assumptions are made in this detection process.

- 1) The absolute range of target speeds is v_m pixels per scan
- 2) The maximum number of missing target points due to the sensors is one in S_n scans
- 3) There can be more than one target in the scene, and the targets may appear and disappear at unknown point in time.

A frame of the infrared image sequences contains a combination of target signal as well as background clutter and additive sensor noise. For simplicity, we suppose that the clutter is totally removed by background suppression techniques. Then we are able to obtain a preprocessed image as follows [2],

$$F(x, y, t_n) = S(x, y, t_n) + [1 - S(x, y, t_n)]N(x, y, t_n) \quad (1)$$

Where x, y are the locations on a discrete 2-D plane, t_n is the frame number, and F is the preprocessed image consisting of the target S and noise N , here the F, S, N are all binary arrays. Thus, $F = 1$ corresponds to either target or clutter. Note that the noise N is independent from pixel to pixel after the background suppression.

B. Iterative Image Generation

As mentioned above, it is impossible to detect target from a single frame because the low SNR makes the target identical as the noise in observation. In this case, we use the accumulated information through frames to enhance the target gradually. An iterative image, which carries the pixels' probabilities to be a target, is generated to represent the accumulated information. In this image, the pixel has a higher grey level means it has a higher probability to be a

target, contrarily, the dark pixels are more possible to be the noise clutter.

We can generate the iterative image $I(x, y, t_n)$ by the following steps.

First, without losing generality, we assume the pixels in the first frame where $F(x, y, t_0)=1$ have the identical probability to be a target. The initial probability can be set at a low level P_0 , namely,

$$I(x, y, t_0) = P_0 \times F(x, y, t_0) \quad (2)$$

Note that P_0 is relative probability and can be greater than 1.

For each frame, we calculate the correlation of the current iterative image $I(x, y, t_{n-1})$ and next infrared image frame using

$$\begin{aligned} R_{t_{n-1}t_n}(x, y) = & \sum_{i=-|v_m|}^{|v_m|} \sum_{j=-|v_m|}^{|v_m|} F(x, y, t_n) \\ & \times I(x+i, y+j, t_{n-1}) \end{aligned} \quad (3)$$

Due to the target's point-size in most infrared image occasions, the sum function in calculating the correlation $R_{t_{n-1}t_n}(x, y)$ may contain only few target pixels but bring many noise influences. So we use the maximizing function in a modified correlation method. The correlation is derived from (4), the $\max\{\cdot\}$ function is to find the maximum value in the data set.

$$R_{t_{n-1}t_n}(x, y) = \max \left\{ \begin{array}{l} \bigcup_{-|v_m| \leq i \leq |v_m|} \bigcup_{-|v_m| \leq j \leq |v_m|} F(x, y, t_n) \\ \times I(x+i, y+j, t_{n-1}) \end{array} \right\} \quad (4)$$

For (x, y) in the image, we do

$$D(x, y) = \begin{cases} \alpha \times F(x, y, t_n) + R_{t_{n-1}t_n}(x, y), & \text{if } R_{t_{n-1}t_n}(x, y) > 0; \\ P_0 \times F(x, y, t_n), & \text{if } R_{t_{n-1}t_n}(x, y) = 0; \end{cases} \quad (5)$$

$$I(x, y, t_{n-1}) = I(x, y, t_{n-1}) - \beta \quad (6)$$

$$I(x, y, t_n) = \max\{I(x, y, t_{n-1}), D(x, y)\} \quad (7)$$

According to the continuity of the target movement, the target should appear in the next frame in the vicinity of the current location. Thus for the pixel where $F(x, y, t_n)=1$, if there exists a probability $I(x+i, y+j, t_{n-1}) > 0$ in the current iterative image, we increase the pixel's probability to be a target by α . Contrarily, if no correlation is found when $R_{t_{n-1}t_n}(x, y) = 0$, we set the pixel's probability to the initial level P_0 , in that the pixel may be a new target after this frame.

In order to offset the missing target points due to the infrared sensors, the current iterative image $I(x, y, t_{n-1})$ minus β is taken into account in generating $I(x, y, t_n)$, so when the target is missing in a certain frame, the $D(x, y)$ turns out to be zero, the iterative image $I(x, y, t_n)$ can still inherit information of target from $I(x, y, t_{n-1})$. Generally, the correlation range is set some bigger than v_m , so that it can allow the information act in calculating the next correlation.

C. Detecting the Target

After repeating the procedure above for k times, we finally get a k -order correlation $R_{t_{k-1}t_k}(x, y)$. Then we compare $R_{t_{k-1}t_k}(x, y)$ with a preset threshold Th . A target is to be detected in position (x, y) if the $R_{t_{k-1}t_k}(x, y)$ is higher than Th .

D. Parameters Consideration

In our iterative method, a couple of parameters should be initialized before the detection begins.

The lower β is, the more information will be inherited when the target missing, however, β should be set high enough to discard the information of noise. As we assumed in section II.A, our image sequences has a maximum target missing rate of 1 in S_n , so β can be set to $P_0/2$ to offset a single frame target missing.

For the noise pixels, the k -order correlation $R_{t_{k-1}t_k}(x, y)$ reaches the maximum when there always be a noise pixel in the corresponding $v_m \times v_m$ region between frames. This probability is expressed by

$$P_1 = (1 - (1 - P_n)^{v_m \times v_m})^{k+1} \quad (8)$$

Where P_n is the probability of the appearance of noise pixels. Suppose the image size is $U \times V$ pixels, considering the independence of noise, P_n can be obtained from a statistic method,

$$P_n = \frac{\sum_{x=1}^U \sum_{y=1}^V F(x, y, t_0)}{U \times V} \quad (9)$$

Provided an anticipant false rate P_f , we chose the order k under the condition

$$P_1 = (1 - (1 - P_n)^{v_m \times v_m})^{k+1} < P_f \quad (10)$$

Thus the threshold is set to

$$Th = P_0 + (k - k / S_n) \times \alpha - (k / S_n) \times \beta \quad (11)$$

Where α, β should satisfy

$$(1 - 1 / S_n) \times \alpha - \beta / S_n > 0 \quad (12)$$

III. THE NEURAL NETWORK STRUCTURE REALIZATION

This section presents the neural network implementation of the target detection method developed in section II.B. According to the iterative procedure described in (2)~(7), a simple structure of neural network has been chosen correspondingly. Fig.1 illustrates a 3-layer neural network to realize one cycle of the method. Supposing the size of input image is $U \times V$ pixels, then input layer A and middle layer B have a number of neurons of $2 \times U \times V$. Now we consider a unit of neurons related to pixel (x, y) , the value of iterative image $I(x+i, y+j, t_{n-1})$ forms the inputs of neuron $A_{1,x,y}$, with a connection weight of $w_{i,j}^{x,y} = F(x, y, t_n)$. Using a Winner-Take-All rule, we can get a correlation output of $A_{1,x,y}$ as described in (4). The neuron $B_{1,x,y}$ and $B_{2,x,y}$ forward compute the $D(x, y)$ in (5). Together with the output of neuron $A_{2,x,y}$, which is $I(x, y, t_{n-1}) - \beta$, we can obtain the input of the neuron (x, y) in Layer F_{n+1} . The value of new iterative image $I(x, y, t_n)$ is finally generated using the Winner-Take-All rule again.

In the next cycle, we change the Layer A's inputs by the newly-generated image $I(x+i, y+j, t_n)$, and update the weights $w_{i,j}^{x,y}$ with the values in next frame $F(x, y, t_{n+1})$. This procedure continues until a threshold has been reached

by the output of neuron $A_{1,x,y}$, when a target has been detected.

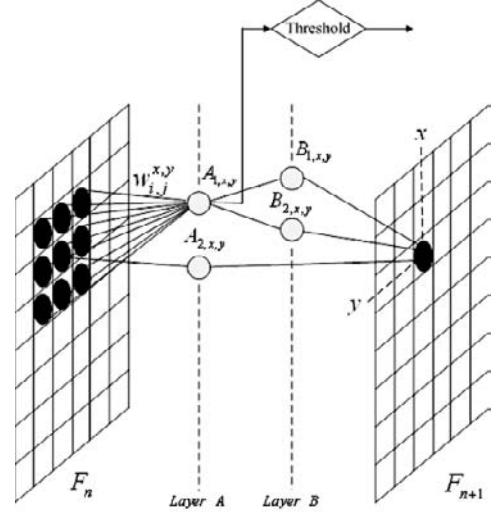


Fig. 1. Neural Network Structure to realize one circle of the processing

IV. SIMULATION AND RESULTS

Computer simulation was carried out to test our method's real-time running ability and detection accuracy. For our simulation studies, we had used a 57-frame infrared video with a resolution of 256×256 , which comprises multiple moving ground targets and a flying aerial target that are not immediately obvious. The infrared video was obtained from <http://www.ee.surrey.ac.uk/EE/VSSP/demos>.

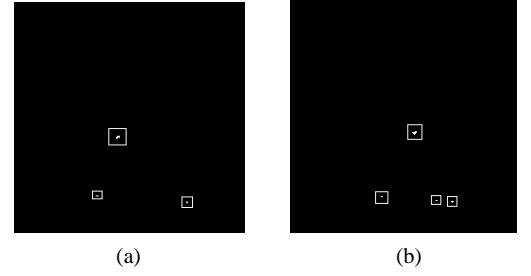


Fig. 2. Simulation results. (a) three targets detected in frame 35, (b) four targets detected in frame 39

After using the windows rejection method in [2] and clutter rejection method as preprocessing, we initialized the parameters as $\alpha = 1, \beta = 0.5, P_0 = 1, k = 13, Th = 11$.

The Fig.2 shows the detection results in the given image frames. In the simulation, three targets were found in frame 35, and four targets were found in frame 39.

Our method has a real-time ability of 6 frames per second on the experimental computer, with PentiumVI 2.0GHz CPU, 512MB memories.

By adding the Gaussian noise to the original images, we have tested the detection capability of our method in low SNR condition. Fig.3 shows the detection result (SNR=3) in frame 35, the same targets were detected as in Fig.2

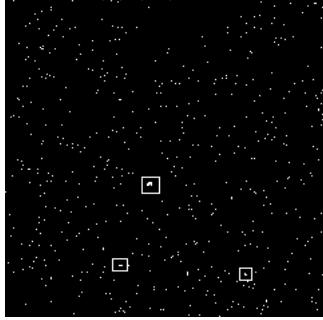


Fig. 3. Simulation results in low SNR condition (SNR=3),
three targets detected in frame 35

V. CONCLUSION

In this paper, a new method for dim target detection in infrared image sequences is developed, the method is based on accumulated information which carries the pixel's capability to be a target. This iterative scheme can be implemented by a simple neural network structure. Compared with the high order correlation method in [2], our scheme has a real-time running ability and a low memory occupation. Not like the neural networks method suggested in [3],[4], our method require no training procedure, therefore, this real-time iterative method is capable in most infrared image sequences that is lack of prior sample and information.

REFERENCES

- [1] M. W. Roth, "Survey of Neural Network Technology for Automatic Target Recognition," *IEEE Trans. Neural Networks*, vol. 1, no. 1, pp. 2843, March 1990.
- [2] Liou, R.J. and Azimi-Sadjadi, M.R., "Dim target detection using high order correlation method," *Aerospace and Electronic Systems, IEEE Transactions on*, Vol. 29, pp:841 – 856, Issue 3, July 1993
- [3] Patra, J.C., Widjaja, F., Das, A., and Ee Luang Ang, "A fast neural network-based detection and tracking of dim moving targets in FLIR imagery," *Neural Networks, 2005. IJCNN '05. Proceedings. 2005 IEEE International Joint Conference on*, Vol.5, pp:3144 – 3149, 31 July-4 Aug. 2005
- [4] Haixin Chen, Zhenkang Shen, and Huihuang Chen, "Detecting dim point target in infrared image sequences using probabilistic neural network," *Aerospace and Electronics Conference, 1994. NAECON 1994., Proceedings of the IEEE 1994 National*, vol.1, pp:137 – 141, 23-27 May 1994

Cooperative Diversity Based on LDPC Code

Weijia Lei¹, Xianzhong Xie², Guangjun Li¹

¹SCIE, University of Electronic Science and Technology of China, Chengdu, China

²KLMC, Chongqing University of Posts and Telecommunications, Chongqing, China

Abstract-Diversity is an effective method to resist the fading effect in wireless channel. Limited by size, weight and cost, it is difficult to use the multi-antenna technique on the terminal of wireless communication. Cooperative communication allows the sharing of the antennas among the mobile terminals which have single antenna. Thus creates virtual multi-antenna, and realizes transmitting diversity. LDPC code is a good linear block code. By using the intrinsic coherence among the bits of the code word, we can create a coded cooperative communication among the mobile users to effectively improve the system performance. This paper proposes a cooperative communication method based on LDPC code, and provides the simulation results.

I. INTRODUCTION

Multiple-input Multiple-output (MIMO) system uses multiple transmitting and receiving antennas to obtain diversity gain, which can effectively resist the fading effect in wireless channel and consequently leads to the improvement of the system performance. In wireless communication systems, such as cellular mobile communication system and wireless sensor network, it is difficult to apply multi-antenna technique in the terminal owing to the limits of size, weight, power and cost. The notion of cooperative communication has been proposed recently, the basic idea of which is that users with single antenna cooperate with each other while transmitting data. As their antennas are shared by all users, a virtual multiple transmitting antennas system is created. The model of cooperative communication between two users in cellular mobile communication system is illustrated in Fig. 1. Each user acts as the cooperative agent for the other. User 1 is the partner of user 2, and vice versa. The transmission process of users in cooperative communication is split into two stages. In the first stage, users transmit their own data to the base station, and at the same time receive the data from their partner. In the second stage, users deal with the received data and then transmit them to the base station. If the distance between users is long enough, the two uplink channels from the users to the base station can be dealt as independent channels. So the base station can receive two independent copies of each user's data, thus realizing the transmitting diversity. Currently there are three main methods of cooperative communication [1][2]:

1. Amplify-and-forward method. Each user receives the signal transmitted by its partner in the first stage, amplifies and transmits them to the base station in the second stage.

2. Detect-and-forward method. Each user attempts to detect and estimate the received signal, tries to recover the data and transmits them to the base station.

3. Code cooperation. In this method, users do not forward the received signal. Their data are encoded into code words, and every code word is split into two parts. Each user

transmits the first part of its own code word, then the second part of its partner's code word. Because the intrinsic coherence among the bits of the code word, if the base station receives different parts of the code word through independent channels, transmitting diversity can also be realized. The code used in cooperation can either be the traditional channel code, or the one specifically designed.

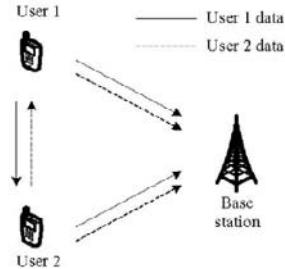


Fig. 1 The model of cooperative communication between two cellular users

T. E. Hunter proposed a coded cooperation method based on convolution code or Turbo code. Low density parity check (LDPC) code is a linear block code with an excellent performance. If the code word is long enough, its performance is better than Turbo code, while the decoding speed is faster. By using the cooperative communication based on LDPC code, we can obtain great diversity gain and improve system performance effectively, without much rise in the system bandwidth and transmitting power, nor would the cost and complexity of the terminal increase evidently.

The second part of this paper introduces the method to realize cooperative communication based on LDPC code. The third provides the simulation results, and the last part is the conclusion.

II. METHOD

Our study focuses on the cooperative communication based on LDPC code between two users in the cellular mobile system. The model is illustrated in Fig. 1. Assume the total rate of code is $R=R_1R_2$, the length of the code word is N , and the length of the information bits is $K=RN$. The code word is split into two parts, the lengths of which are N_1 and N_2 respectively and $N=N_1+N_2$. A full cooperative communication is split into two stages. First, the K bits of information are encoded into a code word at rate R_1 – called the first encoding. The length of the code word is $N_1=K/R_1$. This code word is transmitted to the base station, and also received by its partner. In the second stage, the user decodes the received data. If the decoding is correct, it encodes them

in the systematic code form at the rate R_2 – called the second encoding. The length of the code word is $N = N_1/R_2 = K/R_1R_2 = K/R$. The length of the parity bits of the code word is $N_2 = N - N_1 = (1/R_2 - 1)K/R_1$. Last, the parity bits are transmitted to the base station. The cooperative coefficient is defined as $C_c = N_2/N = 1 - R_2$, which indicates the degree of the cooperation. If the decoding is wrong, the user's own data are encoded and transmitted just as before. The total length of data transmitted by each user is always $N = N_1 + N_2$. Its partner carries out the same operation in the mean time. According to the decoding results of the two users in the first stage, there are four possible cases of cooperation (Fig. 2):

Case 1: both users decode their partners' data correctly in the first stage, so they transmit their partners' parity bits in the second stage. This is a complete cooperation (Fig. 2(a)).

Case 2: neither of the two users decodes their partners' data correctly in the first stage, so they transmit their own parity bits in the second stage. This is non-cooperation (Fig. 2(b)).

Case 3: user 1 decodes user 2's data correctly, but user 2 does not in the first stage. Both user 1 and user 2 transmit user 2's parity bits in the second stage (Fig. 2(c)).

Case 4: similar to case 3, but the roles of user 1 and user 2 are exchanged (Fig. 2(d)).

In cases 1 and 2, the receiver (base station) just needs to combine the data received at the first stage and the second stage for both users. Then it decodes them and gets the N_1 bits data of the first stage – called the first decoding. Last, it decodes the N_1 bits data and gets the K bits of the information – called the second decoding. In case 3, the base station does not receive the parity bits of user 1, so it just does the second decoding for it. At the mean time, the base station receives two independent copies of user 2's parity bits. It combines them in an optimal manner, and then decodes them as it does in cases 1 and 2. Case 4 is similar to case 3, but the roles of user 1 and user 2 are exchanged.

The feedback channel is not necessary between the cooperative users in the code cooperative communication, since they can change to non-cooperative communication mode automatically when the channel between the users is bad. The problem of error propagation does not appear in the code cooperative communication, and its performance is never worse than that of the non-cooperative communication. In contrast, the system performance will degrade dramatically in the amplify-and-forward method or detect-and-forward method when the channel between the users is bad, because error propagation will happen. But what is peculiar to the code cooperation is that the receiver must know to whom the parity bits received at the second stage belong. So indications

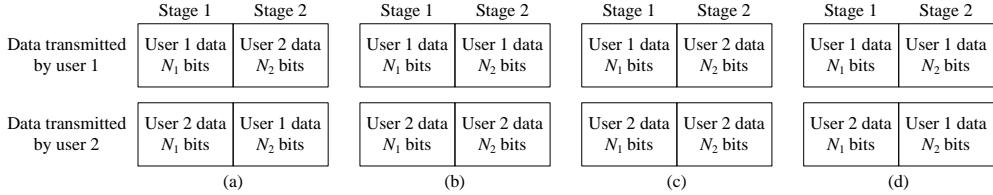


Fig. 2 Four cases of code cooperation

from the users to the base station are necessary, which must be well protected to avoid any serious decoding error in the base station. This will slightly increase the overhead of the system.

In most of the wireless communication systems, for the purpose of error detecting – automatic request repetition (ARQ), the CRC code has been applied to the data section by the data link layer or medium access control sub-layer (MAC). This CRC code can be utilized in the code cooperative communication, and the first encoding can be bypassed, so that the user just detects the error of the received data, with no need to correct it. The code rate of the system is promoted.

Assume the channel between two cooperative users is symmetric. When the channel is good, the code cooperation will be in case 1 for most of the time, and a high diversity gain will be obtained. When the channel is bad, the cooperation will be in case 2 for most of the time, and the performance is close to that in the non-cooperative system. When the channel performance is average, the cooperation will fall into any one of the four cases, and the system performance will be between those of the above-mentioned two situations. In this way, a partial diversity gain will be obtained.

III. SIMULATION RESULTS

To demonstrate the performance of the code cooperation based on LDPC code, simulation has been done. Assume that: the system model is Fig. 1; the channel between the two cooperative users and the uplink channels (between user and base station) are Rayleigh channels, and the fading coefficients of the channels are constant in the period of a code word; receivers (partners and the base station) know the characters of the channels; users are able to judge whether the received data are correct (this is rational for the data with CRC checksum), and the first encoding is not included; the regular binary systematic LDPC code with $N = 504$, $R = 0.5$ [3] is used; modulation method is BPSK; the cooperative coefficient $C_c = 1 - R = 0.5$. The sum-production algorithm is applied for the decoding of LDPC code [3][4].

Fig. 3 is the simulation results when the SNRs of the two users' uplink channels are equivalent. Since the results of the two users are identical, only one user's results have been demonstrated here. The four curves in the figure are the SNR of uplink channel vs. the bit-error-rate (BER) of the code cooperative communication system when the SNR of the channel between the users is 0 dB, 10 dB or 20 dB respectively, and that of non-cooperative communication system. When the channel between users is good, the system

performance is improved obviously, and the diversity gain increases with the increase of the SNRs of the users' uplink channels. For instance, when the SNR of the channel between the users is 20 dB and $\text{BER} = 10^{-4}$, the diversity gain is 5.5 dB. The system performance will decline if the SNR of the channel between the users degrades, but the diversity gain can still be got: when this SNR is 10 dB and $\text{BER} = 10^{-4}$, the diversity gain is 3 dB. When the channel is bad, the performance is similar to that of the non-cooperation system, which has been shown by the curve of $\text{SNR} = 0 \text{ dB}$. The simulation results are identical to our expectations.

Fig. 4 is the simulation results when the SNRs of the two users' uplink channels are not equivalent. The SNR of user 2's uplink channel is fixed to 30 dB, and the SNR of the channel between the users is 20 dB. The SNR of user 1's uplink channel varies from 8 dB to 36 dB. When the SNR of user 1 is lower than user 2, i.e. under 30 dB, its performance is improved greatly. For example, the diversity gain is about 7.5 dB at $\text{BER} = 10^{-3}$, 6.5 dB at $\text{BER} = 10^{-4}$. Although the SNR of user 1 is lower, user 2 can also obtain the diversity gain via the cooperation except when the SNR difference between the two users is greater than 11.5 dB, and the gain increases with the increase of the SNR of user 1. For example, if user 1's SNR is 24 dB or 28 dB, user 2's BER will become 1.22×10^{-4} or 7.58×10^{-5} respectively. In the non-cooperation system, the SNR of user 2 must be 33 dB and 35 dB respectively to achieve the same BER. So the gains obtained by user 2 are 3 dB and 5 dB respectively. When the SNR of user 1 is larger than that of user 2, the gain of user 2 becomes greater than that of user 1. The results illustrate that the user with better uplink channel can help improve the performance of the user with worse uplink channel markedly, and at the same time its performance is also improved, except when the difference between the SNRs of two users' uplink channels is too great. The final result is the great promotion of the system performance.

IV. CONCLUSION

It is validated by analysis and simulation that the system performance can be promoted effectively by cooperative communication based on LDPC code, with no evident rise in the system bandwidth and transmitting power, or any sharp increase in the cost and complexity of the terminal. From the simulation results, we find that the code cooperation will not bring much improvement to the system performance when the channel between the cooperative users is bad, because in this case the cooperation is in case 2 for most of the time. Such a problem can to some degree be solved by using of LDPC code in the first stage. In addition, the cooperative coefficient can also affect the system performance. The best value of it is 0.5 when the SNRs of the two users' uplink channels are the same. It can also be used to adjust the performance balance between the two users when the performances of their uplink channels are not the same. And the power assigning policy between the two users can also be adopted to improve the system performance. Even the space-time code can be applied in the second stage to guarantee the transmission of the parity bits

for both users in all four cases, which will further improve the system performance. This paper discusses the cooperation between two users, but it is not difficult to extend it to the cooperation among multiple users.

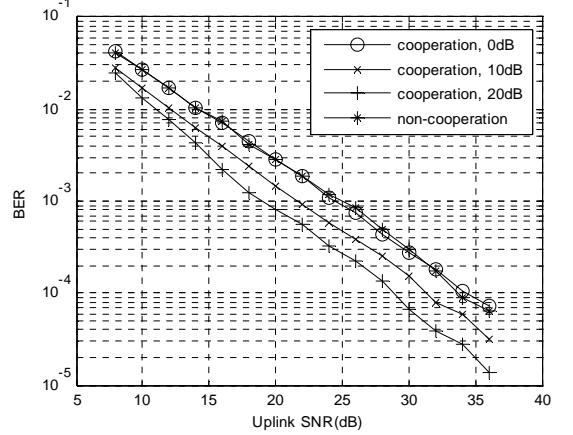


Fig. 3. The performance of the cooperative communication in Rayleigh channel (The SNRs of both users' uplink channels are identical)

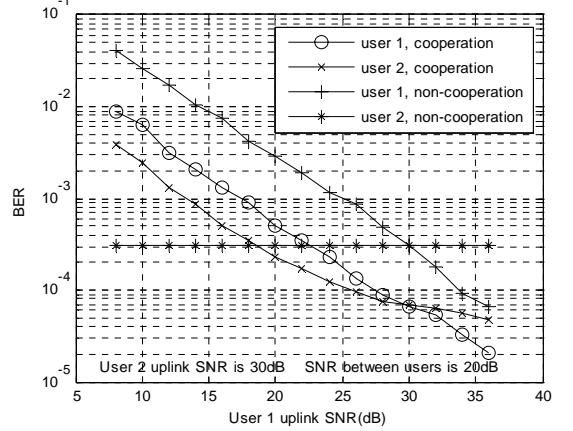


Fig. 4 The performance of the cooperative communication in Rayleigh channel (The SNRs of the users' uplink channels are not identical, user 2's SNR is fixed to 30 dB, the SNR of the channel between the users is 20 dB)

ACKNOWLEDGMENT

This work is supported by Natural Science Foundation Project of CQ CSTC.

REFERENCES

- [1] A. Nosratinia, T. E. Hunter and A. Hedayat, "Cooperative Communication in Wireless Networks." IEEE Communications Magazine, Vol. 42, Issue 10, Oct. 2004, pp. 74-80.
- [2] T. E. Hunter, "Coded Cooperation: A New Framework for User Cooperation In Wireless Networks". Ph. D Thesis, The University of Texas at Dallas, 2004.
- [3] R. G. Gallager, "Low-Density Parity-Check Codes". Cambridge, Mass, MIT Press, 1963.
- [4] M. C. Davey, "Error-correction using Low-Density Parity-Check Codes". Ph. D Thesis, University of Cambridge, 1999.

MEMS Yield Simulation with Monte Carlo Method

Xingguo Xiong¹, Yu-Liang Wu², Wen-Ben Jone³,

¹ Department of Electrical and Computer Engineering,
University of Bridgeport, Bridgeport, CT 06604, USA

² Dept. of Computer Science & Engineering,
The Chinese University of Hong Kong, Shatin, Hong Kong

³ Department of ECECS, University of Cincinnati, Cincinnati, OH 45221, USA
Email: ¹ xxiong@bridgeport.edu, ² ylw@cse.cuhk.edu.hk, ³ wjone@eecs.uc.edu

Abstract. In this paper, Monte Carlo method is used for the simulation of point-stiction defects in MEMS accelerometer devices. The yield of MEMS devices is estimated based on the simulation results. Comparison between simulated yields of BISR/non-BISR MEMS accelerometers demonstrates effective yield increase due to self-repairable design. The simulation results of yield increase versus different initial yields for BISR MEMS accelerometers are in good agreement with theoretical prediction based on previous MEMS yield model. This verifies the correctness of the MEMS yield model.

Keywords: MEMS (Microelectromechanical System), BISR (built-in self-repair), yield, Monte Carlo method, defect simulation.

1 Introduction

In [1], we proposed a built-in self-repair technique for the MEMS comb accelerometer device. The main device of the comb accelerometer consists of n identical modules, and m modules are introduced as the redundancy. If any of the working module in the main device is found faulty during a built-in self-test (BIST), the control circuit will replace it with a good redundant module. In this way, the faulty device can be self-repaired through redundancy. We also developed the yield model [1] to quantitatively evaluate the yield increase due to redundancy repair. Based on the yield model, the yield increase due to redundancy repair versus initial yield for different m and n numbers were plotted. MEMS yield is directly related to the behavior of the defects during microfabrication process and in-field application. In order to verify our MEMS yield model, we need to estimate the MEMS yield by defect simulation, and compare the simulation result with theoretical prediction.

Due to the stochastic nature of defect distribution in micro-fabrication process, Monte Carlo simulation [2] is very suitable

for MEMS defect simulation. In [3], Monte Carlo simulation is used for contamination/reliability analysis of Microelectromechanical layout. In [4], Monte Carlo method is used for the yield estimation of digital microfluidics-based biochips using space redundancy and local reconfiguration. In this paper, we use Monte Carlo method to simulate the point-stiction defects in MEMS accelerometer devices. Based on the Monte Carlo simulation result, we estimate the yields for both BISR (built-in self-repairable) and non-BISR MEMS accelerometers. A comparison between both devices demonstrates an effective yield increase of BISR device compared to non-BISR design. The simulation result of MEMS yield increase versus initial yield is in good agreement with theoretical prediction based on our previous MEMS yield model [1]. This verifies the correctness of our MEMS yield model.

2 Point-stiction Defects and Monte Carlo Simulation

During the fabrication or the in-field usage of MEMS devices, the movable microstructure may be stuck to substrate in one or multiple points. This is different from the stiction problem due to surface forces in surface micromachining techniques, and we denote it as "point-stiction". These local point-stictions can limit or totally block the movement of the movable microstructure, and hence lead to device failure. An example of point-stiction is illustrated in Figure 1. The point-stiction defects can be developed due to various reasons. For example, a pinhole in the sacrificial layer may lead to such point-stiction. A particle on the photolithography mask during the patterning of anchor area may also lead to a point-stiction. Furthermore, a particle may randomly fall into the gap between a movable microstructure and the substrate, and it may block the movable microstructure at that particular point. Even after the device is sealed, particle-resulted point-stiction may still be developed during in-field usage. Thus, point-stiction can be a common defect source for MEMS devices.

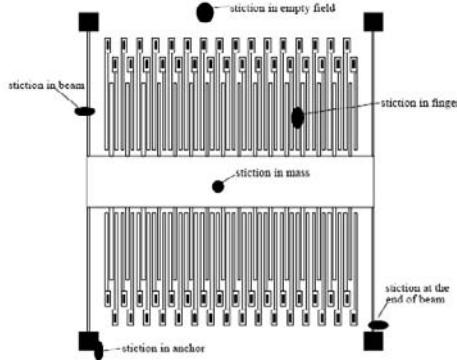


Figure 1. Point-stiction and its formation.

MEMS devices are vulnerable to various defect sources during the fabrication process or in-field usage [5]. The occurrence and the location of these defects are random and cannot be precisely predicted. Such stochastic behavior can be better predicted with statistical simulation methods, such as Monte Carlo simulation [2]. Monte Carlo simulation is a stochastic technique used to approximate the probability of certain outcomes by running multiple trial simulations using random number and probability statistics. In a Monte Carlo simulation, the random selection process is repeated many times to create multiple scenarios. Each time, a value is randomly selected to form one possible solution to the problem. Together, these scenarios give a range of possible solutions with different possibilities. When the simulation is repeated for a large amount of times, the average solution will give an approximate answer to the problem. ANSYS FEM software [6] supports the feature of Monte Carlo simulation in its probabilistic design module.

3 Simulation Strategy

In our research, we use Monte Carlo simulation to simulate the device behavior with point-stiction defects. We made the following assumptions and criteria in our simulation. First, according to Federal Standard 209E [7], the typical particle size in a clean room is $0.1\text{--}5\mu\text{m}$ in diameter. Thus, we set the size of a point-stiction defect in the range of $0.1\text{--}6\mu\text{m}$. Point-stiction defects (square in shape) with random size in this range will be generated and randomly distributed in the device area (including the surrounding empty area). Second, we assume the point-stiction distribution is totally random without clustering effect. However, if clustering effect is considered, the MEMS device yield will be even higher. Third, we use a similar sensitivity selection criterion as [3] for the simulated devices: devices with sensitivity deviation within $\pm 5\%$ is treated as acceptable "good" devices; sensitivity deviation from $\pm 5\%\text{--}30\%$ is treated as parametric defects; deviation larger than 30% will be treated as catastrophic defects. Devices with parametric or catastrophic defects will be discarded in our yield analysis.

In order for fair comparison, we assume equal defect density for both BISR and non-BISR devices in each case of simulation.

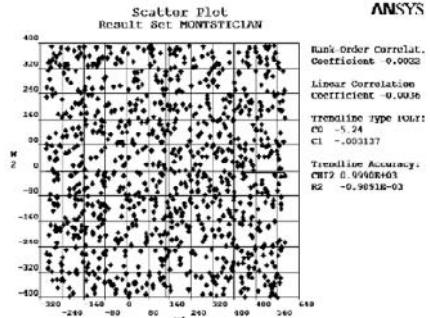


Figure 2. Random defect scattering in Monte Carlo simulation (Case #2: two defects in each of 1000 non-BISR device samples)

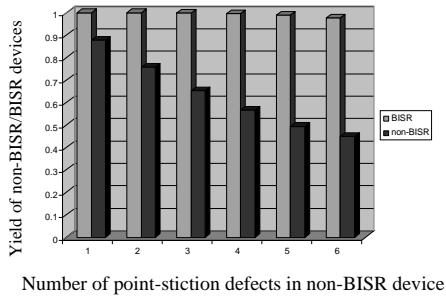
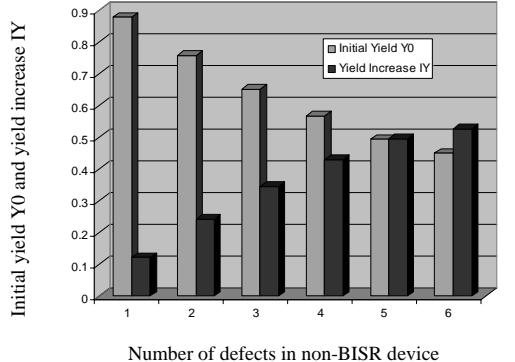
Since the BISR device has about 1.5 times of area when compared to non-BISR device, it contains 1.5 times of amount of point-stiction defects compared to non-BISR device. We simulated six cases of different defect densities: the number of point-stiction defects in non-BISR device ranges from 1 to 6 separately. Correspondingly, we simulated the BWC (Beam Width Compensation) [8] BISR device with 1.5, 3, 4.5, 6, 7.5, and 9 point-stiction defects separately for the six cases. In order to simulate the cases of BISR devices with 1.5, 4.5 and 7.5 point-stiction defects, we simulate 3, 9 and 15 point-stiction defects distributing randomly in double device areas. In this way, the area of one device contains 1.5, 4.5 and 7.5 point-stiction defects separately. We simulated 1000 device samples and derived the device displacement sensitivities with such defects. An example of random scattering of 1000 samples (two defects in each device) of point-stictions generated in Monte Carlo simulation case #2 is shown in Figure 2.

4 Simulation Results and Discussion

Yield comparison between the non-BISR and BISR devices is shown in Table 1. As we can see, the yield of the BISR device in the presence of point-stiction defects is apparently much higher than that of the non-BISR device. Take the simulation case #6 as example, where 6 defects occur in the non-BISR device (and correspondingly 9 defects in the BISR device), the yield of the non-BISR device is 45%, while the yield of the BISR device is 97.7%. A yield increase of 52.7% is observed, and this indicates that a significant yield increase can be achieved for moderate initial yield (e.g., 45% in case 6). This coincides with our previous theoretical prediction [1]. A visual comparison between the yields of non-BISR and BISR devices for different number of point-stiction defects is shown in Figure 3. The yield increase due to redundancy repair for six simulation cases is shown in Figure 4. From the bar chart, it is clearly seen that the BISR design leads to positive yield increase when compared with the non-BISR design for all the six simulation cases. It can be observed that the yield decreases only slightly for the BISR design as the defect density increases, while the yield of non-BISR devices decrease rapidly as the defect density increases.

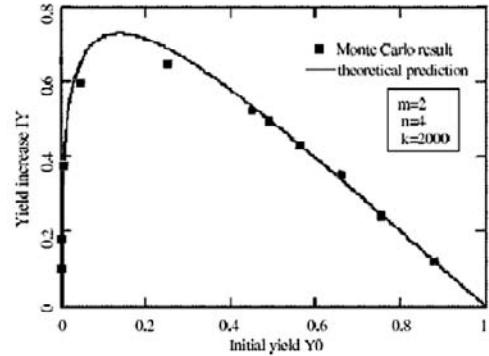
Table 2. Comparison of Monte Carlo simulation results between non-BISR and BISR devices.

Simulation case	#1	#2	#3	#4	#5	#6
No. of defects in non-BISR	1	2	3	4	5	6
No. of defects in BISR	1.5	3	4.5	6	7.5	9
Non-BISR device yield	87.8%	75.7%	65.2%	56.6%	49.4%	45.0%
BISR device yield	100%	100%	99.8%	99.6%	99.0%	97.7%
Net yield increase IY	12.2%	24.3%	34.6%	43.0%	49.6%	52.7%

**Figure 3.** The yield comparison between non-BISR and BISR devices.**Figure 4.** The yield increase due to redundancy repair for six simulation cases.

In the above Monte Carlo simulation, we simulated the cases for large (~ 1) and moderate (~ 0.5) initial yields. In order to find out the yield increase for small (~ 0) initial yield, we further increased the number of defects in non-BISR/BISR devices in our Monte Carlo simulation. Monte Carlo simulation shows that when the defect number is too large ($N=60$ or above), eventually the BISR device yield will also drop to zero, and the yield increase becomes zero. Because in Monte Carlo simulation the defect distribution is totally random, which means a clustering factor of $k=\infty$. Since it is difficult to simulate the case for $k=\infty$ in computer, we simulate the theoretical analysis of the case when $k=2000$ (a large number). The comparison between the theoretical prediction

($k=2000$) and the above Monte Carlo simulation results for yield increase versus initial yield is shown in Figure 5.

**Figure 5.** The comparison between theoretical prediction and Monte Carlo simulation result.

From the figure, we can see that the Monte Carlo simulation results coincide with the theoretical prediction very well. There is some slight difference for moderate initial yield. However, considering the above assumption for the clustering factor k , this discrepancy is reasonable. In the previous theoretical analysis [1], it has been shown that the yield increase due to redundancy repair is most significant for moderate initial yield. If the initial yield is too large (approaching 1) or too small (approaching 0), the yield increase due to redundancy repair is not significant. Monte Carlo simulation result verifies this prediction. This proves the correctness of our MEMS yield model for redundancy repair.

5 Conclusions and Future Research

In this paper, Monte Carlo method is used to simulate the point-stiction defects of MEMS accelerometers. Based on the simulation results of large batch of devices, we estimate the yields for both BISR and non-BISR MEMS accelerometers. Comparison of simulated yields for BISR and non-BISR MEMS devices demonstrates that an effective yield increase can be achieved due to BISR design. The simulation result of yield increase versus different initial yield is in good agreement with theoretical prediction based on our previous yield model. This verifies the correctness of our yield model.

In this paper point-stiction defects are simulated for MEMS yield estimation. However, in reality, the yield can be affect by various defect sources [8], such as etch variation, broken beam, material fatigue, etc. In the future, we will also simulate MEMS yield due to other various defect sources. In this way, the yield estimation will be more accurate and the result can be closer to the real device behavior.

References

1. X. Xiong, Y. Wu, and W. Jone, "Design and analysis of self-repairable MEMS accelerometer," *Proceedings of the 20th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems (DFT'05)*, Monterey, CA, USA, pp. 21-29, Oct. 3-5, 2005.
2. C. P. Robert and G. Casella, *Monte Carlo Statistical Methods*, 2nd edition, June 1, 2005, *Springer*.
3. A. Kolpekwar, T. Jiang, and R. D. S. Blanton, "CARAMEL: Contamination And Reliability Analysis of MicroElectro-mechanical Layout", *Journal of Microelectromechanical Systems*, Vol. 8, No. 3, pp. 309-318, Sept. 1999.
4. F. Su and K. Chakrabarty, "Yield enhancement of reconfigurable microfluidics-based biochips using interstitial redundancy", *ACM Journal on Emerging Technologies in Computing Systems*, Vol. 2, No. 2, pp. 104-128, April 2006.
5. B. Stark (editor), "MEMS Reliability Assurance Guidelines for Space Applications", *Jet Propulsion Laboratory Publication 99-1*, Pasadena, USA, Jan. 1999.
6. URL: <http://www.ansys.com>
7. Federal Standard 209E, 1992, "Airborne Particulate Cleanliness Classes in Cleanrooms and Clean Zones. General Services Administration (GSA)", *GSA Service Center*, Seventh & D Street, SW, Washington DC, USA.
8. X. Xiong, "Built-in self-test and self-repair for capacitive MEMS devices", Ph.D dissertation, University of Cincinnati, 2006.

A Human Interface Tool for System Modeling and Application Development Based on Multilevel Flow Models

Yangping Zhou*, Yujie Dong, Yuanle Ma

Institute of Nuclear and New Energy Technology, Tsinghua Univ.
Nengkelou, Tsinghua University, Beijing 100084, China

Hidekazu Yoshikawa

Graduate School of Energy Science, Kyoto Univ.
Gokasho, Uji, Kyoto 611-0011, Japan

Abstract-Based on the notion of flow of mass, energy and information, Multilevel Flow Models (MFM) is a graphical functional modeling method aiming at providing a semantic basis for using means-end and whole-part decompositions of complex system. This paper proposed a human interface tool, Multilevel Flow Models Studio (MFMS), for system modeling and application development. With a friendly graphical interface, MFMS mainly consists of two modules: an editor module to construct, maintain and configure the MFM model for the target system; an executor to implement the application for Man Machine Interaction based on the MFM model. This MFMS has been applied for developing a demonstration system for operation support of a Nuclear Power Plant and a visual analysis platform for the Nuclear Fuel Cycle system of Japan.

Keywords: Multilevel Flow Models, Man Machine Interaction, Multilevel Flow Models Studio, Graphical Interface

I. INTRODUCTION

Multilevel Flow Models (MFM), firstly introduced by Morten Lind [1], is a graphical functional modeling method based on the notion of flow of mass, energy and information. It aims at providing a systematic basis for using means-end and whole-part decompositions in the modeling of complex system. Algorithms by MFM for measurement validation, alarm analysis and fault diagnosis were proposed, implemented and successfully tested on simulations of several processes [2]. Ohman presented a measurement validation method with MFM [3]. A new consequence analysis approach for performing alarm analysis using MFM was introduced by Dahstrand [4].

MFM models the target system using discrete and abstract representation in terms of goals and functions, and thus is computationally more efficient and valuable for a high level of control, decision, planning, analysis and diagnosis. MFM has been widely applied in various fields since last decade. MFM was successfully used in Guardian, a medical monitoring and diagnosis system under hard real-time conditions [5]. Paassen and Wieringa described the use of MFM as a basis for reasoning for obtaining the actions necessary to achieve the goal or the intentional change of the system [6], which can provide support for operator or for automatic control. Gofuku and Tanata developed a system for diagnostic information display based on MFM [7]. A research based on MFM was proposed to monitor and diagnose a co-generation system, Micro Gas Turbine System [8].

This study is partially sponsored by Kyoto University 21COE Program "Establishment of COE on Sustainable Energy System" (21COE-14219201).
*zhouyp@mail.tsinghua.edu.cn

The first step of a MFM modeling approach is to provide a concise description of a system according to the functional properties of its objects as well as its structural characters, and thus requires not only a profound understanding of system purpose, function, behaviour and structure of this system but also skills on MFM modeling and IT. Unfortunately, the experts who are familiar with the target system usually lack in expertise on MFM modeling method and IT skills as they are engaging in modeling the target system for various purposes such as supervisory, diagnosis, and analysis.

This paper proposed an integrated graphical interface based system, Multilevel Flow Models Studio, which provides assistant from cover to cover, namely, modeling system and developing final application for monitoring, operational instruction and so on. With a friendly graphical interface, MFMS mainly consists of two modules, an editor to intelligently assist user construct, maintain and configure the MFM model; and an executor to implement the application for Man Machine Interaction (MMI) in terms of the established MFM model. The executor can implement different applications by loading different MFM models. The MFM model in this MFMS includes not only functional, structural and behavioral properties of the target system, but also various information and mechanisms for the specific application. The MFM model can be easily revised for improving the performance and usability of the application. In this way, user can concentrate on the fields with which they are familiar. By using Visual C++ .NET, DirectX SDK, MSXML Parser SDK and Microsoft Agent SDK, a prototype MFMS system has been developed and applied to develop a demo operation support system for a Nuclear Power Plant (NPP) simulated by RELAP5/MOD2. In addition, a visual platform for analysing the Nuclear Fuel Cycle (NFC) system is developed by using this MFMS system [9].

The remainder of this paper is organized as follows. A brief introduction of MFM is given in section 2. The design of MFMS is introduced in section 3. Section 4 briefly describes how the prototype MFMS system works to establish, maintain and execute the MFM model in a unified and flexible way. Finally, section 5 is conclusions and perspectives.

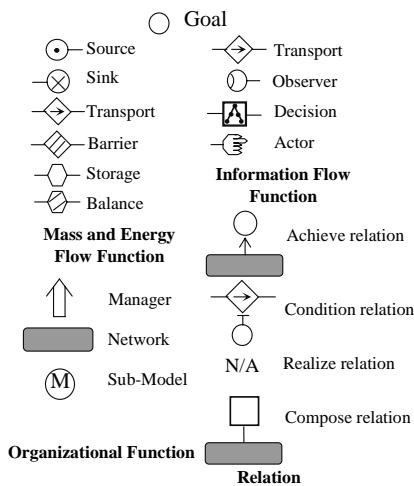


Figure 1. Symbols of Multilevel Flow Models

II. MULTILEVEL FLOW MODELS

MFM is a graphical functional modeling method to explain the semantics of the process system based on the idea of goal, physical component and function. Goal means the objective or purpose that the system or the sub-system is designed or constructed to achieve. Physical component indicates what the system or the equipment consists of. Function is the means by which the physical component will achieve the goal. There are several kinds of relations between goal, function and physical component: realize relation, achieve relation and condition relation and compose relation.

A realize relation affiliates physical component to function by stressing that a physical component is used to realize a specific function. Because MFM do not express physical component in any explicit way and function is the basic element of MFM, realize relation need not be explicitly expressed by any symbols. An achieve relation connects a group of functions to a goal by stressing that these functions are used to obtain a specific goal. A condition relation connects a goal to a function by stressing that the goal must be achieved in order to realize this function. A compose relation connects a structure to a function by stressing that a top-level function is composed of a group of lower functions which is organized as a structure. The symbols that represent goal, functions and relations are shown in Fig. 1. MFM describes and handles character and behavior of the target system with a set of interrelated flow structures, where the hierarchical structure is constructed by using achieve relation, condition relation and compose relation. There are three kinds of flow structures, i.e., mass flow structure, energy flow structure, and information flow structure.

III. DESIGN OF MULTILEVEL FLOW MODELS STUDIO

The relations between target system, MFM model and MFMS are shown in Fig. 2. MFM model will be constructed and maintained according to purpose, behavior, function and structure of the target system with the help of the editor of MFMS. The external multimedia files including text, video, audio and picture are affiliated with the MFM model for enhanced interaction between man and machine. Then, the MFM model is loaded by the executor of MFMS to implement MMI for the specific target system. Simultaneously, the multimedia files for machine support of operation, decision making and analysis will be activated by the executor in terms of the state of the target system.

The framework of MFMS and its MFM model are explained in detail in this section. Firstly, the editor of MFMS is introduced. Then, the executor component of MFMS is described.

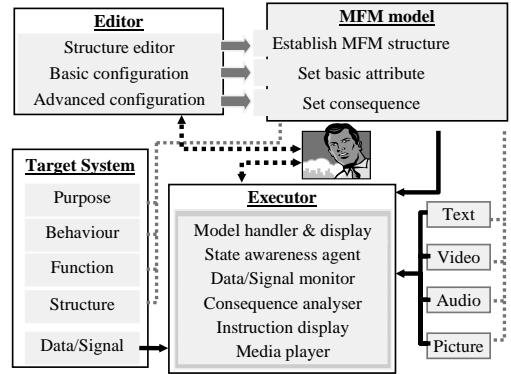


Figure 2. MFMS, MFM model and target system

A. Editor of Multilevel Flow Models Studio

The Editor of MFMS is composed of a structure editor, a basic configuration assistant and an advanced configuration assistant. As shown in Fig. 3, user can conveniently construct the MFM model for MMI by means of these three modules of editor. They will be explained as following.

Structure Editor

With the help of a graphical interface, the MFM model can be constructed in WYSIWYG mode by simple mouse and keyboard operation. Some basic editing functions such as append, select, delete, etc. as well as some intelligent functions such as automatic name generation and auto anti-mistake are provided for constructing the MFM model.

In addition, a MFM structure checker will automatically check the constructed MFM model according to the connecting rules for MFM structure mainly derived from the work of [2] with some modifications. A mistake report will be displayed to user for mistake correcting. These rules are depicted in detail as following:

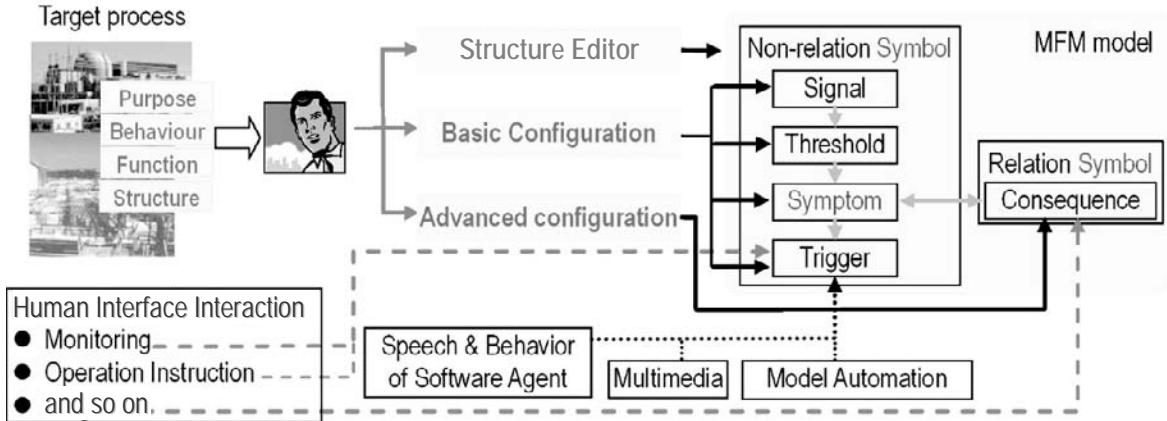


Figure 3. Editing stage of MFMS

- 1) Source and observer must be connected to one and only one transport with output direction.
- 2) Sink and actor must be connected to one and only one transport with input direction.
- 3) Transport must be connected to two and only two other non-organizational functions.
- 4) Balance must be connected to at least two transports.
- 5) Storage must be connected to at least two transports.
- 6) Barrier must be connected to two and only two transports.
- 7) Decision must be connected to at least two transports.
- 8) Network must enclose all energy, mass and information functions and must be connected to at least one achieve relation or compose relation.
- 9) Condition relation must be connected to two and only two symbols among goal, sub-MFM-model and non-organizational function.
- 10) Achieve relation can only be used to connect between goal and network.
- 11) Compose relation can only be used to connect between one organizational function and one non-organizational function.
- 12) Sub-Model function can only be connected to condition relation or compose relation.

Basic Configuration Assistant

Name and explanation of function and goal can be set by simply selecting the relevant symbol. The signal can be selected from a signal list appended to the MFM model. Symbol states and signal thresholds can be set easily by the assistant. Auto color change and auto speech for state awareness can be defined here. Information by text, video, audio and picture can also be affiliated to the symbol state. Graph and text are adopted for understanding the full-scale situation. In order to help the operator capture leading character of target system and follow the foremost instruction,

video, audio and auto speech are utilized for monopolistic state awareness and instruction. The priority of video, audio and auto speech can be customized according to their essentiality and emergency.

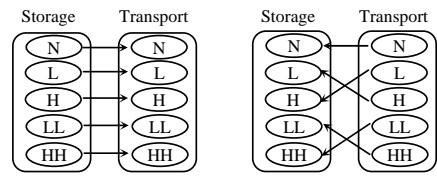


Figure 4. Consequence between a storage and a transport

Advanced Configuration Assistant

The advanced configuration assistant assists user to customize the consequences between functions and goals for the analysis of symbol states. The advanced configuration assistant will automatically set the default consequences between functions and goals and store them in the relevant relation connecting goals and functions in terms of the cause-effect rule of flow model. For example, both a storage function representing an upstream tank and a transport function representing a downstream valve have five possible states: N (Normal volume/flow), L (Low volume/flow), H (High volume/flow), LL (Very low volume/flow) and HH (Very high volume/flow). The consequence between the storage and the transport will be set as Fig. 4 and stored in the connector relation between them. In addition, the default consequence can be modified according to the actual situation of the target system. For example, it can be supposed that the L state of the storage will result in LL state of the transport and the H state of the storage will result in HH state of the

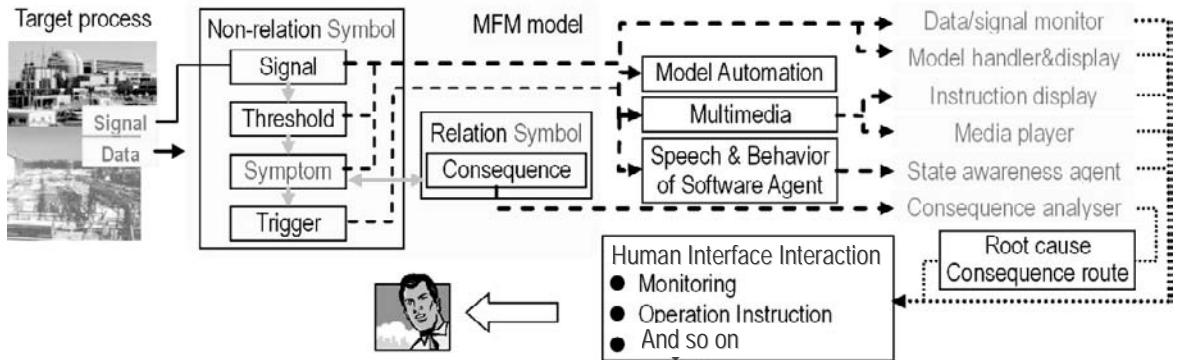


Figure 5. Executing stage of MFMS

transport. The consequence between these two functions can be modified to correspond with this situation by the user with the help of a graphical interface.

B. Executor of Multilevel Flow Models Studio

The executor mainly consists of a model handler & display, a media player, a state awareness agent, a data/signal monitor, an instruction display and a consequence analyser. As shown in Fig. 5, after the executor loads a constructed MFM model aiming at a specific system, these six modules will work cooperatively for implementing the application for analysis, decision making, operation, etc.

Model Handler & Display

The MFM model constructed by the editor is displayed, and data/signal is read and converted to symbol state by the model handler & display. In addition, according to the basic configuration of editor, the color of symbol in MFM model can be modified to indicate the full-scale state of target system in real-time mode. Furthermore, the information of the symbol such as curve display of related data/signal and information of relevant physical component can be observed conveniently.

Media Player

A mini media player that can open common video, audio and picture file is embedded in this MFMS. These files can be automatically activated by the corresponding symbol state. For example, if a video file is affiliated with the LL state of a transport, this video file will be automatically played when the transport is in LL state if the priority of it is fulfilled.

State Awareness Agent

Interface agents are computer programs that aid user in accomplishing tasks carried out at computer [10]. These agents can act autonomously and intelligently on behalf of the user. Here, a human appearing and behaving animation agent will notify the user of the foremost information about the system state and give user advice by speech, gesture and action. The speech content together with its priority for relevant

system state is customized with the help of basic configuration assistant of the editor. The state awareness agent will motivate and help the user to recognize the situation of target system easily.

Data/Signal Monitor

The data/signal of the relevant MFM symbol can be selected and monitored with real-time value and curve display. In addition, the color of the curve will be changed according to the corresponding symbol state.

Instruction Display

According to the situation of physical component and system represented by MFM symbol, the instructional information customized by using the editor can be automatically prompted to user. In order to remind the operator to follow the instruction, the un-executed instructions will be marked with a "Un-access" label. After operator executes the instruction, relevant item for it can be selected to erase the "Un-access" label.

Consequence Analyser

The consequence analyser analyses the consequence in MFM model for alarm analysis, fault diagnosis and decision making. The root cause and its consequence route will be revealed to operator to help the operator analyse alarm and diagnose fault.

IV. APPLICATION OF MULTILEVEL FLOW MODELS STUDIO

A MFMS system has been developed by using Visual C++ .NET, DirectX SDK, MSXML Parser SDK and Microsoft Agent SDK. This MFMS has been applied to develop a demo operation support system for a NPP simulated by RELAP5/MOD2. A visual simulation and analysis platform for the NFC System of Japan is also developed by using this MFMS.

In this section, firstly how the MFMS works to construct the MFM model and to implement the human interface application is explained briefly by introducing a process for developing a demo operation support system of a NPP. Then, the work on the visual simulation and analysis platform for the NFC system is briefly explained.

A. Application to a Demo Operation Support System of Nuclear Power Plant

The interface of the editor is shown in Fig. 6. Firstly, by using the structure editor, the structure of MFM model for the NPP simulated by RELAP5/MOD2 is constructed by using the structure editor. Then, basic configuration assistant affiliates relevant signal with the corresponding MFM symbol by loading a text file which stores the name of the signal. Conversion rules between symbol state and signal can be determined by setting the thresholds of signal. In addition, video, audio, picture and their priorities are affiliated with the symbol state in order that they can be automatically activated to the user in terms of the symbol state. In this way, the operation support with multimedia can be easily achieved. Speech content and behavior for state awareness and instruction by an animated interface agent are also configured here. Finally, advanced configuration assistant sets the consequence relation between the symbols for fault diagnosis and alarm analysis of the NPP. In addition, a MFM structure checker automatically checks and displays the mistakes existing in the structure of MFM model.

By using the editor, a MFM model has been established for operation support of NPP, and then the executor can implement the operation support by loading this MFM model. Fig. 7 shows the scene when executor runs as the operation support system for NPP. The model handler & display shows the state of entire system by color and text. The state awareness agent “genie” will aware operator of crucial information about system state and provide advice on operation with variable human-appearance gesture and speech.

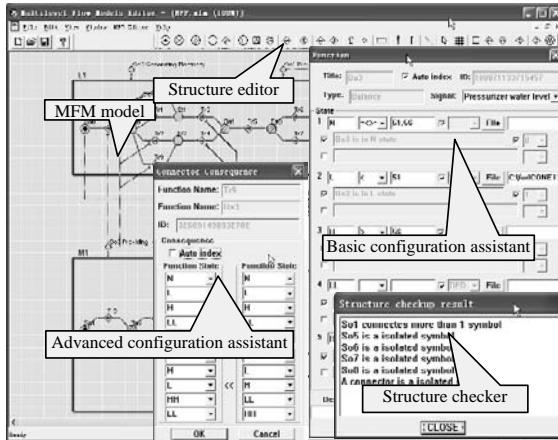


Figure 6. Editor of Prototype MFMS system

Through data/signal monitor, operator can select the signals from the signal list and monitor them with curve or text in real-time mode. The instruction display will instruct the operator for the operation of NPP. The consequence analyser will analyse the consequence existing in the MFM model. Root cause and its consequence route are provided to user for identifying the fault or for analysing the alarm.

B. Application to a Visual Analysis Platform for Nuclear Fuel Cycle

Recently NFC raised social concerns about the issues of economic requirements, environmental appeal and nuclear proliferation. Only under the situation that these conflicting issues reach a consensus among the general public and investor with various background, can nuclear industry become sustainable. By using this MFMS, an analysis platform has been developed in order to help the public and the investor to comprehend various socio-technical issues existing in the NFC system of Japan based on the MFM. Firstly the various flows of mass, energy, information and capital in the NFC system are simulated by using a hierarchy based on MFM. Fig. 8 shows the first level of this MFM model. Then, the NFC system can be analysed visually by exploring the pre-record data, the consequence and multimedia storing in the MFM model. In this way, the visual analysis can be performed from the point of view from economy, society and environment.

V. CONCLUSIONS AND PERSPECTIVES

A graphical interface tool, Multilevel Flow Models Studio, is proposed for the development and maintenance of application for MMI such as operation support, visual analysis, decision-making, etc. In terms of this MFMS, MFM models for different target systems can be constructed, maintained and executed conveniently in order to implement the MMI for different purposes.

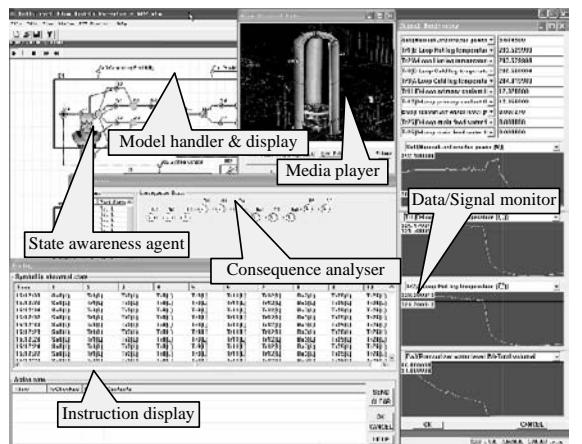


Figure 7. Executor of Prototype MFMS system

In this study, a prototype MFMS system has been developed by using Visual C++ .NET, DirectX SDK, MSXML Parser SDK and Microsoft Agent SDK. A demo operation support system for a Nuclear Power Plant simulated by RELAP5/MOD2 has been developed by using this prototype system. In addition, a visual analysis platform is developed in order that public and investor can comprehend the whole Nuclear Fuel Cycle system more easily.

In the future, the MFMS will be further improved through following several aspects. The conversion relation between signal, data and symbol states will be enriched by taking account into not only the threshold but also more complex equation and logic operation between signal, data and symbol states in order that it can fulfill the complexity of actual situation. In addition, the methodology for consequence analysis among MFM symbols are now been meliorated in order to improve its efficiency and reliability. Furthermore, some other soft computing algorithms, such as Fuzzy Logic, Genetic Algorithms and Neural Network, will be integrated into this MFMS by affiliating some existing software to enhance the reasoning ability of MFMS.

REFERENCES

- [1] M. Lind, "Modeling Goals and Functions of Complex Industrial Plants," *Applied Artificial Intelligence*, Vol.18, No.2, pp.259-283, 1994.
- [2] J.E. Larsson, "Diagnosis Based on Explicit Means-End Models," *Artificial Intelligence*, Vol.80, No.1, 29-93, 1996.
- [3] B. Ohman, "Discrete Sensor Validation with Multilevel Flow Models," *IEEE Intelligent Systems*, Vol.17, No.3, pp.55-61, 2002.
- [4] F. Dahlstrand, "Consequence Analysis Theory for Alarm Analysis," *Knowledge-Based System*, Vol.15, No.1, pp.27-36, 2002.
- [5] J.E. Larsson and B. H. Hayes-Roth, "Guardian: An Intelligent Autonomous Agent for Medical Monitoring and Diagnosis," *IEEE Intelligent Systems*, Vol. 13, No.1, pp.58-64, 1998.
- [6] M.M.V. Passeen and P.A. Wieringa, "Reasoning with Multilevel Flow Models," *Reliability Engineering and System Safety*, Vol.64, pp.151-165, 1999.
- [7] A. Gofuku and Y. Tanaka, "Display of Diagnostic Information from Multiple Viewpoints in an Anomalous Situation of Complex Plants," *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, Vol.5, pp.642-647, Tokyo, Japan, 1999.
- [8] Y. Zhou, H. Yoshikawa, W. Wu, M. Yang and H. Ishii, "Modeling Goals and Function of Micro Gas Turbine System by Multilevel Flow Models," *Trans. of Human Interface Society of Japan*, Vol.6, No.1, pp.59-68, 2004.
- [9] J. Liu, H. Yoshikawa and Y. Zhou, "Study of Visualized Simulation and Analysis of Nuclear Fuel Cycle System Based on Multilevel Flow Model," *Nuclear Science and Techniques*, Vol.16, No.6, pp.358-370, 2005.
- [10] D. Dehn and S. van Mulken, "The Impact of Animated Interface Agents: a Review of Empirical Research," *International Journal of Human-Computer Studies*, Vol.52, No.1, pp.1-22, 2002.

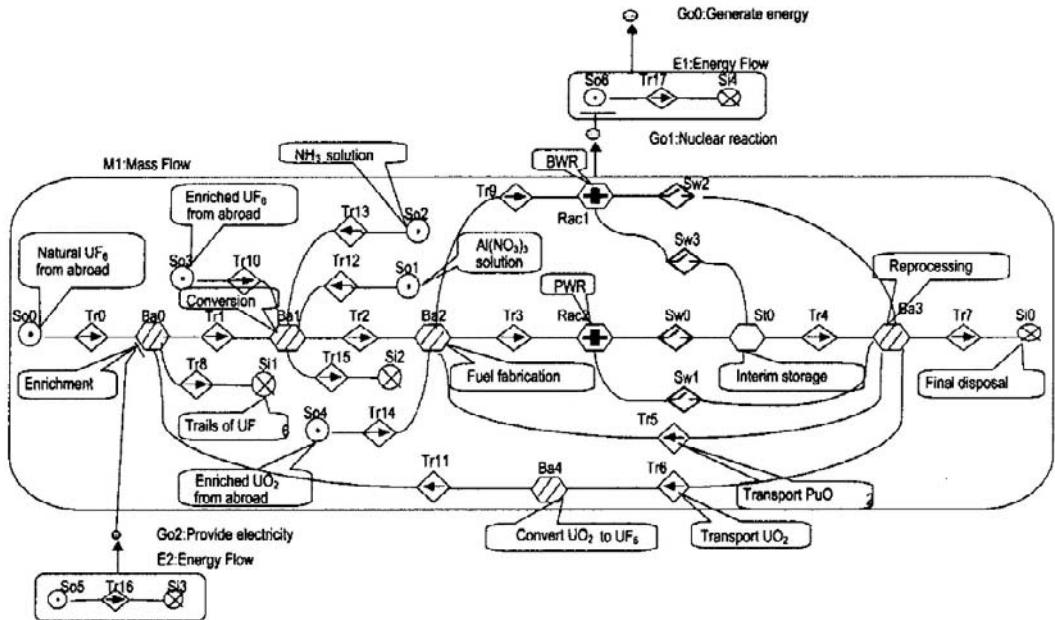


Figure 8. First level of MFM Model for NFC system of Japan

GENETIC ALGORITHM APPROACH IN ADAPTIVE RESOURCE ALLOCATION IN OFDM SYSTEMS

Y. B. Reddy

Dept of math and Computer Science
Grambling State University Grambling, LA 71245
Email: ybreddy@gram.edu

Abstract- Orthogonal Frequency Division Multiplexing (OFDM) is a promising technology for high data rate transmission in wideband wireless systems for achieving high downlink capacities in future cellular systems. In this paper subcarrier and power allocation to each user at base-station is allocated to maximize the user data rates, subject to constraints on total power and bit error rate. First, each sub-channel is assigned to the user with best channel-to-noise ratio for the channel, with random power distributed by water filling algorithm. With the goal of minimize the overall transmit power while ensuring the fulfillment of each user's data rate and bit Error Rate (BER), the needed allocation is proposed through genetic search. The proposed genetic search helps fast convergence and can handle large allocations of subcarriers to users without performance degradation. The simulation results show that genetic algorithm approach will be used where complex computations are involved and near optimal solution are acceptable for optimum resource allocation.

Key words: Genetic Algorithm, fitness, subcarrier, OFDM, frequency, bit error rate

1. INTRODUCTION

OFDM is an alternative wireless modulation technology to CDMA. OFDM transmits digital data efficiently and reliably even in multi-path environments by using a large number of narrow bandwidth carriers. These carriers are regularly spaced in frequency, forming a block of spectrum. The frequency spacing and time synchronization of the carriers is chosen in such a way that the carriers are orthogonal. The name OFDM is derived from the fact that the digital data is sent using many carriers, each of a different frequency (Frequency Division Multiplexing) and these carriers are orthogonal to each other, hence orthogonal Frequency Division Multiplexing.

OFDM is a good contender for the RF (Radio Frequency) interface in 4th generation mobile systems. The multi-carrier nature of OFDM allows the radio channel to be characterized and monitored quickly and easily, presenting numerous opportunities for optimizing the overall system performance, such as:

- minimize Signal to Noise Ratio (SNR) while allocating user subcarriers
- allocate subcarriers to minimize the effects of frequency selective fading
- Dynamically allocate the modulation scheme on an individual subcarrier basis to match the current channel conditions.
- Dynamically change the bandwidth of each user based on the link quality (helps energy spectral density of users with weak bandwidth)

Adaptive modulation is a powerful technique for maximizing the data throughput of subcarriers allocated to a user. Adaptive modulation involves measuring the SNR of each subcarrier in the transmission, then selecting a modulation scheme that will maximize the spectral efficiency, while maintaining an acceptable BER. Adaptive modulation in wireless environment has not been used extensively [10, 22, 28, 29], since the channel response and SNR can change very rapidly, and requires frequent updates to track these changes. Wong [20] investigated the effectiveness of a multiuser OFDM system using an adaptive subcarrier, bit and power allocation and use of adaptive modulation and adaptive user allocation reduced the transmit power by 10 db (ignoring effects of channel tracking errors on the BER performance) [23,27].

Allocating the fixed bandwidth for each user regardless of the received signal power creates problems for those users having low signal strength. The main aim of the adaptive bandwidth allocation is to maintain communications with users that have low received signal strength. This is achieved by reducing their bandwidth to the point where the transmitted power spectral density is high enough to support communications at a low data rate. In order for the adaptive techniques to work effectively all users in the system must be frequency and time synchronized to each other in the reverse link to base station where base station requires complete knowledge of channel response. The following points are used for adaptive bandwidth algorithm [30]:

- Allocate all users an equal number of subcarriers
 - a) Find the mean SNR over entire system bandwidth for each user and allocate subcarriers
 - b) Sort the SNR response that user being allocated and allocate the subcarriers in descending order
- Calculate the SNR of all users and find minimum SNR of the subcarriers allocated to each user (SNR must be greater than threshold)
- Redistribute the free bandwidth to the needed users and redistribute the subcarriers to users if necessary
- Repeat the steps till SNR is above the threshold

Sometimes a best way is to allocate the subcarriers in a round robin fashion, but optimization may be difficult to achieve. When each sub channel is assigned to the user with best subchannel gain and power is distributed by water-filling algorithm then sum capacity can be maximized in adaptive optimization problems [9]. In this adaptive optimization problem, users with lower average channel gains may be unable to receive any data due to priority for users with higher channel gains. But in wireless systems, different users require different data rates

and users must have privilege different levels of services. With the goal of minimize the overall transmit power while ensuring the fulfillment of each user's data rate and bit Error Rate (BER), the needed allocation is proposed through genetic search [19].

2. SYSTEM MODEL

In the adaptive modulation, QAM (Quadrature Amplitude Modulation) schemes with different constellation sizes (M-QAM or Multiple QAM) are provided at the transmitter. For each transmission, the modulation scheme, and possibly also the transmit power, are adjusted to maximize the spectral efficiency, under BER and average power constraints, based on the instantaneous predicted SNR. The basic model for signal passed through AWGN channel is [24, 25]

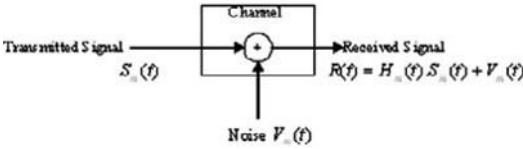


Fig. 1 Basic Model for signal passed through AWGN Channel

Where $H_m(t)$ is the channel frequency response and $V_m(t)$ is an iid (interface identifier sequence) sequence of zero mean Gaussian random variable with variance g_v^2 .

In multi-user OFDM system, after receiving complete channel information, the resource allocation scheme selects different numbers of bits from different users to form OFDM symbol. The joint allocation of subcarriers and power poses heavy computational burden to achieve optimal solution. So, separating subcarrier and power allocation may reduce the complexity, since number of variables reduces almost half. Assume that the subcarrier allocation is performed before power allocation then the optimization problem for efficient resource allocation is [5, 10, 20]:

$$P_{k,n} = \min_{c_{k,n}, \rho_{k,n}} \sum_{n=1}^N \sum_{k=1}^K \frac{f_k(c_{k,n})}{g_{k,n}^2} \times \rho_{k,n} \quad (1)$$

Where

N denotes number of subcarriers
 K denotes number of users

$c_{k,n}$ denote the number of bits assigned to n^{th} subcarrier for the k^{th} user. The parameter $c_{k,n}$ determines the adaptive modulation mode (BPSK, 16 QAM, or 64 QAM) for transmission for each carrier.

$c_{k,n} \in \{0, 1, 2, \dots, M\}$, where M is the maximum number of bits per symbol that can be transmitted by the subcarrier

$g_{k,n}$ denote the channel gains over all N subcarriers for the k^{th} user

$$R_k = \sum_{n=1}^N c_{k,n} \quad \text{for } k = 1, \dots, K \quad (2)$$

is the number of bits that need to be transmitted in an OFDM symbol.

$$\sum_{k=1}^K R_k \leq ND_{\max} \quad \text{for } k = 1, \dots, K \quad (3)$$

D is the set of the positive integers of bits on a subcarrier and D_{\max} is the maximum number bits per subcarrier.

$$\rho_{k,n} = \begin{cases} 1 & \text{if } c_{k,n} \neq 0 \\ 0 & \text{if } c_{k,n} = 0 \end{cases} \quad (4)$$

Variable $\rho_{k,n}$ is either 1 or 0, and the sum of all $\rho_{k,n}$ is equal to 1 for any particular n (subcarrier allocation). This implies that only one user can employ the n^{th} subcarrier.

To solve the above equations (1) – (4) for $c_{k,n}$ and $\rho_{k,n}$ requires many computations. So we can use an integer programming or any special technique like genetic algorithm for optimum search. For Adaptive Subcarrier Allocation (ASA) we use average number of bits per subcarrier and average channel gain allocated to each user. The ASA model consists of initial subcarrier allocation and residual (selected) subcarrier allocation. The average channel gain on the selected subcarrier and pre-selected subcarriers is [10]:

$$G_k^* = (\sum_{n=1}^N \rho_{k,n} g_{k,n}^2 + g_{k,n}^*) / (s_k + 1) \quad (5)$$

where

n^* is the selected channel

$s_k = \sum_{n=1}^N \rho_{k,n}$ is the number of allocated subcarriers for k^{th} user

The fixed average number of bits c_k^* is obtained by

$$c_k^* = \frac{R_k}{s_k^*} \quad (6)$$

s_k^* is the fixed number of subcarriers (initial allocation) obtained by greedy approach [20] for k^{th} user subject to condition in equation (3). Let S^* be the updated allocation of subcarriers and G_k^* be updated channel gain, then change in transmit power is given by

$$\Delta P_k^* = (\frac{s_k}{G_k} - \frac{s_k + 1}{G_k^*}) f_k(c_k^*) \quad (7)$$

and G_k , the average channel gain square of allocated subcarriers for k^{th} user, is given by

$$G_k = \left(\sum_{n=1}^N \rho_k g_{k,n}^2 \right) / s_k$$

Substituting equation (6) in equation (7) we get

$$\Delta P_k^* = \frac{s_k}{G_k} f_k \left(\frac{R_k}{s_k} \right) - \frac{s_k + 1}{G_k^*} f_k \left(\frac{R_k}{s_{k+1}} \right) \quad \dots \quad (8)$$

Calculate the transmit power, update the subcarrier allocation indicator, and average channel gain.

3. GENETIC ALGORITHM FOR ADAPTIVE SUBCARRIER AND BIT ALLOCATION

What are Genetic Algorithms?

Genetic algorithm (GA) is a method for solving both constrained and unconstrained optimization problems that is based on natural selection and natural genetics [7, 12, 11]. The GA repeatedly modifies a population of individual solutions. At each step, the GA selects individuals at random from current population to be parents and uses them produce the children for the next generation. Over successive generations, the population ‘evolves’ toward an optimal solution. The GA can be applied to variety of problems that are not well suited for standard optimization algorithms, including problems in which the objective function is discontinuous, non-differentiable, stochastic, or highly nonlinear. The GA uses following three main rules at each step to create next generation from the current population:

1. **Selection** selects the individual parents that contribute for the next generation
2. **Crossover** combines two parents to form children for the next generation
3. **Mutation** apply random changes to individual parents to form children

In GA, a fitness function is used to represent the objectives of optimization during genetic operations. The parameters or variables to be optimized are individuals in GAs. GAs will evaluate a certain number of individuals in a generation based on the fitness function. Individuals with better fitness survive and those with lower fitness die off, in order to finally locate individuals with the best fitness as the final solution. GAs are capable of locating the global optimum of the fitness function in the specified search domain, provided a sufficient population size and number of generations are given. In some applications local optima as well as global optima are also of interest. The sharing function method is able to locate the multiple local optima as well as the global one(s). The GAs usually contains the following steps:

- Generate initial population
- Calculate fitness for all individuals in the current population
- Perform the operators selection, crossover, and mutation
- Create new population

One of the problems with GA is that GA search process may only produce local optimal solutions instead of the global. This is mainly because the GA generated individuals at later generations may be centered in a local optima and lack diversity

to explore other regions where the global optimal might resides. This problem was solved by mutation probability to generate the new individuals to explore other regions in the search domain.

Genetic Algorithm based Allocation

The optimization problem to be solved by GAs is given in Equation (8). The processing steps in GA based algorithm are as follows:

1. **Generate chromosome of N elements** (*minimum length of chromosome is assumed as 30 thus there are 30 subcarriers*) and total number of chromosomes (population) as 20 for the experiment. Each element in the chromosome is a subcarrier allocated to a user (one user may be allocated more than one subcarrier). Thus the population is a 2-D array, where the rows represent chromosome number and column of a row represents subcarriers.
2. **Evaluate**- use the water-filling method to allocate each user’s bits and subcarrier and calculate the overall transmission power as the fitness of each chromosome. The less the overall power is, the higher the fitness of the chromosome.
3. **Generate** the new population using crossover and mutation (see Appendix A) probability.
4. **Repeat** step 2 and step 3 till the system converges.

In this paper, we calculated each user’s power requirement and the total transmission power required by all users. The subcarriers allocated as per the user’s request arrives. The fitness is equal to the power required for all users or required by all subcarriers allocated to users. The lower the value of power gain $\Delta P_{k,n}^*$ is the higher fitness.

The genetic algorithms had built-in selection of stronger individuals to be the winners from the old generation to new generation. Each chromosome had the format shown in Fig. 2. The value of each element in the array (chromosome) is confined to a user signal and randomly generated. The array represents a solution to the optimization problem.

Chromosome element -1	Chromosome element -2	-----	Chromosome element n
Subcarrier 1	Subcarrier 2	-----	Subcarrier n

Fig. 2 Coding of Genetic Algorithm

For the optimization of our subcarrier and bit allocation problem, the final optimal allocation is sure to have the following features:

- Equation (1) shows that the power gain $p_{k,n}$ can be achieved by channel gain $g_{k,n}$ (larger the channel gain lower the power needed). Therefore, the subscriber with largest channel gain will find the lowest transmission power as in equation (1).
- From equation (3), the number of subcarriers that each user needs according to the rate R_k as given in equation

$$(2) \text{ i.e. } R_k = \sum_{n=1}^N c_{k,n} \text{ for } 1 \leq k \leq K$$

The number of subcarriers that a user k can take is given by m_k :

$$m_k = \frac{N \cdot R_k}{\sum_{k=1}^K R_k} \quad 1 \leq k \leq K \text{ when } \sum_{k=1}^K m_k \leq N$$

Now generate k users so that the total users can take maximum of N subcarriers. Allocate the subcarrier to the user k that has largest channel gain at this subcarrier, i.e. max $g_{k,n}^2$. If total bits allocated for user k is with one subcarrier is c_k , then bits allocated for user k with n subcarriers is $\{n\} \cup c_k$.

We improved the GA processing by the following steps: (1) Add high fitness chromosome at the end of each generation or while forming the new generation. The searching time was reduced by adding the good genes to the population at the end of each generation because it converges quickly. (2) Vary the chromosome size to choose those sizes which result in faster convergence and generate better solution.

4. SIMULATION RESULTS

In this section, we compare the results of the genetic algorithm model with the results of Kim's algorithm [10]. For simulation we initially selected the length of chromosome as 20, population size as 30 and the data rate as 256. The target bit error rate (BER) is set to 10^{-3} . The bit allocation vector can take 0 bits (no modulation), 2 bits (QPSK) and 4 bits (16 QAM) in the present work. The other parameters are as follows:

- Each element of the chromosome represents a subcarrier
- One or more subcarriers are assigned to each user.
- The total transmission power is considered instead of one user's transmission power, so a balance among the users is maintained.
- Subcarriers allocated according to need (in ASA residual or fixed allocation + selected allocation)
- Population: 30
- Generations: 10 to 100
- Crossover: 0.6
- Mutation: 0.03

The subcarrier allocation algorithm was used to calculate the power requirement by many authors [2, 10, 19, 21]. The non-GA application provided in Fig. 3 and Fig. 4 concludes that the cumulative transmit power required linearly increases as the number of subcarriers allocated to the users and is comparable with Kim's results [10] and Ehsan's results [2]. The convergence of transmit power assigned each user does not happen irrespective of channel assignment. In figures, Fig. 5 (non-adaptive allocation) and Fig. 6 (adaptive allocation), a GA implementation with 8 users, 20 channels, and 30 populations, converges within 10 generations particularly in the case of minimum power requirement (blue curve – top most curve of Fig. 5 and Fig. 6). The adaptive application converges much faster

and produces better results compared to Kim's algorithm (see Fig. 4 of Kim) [10] and non-adaptive case of present results (Fig. 5).

5. CONCLUSIONS

The adaptive allocation of subcarrier and power allocation is discussed. The GA model takes flexible number of users and subcarriers (chromosome size). The adaptive allocation of subcarrier and power allocation converges little better than non-adaptive case. The results confirm that GA model performs better than simple adaptive allocation or water-filling algorithm.

ACKNOWLEDGEMENT

The research work was supported by Air Force Research Laboratory/Clarkson Minority "Leaders" Program through contract No: FA8650-05-D-1912. The author is thankful to Dr. Connie Walton-Clement, Dean College of Arts and Sciences for the continuous support.

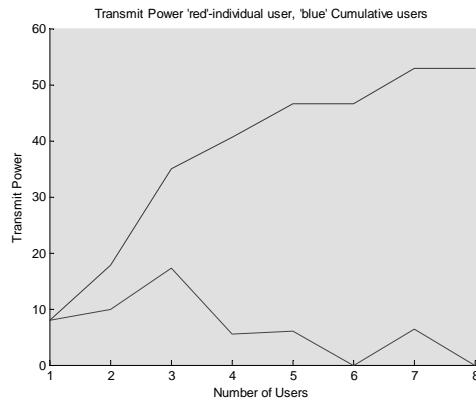


Fig. 3 Transmit Power required by 8 users and 20 channels when channels are assigned as FRFA

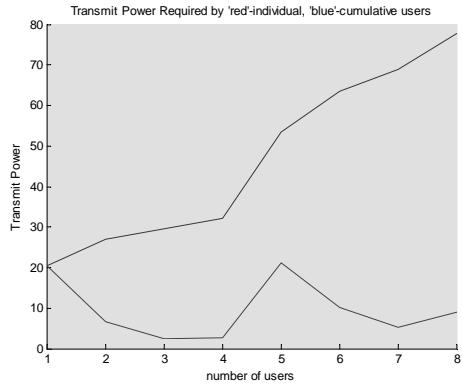


Fig. 4 Transmit Power required by 8 users and 30 channels when channels are assigned as FRFA

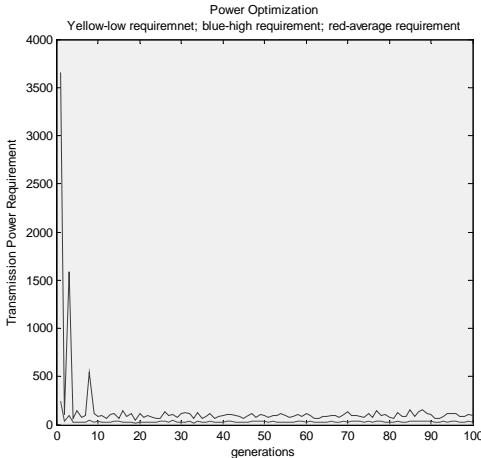


Fig. 5 Optimization of Transmission Power Requirement using Genetic Algorithm (8 users and 20 channels)

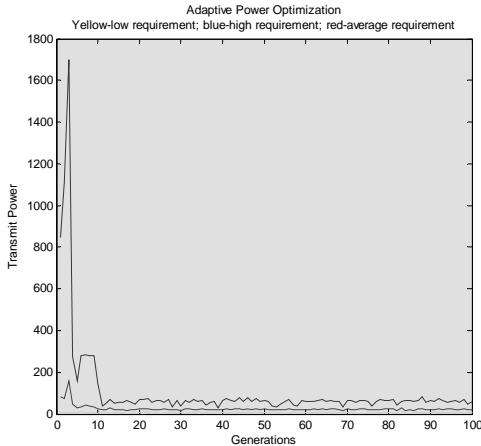


Fig. 6 Optimization of Transmission Power Requirement using Genetic Algorithm (8 users, 20 Channels) adaptive allocation of channels

Appendix A (Genetic Algorithm Terminology)

alleles: The chromosomes are composed of genes, which may be represented by 0 or 1.

crossover: Crossover is a recombinant operator that takes two individuals and cuts their chromosome strings at some randomly-chosen position. This produces two "head" segments and "tail" segments. The tail segments are then swapped over to produce two new full length chromosomes.

xxx xxxx	xxx00000
0000000	000xxxx

The two offspring chromosomes each inherit some genes from each parent. This is *single point crossover*. Crossover is not necessarily applied to all pairs of individuals selected for mating. A choice is made depending on a probability specified by the user and this is typically between 0.6 and 1.0. If the crossover is not applied, the offsprings are simply duplications of the parents.

mutation: Substitute one or more bits of an individual randomly by a new value (0 or 1)

10010010 1001010101

↓
10010010 0001010101

fitness function: A fitness function must be devised for each problem; given a particular chromosome, the fitness function returns a single numerical fitness value, which is proportional to the ability, or utility, of the individual represented by that chromosome.

REFERENCES

- [1] M. Y. Alias, S. Chen, L. Hanzo, "Genetic Algorithm Assisted Minimum Bit Error Rate Multiuser Detection in Multiple Antenna Aided OFDM", Proc of VTC '04, pp 548-552, 2004.
- [2] Ehsan Bakhtiari and Babak H. Khalaj, "A new Joint Power and Subcarrier Allocation Scheme for Multiuser OFDM Systems", 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, Beijing, China, Vol. 2, PP 1959 – 1963, Sept 7 – 10, 2003.
- [3] J. Campello, "Optimal discrete bit loading for multicarrier modulation systems", Proc. IEEE ISIT '98, August 16-21, Boston, USA, 1998.
- [4] Yung-Fang Chen, Jean-Wei Chen, and Chih-Peng Li, "A Real-time Joint Subcarrier, bit and Power allocation Scheme for Multiuser OFDM-based Systems", IEEE VTC'04, 2004.
- [5] Jung Min Chio, Jin Sam Kwak, Ho Seok Kim, and Jae Hong Lee, "Adaptive Subcarrier, Bit, and Power Allocation Algorithm for MIMO-OFDM System", VTC 2004, May 17-19, 2004.
- [6] David A Coley, "An Introduction to Genetic Algorithms for Scientists and Engineers", World Scientific, ISBN: 981-02-3602-6, 2003.
- [7] David E. Goldberg, "Genetic Algorithms in Search, Optimization, and Machine Learning", Addison-Wesley, 1989.
- [8] Jan-Jaap van de Beek, Ove Edfors, Per Ola Borjesson, Mattias Wahlgqvist, and Christer Ostberg, "A conceptual Study of OFDM-based Multiple Access Schemes", Technical Report# 10/0363-5/FCPA 109 0001, August 21 1996.
- [9] Jiho Jang and Kwang Bok Lee, "Transmission Power Adaptation for Multiuser OFDM Systems", IEEE Jan Selected Areas Communications, Vol 21, No. 2, February 2003.
- [10] Ho Seok Kim, Jin Sam Kwak, Jung Min Choi, and Jae Hong Lee, "Efficient Subcarrier and Bit Allocation Algorithm for OFDM System with Adaptive Modulation", IEEE Vehicular Technology Conference, V59, pp 1816-1820, 2004.

- [11] Zbigniew Michalewicz, "Genetic Algorithms + Data Structures = Evolution Programs", 3rd ed, Springer, ISBN: 3-540-60676-9, 1999.
- [12] Melanie Mitchell, "An Introduction to Genetic Algorithms", MIT Press, ISBN: 0-262-13316-4, 1996.
- [13] J. G. Proakis, "Digital Communications", 4th ed. New York, McGraw-Hill, 2000.
- [14] H. Rohling, K. Bruninghaus, and R. Grunheid, "Comparison of multiple access schemes for an OFDM downlink system," Multi-Carrier Spread Spectrum, K. Fazel and G. Fettweis, eds. Norwell, MA: Kluwer, pp 23-30, 1997.
- [15] William Stallings, "Communications and Networks", Prentice Hall, ISBN: 0-13-040864-6, 2002.
- [16] Tom M. Mitchell, "Machine Learning", McGraw Hill, 1997, ISBN: 0-07-042807-7.
- [17] M. Wahlqvist et al., "Capacity comparison of an OFDM based multiple access system using different dynamic resource allocation", Proc Vehicular Technology Conf., vol 3, pp 1664-1668, 1997.
- [18] Lan Wang and Zhisheng NIU, "An Efficient Rate and Power Allocation Algorithm for Multiuser OFDM Systems", IEICE Trans. Commun., Vol. E88-B, No.12 December 2005.
- [19] Yongxue Wang, Fangjiong Chen, and Gang Wei, "Adaptive Subcarrier and Bit Allocation for Multiuser OFDM System Based on Genetic Algorithm", IEEE 2005.
- [20] Cheong Yui Wong, Roger S. Cheng, "Multiuser OFDM with adaptive Subcarrier, bit and power Allocation", IEEE JSAC, Vol. 17, No. 10, pp 1747-1758, Oct 1999.
- [21] Cheong Yui Wong, C. Y. Tsui, Roger S. Cheng, and K. B. Letaief, "A Real-time Subcarrier Allocation Scheme for Multiple Access Downlink OFDM Transmission", 1999 IEEE International Conference on Vehicular Technology, VTC'99-FALL, Amsterdam, The Netherlands, Sept. 1999.
- [22] Cheong Yui Wong, Roger S. Cheng, K. B. Letaief, Ross D. Murch, "Multiuser Subcarrier Allocation for OFDM Transmission using Adaptive Modulation", 1999 IEEE International Conference on Vehicular Technology, VTC'99-SPRING, pp. 290-294, Houston, TX, May 1999.
- [23] Guodong Zhang, "Subcarrier and Bit Allocation for Real-time Services in Multiuser OFDM Systems", IEEE International Conference on Communications, Paris, France, Vol. 5, pp 2985-2989, June 20-24, 2004.
- [24] X. Gao and M. Naraghi-Pour, "Computationally Efficient Resource Allocation for Multiuser OFDM Systems", Proceedings of the IEEE Wireless Communication and Networking Conference, (WCNC2006), April 3-6, 2006, Las vegas, NV.
- [25] John G. Proakis, "Digital Communications", 4th ed, McGraw Hill, 2001.
- [26] W. Rhee and J. M. Cioffi, "Increasing in Capacity of Multiuser OFDM System Using Dynamic Subchannel Allocation," Proc. IEEE Int. VTC, vol. 2, pp 1085-1089, 2000.
- [27] Z. Shen, J.G. Andrews, and B.L.Evans, " Optimal Power Allocation in Multiuser OFDM Systems", Proc. IEEE Asilomar Conf. on Signals, Systems, and Computers, Vol.1, pp 1147-1151, 2003.
- [28] S. Falahati, A. Svensson, T. Ekman, and M. Sternad, "Adaptive Modulation Systems for Predicted Wireless Channels", IEEE Trans. on Communications, vol. 52, No. 2, 2004.
- [29] C. Tang and V. J. Stolpman, "Multiple Users Adaptive Modulation Schemes for MC-CDMA", Nokia, 7th August 2004.
- [30] E. P. Lawrey, "Adaptive Techniques for Multiuser OFDM", Thesis, James Cook University, 2001.

Real-time Vehicle Detection with the Same Algorithm both Day and Night Using the Shadows Underneath Vehicles

Yoichiro Iwasaki and Hisato Itoyama

Department of Information Engineering, Graduate School of Engineering, Kyushu Tokai University
9-1-1, Toroku, Kumamoto 862-8652, Japan

Abstract- We propose a vehicle detection method for traffic flow images obtained from a video camera set up on a low place such as the roadside, or the sidewalk. The method uses the shadows underneath vehicles as the means of detecting them. The method distinguishes the size of each vehicle according to the distance between the front- and rear-tires, and also the lanes on which vehicles exist. The method has the advantage of creating and updating automatically a background image, and of estimating and updating automatically a threshold value to binarize background subtraction images in order to enhance the vehicle detection accuracy. As a result, vehicle detection can be achieved by the same algorithm both day and night. The proposed algorithm can realize a high-speed processing without complicated calculations, and a real-time vehicle detection by using a general-purpose personal computer. Experimental results by use of traffic images in fine, cloudy, rainy weather, and at night show that the vehicle detection accuracy is 94.9%.

I. INTRODUCTION

In vision-based traffic monitoring, it is desirable to set up a camera on a high place in order to secure a wide measurement area, and to prevent the overlapping of vehicles. In many cases of the previous studies for vision-based traffic monitoring, images obtained from a camera set up on a high place are used [1][2][3]. However, the location of traffic monitoring is restricted if we use the high places such as buildings, or pedestrian bridges. The construction of a pole is needed for setting up a camera if such a high place does not exist near the measurement area.

This paper proposes a real-time vehicle detection method for traffic flow images obtained from a video camera set up on a low place such as the roadside, or the sidewalk. By using the proposed method, a measurement area can be selected more freely, and traffic flow data such as traffic volumes, space headways, etc. can be collected more easily.

In vehicle detection, various algorithms have been proposed. Some of them are shown below.

Cucchiara *et al.* [1] used spatio-temporal analysis in daytime images, and morphological analysis of headlight pairs in night images. Yoneyama *et al.* [2] proposed a method of eliminating moving cast shadows for robust vehicle extraction.

The method proposed by Uchimura *et al.* [3] was based on edge detection and template matching. A vehicle detection method based on edge detection in a tunnel was proposed by Kuboyama *et al.* [4]. The method proposed by Kate *et al.* [5] was intended for image data from a single camera placed in a moving vehicle, and a combination of three clues were used: shadow, entropy, and horizontal symmetry. Vehicle detection methods which aim at vehicular side views were fewer. For example, Imai *et al.* [6] used minutia matching to detect vehicular side views, and the method proposed by Nakanishi *et al.* [7] was based on spatio-temporal image analysis.

The proposed method uses only the shadows underneath vehicles as the means of detecting them, and of discriminating the lanes on which they exist. The shadows underneath vehicles exist not only in fine weather but also in other weather conditions since the bottom of a vehicle is extremely close to the surface of a road. Our observations confirmed that the shadows underneath vehicles exist even in cloudy, rainy weather, at twilight, and night illuminated by streetlights.

The proposed algorithm offers a high-speed processing without complicated calculations compared with other vehicle detection methods shown above, and a real-time vehicle detection by using a general-purpose personal computer.

Yoneyama *et al.* [8] pointed out that most daytime detection methods lose their accuracy when directly applied to nighttime detection. However, the proposed method can achieve vehicle detection both day and night by the same algorithm with a high accuracy.

II. PROPOSED VEHICLE DETECTION ALGORITHM

A. Detecting Locations of Vehicles and Discriminating their Sizes

An input image is a gray scale image, the size of the image is 640x480 pixels, and a pixel has 256 gray levels. The height of the installation of a video camera is about 1.7m, and the measurement is done at a general street of multilane.

A background subtraction is done by (1), the obtained background subtraction image is binarized, and the binary image in which only vehicles and their shadows exist is obtained. In the binarization, the regions of vehicles and their shadows are converted to white pixels, and the background

regions are converted to black ones. To prevent detecting the white line on the road because the camera moves slightly, erosion and dilation are done for the binary image.

$$f_{\text{sub}}(i, j, t) = \begin{cases} g(i, j, t-T) - f(i, j, t) : g(i, j, t-T) - f(i, j, t) > 0 \\ 0 : \text{otherwise} \end{cases} \quad (1)$$

where i and j are x and y coordinates, t is time, T is the time interval of the input images, $f_{\text{sub}}(i, j, t)$ is the background subtraction image, $g(i, j, t-T)$ is the previous background image with the time interval T which contains no vehicle, $f(i, j, t)$ is the input image.

We will discuss later a method of creating and updating a background image, and a method of estimating and updating a threshold value to binarize images in Sections B and C, respectively.

A vertical projection is done by searching white pixels along the vertical columns in the binary image. If there is one white

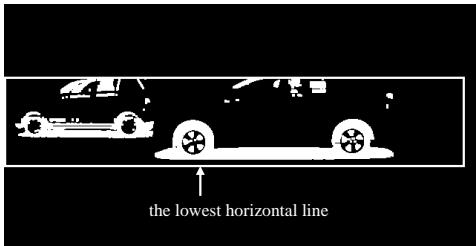


Fig. 1. The measurement area and the lowest horizontal line.

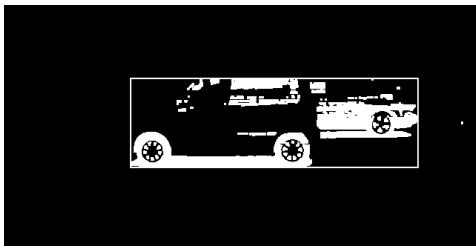


Fig. 2. The region of vehicles and their shadows.

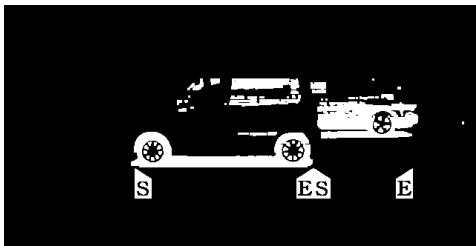


Fig. 3. Left and right edges of shadows.

pixel at least in a vertical column, the black pixel at the same row on the lowest horizontal line in the measurement area is changed into white. The white box in Fig. 1 shows the measurement area. Although the lowest horizontal line in Fig. 1 is drawn in white, the white pixels do not exist in the actual images. If eight pixels or more are white in fifteen continuous pixels on the lowest horizontal line, corresponding fifteen continuous pixels are connected. Fig. 2 shows a result of the vertical projection. The location and width of the lower horizontal line in the rectangle in Fig. 2 is obtained by the processing described above. The height of the rectangle is decided from the height of the measurement area. By this processing, the vehicle and shadow regions are grasped roughly.

Next, the connected components of the shadows underneath the vehicles on/over the lower horizontal line of a rectangle are searched. The shadow region underneath each vehicle is distinguished by the difference between the vertical positions of shadows, and each pair of left and right edges of the shadow is identified. Fig. 3 shows a result of identifying left and right edges of the shadows. The "S" and "E" in Fig. 3 indicate the left and right edges, respectively. Moreover, a horizontal projection for the rectangle region just over each shadow is done by summing up the number of black pixels along the horizontal rows. Each boundary position between a vehicle and the shadow underneath the vehicle can be identified from the horizontal projection result because the frequency of the black pixels increases extremely at the boundary position. Fig. 4 shows a distribution of black pixels, and the arrow shows the boundary position.

A tire, which touches a road, is black, and the gray-level values of the tire and those of the shadow underneath the vehicle are very similar. The regions of tires become the white pixels that are the same as the regions of shadows when a binary image is created. Therefore, the region of the shadow and the tires of the vehicle can be scanned as one connected component, and then the positions of the tires can be identified. As a result, the length of a wheelbase plus a wheel diameter can be obtained, and the length is used as the information to distinguish the size of each vehicle. Fig. 5 shows a detection result. In Fig. 5, the sideways arrow shows the boundary

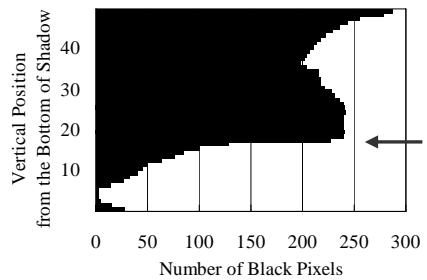


Fig. 4. A distribution of black pixels.

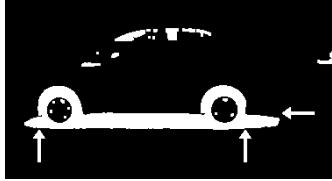


Fig. 5. The positions of tires and the boundary between the vehicle and its shadow.

position, and the two upward arrows show the both edges of front- and rear-tires.

There is a difference in the vertical position of each lane in the images of vehicular side views. Therefore, if the vertical positions of the vehicles can be measured, the lanes on which vehicles exist are specified. The proposed algorithm discriminates the lanes on which vehicles exist from the measured boundary positions.

Even if the positions of front- and rear-tires cannot be obtained, the vehicle location can be detected from the location of the shadow underneath the vehicle.

B. Creating and Updating a Background Image

Since gray-level values in the background region change from time to time due to environmental factors, it is important to update the background image in a short time interval in order to enhance the vehicle detection accuracy.

An initial background image is created in advance by use of a background image renewal processing method proposed in [9] from 30 continuous image frames. In the process of creating the initial background image, moving objects are eliminated automatically.

First, we will explain the background image renewal processing method by using (2), (3), and Fig. 6, which are proposed in [9].

$$h(i, j, t) = f(i, j, t) - g(i, j, t - T) \quad (2)$$

$$g(i, j, t) = g(i, j, t - T) + \text{Table}\{h(i, j, t)\} \quad (3)$$

where $\text{Table}\{h(i, j, t)\}$ is the response function shown in Fig. 6.

If $h(i, j, t)$ is within the range from $-H$ to H , the pixel position is assumed to be in the background region, then the gray-level value at the position in the previous background image is updated rapidly by use of $\text{Table}\{h(i, j, t)\}$. On the other hand, when $h(i, j, t)$ is under $-H$ or over H , the gray-level value is also changed and updated in a long period of time. Therefore, the response function is effective for the change of gray-level values not only due to environmental factors but also due to the noises, garbage on the road, the movement of a camera, etc. which are not caused by the environmental factors. The speed of these updates depends on the shape of the response function in Fig. 6. The method proposed in [9] takes

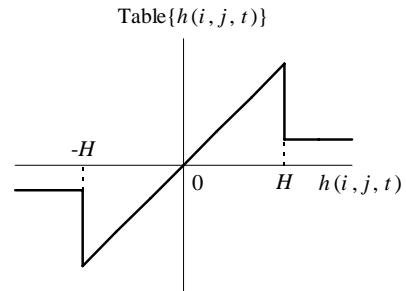


Fig. 6. The response function proposed in [9].

the stopped vehicles into the background region in a long time. Therefore, the stopped vehicles cannot be detected. So we propose a method of adding a new algorithm to the method in [9]. Next, we will explain the new algorithm.

The measurement area is divided into 45x15 blocks shown in Fig. 7. The mean and the variance of gray-level values in each block in a background absolute subtraction image given by (4) are calculated.

$$f_{\text{abs_sub}}(i, j, t) = |f(i, j, t) - g(i, j, t)|, \quad (4)$$

where $f_{\text{abs_sub}}(i, j, t)$ is the background absolute subtraction image.

In this process, absolute values are adapted as the background subtraction factor in contrast with (1). If the mean or the variance is greater or equal to the threshold values, it is assumed that there is an object like a vehicle, then the block is not updated. By only the variation of gray-level values in a very small area such as a pixel, the existence of a vehicle cannot be judged. By comparing the information obtained from many pixels in a block, the existence of a vehicle can be identified. Fig. 8 shows that there are extreme differences in the means and the variances of gray-level values between the blocks in which an object like a vehicle exists and the blocks in which no object exists. Therefore, it is easy to determine the threshold values.

In addition, when a block is not updated continuously over 30 frames in the past, the surrounding eight blocks are examined. If the seven or more blocks of the surrounding eight blocks are updated, it is assumed that the judgment of not updating is wrong, then the block is updated immediately. Because the outermost blocks in the measurement area do not have the surrounding eight blocks, it is assumed that the insufficient blocks are updated continuously. Fig. 9 shows an example of updating a background image using proposed algorithm. Fig. 9 shows that the blocks of the vehicles and their shadows are not updated, and the gray and white blocks are updated. At night, the blocks which contain the reflection of headlights are not updated either. The white is a block for

which the update is begun because the miss judgment turned out.

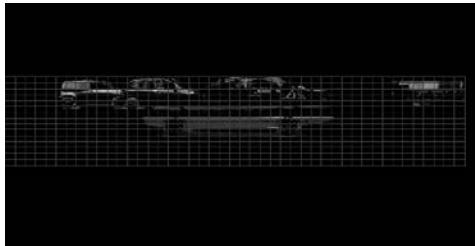


Fig. 7. The division of the measurement area into 45x15 blocks.

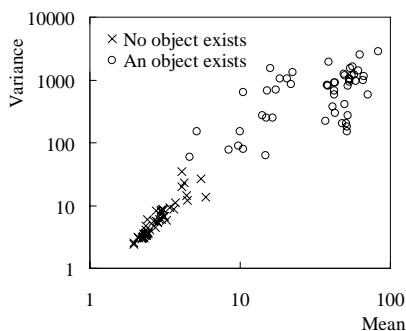


Fig. 8. Means and variances of gray-level values in blocks.



Fig. 9. Updating a background image.

We have experimented with the numbers of divisions: 20x5, 30x10, 40x15, 45x15, and 50x20. As a result, the update accuracy was the highest at 45x15 blocks in the five kinds.

The proposed algorithm on updating a background image can reduce the influences of environmental factors, noises, garbage on the road, the movement of a camera, etc.

C. Estimating and Updating a Threshold Value to Binarize Images

To determine the threshold value to binarize the background subtraction images obtained by (1), we use discriminant analysis method [10]. To apply this thresholding method when several vehicles exist in the measurement area, the information on the blocks in updated background images is used. The number of the blocks which are not updated is counted. As a result, the threshold value is determined and updated when it is judged that there are several vehicles in the measurement area.

The update of the threshold value is executed with 100 frames interval at least. If vehicles do not exist in the measurement area when updating the threshold value, the update is skipped to the frame which contains vehicles in the measurement area. When a rapid change of the threshold value is caused by the mischoice of the image, the update of the threshold value is put off till the next update.

It is confirmed that this thresholding method can be applied without initialization to traffic images in fine, cloudy, rainy weather, and at night.

III. EXPERIMENTAL RESULTS

We have evaluated the validity of the proposed method by using traffic flow images in fine, cloudy, rainy weather, and at night captured from a camera position on the National Root 57 in Kumamoto City, Japan.

Table 1 shows the results of vehicle detection. The vehicles whose shadows cannot be seen behind other vehicles are not included in Table 1.

Fig. 10 shows some results of vehicle detection. The white boxes in Fig. 10 show the vehicles whose front- and rear-tires are detected, and the black boxes show the vehicles detected

TABLE 1
RESULTS OF VEHICLE DETECTION

Conditions	Number of frames	Number of the frames which contain vehicles	Number of vehicles	Detected vehicles (Accuracy)	Mis detection	Overdetection
Fine weather	2000	600	733	733 (100%)	0	0
Cloudy weather	2000	821	965	965 (100%)	0	0
Rain	2000	832	945	838 (88.7%)	107	49
Night	2000	680	720	654 (90.8%)	66	7
Total	8000	2933	3363	3190 (94.9%)	173	56

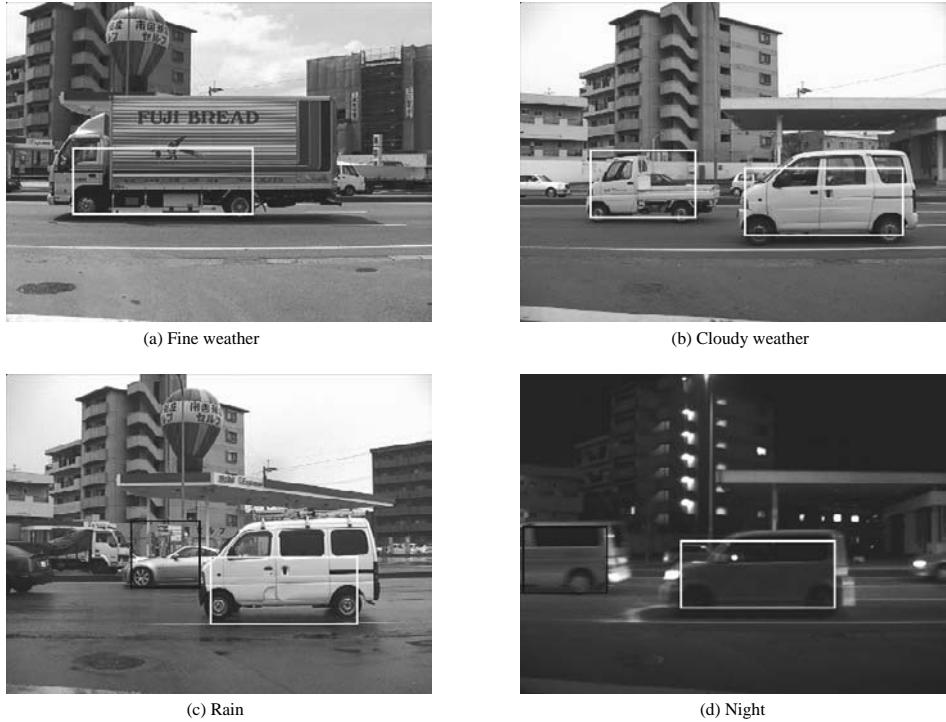


Fig. 10. Some results of vehicle detection.

from the location of their shadows because both positions of tires cannot be measured.

The personal computer used in the experiments has a Pentium IV 3.73GHz CPU, a video capture board, and a 2GB RAM. The system is developed by Visual C++ under Windows XP. Vehicle detection is achieved more than nine frames per second even for heavy traffic scenes.

IV. CONCLUSIONS

We proposed a real-time vehicle detection method that uses the shadows underneath vehicles as the means of detecting them. The method distinguishes the size of each vehicle according to the distance between the front- and rear-tires, and also the lanes on which vehicles exist. The method uses a new algorithm for automatic renewal of the background image, and has the advantage of estimating and updating the threshold value to binarize image in order to enhance the vehicle detection accuracy. As a result, the proposed method can achieve a vehicle detection in fine, cloudy, rainy weather, and at night by the same algorithm with a high accuracy.

In the traffic monitoring which aims at vehicular side views, we confirmed that the shadows underneath vehicles can be

used as the object of a reliable vehicle detection.

REFERENCES

- [1] R. Cucchiara, M. Piccardi, and P. Mello, "Image Analysis and Rule-based Reasoning for a Traffic Monitoring System," *Proc. IEEE/IEE/JSAI Int. Conf. Intelligent Transportation Systems*, pp.758-763, October 1999.
- [2] A. Yoneyama, C. H. Yeh, and C. -C. J. Kuo, "Moving Cast Shadow Elimination for Robust Vehicle Extraction based on 2D Joint Vehicle/Shadow Models," *Proc. IEEE Conf. Advanced Video and Signal Based Surveillance*, pp. 229-236, July 2003.
- [3] K. Uchimura, and K. Matsushima, "Traffic Flow Measurement Considering Occlusion," *Trans. IEE Japan*, vol. 122-C, no. 12, pp. 2120-2127, December 2002 (in Japanese).
- [4] H. Kuboyama, and S. Ozawa, "Measurement of Heavy Traffic in a Tunnel from Image Sequences," *IEICE Trans.*, vol. J85-D-II, no.2, pp. 210-218, February 2002 (in Japanese).
- [5] T. K. ten Kate, M. B. van Leeuwen, S. E. Moro-Ellenberger, B. J. F. Driessens, A. H. G. Versluis, and F. C. A. Groen, "Mid-range and Distant Vehicle Detection with a Mobile Camera," *Proc. 2004 IEEE Intelligent Vehicles Symposium*, pp. 72-77, June 2004.
- [6] S. Imai, Y. Imai, and M. Iwashashi, "Traffic Monitoring System based on Minutia Matching," *Proc. 2005 IEICE General Conf.*, AS-2-2, March 2005 (in Japanese).
- [7] T. Nakanishi, A. Shio, and K. Ishii, "Automatic Vehicle Image Extraction Based on Spatio-Temporal Image Analysis," *IEICE Trans.*, vol. J77-D-II, no.9, pp.1716-1726, September 1994 (in Japanese).

- [8] A. Yoneyama, C. -H. Yeh, and C. -C. J. Kuo, "Robust Vehicle and Traffic Information Extraction for Highway Surveillance," *EURASIP Journal on Applied Signal Processing*, vol. 2005, issue 14, pp. 2305-2321, 2005.
- [9] T. Tanizaki, K. Ueda, K. Ikegaya, and I. Horiba, "A Detection of Wet Condition on Road Using a Background Image Renewal Processing," *IEICE Trans.*, vol. J80-D-II, no.9, pp. 2270-2277, September 1997 (in Japanese).
- [10] N. Otsu, "An Automatic Threshold Selection Method Based on Discriminant and Least Squares Criteria," *IECE Trans.*, vol. J63-D, no. 4, April 1980 (in Japanese).

An Authentication Protocol to Address the Problem of the Trusted 3rd Party Authentication Protocols

Y. Kirsal and O. Gemikonakli

Middlesex University

The Burroughs, Hendon

London, NW4 4BT, UK

Abstract- The development of authentication protocols to secure networks, data and resources is one of the main interests in ensuring secure communication in modern world. Kerberos is a widely used computer network authentication protocol which allows individuals communicating over an insecure network to prove their identity to one another in a secure manner. This paper presents a general approach for the analysis and verification of authentication properties in Kerberos. The work presented is an attempt to combine Kerberos and Key-Exchange Protocol with the aid of the security protocol compiler, CASPER and the Failures-Divergence Refinement (FDR) in order to minimize the success of attacks against protocol's authentication. FDR is used to generate Communicating Sequential Processes (CSP) definition of the protocol. An authentication protocol has been developed to improve secure authentication in Kerberos.

I. INTRODUCTION

The use of networked computer systems is increasing rapidly. This makes users aware of the need to protect their data, systems and resources from network based attacks, and unauthorised access, and to ensure reliable, secure communications, privacy and data integrity. Authentication, which is the reliable means of identity verification, is largely thought of as a means of preventing unauthorised access or malicious penetration to systems and networks. In other words, authentication and access control paradigms play vital roles towards attack prevention [1].

Kerberos is a commonly used mechanism for authentication purposes. Kerberos utilises symmetric cryptography as well as public key cryptography, to provide authentication for client-server applications. Its implementations allow the introduction of additional algorithms for encryption and check summing. The core of Kerberos architecture is the Key Distribution Centre (KDC). The KDC stores authentication information and uses it to securely authenticate users and services. The KDC acts as a trusted third party in performing these authentication services. Due to the critical function of the KDC, multiple KDCs are normally utilized. Each KDC stores a database of users, servers, and secret keys. However, since the KDCs store secret keys for every user and server on a network, it is essential to do this with maximum security. If an attacker can gain administrative access to the KDC, he would have access to the complete resources of the Kerberos realm. Kerberos tickets are cached on the client systems. If an attacker gains administrative access to a Kerberos client system, he can impersonate the authenticated users of that system. In other

words, the authentication service communicates with the Ticket Granting Service (TGS) and then authenticates the client with a ticket. The TGS receives the ticket from the client and checks its validity and replies to the client with a new ticket. Client can use this ticket to request services. Since the TGS is not authenticated (i.e. it is assumed that it is trusted), a masquerading TGS (any client) can impersonate the TGS of the network.

In addition to these, Kerberos exhibits some other vulnerabilities widely reported in literature. Some of these vulnerabilities include among others those known as aided attacks such as replay of old messages, password guessing, SSID sniffing, jamming, masquerading injection, cracking and rogue points or access points, denial of service attacks and session hijacking [2]. There are remarkable efforts to enhance the security capability of this popular authentication mechanism, Kerberos. These efforts are of two categories; public key assistance and the addition of a proxy server [5].

The CSP is an abstract language designed specially for the description of communication patterns of concurrent system components that interact through message passing. The aim of the CSP approach is to reduce questions about security protocols and their properties and ensure that CSP processes satisfy particular specifications [11]. This approach forces the separation of properties and protocols and allows discussion of what is meant by particular kinds of security properties, independent of the protocols that are intended to achieve them. In other words, CSP is particularly suitable for describing protocols close to the level we think of them. Schneider states that formalisation of the protocol into CSP exhibits issues and forces design decisions that may not have been distinctly stated in the original protocol description [11].

FDR is a model-checking tool for state machines, with foundations in the theory of concurrency based around CSP. Its method of establishing whether a property holds is to test for the refinement of a transition system. This is done by capturing the property in question by the candidate machine. There is also the ability to check determinism of a state machine, and this is used primarily for checking security properties [3].

Lowe states that, firstly, each agent in a protocol is modelled as a CSP process, the most general intruder who can interact with the protocol is also modelled as a CSP process and finally, FDR returns a trace if it finds that protocol specification is not met, which means that the trace is an attack upon the protocol [4]. As explained above this method has proved success in

finding attacks upon a number of protocols, however, producing the CSP description of a system needs time and substantial experience in order to avoid mistakes.

To address these concerns, CASPER has been developed [4]. CASPER is a program that automatically produces a CSP description from a more abstract description, thus simplifying the modelling and analysis process. A CASPER script could be divided into two parts: a general part that specifies a model of a system running the protocol, and a specific part that defines given functions, the parameters of the protocol.

Kerberos Authentication Protocol was simplified and tried as an example by Lowe and failed because of replay attacks. In addition to this, Key-Exchange Protocol is also tried, however, unlike Kerberos example it succeeded.

This paper presents the initial steps in developing a specific authentication protocol that has properties of Kerberos and Key Exchange and provides authentication of servers based on a previously proposed framework [10]. This framework proposes a security solution to be employed in wireless LANs; an area where the need for high security requirements is beyond doubt. This framework relies on the provisions of IEEE 802.1x standard. It also uses similar infrastructure components as Kerberos but significantly provides for authentication of servers. Throughout this work, CASPER and FDR are used in protocol development and testing.

II. RELATED WORK

In order to address users' demands for higher security, scientists and engineers have developed various specifications regarding security protocols and built many security protocols around these specifications. Lowe points out that, most of these protocols agreed upon a cryptographic key or achieved authentication specifications [7]. Abadi and Needham have expressed a similar view [1]. Their study indicates that cryptographic protocols are prone to various types of attacks.

Kerberos is based on Needham-Schroeder Authentication Protocol [8]. It uses key distribution, that is to say, clients and servers use digital tickets to identify themselves to the network and secret cryptographic keys for secure communications.

Kerberos is now in its fifth release, version 5, an improvement of version 4. Though, version 4 is still in commercial implementation, it exhibited vulnerabilities such as reliance on symmetric encryption, dependence on IP addresses, and others that were attributable to the Athena environment. The success of password guessing and replay attacks against Kerberos and weaknesses as a result of Kerberos' requirement of a trusted path have been clearly identified as limitations of Kerberos [2].

Horbitter and Menascé have drawn attention to the performance evaluation of the Kerberos Security Protocol in two different achievements [5].

Nevertheless, as a result, it is possible to say, although some additional public-key infrastructures have been added to various stages of Kerberos, in terms of server and network capacity, they are suitable for simpler networks and could not work with more than one application server. A proxy server is used to increase encryption process for both client and server;

however it produces delays during the transactions of authentication messages between client and server. Recent increases in the speed of wireless networks outperformed proxy servers, leading to insufficient services which resulted in increased response times.

Beside these, Kerberos' operation is system and application independent. Kerberos provides a mutual authentication between a client and a server. The Kerberos protocol assumes that initial transactions take place on an open network where clients and servers may not be physically secure and packets travelling on the network can be monitored and even possibly modified. Kerberos is independent of the security features defined in IEEE 802.11.

The framework's three entities (supplicant, authenticator, authentication server) mutually authenticate each other prior to data traffic [10]. It was built on the assumption that none of the parties should be trusted in a wireless local area network communication environment.

The Kerberos KDC software runs on secure hardware. It is assumed that, a roaming user wishes to access an application running on a server somewhere in the network. The user first establishes a secure connection with the Kerberos KDC. After exchanging authentication information, the user, if authorized, gets a "ticket" from TGS which grants access to the desired application. However, if the TGS is not authenticated, i.e. it is assumed that it is trusted; a masquerading TGS can impersonate the TGS of the network. In order to prevent ticket hijacking, Kerberos KDC must be able to verify that the user presenting the ticket is the same user to whom the ticket was issued. This is shown in the Fig.1.

In order to model protocols, the participants in the protocols are modelled as well [11, 13]. In a simple protocol, it is assumed that there are two communicating principals, A and B and an adversary who is the attacker. In [11], the attacker is modelled as having capacity to intercept messages in all directions, modify messages, inject new messages and transmit messages. As Eneh and Gemikonakli [13] point out, to present the model of the attacker in CSP, initial steps involve determining the extent of information that could be available to an attacker with aforementioned potentials.

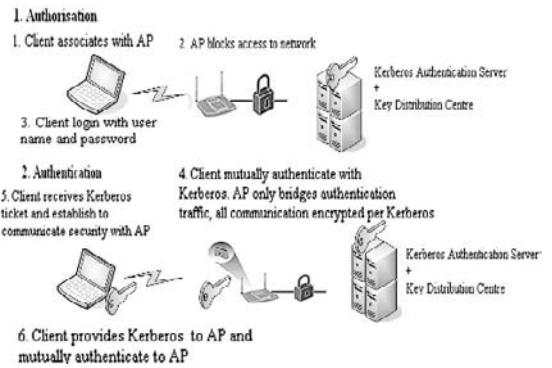


Fig.1. Kerberos in action in a wireless network

The attacker on network is represented as follows [11]:

- a) with unknown number of clients:
 $\text{NET} = (\| \text{j } \text{USER } \text{USER}_j) \mid [\text{trans}, \text{rec}] \mid \text{ATTACKER}$
- b) with only two participants (client/agent):
 $\text{NET} = (\text{USER}_A \parallel \text{USER}_B) \mid [\text{trans}, \text{rec}] \mid \text{ATTACKER}$

Also, in [11], valid theorems are presented and the description of the attacker is given as follows:

$$\text{ATTACKER sat } (\text{INIT} \cup (\text{tr} \Downarrow \text{trans})) \vdash \text{tr} \Downarrow \text{rec}$$

This theorem is used here to explain that the sets of all the messages that pass through the rec channel are a function of the initial knowledge of the attacker and the sets of the messages input on the trans channel. Additionally, the description of the attacker is represented as follows in [11]:

$$\text{ATTACKER(S)} = \text{trans? i?j?m} \rightarrow$$

$$\text{ATTACKER(S U \{m\})}$$

$$\square \quad i, j \in \text{USER}, S \not\models m \text{ rec.i!j!m} \rightarrow \text{ATTACKER(S)}$$

Apart from the above CSP codes, Lowe gives the syntax for CASPER scripts [4]. The two parts of CASPER are further split into four sections each:

```

script ::= free-vars-section processes-section
          prot-desc-section spec-section
          act-var-section [functions-section]
          system-section intruder-section
    
```

Each section of the CASPER script has different tasks. "#Free variables" section declares the type of the free variables and functions used in the definition of the protocol. "#Processes" section declares the agents taking part in the protocol and gives information about their state. "#Protocol description" section defines protocol itself, by giving the messages that run the protocol. "#Specification" section shows the requirements of the protocol. "#Actual variable" section declares the datatypes used in the system to be checked with FDR. "#Functions" section gives definitions for the functions used in the protocol. "#System" section defines the system, in terms of the number and types of agents, and finally "#Intruder" section gives the identity and initial knowledge of the intruder.

III. WORK IN PROGRESS

Despite the multiplicity of authentication approaches and proposals for improving security of networks, threats of penetration and other forms of attacks have continued to evolve, increasing in number and complexity.

The proposed framework [10] provides a background for the design of security solutions for wireless local area networks that require high level of security. The requirement for network security is consistent with permitting authorised access to information and services, while preventing unauthorised users from gaining access to and corrupting the network. Since the Kerberos Authentication Protocol is a trusted third party authentication protocol, its paradigms and entities are finalised for the proposed framework [10].

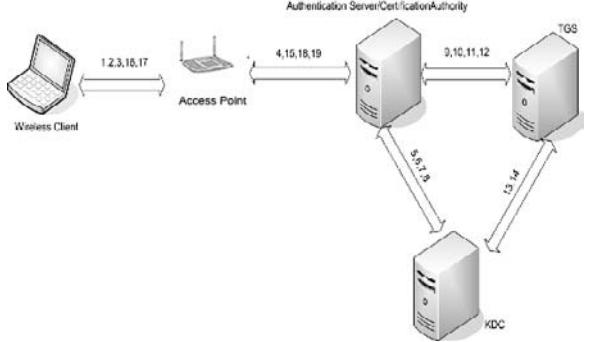


Fig. 2 Proposed Framework

The framework is such that both the program and data containing the credentials of the legitimate entities of a particular wireless LAN environment are installed on each of the entities as well as TGS and KDC. The credentials are the identities of the devices (such as MAC addresses) and they are stored with cryptographic protection. The program adopts the challenge-response paradigm. The interactions between the entities are represented using numbers 1 – 19. As indicated in Fig. 2, numbers 1, 2, 3, 16, 17 represent the interactions between the client and the access point while numbers 4, 15, 18, 19 represent the interactions between the access point and the authentication server. The numbers 5, 6, 7, 8 and 9, 10, 11, 12 represent the interactions between application server & KDC, and application server & TGS respectively. Also, numbers 13, 14 represent the interactions between KDC and TGS.

The protocol proposed in this paper is a combination of Kerberos Authentication Protocol and Encrypted Key Exchange Protocol. Kerberos Authentication Protocol has failed on one of its specifications resulting in a "replay message attack." However, the protocol description and specifications of the Key Exchange Protocol emphasises that, no such attack is found.

The aforementioned two authentication protocols are combined, in order to find a solution to the framework in [10].

The following script is the part of the combined protocol:

```

#Processes
INITIATOR(A,S,na,ns) knows Skey(A),
PK,SK(A),passwd(A,B)
RESPONDER(B,nb) knows SKey(B), PK,SK(B), passwd(A,B)
SERVER(S,kab) knows SKey, PK, SK, passwd
#Protocol description
0. -> A : B
[B != A]
1. -> A : S
2. A -> S : B
3. S -> A : {ts, B, kab}{SKey(A)}{passwd(A,B)}
4. S -> A : {ts, A, kab}{SKey(B)}{passwd(A,B)} % enc
5. A -> B : enc % {ts, A, kab}{SKey(B)}{passwd(A,B)}
6. A -> B : {A, ta, na}{kab}
7. B -> A : {ta, na, nb}{kab}
8. A -> B : {nb, ta}{kab}
    
```

#Intruder Information

Intruder = Mallory

```
IntruderKnowledge = {Alice, Bob, Mallory, Sam, Nm, PK,
SK(Mallory), \
SKey(Mallory).passwd(Mallory,Alice), passwd(Mallory,Bob)
passwd(Alice,Mallory), passwd(Bob,Mallory), \
passwd(Mallory,Mallory)}
```

Guessable = Password

Crackable = Password

When tested through FDR, and improved throughout the development cycle, due to the strength of the encryption and authentication specifications introduced, there were no attacks found, even when new options “Guessable” and “Crackable” of password are added to “#Intruder Information” section under the “Intruder knowledge” option.

With this, the use of Kerberos for authenticating wireless LAN users and nodes is proposed and the proposed protocol is the first step in improving the security of Kerberos Authentication Protocol for wireless LANs based on the proposed framework [10]. The aim is to further improve “#Protocol description” section so that, it prevents or at least delays replay message attacks, masquerading of authentication server, KDC and TGS of the Kerberos Protocol.

IV. DISCUSSIONS

This paper is concerned with the expression of particular security properties and protocols within CSP and FDR, as well as a compiler tool, CASPER that provides a foundation for analysis and verification.

Additionally, in terms of authentication and authorisation, security aspects of the Kerberos Authentication Protocol are discussed in both wired and wireless networks. Also, this protocol’s availability is checked with a security analyser tool CASPER, and the work has proceeded with improvements.

The model, presented above is modelling of the addition of a new variant on Kerberos for IEEE 802.11b LANs.

The proposed protocol that has improvements over Kerberos authentication is designed to improve security and minimize possible attacks.

In this paper, the theoretical grounds of a commonly used protocol, Kerberos, its implications and the capability of the attacker under assumptions of possible deductions are presented with inductive capability in CASPER/FDR.

As mentioned in the previous paragraphs, firstly Kerberos Authentication protocol’s capability is checked. After that, new protocol model is designed to minimise possible attacks. This protocol is the initial steps for the proposed model. Since it minimizes the possible attacks, new improvements will be introduced on the specifications and description of the protocol.

In order to increase the strength of Kerberos and form a complete security model of wireless networks with all the participants, the developed protocol model will be analysed further. Also, to find the best approaches against attacks, validation of “delaying decryption” and “timed authentication” properties will be tried.

V. CONCLUSIONS

Owing to the fact that even highly secured networks and computing resources remain vulnerable due to the rapid evolution of attacks, it becomes highly necessary to improve security authentication and authorisation of networks and computer resources for unassailable attackers. These vulnerabilities result from errors associated with the design of the protocols and with the verification processes of the protocols considered. Inadequate verification provides the devastating impressions about the strength or capability of authentication protocols.

CASPER is used to demonstrate the feasibility of modelling authentication protocol participants in such a manner to capture their full potentials. This provides a basis to extrapolate the possibilities of what the intruder can achieve with certain knowledge, and where this is achieved.

This paper identifies the merits and weaknesses of the Kerberos Authentication Protocol, and in the light of this, proposes a new protocol with improved specifications that provides a background and initial steps for design of security solutions for Kerberos Security Protocol for IEEE 802.11b wireless local area networks that require high level of security. Additionally, this paper presents a CASPER model for modelling and analysing the proposed protocol.

REFERENCES

- [1] M. Abadi and R. Needham. “Prudent Engineering for Cryptographic Protocols.” *IEEE Transactions on Software Engineering*, vol. 22(1): pp. 6-15, 1996
- [2] S. M. Bellovin, and M. Merritt. “Limitations of the Kerberos Authentication System”, *USENIX winter 1991*, pp.253-268, 1991
- [3] A. W. Roscoe “CSP and Determinism in Security Modelling”. *IEEE Symposium on Security and Privacy*. pp. 114-127, 1995
- [4] G. Lowe. “CASPER: A Compiler for the Analysis of Security Protocols”. *Proceedings of the 10th Computer Security Foundation Workshop*. pp.18-30., 1998
- [5] A. Harbitter and D. A. Menascé . “A Methodology for Analyzing the Performance of Authentication Protocols”. *ACM Transactions on Information and System Security*, vol. 5(4): pp. 458-491, 2002.
- [6] C. A. Hoare. “Communication Sequence Process”. *Prentice- Hall*, International Englewood Cliffs. New Jersey. 1985
- [7] G. Lowe. “An Attack on the Needham-Schroeder Public-key Authentication Protocol.” *Information Processing Letters*. Vol: 56(3), pp. 131-133, 1995.
- [8] A. Mishra and W. A. Arbaugh. “An Initial Security Analysis of the IEEE 802.1X Standard”, *White paper*, UMIACS-TR-2002-10, February 2002.
- [9] M. R. Needham and M.D. Schroeder. “Using Encryption for Authentication in Large Networks of Computers.” *Communication ACM* (21) pp.993-999, 1978
- [10] Y. Kirsal, A. Eneh and O. Gemikonakli, “A Solution to the Problem of Trusted Third Party for IEEE 802.11b Networks”. *PGNET2005*, Liverpool UK, pp.333-339, 2005
- [11] S. Schneider. “Verifying authentication protocols with CSP” *10th Computer Security Foundations Workshop*, IEEE. pp.741-758, 1997
- [12] “Security White Paper Evolution, Requirements, and Options” Available: <http://wifiplanet.com/tutorials/articles.php/965471> [Accessed: 27 April 2005]
- [13] A. H. Eneh., O. Gemikonakli and R. Comley. “Security of Electronic Commerce Authentication Protocols in Economically Deprived Communities”, The Fifth Security Conference 2006, Las Vegas, Nevada, April 2006, ISBN: 0-9772107-2-3.

Autonomous Agents based Dynamic Distributed (A2D2) Intrusion Detection System

Yu Cai, Hetal Jasani
Michigan Technological University
cai@mtu.edu

Abstract

In this paper, we propose a highly-configurable, well-integrated Autonomous Agents based Dynamic Distributed (A2D2) intrusion detection framework. A2D2 supports a hybrid, integrated and flexible intrusion detection model which consists of a family of intrusion detection agents. Agents can dynamically download and install appropriate modules, signatures and policy files from the central server based on operational requirements. A group key management system is used to provide secure and scalable group communication and group management in A2D2. Flexible intrusion response mechanisms are designed. A data fusion and event analysis engine (mEngine) and an object-based intrusion modeling language (mLanguage) are also designed. Both mEngine and mLanguage are domain-independent.

1. Introduction

Network security is one of the most critical issues in today's computer-dominated society. Security threat monitoring and surveillance are mostly performed using Intrusion Detection Systems (IDS). However, most IDSs in use today have a number of problems that limit their configurability, interoperability, efficiency and scalability.

This paper proposes a highly-configurable, well-integrated Autonomous Agents based Dynamic Distributed (A2D2) intrusion detection framework. The key idea of A2D2 is to use autonomous agents (hereby referred to as AA) as independently-running entities to provide unified management interfaces for intrusion detection, intrusion response, information fusion and dynamic reconfiguration. AAs are designed to carry out tasks in a flexible, adaptive and intelligent manner that is responsive to changes in the environment. AAs significantly improve the configurability, controllability and manageability of the distributed IDS.

The key features of A2D2 are listed below

1) A2D2 supports a hybrid, integrated and flexible intrusion detection model. The intrusion detection network consists of a family of AAs: active AAs which are normal intrusion detection agents, hibernative AAs which are usually in hibernation but can turn active upon requests, mobile AAs which can travel among network hosts and take actions at target spots, and auxiliary AAs which provide interfaces between the A2D2 framework and the existing IDSs from other vendors.

2) A2D2 is designed as an open framework using modular structure. AAs can dynamically and intellectually download and install appropriate modules, signatures and policy files from the central servers. This greatly alleviates the headache of software deployment, maintenance and management. At the same time, new intrusion detection techniques and capabilities can be easily integrated into

the A2D2 framework. This allows different organizations and individuals to contribute to the development of A2D2.

3) A group key management system is used to provide secure and scalable group communication and group management for heterogeneous entities (including multiple AAs) in A2D2. The group key system can ensure the confidentiality, authenticity, and integrity of messages delivered between group members. In A2D2, all participating nodes are authenticated, and all control messages and data are encrypted. This is a necessary measure against insertion and evasion attacks on distrusted IDS itself.

4) A2D2 is organized in a hierarchical structure which improves system scalability. Intrusion detection AAs are at the bottom of hierarchy. Multiple layers of data fusion AAs and control AAs can be used to correlate intrusion detection data and take intrusion responses. The central servers are at the top of hierarchy, which provide global intrusion data fusion, intrusion responses and system management.

5) Flexible intrusion response mechanisms are designed in A2D2. First, global intrusion response over the network and local intrusion response on local hosts or subnets are combined together. Second, new Quality-of-Service(QoS) based intrusion responses on routers and backend servers are designed, in addition to classic intrusion responses on firewall. Third, dynamic IDS reconfiguration for intrusion response is designed.

6) A data fusion and event analysis engine (mEngine) and an object-based intrusion modeling language (mLanguage) are designed. Both mEngine and mLanguage are domain-independent. In A2D2, confidence-level based data fusion techniques are used. This enables IDS systems to be flexible in raising alerts and enables network systems to be flexible in intrusion response.

The rest of this paper is organized as follows. In Section 2, we survey the related works. In Section 3, we present the design of A2D2. In Section 4 we discuss the implementation issues. The conclusion is in Section 5.

2. Related Works

IDSs play a vital role in protecting and monitoring the network infrastructure. IDSs are based on the principle that attacks on computer systems and networks will be noticeably different from normal activities. The job of IDS is to detect these abnormal patterns by analyzing information from different sources.

IDSs may be classified into host-based IDSs, network based IDSs and distributed IDSs, according to the source of the audit information used by IDSs. Host-based IDSs get data from host audit trails; network-based IDSs use

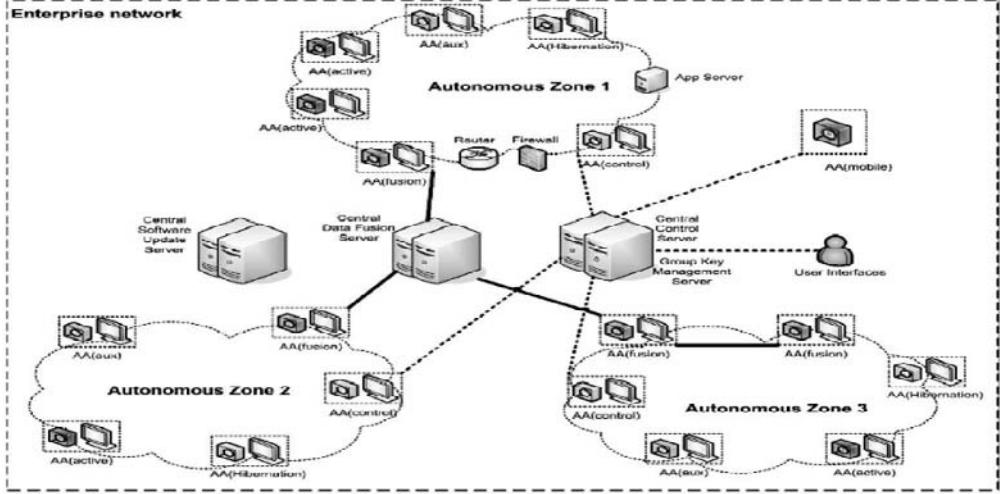


Figure 1: The architecture of A2D2 framework

network traffic as the data source; distributed IDSs gather audit data from multiple hosts and the network.

There has been a shift from a centralized and monolithic IDS framework to a distributed one. Distributed IDSs usually include multiple sensors or agents for intrusion detection, and data fusion modules for fusing information from numerous sources. It can effectively protect large-scale networks in the dynamic environment. Significant work has been done in this field [2, 4, 11, 13, 15, 21, 22, 23, 26, 27].

Despite the best efforts from intrusion detection community, most IDSs in use today still suffer from a number of limitations that are listed below.

- Configurability, controllability and manageability. Today's networks are dynamic. Most current IDSs lack the ability to support flexible on-demand reconfiguration and dynamic deployment of new sensors. More specifically, IDSs should support tasks like creating new detection sensors, loading attack signatures at run-time, taking flexible intrusion responses, being adaptive to changes in environment, and detecting new attacks.

- Interoperability. Today's networks are heterogeneous. Most current IDSs are developed and operated in specific domains and environments. It is a complicated and error-prone task to integrate multiple IDSs. Mechanisms need to be designed to support the effective integration, cooperation and collaboration of heterogeneous IDSs.

- Scalability, extensibility and Robustness. IDSs should be scalable to monitor large-scale networks with minimal overhead imposed. IDSs need to be extensible to incorporate new capabilities and new technologies. IDSs need to protect themselves from attacks. They should recover quickly from system crashes or network failure.

- Effectiveness. Most current IDSs suffer from high false alarm rate, including false positive and false negative. IDSs should be designed to produce real-time, high-confidence detection results by fusing information from multiple data sources.

Some existing distributed IDSs also use sensors, agents or autonomous agents [2, 4, 11, 13, 15]. The uniqueness of AAs in A2D2 is summarized as follows. The AAs in A2D2 are designed to carry out complicated tasks in a flexible and intelligent manner which supports dynamic deployment and reconfiguration. Second, by delegating certain tasks from central servers to autonomous local agents, the communication overhead is greatly reduced, and the intrusion response time is shortened. Third, AAs provide fail-over protection and improve the system robustness. The impact of failed agents is limited to local hosts or subnets.

3. System Design

3.1 Autonomous Agents

Figure 1 shows the architecture of the A2D2 framework. The example network is divided into three autonomous zones, which can be based on subnets. Each autonomous zone consists of multiple intrusion detection agents, data fusion agent(s) and control agent(s), where intrusion detection is done independently. There are of six types of AAs and three types of central servers in A2D2 architecture.

- Active Intrusion Detection AA (or active AA). Active AAs run as intrusion detection agents which monitor network traffic and transfer collected intrusion detection information to data fusion agents. The intrusion detection can be host-based or network based. Active AAs can load intrusion detection signatures, policies and additional modules at run-time without restarting the whole A2D2 system. Active AAs can also take local intrusion response.

- Hibernative Intrusion Detection AA (or hibernative AA). Hibernative AAs usually stay in hibernation and impose almost no overhead on local hosts and the network. Upon receiving “wake-up” command from control agents, they turn into active AAs. The rationale behind this is as follows. Excessive intrusion detection agents and data traffic will impose unacceptable overhead on network systems. Therefore, if no attacks, some AAs

should hibernate; if there is an attack alarm, the hibernating AAs in the affected area should turn into active mode to watch intrusion closely; if alarm is off, those AAs should hibernate again.

- Mobile Intrusion Detection AA (or mobile AA). Mobile AAs are mobile software agents that can travel from one computer to another computer in the network. They are controlled directly by the central servers and can visit a series of hosts. The mobile agents are executed locally on these hosts to support certain tasks, like intrusion detection, or deployment of new AAs. The reason of using mobile AA is that they can be sent to security hot spots or blank spots to install new AAs or perform other tasks with great flexibility.

- Auxiliary AA. This type of AA is used to integrate A2D2 and the existing IDSs from other vendors, like the proprietary IDSs or Snort. Auxiliary AAs provide interfaces between multiple IDSs so they can share audit information and take coordinated intrusion responses. Different interface modules can be plugged into auxiliary AAs based on operational requests. The reason to have auxiliary AAs is to take advantage of the existing intrusion detection resources.

- Data fusion AA. This type of AA runs as information fusion agent, which collects and fuses information from multiple data sources, and generates intrusion detection analytical results with a value of 0-1. Different information fusion modules, like neural network or belief network, can be plugged into data fusion AAs.

- Control AA. This type of AA gets intrusion detection analytical results from data fusion agent. Based on intrusion response policies, control AAs make decisions on appropriate actions and notify corresponding entities. New QoS-based intrusion responses on routers and backend servers are designed in addition to classic intrusion responses on firewall, like packet filtering and rate limiting. The control AA also keeps track of all agents in its domain and maintains an agent information table.

AAs play a central role in A2D2 framework. AAs can receive high-level control commands and take predefined actions. Based on operational requirements, different modules can be plugged in, loaded and unloaded dynamically on AAs. AAs greatly simplify the deployment, configuration and management of distributed intrusion detection system.

3.2 Central Servers

The three types of central servers in A2D2 framework are listed as follows.

- Central data fusion server. It collects refined intrusion detection information from data fusion AAs and conduct information fusion for the whole network. It generates global intrusion detection results with a confidence level of 0-1.

- Central control server. It gets global intrusion detection results and makes decision on global intrusion responses, including QoS-based response on router and end server, firewall-based response, and IDS dynamic reconfiguration. Group key management system is installed and configured on central control server so that it

can keeps track of all agents in the network and maintains an AA information database. It also controls mobile AAs directly. Three end-user interfaces are provided for system administration: web-based, prompt-based and script-based.

- Central update server. It contains a software module repository, an intrusion signature database, and a collection of response policies. Two software installation modes are supported. Pull mode, modules, policies and signatures are pulled by agents from the central server; push model, the central server will push modules, policies and signatures to agents.

The AAs and central servers in A2D2 form a hierarchical structure. Local control AAs can only send control commands to agents in its authorized domain. Central control server can send commands to all agents in the network and can override commands from local control AAs.

The central servers may become a single-point of failure. To improve performance and robustness, server cluster may be used. Also, redundant upstream agents or servers can be used and configured, which is similar to the use of redundant DNS servers.

3.3 Intrusion Response

A2D2 provides flexible intrusion response. First, global intrusion response over the network and local intrusion response on local host or subnet are used together. The local intrusion response is decided by local intrusion detection agent based on local response policy, which can greatly reduce the response time and communication overhead. The local intrusion response is also useful to detect and defense against internal attacks.

Second, in addition to classic intrusion responses on firewall like packet filtering and rate limiting, new QoS-based intrusion responses (Figure 2) on front-end router and back-end server are designed. On router, traffic classification is used to classify the incoming traffic based on the confidence level of incoming traffic. On backend application server, QoS resource management mechanism is designed to provide differentiate services to each traffic class.

The rationale of QoS-based intrusion response is as follows. QoS is usually the target of attacks; but it can also be used to fight against attacks. Most current IDSs suffer from the high false alarm rate problem. Instead of classifying traffic into legitimate (0) and malicious (1), we can use a confidence level (0-1) outputted by information fusion modules to measure the legitimacy of the incoming traffic. Traffic with low confidence level (as attacking traffic) will be allocated with more system resources, and vice versa.

3.4 Data Fusion and Event Analysis Engine

Multi-sensor data fusion is a challenging issue in distributed IDS. The effectiveness of distributed IDS relies heavily on data fusion and event analysis. Tremendous work has been done in this field [3, 14, 18, 19, 20].

In A2D2, we implemented two commonly-used data fusion techniques, belief network and neural network [12]. The implementation of other data fusion modules will

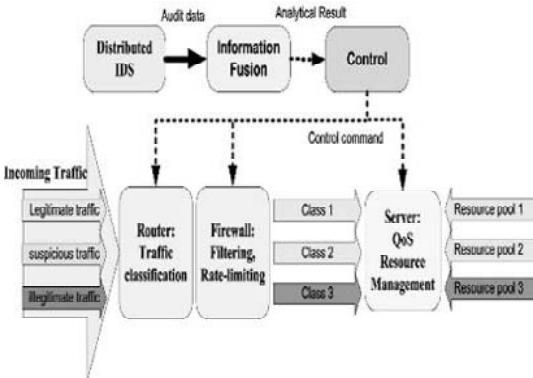


Figure 2: QoS-based intrusion response

depend on time and budget constraints. The openness of A2D2 framework makes it easy to incorporate new techniques and capabilities into the system.

We propose a multi-stage data fusion and event analysis engine (mEngine) in A2D2. The architecture of mEngine is illustrated in Figure 3. It is designed to be a domain-independent architecture. The mEngine starts with a preprocessing module which examines incoming data to ensure validity like data source, data format and required attributes. The noise filtering module filters out unwanted background noise. Kalman filter [1] is a recursive filtering algorithm for stochastic dynamic systems, which is robust to background noise existing in the monitored data. The duplicate reduction module removes duplicated information reported by multiple agents.

Then data moves from data processing stage to information analysis stage. The instance clustering module is responsible for clustering data into attack instances. The host/network integration module associates network-based data with host-based data that are related to the same attack instance. The hotspot identification module identifies suspicious activity instances and security hotspots in the network.

Next, data moves into knowledge analysis stage. The multi-step analysis module is responsible for identifying attacks involving multiple steps. A connection-history based anomaly detection algorithm based on [25] will be designed and implemented. The idea here is to detect the trend, not the burst. Therefore, this module is useful to identify attacks and worms at early stage. Based on the analytical result, precocious response actions will be taken, for example, waking up hibernative AAs, relocating mobile AAs and classifying traffic with lower priority.

The distribution analysis module identifies attacks based on traffic distribution analysis. The basic approach is to derive traffic distribution features from the normal network traffic and use them as a baseline for comparison. It can identify previously unknown and new attacks. We plan to design the module based on byte frequency distribution approach [17] and position-aware distribution signature [24] approach.

The last element in mEngine is the threat assessment module. It is used to evaluate the impact of attacks, determine the effectiveness of analytical results, and prioritize the output results. The analytical results of mEngine are values between 0-1 indicating confidence

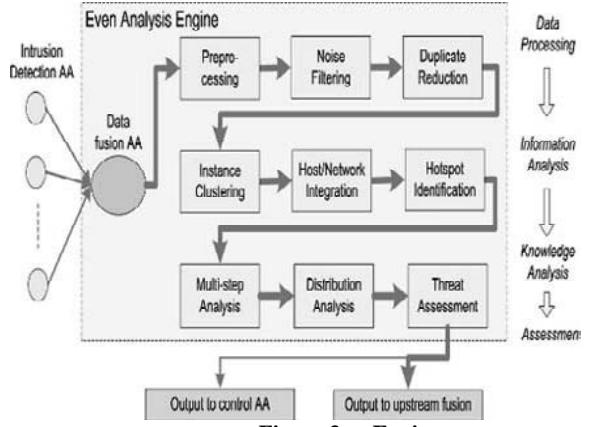


Figure 3: mEngine

level. The control AA will determine response actions based on these values and response policies. Also, the refined intrusion detection dataset is outputted to upstream data fusion entities.

3.5 Intrusion Modeling Language

Intrusion modeling languages have received a lot of attention from the intrusion detection community [5, 9].

In A2D2, we plan to design a new multi-class intrusion modeling language (mLanguage). The mLanguage uses C/C++ alike syntax to reduce the learning curve. The mLanguage is designed to be an Object-based language because object-based technique has become especially popular in scripting languages, with abstraction, encapsulation, reusability, and ease of use being the most commonly cited reasons. The other benefit of Object-based technique is to be compatible and inter-operable with XML and Web Services.

There are six classes predefined in mLanguage which are listed below. Users may define new classes based on their needs.

- **Event.** It describes network “event”, or “activity”, for example, a scan action.
- **Source.** It describes the source of attack, like IP address, port number and running services.
- **Target.** It describes the target of attack.
- **State.** It describes the state and status of attacks and the network.
- **Transition.** It describes the transition of state and event. This is useful for multi-step attacks.
- **Response.** It describes intrusion responses with confidence level.

To illustrate mLanguage, let’s look at a scenario. An attacker exploits a buffer overflow vulnerability on an e-Commerce web server. From the Web server, the attacker tries to mount a file system to access some sensitive data. This attack may be observed by multiple AAs. For instance, a signature-based network IDS may detect the buffer overflow attack, and an anomaly detection component may detect the unusual file access. The mEngine is responsible to correlate and fuse different pieces to get a whole picture of the attack. A piece of mLanguage code describing the attack is shown in example 1.

Example 1: A piece of mLanguage code describing buffer overflow & remote execution attack.

```

1: Module Buffer-Overflow-Attack {
2: Set source = CreateObject ("mLang.Source")
3: Set target = CreateObject ("mLang.Target")
4: source.list = (141.218.2.22, 141.218.2.11)
5: target.list = (128.121.82.88 : port 443)
6: Event event1 {
7:   .type = bufferOverflow
8:   .timestamp = 04092006121311
9:   .target = target.list[0]
10: Event event2 {
11:   .type = exploitRemoteExec
12:   .timestamp = 04092006141751
13:   .target = target.list[0]
14: if event2.timestamp > event1.timestamp then
15:   state.current = attackSucceed
16:   state.timestamp = event2.timestamp
17:   response.type = block
18:   response.confidenceLevel = 1
19: else
20:   transition.action = exploitRemoteExec
21:   transition.timestamp = event2.timestamp
22:   transition.location = event2.target
23:   response.type = block
24:   response.confidenceLevel = getConfidenceLevel()
25: end if
26: }

```

4. Implementation issues

A prototype of A2D2 framework is under development on the Linux kernel 2.4 and Windows Server 2003 systems, and will be migrated to other OSs and platforms.

4.1 Autonomous Agents

A generic software agent was designed. Since it needs to run across multiple platforms, a Java-based agent installation program was used. However, due to the performance issue and the need to access low-level system calls, a C-based agent program was used.

The possibility of integrating the software agent into the OS kernels will be investigated. This can greatly improve the agent performance. However, kernel implementation is costly and error-prone, and may not be feasible for some proprietary OSs.

Second, different function modules are under development. For example, intrusion detection modules for active AA and hibernative AA; interface modules for auxiliary AA; and control modules for control AA.

Below is the process of agent installation in A2D2. First, a java installer is executed by system administrator for manual installation or by mobile AA for automatic installation. Second, the installer program will contact the

central software server(s), download a C agent module based on current platform information, and install the module on local host. Third, the newly-installed C agent program takes control from the Java installer. The software agent supports dynamic modules. It can intellectually scan current systems and the network to decide what additional modules are needed. It then downloads and installs the modules. It can load and unload modules at run-time without restarting itself. It also supports network socket communication to receive high-level control commands from upstream control agents or central servers.

Third, a framework to support mobile agents will be investigated. Mobile agents refer to self contained and identifiable computer programs that can move within the network and act on behalf of the user. Agents can function independent of each other or cooperate to solve problems.

By helping to disperse centralized network management tasks to subnet hosts, mobile agent technology helps conserve network bandwidth and improves management efficiency.

To the best of our knowledge, currently there are over 20 academic and industry mobile agent systems available [7, 8]. We plan to investigate current mobile agent frameworks and choose one for A2D2. The selection criteria are source code availability, system performance and robustness. We will customize the mobile agent framework to fit A2D2.

4.2 Central Servers

Central data fusion server, central control server and central software server was designed and developed. The central servers provide global data fusion and system control over the network. Agent information database was designed for control AA and central control server to keep track of agent information like location, state, modules, versions, message received and action taken. A software repository containing modules, signatures and policy files will be designed for central software server.

Second, the A2D2 framework is based upon a group communications model. All participating nodes are authenticated. All control messages and data exchanged are encrypted. As a result, securing group communications becomes a critical issue in A2D2. A group key management system [16, 29] establishes and maintains group keys for groups of clients. A group key may be an encryption key, a signing key, a security-association in IPSec, etc. In [29], the authors present the design and architecture of a scalable group key management system called Keystone. Keystone uses a novel key graph technique for scalable group key management. We integrated the A2D2 framework on the top of Keystone system.

Third, the central servers may become a single-point of failure. To improve performance and robustness, server cluster may be used. The Linux Virtual Server (LVS) is a highly scalable and highly available server cluster technique, which is fully transparent to end users. The use of LVS was incorporated in A2D2.

A key goal of A2D2 is to provide real-time intrusion detection and response. The delay of intrusion detection primarily comes from the following two sources.

- The overhead of secure group communication between entities. Our past experience with keystone and secure group communication indicates that the overhead should be in an acceptable range [6, 28]. One solution to reduce overhead is to use faster authentication and encryption/decryption methods [10].
- The latency of mEngine when conducting data fusion and event analysis. One solution to reduce latency is to use local response and signature-base detection. The other possible solution is to output intermediate results during analysis in mEngine.

5. Conclusion

Security threats have increased in sophistication, frequency and complexity. Security has become the Achilles hill of organizations of all sizes. There is a growing mismatch between the level of protection that organizations' security measures are providing and the level needed to address their actual degree of risk.

A2D2 framework is designed to use autonomous agents as independently-running entities to provide unified interfaces for intrusion detection, intrusion response, information fusion and dynamic reconfiguration. The prototype is still under development.

References

- [1] B. D. O. Anderson and J. Moore. Optimal Filtering. Prentice Hall Publishing, 1979.
- [2] J. Balasubramanyan and G. Fernandez. An architecture for intrusion detection using autonomous agents. In Proc. of Annual Computer Security Applications Conference (ACSAC), 1998.
- [3] T. Bass. Intrusion detection systems and multisensor data fusion. Communications of the ACM, 43(4):99–105, 2000.
- [4] S. S. Chen, S. Cheung, and R. Crawford. GrIDS: A graph based intrusion detection system for large networks. In Proc. of 19th National Information Systems Security Conference, 1996.
- [5] S. Cheung, U. Lindqvist, and M. W. Fong. Modeling multistep cyber attacks for scenario recognition. In Proc. of Third DARPA Information Survivability Conference and Exposition (DISCEX), 2003.
- [6] E. Chow, Y. Cai, D. Wilkinson, and G. Godavari. Secure collective defense system. In Proc. of IEEE Globecom, 2004.
- [7] J. Claessens, B. Preneel, and J. Vandewalle. (how) can mobile agents do secure electronic transactions on untrusted hosts. ACM Transactions on Internet Technology (TOIT), 3(1):160–186, Feb. 2003.
- [8] T. C. Du, E. Li, and A. Chang. Mobile agents in distributed network management. Communications of the ACM, 46(7):60–96, July 2003.
- [9] S. Eckmann, G. Vigna, and R. Kemmerer. STATL: an attack language for state-based intrusion detection. Journal of Computer Security, 10(1):71–104, 2002.
- [10] N. Ferguson, D. Whiting, and B. Schneier. Helix: Fast encryption and authentication in a single cryptographic primitive. Lecture notes in computer science, 2887:330–346, 2003.
- [11] R. Gopalakrishna and E. Spafford. A framework for distributed intrusion detection using interestdriven cooperating agents. In Proc. of International Symposium on Recent Advances in Intrusion Detection (RAID), 2004.
- [12] D. L. Hall. Handbook of Multisensor Data Fusion, 1st edition. CRC Publishing, 2001.
- [13] J. Hochberg, K. Jackson, and C. Stallings. NADIR: An automated system for detecting network intrusion and misuse. Computers and Security, 12(3):235–248, 1993.
- [14] K. Julisch. Clustering intrusion detection alarms to support root cause analysis. ACM Trans. on Information and System Security, 6(4):443–471, 2004.
- [15] R. A. Kemmerer and V. Giovanni. Hi-DRA: intrusion detection for internet security. Proceedings of the IEEE, 93(10):1848–1857, 2005.
- [16] Y. Kim, A. Perrig, and G. Tsudik. Tree-based group key agreement. ACM Transactions on Information and System Security, 7(1):60–96, Feb. 2004.
- [17] C. Kruegel and G. Vigna. Anomaly detection of web-based attacks. In Proc. of ACM Conference on Computer and Communication Security (CCS), 2003.
- [18] W. Lee. Applying data mining to intrusion detection: the quest for automation, efficiency, and credibility. ACM SIGKDD Explorations, 4(2):35–42, 2002.
- [19] P. Ning, Y. Cui and D. S. Reeves. Techniques and tools for analyzing intrusion alerts. ACM Trans. on Information and System Security, 7(2):274–318, 2004.
- [20] P. Ning, S. Jajodia, and S. Wang. Abstraction-based intrusion detection in distributed environments. ACM Trans. on Information and System Security (TISSEC), 4(9):407–452, 2001.
- [21] P. A. Porras and P. G. Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In Proc. of 20th NIS Conference, 1997.
- [22] S. R. Snapp, S. E. Smaha, T. Grance, and D. M. Teal. The DIDS (Distributed Intrusion Detection System) Prototype. In Proc. of USENIX Technical Conference, 1992.
- [23] E. H. Spafford and D. Zamboni. Intrusion detection using autonomous agents. Computer Networks, 34(4):547–570, 2000.
- [24] Y. Tang and S. Chen. Defending against internet worms: A signature-based approach. In Proc. of IEEE Infocom, 2005.
- [25] T. Toth and C. Kruegel. Connection-history based anomaly detection. In Proc. of IEEE Workshop on Information Assurance and Security, 2002.
- [26] G. Vigna, F. Valeur, and R. Kemmerer. Designing and implementing a family of intrusion detection systems. In Proc. of Eur. Software Engineering Conf. and ACMSIGSOFT Symp. Foundations of Software Engineering (ESEC/FSE), 2003.
- [27] G. B. White, E. A. Fisch, and U. W. Pooch. Cooperating security managers: A peer-based intrusion detection system. IEEE Network, 5(3):20–23, 1996.

- [28] D. Wilkinson, C. E. Chow, and Y. Cai. Enhanced secure dynamic dns update with indirect route. In Proc. of the IEEE Information assurance workshop, 2004.
- [29] C.K. Wong, M. Gouda, and S.S. Lam. Secure group communications using key graphs. IEEE/ACM Transactions on Networking, 8(1):16–30, Feb. 2000.

Modeling and Implementation of Agent-Based Discrete Industrial Automation

Yuval Cohen*

Department of Management and Economics
The Open University of Israel
Raanana, Israel, 43107

Ming-En Wang, Bopaya Bidanda

Department of Industrial Engineering
The University of Pittsburgh
Pittsburgh, USA, 15261

Abstract - In shop floors dominated by programmable logic controllers (PLCs), the implementation of flexible control has been held back due to difficulties in generation and modification of the PLC code. This paper presents a technique that not only automates the PLC code generation and modification, but also integrates it into a framework of process planning and scheduling. The purpose of this technique is to enable a specific set of software agents to automate the specification, generation, validation, and implementation of discrete shop-floor control systems. The first part of the paper presents a framework of five software agents that interact with each other to plan model and implement flexible manufacturing using current control equipment (i.e. PLCs). The framework specifies the roles and rough communications protocols of each agent. The five agents are: (1) Process planning agent, (2) Scheduling agent, (3) Modelling and simulation agent, (4) Validation and exception handling agent, and (5) PLC language translation agent. The second part of the paper addresses the operations details of each agent. For this purpose, it presents a new technique used to model, validate and generate the PLC code. We named this technique Three Levels Approach (TLA) to reflect the three levels of detail used to describe the manufacturing process.

I. INTRODUCTION

Major part of discrete industrial automation hardware is controlled by Programmable Logic Controllers (PLCs). The ever increasing need for better modelling and implementation of automation was not satisfactorily fulfilled by any of the existing techniques [1]. There is ongoing research for a simpler, faster, and friendlier model, that would be easier to

change and debug [2]. This paper presents a technique that not only automates the PLC code generation and modification but also integrates it into the framework of process planning and scheduling. The purpose of this technique is to enable a specific set of software agents to automate the specification, generation, validation, and implementation of discrete shop-floor control systems.

The realization that software agents offer potential for greater manufacturing flexibility has brought research interest in variety of facets of this subject. The following are some examples of this broad research: Reference [3] suggests a three level control scheme: (1) shop floor level, (2) Intelligent agent controller, and (3) Equipment controller. Reference [4] investigates four functions of manufacturing agents: (1) internal resource management, (2) reflexivity mechanism, (3) goal adjustment mechanism, and (4) collaborative management. Reference [5] shows that production agents can improve the utilization of the shopfloor. Reference [6] specifies five basic protocols for autonomous agent network, and reference [7] describes the usage of multi-agent for production and manufacturing planning.

However, the promise of real manufacturing flexibility is still a distant dream for most shopfloors. Part of the reason for this is due to the need to deal directly with switches and Boolean logic of sensors and actuators. Another reason is that the operation logic is complex driving up the cost of human intervention and programming maintenance.

The proposed approach is different than other approaches in several respects.

First, it is recognized that while automation reduces (or even eliminates) human involvement in the mechanical processing, it

* Corresponding author: Tel.: (972) 9-778-1883; Fax: (972) 9-778-0668; E-mail: yuvalco@openu.ac.il

still requires human involvement over time in maintenance and changes to the control system. Therefore, a new easy to follow graphical scheme for modeling the operation of the control system is presented. The resulted graphical model is easy to follow, debug, and change. The paper also describes how a software agent can build the graphical model without human intervention.

Secondly, it is recognized that automation is implemented using switches, actuators, and sensors that are typically controlled by PLCs. Therefore, an algorithm was developed to translate the graphical model into PLC code.

The third difference is the recognition that work allocation to software agents could follow work allocation to humans in that each individual agent specializes in certain jobs.

The first part of the paper presents a framework of five software agents that interact with each other to plan model and implement flexible manufacturing using current control equipment (i.e. PLCs). The framework specifies the roles and communication protocols of each agent. The five agents are: (1) Process Planning agent, (2) Scheduling agent, (3) Modeling and Simulation agent, (4) Validation and exception handling agent, (5) PLC language translation agent.

The second part of the paper presents the new technique used to model, validate and generate the PLC code. We named this technique Three Levels Approach (TLA) to reflect the three levels of detail used to describe the manufacturing process. Each of the three levels of the TLA is modeled differently.

The first (least detailed) level describes the flow of products through the manufacturing processes and availability of resources. A specific Petri Net (PN) modeling approach is used here to avoid deadlocks. Even though Petri nets are a powerful analytical and modelling tool they suffer deficiencies discussed in [1, 2]. These deficiencies make it cumbersome and awkward to model and implement the second and third levels. Using the proposed method is much easier, simpler, and takes full advantage of the information structure of each level.

A significant advantage of the proposed scheme is that it can be translated into (and recovered from) any PLC language.

The second level describes the actions performed by the manufacturing system in a processing step. At the second level, each node of the PN that describes a task is further described by an Embedded Actions State Diagram (EASD).

The third level describes the changes in low level elements, such as inputs, outputs, and registers, required for executing the process. The third level is presented by a new type of graphical scheme named *E-transition* (for Elementary transition). E-transitions describe changes in low level elements, such as inputs, outputs, and registers, required for executing the EASD.

Some advantages of the TLA modeling technique are: (1) It takes into account all possible states (2) It avoids deadlock. (3) It could be easily followed and understood. (4) It eliminates the need to check all the systems states (5) It could be translated to PLC code and back.

II. THE FIVE SOFTWARE AGENTS FRAMEWORK

In this section we propose a framework of five different software agents that collaborate to control the shopfloor. Figure 1 describes the five agents and their interactions.

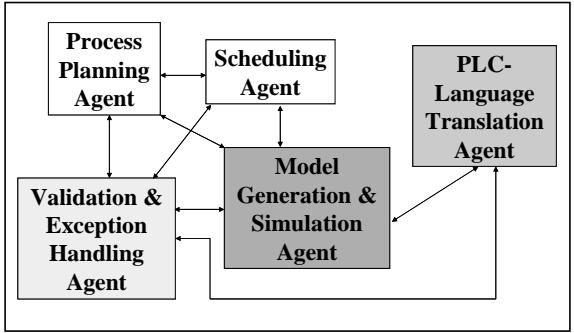


Figure 1: The proposed framework for Agent-Based Shop-Floor Control

In figure 1, the process planning agent generates the processes required to manufacture the various products, the resources needed for each process step, the precedence constraints, and time estimate of each processing step. The scheduling agent schedules the various processes and thus, the production plan is ready to be translated into a detailed manufacturing model by the model generation and simulation agent. After the model is ready it is tested by the validation and exception handling agent, if the code is immaculate it goes to the PLC language translation agent. Otherwise it goes back with feedback to the model generation agent for the required changes.

The advantages in designing such a framework were the ability of the agents to work simultaneously, autonomously, and in a modular manner (that is, if an agent is taken off line, the other agents can still work on some of their processes). The scope of work allocation according to the specialization of the agent is close in its nature to work allocation to humans. The intent is to form a team of agents, each with its own specialty, that are collaborating together and are working simultaneously in an asynchronous manner.

Considerable research has been done on process planning and scheduling agents (for example see [3,4, 6,7,12,13]), and therefore we shall skip the discussion of these two agents. However, very little has been done in implementing the control by means of PLC code. This is the main role of the other three agents: (1) Model simulation and generation agent, (2) Validation and exception handling agent, and (3) PLC language translation agent. For these three agents we present here a graphical modeling and translation technique that enable them to work efficiently and produce a plan that is easy for humans to follow. This technique has three levels and is the basis for the

whole approach and therefore we call it Three Level Approach (TLA). Specifically, we established the following tools for the usage of the three agents:

1. For the Model Generation and Simulation agent - we established:

- The graphical model (TLA)
- A systematic methodology to construct TLA

2. For the validation and exception handling agent - we established:

- Validation & verification method (based on Petri-Nets)
- Run-time tracking and error handling method

3. For the PLC language translation agent - we established:

- A two-way translation algorithm (to ladder diagram and back)

The TLA methodology is presented in section 3 along with most of the above established methods.

III. THE THREE LEVELS GRAPHICAL MODEL

Each of the three levels of the TLA is modeled differently. The first (least detailed) level describes the flow of products through the manufacturing processes and availability of resources. A specific Petri Net (PN) modeling approach is used here to avoid deadlocks. At the second level, each node of the PN that describes a task is further described by an Embedded Actions State Diagram (EASD). Finally, the third level is presented by a new type of graphical scheme named *E-transition* (for Elementary transition). E-transitions describe changes in low level elements, such as inputs, outputs, and registers, required for executing the EASD. Each of these three levels is discussed in detail below.

A. Petri Net for high level Modeling (First Level)

The first and least detailed level describes the flow of products through the manufacturing processes and availability of resources. A Petri Net (PN) modeling approach adapted from [10] is proposed at this level. For a broad overview of PN theory the reader is referred to [11]. PN nodes called places are used to denote the status of machines and parts. Each machine or part can be either idle or involved in a task. Thus, a PN place denotes either an idle resource or a task (involving a product/part or and at least one machine). PNs are well suited to model parallel actions and flow of entities. PNs also enable methods for detection and avoidance of deadlocks and

resource availability problems. However, PN is cumbersome and awkward for modeling the lower levels [8, 9].

A robotic cell that is used to demonstrate the model. The robot moves products between the machines and buffers. Figure 2 uses the proposed PN to describe the production process of a product type that is first machined by machine 1, before being processed by machine 2, and then is placed at the departure dock. Two types of PN places are used: task places and resource/s places. Identification of the necessary tasks and related resources should be done during the analysis stage, and is outside the scope of this paper. In figure 2 tasks are shaded.

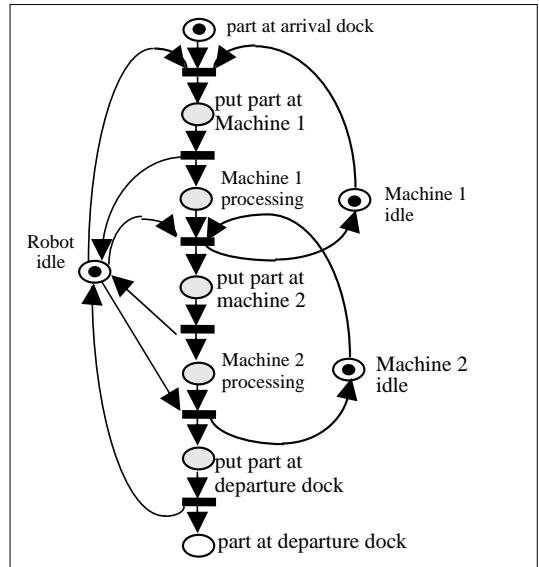


Fig. 2. Petri net describing the production process of high level Petri net description of production process (task places are shaded).

B. Embedded Actions State Diagram EASD (Level 2)

Each node of the PN that describes a task is further described by an Embedded Actions State Diagram (EASD). Each state in the EASD describes an action (a single combination of outputs). Note that inputs are ignored at this stage. This not only eliminates the complexity of input-output relationships, but also provides a clearer view of a system's functionality and enables the designer to focus on small portions of information at a time. Since we tend to think of any discrete process in terms of actions, EASD offers a natural, simplified, and clear functional description. An EASD for an automatic drill press is depicted Figure 3. States are

denoted by numbers and transitions by capital letters. The EASD does not include all the details regarding inputs, outputs, and variables. These details are embedded in E-Transitions, and discussed in section 4.

C. E-Transitions (Level 3)

At the third level, the EASD is further exploded into a new type of a graphical scheme named E-Transition (for Elementary transition). E-Transitions describe the changes in low level elements such as inputs, outputs, and registers, required for executing the EASD. E-Transitions arrange the elements in a meaningful way that enables immediate comprehension of a low level code. The E-Transitions are composed of the following elements: 1) places, 2) triggers, and 3) arcs. These elements are all depicted in figure 3. Each transition is activated by one or more triggers. The triggers are denoted by triangles pointing at a thick vertical line that symbolizes the transition. Places (denoted by circles) represent the inputs, outputs, events, and variables.

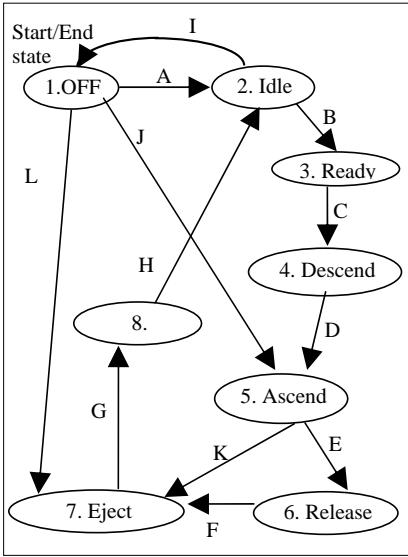


Fig. 3. An example of the Embedded Actions State Diagram — EASD (second level of TLA) for the PN place “machine 1 processing” from figure 2.

Events are assigned places with additional symbol to denotes the type of event (turn ON, and shut OFF). Places that use non-binary data (e.g., timers and counters) are denoted by rectangles. Additionally, places are added for logically denoting the states of the system. For example, transition C

from state 3 to state 4 uses the corresponding ST3 and ST4 variables.

Two arc types used to activate triggers are as follows:

1. An enable arc (---►) the triggers can fire only while the source place holds a token.
2. A disable arc (---●) the triggers can fire only while the source place is OFF.

Enable and disable arcs are drawn with dashed lines to denote that they do not activate or deactivate elements. Tokens are used to denote activated places. Two types of arcs used to identify the effects of a transition as follows:

1. Activate arc (---►) turns ON the TLA place when the Transition is activated.
2. Deactivate arc (---☒) turns OFF the TLA place when the Transition is activated.

Each trigger is invoked by places linked to the trigger by enable or disable arcs. Note the usage of the source state (STi) variable of the Transition to facilitate trigger's identification as one of the trigger's conditions. After the trigger is activated, a transition from the source state (i) to another state (j) occurs immediately. Each E-Transition also resets the source state variable (STi) and sets the destination state variable (STj). Note that each trigger has only one E-Transition, but a transition may have more than one trigger. Finally, the E-Transitions can be integrated into the EASD of the TLA as shown in figure 4.

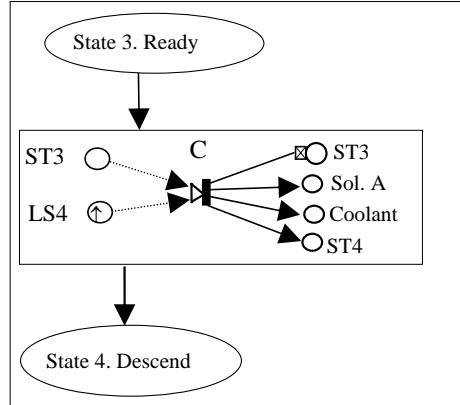


Fig. 4. A segment of the TLA integrating an E-Transition for transition C in the EASD of figure 3.

IV. SYSTEMATIC LADDER DIAGRAM GENERATION

A Ladder Diagram (LD) is chosen to illustrate the implementation of the model. The generated LD rungs are arranged in three main blocks as follows: 1) events identification

2) transition triggers, and 3) transition effects. Backward translation is also possible (Cohen and Bidanda, 1997) but is not presented here. The construction of the above three blocks is presented next.

A. Events Identification

Inputs and outputs change their voltage level when turned ON or OFF. These changes are referred as rising or falling edges. The international standard IEC 1131-3 defines special LD contacts for detecting rising and falling edges. A rising edge corresponds to a TLA place with “↑” and a falling edge to a TLA place with “↓”.

B. Transition Triggers

Each trigger activates onE-Transition. Each transition is assigned an internal variable in the LD. When theE-Transition is enabled that variable will be turned ON. In order to implement this logic, a set of rules is described as follows:

- I. Each TLA trigger forms an LD rung.
 - II. Each place (in E-Transition) that is input to a trigger forms a contact: (enable arc forms a normally open (NO) contact, and disable arc a normally closed (NC) contact).
 - III. The LD rung output is a variable that corresponds to the invoked transition.
- Figure 5 depicts a ladder diagram segment corresponding to the triggers of transitions C. These variables are used in figure 6.

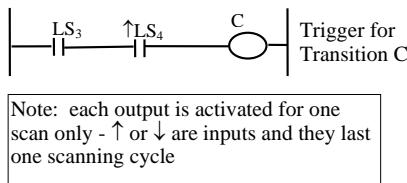


Fig. 5. Ladder Diagram segment for triggering transition C of the EASD in figure 3.

C. Transition Effects

The rules for establishing the ladder diagram portion of transition's effects is as follows:

1. Dedicate a rung for each output place of the E-Transition and add to it a corresponding LD output (e.g., the right hand places of figure 4 are translated into outputs in figure 6).
2. In each rung add a contact that corresponds to the relevant transition.
3. Activation arcs are translated into latched outputs, and Turn-off arcs are translated into Unlatched outputs.

Figure 6 depicts a ladder diagram segment corresponding to the effects of transition C

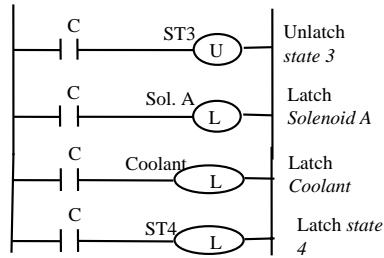


Fig. 6. A Ladder Diagram (LD) segment for the effects of transition C (see figure 4).

V. CONCLUSION

In this paper a new discrete control modeling technique is presented along with a framework for a team of software agents that can plan and implement the control on existing control equipment. The technique efficiently divides control modeling into three embedded levels. Each level is based on a simple graphic symbol system and is suited to take advantage of the underlying elements it models. TLA may be translated automatically into PLC code such as ladder diagrams and have the following additional advantages:

It greatly simplifies the generation, verification, and validation of PLC code:

- ◆ The model is easy to understand due to:
 - a. Focus on the functionality
 - b. familiar concepts
 - c. Use of graphical representation which allows and visualization of code, as well as peer and customer review
- ◆ The model enables simulation and visualization of operation
- ◆ Enables High-level verification instead of code verification.
- ◆ Can assist in real-time tracking and failure analysis of the control system.

Some future research directions include :

- ◆ Validation on manufacturing shop floor.

- ◆ High-level agent communication protocol for shop-floor control.
- ◆ Code reuse maximization.
- ◆ Development of new information standards for Mfg.; e.g., XML-like markup.

REFERENCES

- [1] Neidart, R., "The object oriented paradigm and industrial control", *Proceedings of the 20th Annual EASD International Programmable Controller Conference & Exposition, Detroit, MI*, pp. 495-505, 1991.
- [2] French, A. "Software engineering applied to programmable controller software design", *ISA Transactions*, Vol. 29, No.2, pp. 23-32, 1990.
- [3] Choi K, Kim S., and Yook S."Multi-agent hybrid shop floor control system", *International Journal of Production Research*, Vol. 38, No. 17, 4193-4203, 2000
- [4] Huang C. Y. and Nof Y. S., "Autonomy and viability - measures for agent-based manufacturing systems", *International Journal of Production Research*, Vol. 38, No. 17, pp. 4129-4148, 2000.
- [5] Ottaway T. A. and Burns J. R. "Anb adaptive production control system utilizing agent technology", *International Journal of Production Research*, Vol. 38, No. 4, pp. 721-737, 2000.
- [6] Huang C. Y. and Nof Y. S., "Autonomy and viability - measures for agent-based manufacturing systems", *International Journal of Production Research*, Vol. 38, No. 3, pp. 607-624, 2000.
- [7] Sun J. , Zhang Y. F., and Nee A. Y. C., "A distributed multi-agent environment for product design and manufacturing planning", *International Journal of Production Research*, Vol. 39, No. 4, pp. 625-645, 2001.
- [8] Cohen, Y. and Bidanda, B., "A discrete control modeling technique for automated industrial systems", *Proceedings of the Embedded Computing Conference (ECC-96)*, Paris, France, pp. 279-287, 1996.
- [9] Cohen, Y. and Bidanda, B., "A new discrete control modeling technique for automated industrial systems" *Technical Report 97-2*, Dept. of Industrial Engineering, University of Pittsburgh, 1997.
- [10] Jeng, M. D. and F. DiCesare, "Synthesis using resource control nets for modeling shared resource systems", *IEEE Transactions on Robotics and Automation*, Vol. 11, No. 3, pp. 317-327, 1995.
- [11] Murata, T., "Petri nets: properties, analysis, and applications", *Proceedings of the IEEE*, Vol. 77, No. 4, pp. 541-580, 1989.
- [12] Babayan A. and He D., "Solving the n -job 3-stage flexible flowshop scheduling problem using an agent-based approach", *International Journal of Production Research*, Vol.42 , No. 4, pp. 777-800, 2004.
- [13] Shin M. and Jung M., "MANPro: mobile agent-based negotiation process for distributed intelligent manufacturing" *International Journal of Production Research*, Vol.42 , No. 2, pp. 303-321, 2004.

Performance of CBR and TCP Traffics in Various MANET Environments

Z. M. Yusof, J.A. Flint and S. Datta

Department of Electronic and Electrical Engineering
Loughborough University
LE11 3TU, UK

Abstract-Many MANET Routing Protocols have been made available to suit the numerous possible scenarios created from robust mobility environments. This paper describes the performance analysis of CBR and TCP traffic using the selected routing protocols which can be used for reference in the future performance analysis of MANET. Simulation results have also shown the difference characteristics of the MANET routing protocols where the on-demand protocols performs better than the proactive protocols in the environments with high density and fast moving nodes.

I. INTRODUCTION

The Mobile Ad hoc network (MANET) [1] is a collection of nodes which move independently and communicate between points by using intermediate nodes as routers. Initially developed for military use [2], MANET now has numerous civil applications due to the advance in use of mobile telephone and GPS systems. Its ability to enable distributed applications among nodes in environments without infrastructure makes it an attractive area to research and one area focused on in this paper is the routing protocol performance in a robust environment.

Since each node handles its own routing procedure, MANET performance is greatly affected by the density and speed of the nodes [3]. Various types of routing protocols are available to support the many possible scenarios generated by ad hoc applications which involve the generation of traffic from the likes of UDP and TCP data packets.

There are a variety of MANET protocols and ways to classify them. The most popular classifications are the Proactive or Table-driven, and Reactive or On-Demand which are becoming the commonly used routing strategies [4]. The Proactive routing protocols at each node maintain consistent and up-to-date routing information to all nodes while the Reactive routing protocols create routes as and when required. The three routing protocols which have been selected for the simulations in this paper are the DSDV, DSR and AODV.

A. DSDV

Destination-Sequenced Distance Vector (DSDV) is a proactive protocol [5] which exchanges routing information periodically allowing each node in the network to maintain a routing table in which all possible destinations within the

network and number of hops to each destination is recorded. The drawback of this update procedure is that it increases the volume of control traffic and adversely affects the network. It becomes difficult to maintain the routing table properly when the number of nodes in a network gets larger and the mobile nodes move around quickly.

B. DSR

Dynamic Source Routing (DSR) is a reactive routing protocol where [6] node sends packets to a destination according to the routing information contained in its route cache. It initiates route discovery if there is no route information to destination by broadcasting a route request packet (RRP) which contains the address of the destination along with the source node address and a unique identification number. If a node that does not know the route to the destination receives the RRP, it adds its own address to the route record of the packet and then forwards the packet to the next node. Then the destination node or a node that knows the route to the destination sends back the route reply.

C. AODV

Ad Hoc On-Demand Distance-Vector Routing (AODV) [7] is a source-initiated on-demand-driven protocol. It minimizes the number of required broadcast by creating routes on an on-demand basis and not maintaining a complete list of routes. When a source wants to send a message to some destination node and does not already have a valid route to that destination, it initiates a path-discovery process to locate the other node by broadcasting a route request (RREQ) packet to its neighbours. The nodes that receives the RREQ packet then forward the request to their neighbours, and this process repeats until the RREQ packet reaches either the destination or an intermediate node that knows the route to the destination.

II. SIMULATION EXPERIMENT SETUP AND METRICS

The simulation phase is often the required step of the whole MANET deployment. Ideally real measurements should be made at the receiving node but it is not really viable because of too many attributes to consider. Simulation software provides basic propagation models like free space (FRIIS) and shadowing, and also provide the means to create non extended

model to support any specific environment. In this paper a Rayleigh Fading channel model is also included as part of the simulation.

Network Simulator 2 or NS2 [8] is a discrete event driven simulator targeted at networking research, which provides support for simulation of TCP, routing, and multicast protocols over both wired and wireless networks. Rice Monarch Project [9] has made extensions to the ns-2 network simulator that enable it to accurately simulate mobile nodes connected by wireless network interfaces, including the ability to simulate multi-hop wireless ad hoc networks. NS2 has been used for all the simulations done for this performance analysis.

A. Simulation Parameters

The purpose of the simulations is to compare the performance of ad hoc routing protocols in various conditions where the nodes can be in a stable, moderately stable and highly robust scenario. The AODV, DSR, both On Demand protocols, and DSDV the Proactive protocol are the three protocols being simulated. The results enable us to establish the theories of the ad hoc network and also be made as the baseline to refer to in the following stages of simulations.

Both Continuous Bit Rate (CBR) and Transmission Control Protocol (TCP) traffic sources were applied using the same parameters throughout the simulations. This approach allows comparisons to be made of the performance of the routing protocols in various conditions.

The classifications of scenarios are based on the number of nodes which are 20, 50, and 100 for low, medium and high number of nodes respectively, and the speeds are 5, 15, and 25 metres per second (ms) for low, medium and high respectively which covers a range of simulation conditions. Nine scenarios are created for the simulations with the combination of number of nodes and speeds. The combination details are listed in Table I.

The mobility model uses the random waypoint model in a rectangular field with a size of 1500 m x 1000 m for the CBR and TCP traffic simulations. Transmission range for each node is assumed to be uniform and is limited to 250 m in the no fading case. Each packet starts moving from a random location to a random destination with the defined speeds. Once it reaches the destination, it goes to another random targeted node after a pause of 1.00 second. Each simulation runs for 900 simulated seconds.

TABLE I
SCENARIO DETAILS

	<i>Scenario</i>	<i>No. of Nodes</i>	<i>Node Speed (m/s) / (km/h)</i>
1	Low Node/Low Speed (LNLS)	20	5/18
2	Low Node/Med Speed (LNMS)	20	15/54
3	Low Node/High Speed (LNHS)	20	25/90
4	Med Node/Low Speed (MNLS)	50	5/18
5	Med Node/Med Speed (MNMS)	50	15/54
6	Med Node/High Speed (MNHS)	50	25/90
7	High Node/Low Speed (HNLS)	100	5/18
8	High Node/Med Speed (HNMS)	100	15/54
9	High Node/High Speed (HNHS)	100	25/90

B. Performance Metrics

The performance was evaluated using the following metrics:

- i. *Packet delivery ratio*: is the ratio of data packets sent by the source node to those actually being received by the destination node. This is done by counting the number of sent and received packets at the routing agent (AGT) from the NS2 trace file.
- ii. *Overhead packet*: is the number of routing packets transmitted reaching the router and the MAC layer. This is done by counting the packets that reached the router (RTR) and the MAC layer (MAC) of the receiving nodes from the NS2 trace file.

Packet delivery is very effective for best-effort traffic like CBR. Routing overhead evaluates the efficiency of the routing in the protocols while MAC overhead measures the effective use of wireless medium by the data traffic.

III. SIMULATION RESULTS – NO FADING

A. CBR-traffic

The data packet is fixed at 512 bytes at the rate of 4 packets per second. The number of active connections is half the number of nodes.

The simulation results are plotted as follows:

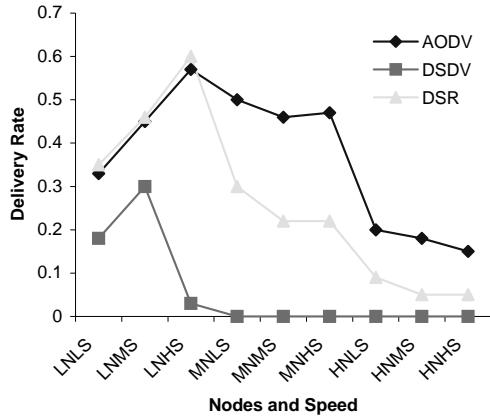


Fig. 1. Graphic representations for the CBR Packets Delivery Rate for Various Speed and Nodes

While DSR and AODV share the on-demand behaviour in that they initiate routing activities only in the presence of data packets in need of routing, many of their routing strategies are different. In particular, DSR uses source routing, whereas AODV uses a table-driven routing framework and destination sequence number [10]. The simulation results show that AODV and DSR have almost identical performance when the nodes and sources are low, with DSR slightly edged AODV. By using source routing, DSR has access to a significantly greater amount of routing information than AODV through the caching. Also, in DSR, using a single request-reply cycle, the source can learn routes to each intermediate node on the route in addition to the intended destination. Each intermediate node can also learn routes to every node on the route [11].

As the simulation load gets increasingly heavy, AODV maintains its performance while DSR begins to decline towards the end of simulation as it turned to be at the most strained condition. This is due to the DSR caching becoming less effective at higher speeds where the cached information became stale much faster [12].

The proactive protocol DSDV was unable to proceed in a strained scenario where it could only managed to work half way in the low-node high-speed scenario and unable to proceed in the further robust scenario. The nature of proactive protocol does not work well in a dynamic scenario since the routing table could not be updated quickly enough, thus making the entries to stale, causing the packets to be forwarded over broken links. Since DSDV maintains only one route per destination, each packet that the MAC layer unable to deliver was being dropped since there were no alternative routes.

B. TCP-traffic

TCP is a protocol which guarantees reliable and in-order delivery of sender to receiver data and which is why the simulation results show a very high delivery rate. In the scenario of minimum nodes and lower speed the delivery rates are almost 100% with possibilities of packets failed to arrive due to them being dropped as the simulation ended. Nevertheless, a 2% reduction of delivery rate would have a significant impact for TCP-traffic transmission. The trend clearly shows that the higher the speed causes a reduction in delivery rate despite of the reliable mechanism of TCP. The results show high and relatively stable results for both AODV and DSR routing protocol.

TABLE II
TCP PACKET DELIVERY RATE FOR VARIOUS SPEED AND NODES

	AODV	DSDV	DSR
LNLS	0.99	0.99	0.99
LNMS	0.98	0.0	0.99
LNHS	0.98	0.0	0.99
MNLS	0.98	0.0	0.99
MNMS	0.97	0.0	0.99
MNHS	0.97	0.0	0.99
HNLS	0.98	0.0	0.99
HNMS	0.96	0.0	0.97
HNHS	0.95	0.0	0.98

IV. SIMULATION WITH RAYLEIGH FADING

Multipath propagation can cause fast fading to occur when a transmitter and receiver are surrounded by objects which reflect and scatter the transmitted energy causing several waves to arrive at the receiver via different routes. Both Rayleigh and Ricean distributions are the statistical model which provide good approximation on the effect of a propagation environment for mobile fading channel for No Line of Sight (NLOS) and Line of Sight (LOS) situations respectively. This model assumes that the power of a signal that has passed through a communication channel will vary randomly [13].

According to H. Bai et. al [14] the best simulation model for a dynamic scenario like in a highway is by including the Rayleigh fading in the propagation model. In this simulation the Rayleigh and Ricean fading extension module [15] is used as the propagation model in NS2. The formula for Rayleigh distribution is very much similar and if the Rice factor k is set to zero the two distributions are identical. This module uses Ricean distribution by considering Rayleigh fading as a case where the magnitude component is zero.

This modelling uses a pre-computed dataset containing the components of a time-sequenced fading envelope. It is used as a lookup table during simulation run to model a wide range of parameters. Adjusted parameters are the time-average power,

P, the maximum Doppler frequency, f_m , and the Ricean K factor. It is also assumed that the small scale fading envelope is used to modulate the calculations of a large scale propagation model like two-ray ground or some other deterministic model.

The simulation shows a consistent set of results with the earlier simulations without the fading. It shows slightly lower delivery rates reflecting a more accurate result. The set of results labelled rcAODV and rcDSR are shown alongside the previous results for comparison in Fig. 3.

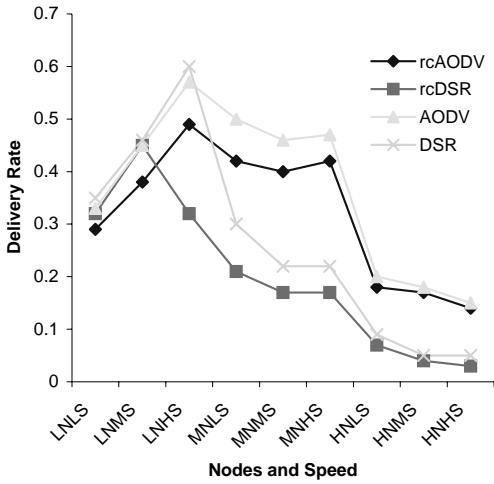


Fig. 2. Graphic representations for the CBR Packets Delivery Rate for Various Speed and Nodes using the Rayleigh Fading Model

A. Overhead Performances

The measurements of overhead show the efficiency of the routing and the effective use of wireless medium by the data traffic. This section provides the overhead analysis from all the simulation results. The actual results are presented in Figures 3 -5.

Basically all the results show similar pattern with the overheads for both routing and MAC packets increased as the number of nodes and speed increased. TCP produced less overhead compared to both CBR packets.

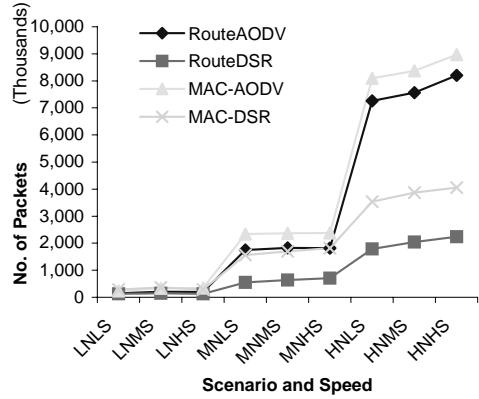


Fig. 3. Routing and MAC Overhead for CBR traffic

AODV requires more overhead than DSR because each of its discoveries typically propagates to every node in the network. DSR has the lowest number of packets but higher than AODV if measured in bytes. Although DSDV unable to complete the simulation, it has approximately constant overhead regardless the speed due to its proactive nature.

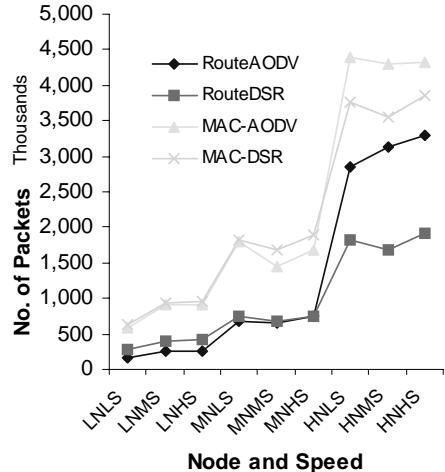


Fig. 4. Routing and MAC Overhead for TCP traffic

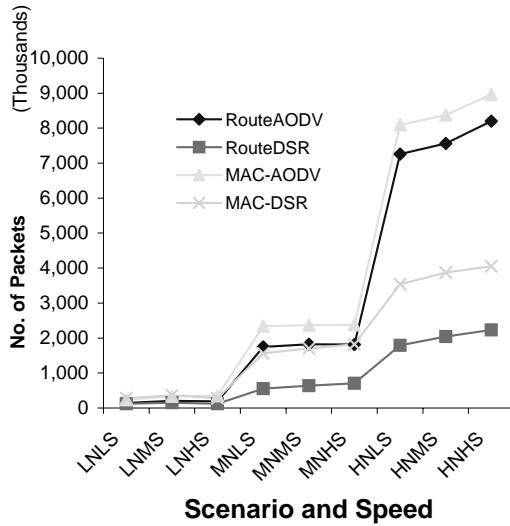


Fig. 5. Routing and MAC Overhead for CBR traffic with Fading

V. CONCLUSION

The simulation exercises have shown that overall AODV performed better in the majority of the scenarios with CBR traffic showing more variable results when compared to TCP. DSDV managed only to perform well in a more predictable physical arrangement of nodes. TCP in general produces a lower MAC and routing overhead when compared to CBR. Of the on-demand routing protocols our experiments clearly demonstrate that the MAC and routing overheads for AODV are much higher, however much better performance in delivery route can be achieved.

The incorporation of Rayleigh Fading channel in the simulation is expected to give some insights on the effect of fading for future work which is the performance of routing protocols in a vehicular environments.

REFERENCES

- [1] IETF "Mobile Ad hoc Network (MANET)," vol. 2004, pp. 3, 24 March 2006. 2006.
- [2] C. E. Perkins, *Ad Hoc Networking*. first ed. New Jersey, USA: Addison-Wesley, 2001.
- [3] T. D. Dyer and R. V. Boppana, "A comparison of TCP performance over three routing protocols for mobile ad hoc networks," in *ACM Symposium on Mobile Ad Hoc Networking & Computing*, 2001
- [4] S. J. Lee, J. Hsu, R. Hayashida, M. Gerla and R. Bagrodia, "Selecting a Routing Strategy for Your Ad Hoc Network," *Elsevier Computer Communications*, vol. 26, pp. 723-733, 2003.
- [5] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proceedings of the Conference on Communications Architectures, Protocols and applications*, 1994, pp. 234 - 244.
- [6] D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Kluwer Academic Publishers*, 1996.
- [7] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the Second IEEE Workshop on Mobile Computer Systems and Applications* 1999, pp. 90.
- [8] Information Sciences Institute University of Southern California "The Network Simulator NS-2," vol. 27 October 2004, pp. 2, 2006.
- [9] The Rice University Monarch Project "Rice Monarch Wireless and Mobility Project Extension to NS-2," vol. 2004, 5 Nov 2000. 2000.
- [10] C. E. Perkins, E. M. Royer, S. R. Das and M. K. Marina, "Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks," *IEEE*, vol. 8, pp. 16-28, 2001.
- [11] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 1998, pp. 85 - 97.
- [12] M. K. Marina and S. R. Das, "Impact of Caching and MAC Overheads on Routing Performance in Ad Hoc Networks," *Elsevier Computer Communications*, vol. 27, pp. 239-252, 2003.
- [13] S. R. Saunders, *Antennas and Propagation for Wireless Communication Systems*. ,first ed.England: John Wiley & Sons Ltd, 2001.
- [14] H. Bai and M. Atiquzzaman, "Error Modeling Schemes for Fading Channels in Wireless Communications: A Survey," *IEEE*, vol. 5, 2003.
- [15] R. J. Punnoose, P. V. Nikitin and D. D. Stancil, "Efficient simulation of ricean fading within a packet simulator," in *Vehicular Technology Conference 2000* 2000, pp. 764-767.

Index

- 3-D reconstruction process, 199
3G Networks, 453–455, 457
3GPP, 437–442
- Accelerometer, 85, 86, 501–504
Accumulated information, 493–496
Adaptive control, 257, 259, 261
Adaptive mechanism, 376
Adaptive model, 259, 260
Adaptive modulation, 511, 512
Admittance controller, 294, 296–298
Aeronautic profiles, 136–140
Analitic model, 85, 87
Analog computer, 449, 450
Anomaly detection, 235, 530
AODV, 97, 98, 419–424, 543, 545
Application development, 101, 507–509
Arbitrarily-oriented, 199, 246, 260, 465
ARIADNE, 353–357
Artificial neural network, 34, 409, 463–465
ASDS, 287–291
Asymmetric cryptography, 299
Asynchronous Connection-Less, 385
ATIM window, 316
ATM, 107, 149
Authenticated encryption, 459–461
Authenticating MAODV, 299, 301–303
Autocorrelation function, 58, 59, 219, 220
Automatic Target Recognition, 493
Autonomous agents, 527, 528–531, 532
Autonomous Control Mechanism, 282–284
- Banyan networks, 107
Baseline networks, 54, 107, 108, 530
Base Station Controllers, 365–368
Bayesian classifier, 125
Bearings diagnosis, 141, 142, 145, 146
Bipolar transistors, 75, 76
Bispectrum, 145–148
BISR, 501–503
Bit error rate, 33, 248, 311, 375, 458, 512, 514
Blade manufacturing, 135, 137, 139
Block cipher, 241, 369, 459, 460
Block-cipher mode-of-operation, 459
Blowfish, 241–244
Bluetooth, 61, 176, 385–387
BPSK, 512, 598
Brute force attack, 353, 355, 356, 371
- CAD model, 200, 261, 293
Carrier sense ranges, 311, 312
- CBC-LP decryption, 190, 191
CBC-LP encryption, 190, 191
CBR, 169, 302, 312, 543–545
CDMA, 366, 367, 511
Cellular telephony, 365
Change detection, 229, 234
Charging circuit, 413, 414
Client/server, 5, 79, 80, 83, 90, 173, 345–347, 525, 526
Closed loop, 101, 103, 119, 121, 123, 124, 257, 259, 260, 397, 399, 453, 454, 481–485
Clustering, 125, 206, 426–428, 503, 532
Clustering algorithm, 245–249
Clustering coefficient, 428–430
CMOS circuit, 401, 403, 404
CNC, 257, 258
Code Division Multiple Access, 367
Command charging circuit, 413–415
Commercial Off-The-Shelf, 329
Communicating Sequential Processes, 523–526
Component failures, 323, 326, 327
Computational complexity, 231, 269, 271, 274, 299–301, 375, 472, 481
Computational process, 67, 230
Computation offloading, 27–29
Congestion control, 405–407, 470
Connection admission control, 471
Conservative distributed simulation, 443–448
Constrained optimization, 34
Context-awareness, 379
Continuous model, 257, 258, 261
Continuous time domain model, 113, 115
Controller design, 481–485
Control system, 37, 40, 89, 183, 257, 275, 276, 397, 481, 484, 539
Convergence Module, 62–64
Copper vapor laser, 413, 414, 416
COSMOS, 135, 136
Crossbar switches, 107
Cross-layer RRM, 31, 33, 34
Cryptography, 6, 8, 187–192, 299, 353, 369
Cumulative distribution, 55, 56, 59, 220
Curvelet coefficient, 305–307
Curvelet transform, 305, 306
Cyclostationary, 141–144
- Data acquisition, 86, 89, 329
DC-BLOT, 33, 35
DC motor control, 397, 399
DDoS, 235–240
Decryption, 6, 191, 241, 370

- Defective rolling element, 141, 145–147
 Defect simulation, 501
 Denial of service, 83, 235, 354, 356, 523
 Differential drive robot, 37, 39, 41
 Differential image, 229–234
 Digital adaptive filter, 269, 271, 272
 Dim target detection, 493–496
 Directional antennas, 165–170
 Discrete cosine transform, 305
 Discrete fourier transform, 49
 Discrete time domain, 481–485
 Distributed control application, 94, 223
 Distributed denial-of-service, 235–239
 Distributed Network Protocol, 333, 337, 340
 DNP3, 335, 337, 338, 340, 341
 DNPsec, 337–341
 DNPsec functionality, 337, 340
 Docking simulations, 70–72
 DPMAC protocol, 168
 DRBTS, 318
 Driver system, 287–291
 Droplet acceleration, 211–216
 DSDV, 419–424, 543, 545
 Dummy controller, 383
 Dynamic Channel Allocation, 409
 Dynamic distribution, 43, 527–532
 Dynamic source routing, 165, 541
- Ebers-Moll model, 75, 76
 E-democracy, 79, 80, 83, 84
 ELK mechanisms, 359
 Embedding algorithm, 306, 307
 Encryption, 6, 361, 370, 459, 526
 Energy recovery, 413, 414
 Entropy, 236–240, 381
 Equilibrium state, 404–407
 Euclidean distance, 129, 246
 Event connections, 227, 228
 E-Vote, 79, 80
 Exactly periodic subspace decomposition (EPSD), 49, 50
- Factory automation, 223
 Failure injection, 323, 325
 Fairness, 32, 33, 311, 313, 314, 316, 405, 406
 Fairness enhancement, 311–315
 False negatives, 235, 236, 489, 490, 491, 528
 False positives, 235, 236, 489, 490, 491
 Fast Fourier transform, 49
 Fast mobile , 438
 FEA analysis, 85, 87
 Feature extraction, 131–133
 Feedback system, 397, 399
 FER algorithm, 313–315
 FETT, 131–133
 Filter adaptation, 272
- Firewall, 79, 82, 84, 236, 343–346, 529
 Fly Back converter, 413, 414
 Force-feedback, 293, 294
 Force-reflecting, 293–298
 Forecasting, 171, 463
 Fractional order hold, 257–260
 Frequency domain analysis, 119–121
 Function block, 223–225
 Fuzzy logic, 17
 Fuzzy logic network, 17–19
- Gaussian pulse, 401–403
 Gauss-Lucas theorem, 157
 Generalized transfer functions, 275, 277–279
 Genetic algorithms, 199–204
 Geographical Information System, 453, 455, 458
 Geometric rectification, 113
 GoS, 149–154
 Gradient filters, 231–233
 Group-based mobility, 425–427
 GSM, 365–368
 Guarantee of Service, 149
- Handoff management, 431–435
 Haptic feedback, 67–72
 Hardware-in-the-loop, 89
 Hearing disabilities, 347, 349, 351, 352
 Herst parameter, 172, 173
 Hierarchical cellular network, 431, 432
 Higher-order statistics, 145
 High frequency applications, 401–404
 Hint key distribution, 353, 359, 362
 Home location register, 365
 Honeypots, 49–54
 Hopfield Neural Network, 409–412
 HORSEI2, 299–302
 HORSE again, 299, 300
 HTTP, 80, 82, 219, 344, 345
 Human interface tool, 505–509
 Human machine interface, 333
 Hurwitz polynomials, 155, 157
 HWM, 419, 421, 423, 424
 Hybrid algorithm, 1–4
 Hybrid network, 95
 Hysteresis losses, 389, 391
- Identifiability, 195, 196
 IEC61499, 223, 224, 226, 228
 IEEE 802.11, 24, 165, 168, 175, 311, 318, 385, 524
 IEEE 802.11b/g, 287, 289, 290
 IGBT, 413, 414, 416
 Image compression, 269–273
 Image orientation, 113–116
 Image processing, 125, 131–133
 Implementation complexity, 31
 Independent component analysis, 305

- Induction heating, 389, 390, 392–394
Industrial automation, 535–539
Industry scheduling, 263–266
Information security, 343–345
Infrared image, 493, 495, 496
Initialization vector, 189, 190, 369–371
Integer programming, 365, 368
Intellectual property, 11, 16, 172
Intelligence Equipment Devices, 337
Intelligent agents, 263, 264
Interference, 141–144, 176
International Organization for Standardization, 175
Internet traffic, 219
Intrusion detection, 79, 487, 488, 490, 527, 530, 531, 532
Inverse kinematics, 104, 106, 295, 296
IP, 11–13, 15–16, 61, 63, 65, 81, 83, 149, 151, 236, 345
IPv6, 64, 95, 437, 439
IRS satellites, 113, 114
ISM, 175, 176, 178, 179, 291, 385, 387
ISP, 235–240
Iterative method, 493–496
- Kalman filter, 381, 383
Kerberos, 525, 526
Key distribution, 353, 355–358, 361, 523, 524
Key-Exchange Protocol, 523, 524
Kinematics, 101, 103, 104, 106, 295, 296
- LabMap, 89, 91, 92, 94
Laparoscopy, 205
Latency, 93, 96, 98, 302, 323, 325, 532
LDPC code, 497–499
Legacy 802.11, 316
Length-preserving, 187–192
Level of privacy, 379, 380, 383, 384
Lightweight technologies, 5, 8
Linear approximation, 172
Linear differential equation, 12, 449
Linear feedback shift registers, 369
Linearization, 1, 479
Linear matrix inequalities (LMI), 119, 122, 123
Linear transformation, 113, 125, 141, 206, 463
Link state approach, 469
LLC, 175, 251
Load impedance modeling, 389, 390, 392, 393
Location communication system, 381
Location prediction engine, 379, 382–384
Location privacy, 65, 379–384
Logical Link Control, 175
Logical processes null messages, 443
Logo watermarking, 305, 307, 308
Long-range dependence, 55, 58, 219
Lookahead, 443–448
- LPSRA, 205
Lyapunov function, 35, 155
- MAC, 33, 89, 97, 165, 166, 168, 169, 175, 488, 545
Macro Model, 282–284
Mahalanobis distance, 125
MANET Routing, 95, 98, 419–421, 541
Man-in-the-middle attack, 353, 354, 356
Man Machine Interaction, 505
Maple, 123, 277–280
Markov Chain, 11, 13, 14, 56, 58, 107
Markov Modulated Poisson Process (MMPP), 55, 56, 57
Mathematical model, 103, 110, 160, 371, 394, 443–445, 476–480
Mean curvature, 389–394
Mechanical press, 85, 87
Media framework, 27–30
Media middleware, 29, 30
Medium access control, 33, 165, 166, 175, 251, 311, 598
MEMS, 501–506
Microfabrication, 501
Middleware, 27, 29, 89, 90, 92–94
Migration interval, 53, 54
Milling Forces, 257–261
MIMO, 32, 277, 279, 497
Misbehaviour classification, 317, 320, 321
Mobile, 27, 39, 43, 44, 61, 62, 64, 65, 97, 101, 103, 104, 165, 169, 287, 294, 299, 317, 318, 347–351, 365, 367, 368, 379, 381, 382, 409, 419–421, 425, 426, 431, 437
Mobile Ad-hoc Networks (MANET), 95–98, 165, 168–170, 299
Mobile communication, 274, 347–351
Mobile network design, 365–368
Mobility management, 63, 65
Mobility models, 95–97, 169, 419, 421, 424–427, 434
Mobility prediction, 381, 383, 453, 455, 456
Modeling and simulation, 101, 337, 467
Modeling trust, 317–321
Model of component, 159, 160
Model of function, 159, 160
Molecular docking, 67, 71, 72
Monte Carlo method, 501–503
Motion control, 296, 382, 383
MPI layer, 228
MPLS, 149–152, 154
Multi-agent system, 263–265
Multi-antenna technique, 497
Multicast, 89–91, 93, 94
Multicasting, 89–91, 299
Multihoming, 61, 62, 66
Multi-hop, 245, 311, 542
Multilevel flow models, 505–510

- Multilevel flow models studio, 505–510
 Multisim simulator, 449
 Multistage interconnection networks, 107
 Mutation, 200, 203, 267, 276, 514
 Mutual defection, 281, 286
 Mutual repairing, 281
 Navigation, 43, 44, 453
 Network measurement, 323
 Network performance, 323, 324, 337, 425, 427, 428, 430
 Network services, 323, 325, 419
 Networks-on-chip, 11–16
 Network topologies, 17, 31, 32, 150, 247, 248, 323, 324, 326, 339, 341, 423
 Network traffic, 56, 89, 94, 98, 219
 Neural network, 1–3, 33–35
 Newtonian mechanics, 67
 Non-commutative polynomials, 275, 276, 278
 Nonlinear control systems, 275, 276
 Non-linearities, 119, 122, 136
 Nonlinear systems, 277, 278, 281, 282, 465
 Null message algorithm, 443, 446, 447
 Null message exchange, 443, 444
 Obstruction removal, 131–133
 OEM, 475–479
 OFDM, 31–33, 288, 513, 515
 OMAP architecture, 27, 28
 On-demand protocols, 97, 541
 On-demand routing protocols, 165, 170, 356, 545
 Online technique, 49–54
 Operations research, 11, 17, 40, 219, 263, 265, 272–274, 347–349
 OPNET, 165, 168, 169, 323, 325, 337
 Optimal location, 126, 128, 129
 Optimal routing, 469, 470, 472
 Optimization, 23, 33–35, 69, 119, 154, 201–203, 266, 370, 445, 464, 472, 511, 513
 Optimization algorithm, 257, 466, 513
 OreTools, 27, 278, 280
 Orthogonal frequency–division multiplexing, 31, 32
 Orthogonal transform, 269–271
 OSPF protocol, 323, 326
 Packet latency, 302
 Packet loss concealment, 375–377
 Packet switching, 107, 110, 149–152
 Parallel computer systems, 107
 Parallel robots, 101–106
 Partially-overlapped, 199–201, 203
 PASS-card, 5, 7, 8
 Passive control, 70–72
 Passivity, 155–157
 PD controller, 119–121, 296, 297
 P-domain, 481, 482, 485
 Peer-to-peer, 89–91
 Performability estimation, 323–325, 327
 Performance analysis, 55, 56, 107, 109, 168–170
 PIC-microcontroller, 397–399
 Piconet, 385, 387
 Piezoelectric, 85, 86
 Point-to-point, 176, 178–180
 Predistortion scheme, 1, 3, 4
 Prevention systems, 79
 Preventive protocol, 165
 Prisoner’s dilemma, 281, 282, 286
 Programmable logic controllers, 223, 535
 Proxy signature, 193–196
 Pulsed power supply, 413
 Pyramidal decomposition, 269
 Quadrature amplitude modulation, 1, 3, 32, 512
 Quality of service (QoS), 31, 32, 89–94, 149, 171, 311, 325, 379, 432, 453, 458, 469, 470, 527
 Radial basis function, 1–4
 Range images, 199–204
 Rayleigh fading, 32, 35, 543–545
 RBAC, 329–335
 Real-time, 27, 28, 30, 34, 35, 43, 67, 92, 111
 Reconfigurability, 101, 227
 Recovery oriented computing, 281
 Reduced order controller, 481–485
 Registration, 62, 172, 199–204
 Remote sensing, 113
 Remote Terminal Units, 337
 Replay attack, 353, 356, 524
 Rescue Frames, 311, 313–315
 Resonant tunneling diode, 75, 76
 RFID, 475–480
 RGB space, 125–129
 RIP protocol, 326, 327
 Robot arm, 205
 Robotic applications, 37, 397, 399
 Robust stability, 119–121
 Role-Based Access Control, 329, 330
 Routing protocols, 95–98, 165, 245
 RTS/CTS, 168, 312
 Runge-Kutta method, 35
 Safe logon, 5–9
 SCADA systems, 331–335
 SCARA robot, 293–295, 298
 Scheduling, 27, 31, 33, 166, 223–225, 263, 264, 266, 536
 Seamless handoff, 437, 442
 Secret key, 6, 187, 189, 190, 193, 196, 301, 302, 353–355, 359, 361, 362, 369, 523

- Secure communication, 5, 8, 319, 354, 359, 488, 523, 524
 Security attacks, 355, 357
 Security policy, 329, 330, 343
 Security solutions, 524–526
 Segmentation, 125, 126, 129, 130, 205, 206, 209, 270
 Self-configuring, 287, 289–291
 Selfish agents, 281, 282, 286
 Self-learning, 381
 Self-repairing network, 281–284
 Self-similarity, 55, 107, 171, 173, 219
 Semantics, 223–227
 Sensor cluster, 247, 487–491
 Sensor position, 246, 247
 Sensor reliability, 317
 Shadow removal, 131, 132
 Sheet metal forming, 135, 139, 140
 Simple intrusion detection, 487, 488, 490
 Simulation, 4, 19, 20, 45, 46, 51, 65, 66, 68, 69, 72, 109–111, 141, 169
 Skew distribution, 236, 245, 247, 249
 Skin effect, 389, 393
 Slithering motion, 43, 45
 Small world communication, 426
 SnakeBOT, 43–46
 Snake-like robot, 43–46
 SNR, 493, 496, 498, 499, 511, 512
 Spectrum pyramid, 271–276
 Speech disabilities, 347–351
 Speech quality, 375, 376, 377
 Stability, 17, 20, 35, 72, 119, 121, 135, 155, 481, 482
 Stability conditions, 58, 59, 119–121, 123
 Steerable pyramids, 305
 Stereo images, 114
 Stochastic communication, 11, 12, 14–16
 Stochastic modeling, 13, 14, 16
 Stochastic signal processing, 381
 Supply chain, 475, 476, 479, 480
 Switching elements, 107
 Symmetric cryptography, 187, 301, 369, 523
 Synchronous Connection Oriented, 385
 System-on-chip, 11
 Tail index, 219–222
 Task partitioning, 30
 TCP/IP, 28, 91, 150, 175
 TCP sockets, 89, 150
 TDMA, 367
 Telemanipulation, 293–295
 Teleoperation, 295, 296, 298
 Telnet server, 344
 Thresholding, 207, 520
 Throughput, 31, 33, 35, 66, 107–111, 167, 169, 170, 314, 315, 317, 389, 423, 429, 430, 432, 488, 511
 Time-constrained task scheduling, 27
 Time Division Multiple Access, 367
 Topology, 16, 49, 51, 101, 247, 327, 328, 342, 343, 414, 426, 444, 453, 455, 472, 487
 Transfer function, 120, 155, 260–263, 277–280, 282, 481–483, 484
 Transient response, 15, 259, 260, 262, 263, 487
 Transport layer, 61–65, 89, 91, 150
 Trust formation, 317, 319–321
 TTY, 347, 349
 UDP, 50, 52–54, 90, 91, 94, 98, 312, 427, 541
 Underneath vehicles, 517, 521
 Uneven terrain, 43, 44
 Unforgeability, 195, 196
 Unicast, 89, 91–93, 313, 420
 Uniform repair rate, 281, 282
 Universal hash function, 459
 Universal Mobile Telecommunication System, 437, 453
 UTMS, 437
 Vertical handoff, 431–433, 435, 437
 Video conferencing, 28, 131
 Video streaming, 29, 32, 385, 386, 431
 Video transmission, 29, 385–387
 Virtual circuits, 149
 Virtual environment, 293, 295
 Virtual model, 101, 103–105
 Virtual Private Networks, 149
 Voice over IP protocol (VoIP), 55–60
 VPN, 149
 VRML, 293
 Walsh-Hadamard transform, 272
 Waterjet technology, 181–184
 WCDMA, 453–455
 Web security, 79–81, 84
 Web Server, 8, 79–84, 219, 236, 530
 Web services, 5, 8
 Wegman-Carter authentication, 459
 Wi-Fi, 175–177, 179, 289, 313, 316, 385, 387
 Wireless scheduling, 31, 33
 Wireless sensor networks, 247–249, 251, 317, 353, 359, 487, 490, 497
 WLAN, 175, 289, 293, 377–379, 385, 387, 431–435, 437, 439–442
 WSN, 317–321
 Zero order hold, 257, 258, 482, 484