

Tarek Sobh
Khaled Elleithy
Ausif Mahmood *Editors*

Novel Algorithms and Techniques in Telecommunications and Networking

Novel Algorithms and Techniques in Telecommunications and Networking

Tarek Sobh · Khaled Elleithy ·
Ausif Mahmood
Editors

Novel Algorithms and Techniques in Telecommunications and Networking



Editors

Tarek Sobh
University of Bridgeport
School of Engineering
221 University Avenue
Bridgeport CT 06604
USA
sobh@bridgeport.edu

Khaled Elleithy
University of Bridgeport
School of Engineering
221 University Avenue
Bridgeport CT 06604
USA
elleithy@bridgeport.edu

Ausif Mahmood
University of Bridgeport
School of Engineering
221 University Avenue
Bridgeport CT 06604
USA

ISBN 978-90-481-3661-2 e-ISBN 978-90-481-3662-9
DOI 10.1007/978-90-481-3662-9
Springer Dordrecht Heidelberg London New York

Library of Congress Control Number: 2009941990

© Springer Science+Business Media B.V. 2010

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.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This book includes the proceedings of the 2008 International Conference on Telecommunications and Networking (TeNe).

TeNe 08 is part of the International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 08). 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 08 is a high-caliber research conference that was conducted online. CISSE 08 received 948 paper submissions and the final program included 390 accepted papers from more than 80 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 08 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 and we are confident that you will find the papers included in this volume interesting and useful. We believe that technology will continue to infuse education thus enriching the educational experience of both students and teachers.

Tarek M. Sobh, Ph.D., PE

Khaled Elleithy, Ph.D.,

Ausif Mahmood, Ph.D.

Bridgeport, Connecticut

December 2009

Table of Contents

Acknowledgements	xiii
List of Reviewers.....	xv
1. Ip Application Test Framework	1
<i>Michael Sauer</i>	
2. Cross-Layer Based Approach to Detect Idle Channels and Allocate Them Efficiently Using Markov Models	9
<i>Y. B. Reddy</i>	
3. Threshold Based Call Admission Control for QoS Provisioning in Cellular Wireless Networks with Spectrum Renting	17
<i>Show-Shiou Tzeng and Ching-Wen Huang</i>	
4. Ontology-Based Web Application Testing	23
<i>Samad Paydar, Mohsen Kahani</i>	
5. Preventing the “Worst Case Scenario:” Combating the Lost Laptop Epidemic with RFID Technology	29
<i>David C. Wyld</i>	
6. Information Security and System Development	35
<i>Dr. PhD Margaretha Stoll and Dr. Dietmar Laner</i>	
7. A Survey of Wireless Sensor Network Interconnection to External Networks	41
<i>Agnius Liutkevicius et al.</i>	
8. Comparing the Performance of UMTS and Mobile WiMAX Convolutional Turbo Code.....	47
<i>Ehab Ahmed Ibrahim, Mohamed Amr Mokhtar</i>	
9. Performance of Interleaved Cipher Block Chaining in CCMP.....	53
<i>Zadia Codabux-Rossan, M. Razvi Doomun</i>	
10. Localization and Frequency of Packet Retransmission as Criteria for Successful Message Propagation in Vehicular Ad Hoc Networks	59
<i>Andriy Shpylchyn, Abdelshakour Abuzneid</i>	
11. Authentication Information Alignment for Cross-Domain Federations	65
<i>Zhengping Wu and Alfred C. Weaver</i>	
12. Formally Specifying Linux Protection.....	71
<i>Osama A. Rayis</i>	
13. Path Failure Effects on Video Quality in Multihomed Environments	81
<i>Karena Stannett et al.</i>	
14. Reconfigurable Implementation of Karatsuba Multiplier for Galois Field in Elliptic Curves	87
<i>Ashraf B. El-sisi et al.</i>	

15. Nonlinear Congestion Control Scheme for Time Delayed Differentiated-Services Networks 93
R. Vahidnia et al.
16. Effect of Packet Size and Channel Capacity on the Performance of EADARP Routing Protocol for Multicast Wireless ad hoc Networks 99
Dina Darwish et al.
17. Improving BGP Convergence Time via MRAI Timer 105
Abdelshakour Abuzneid and Brandon J. Stark
18. Error Reduction Using TCP with Selective Acknowledgement and HTTP with Page Response Time over Wireless Link 111
Adelshakour Abuzneid, Kotadiya Krunalkumar
19. Enhanced Reconfigurability for MIMO Systems Using Parametric Arrays 117
Nicolae Crișan, Ligia Chira Cremene
20. Modified LEACH – Energy Efficient Wireless Networks Communication 123
Abuhelaleh, Mohammed et al.
21. Intrusion Detection and Classification of Attacks in High-Level Network Protocols Using Recurrent Neural Networks 129
Vicente Alarcon-Aquino et al.
22. Automatic Construction and Optimization of Layered Network Attack Graph 135
Yonggang Wang et al.
23. Parallel Data Transmission: A Proposed Multilayered Reference Model 139
Thomas Chowdhury, Rashed Mustafa
24. Besides Tracking – Simulation of RFID Marketing and Beyond 143
Zeeshan-ul-Hassan Usmani et al.
25. Light Path Provisioning Using Connection Holding Time and Flexible Window 149
Fatima Yousaf et al.
26. Distributed Hybrid Research Network Operations Framework 155
Dongkyun Kim et al.
27. Performance of the Duo-Binary Turbo Codes in WiMAX Systems 161
Teodor B. Iliev et al.
28. A Unified Event Reporting Solution for Wireless Sensor Networks 167
Faisal Bashir Hussain, Yalcin Cebi
29. A Low Computational Complexity Multiple Description Image Coding Algorithm Based on JPEG Standard 173
Ying-ying Shan, Xuan Wang
30. A General Method for Synthesis of Uniform Sequences with Perfect Periodic Autocorrelation 177
B. Y. Bedzhev and M. P. Iliev

31.	Using Support Vector Machines for Passive Steady State RF Fingerprinting..... <i>Georgina O'Mahony Zamora et al.</i>	183
32.	Genetic Optimization for Optimum 3G Network Planning: an Agent-Based Parallel Implementation..... <i>Alessandra Esposito et al.</i>	189
33.	A Survey About IEEE 802.11e for Better QoS in WLANs..... <i>Md. Abdul Based</i>	195
34.	Method of a Signal Analysis for Imitation Modeling in a Real-Time Network	201
	<i>Igor Sychev and Irina Sycheva</i>	
35.	Simple yet Efficient NMEA Sentence Generator for Testing GPS Reception Firmware and Hardware..... <i>V. Sinivee</i>	207
36.	Game Theoretic Approach for Discovering Vulnerable Links in Complex Networks	211
	<i>Mishkovski Igor et al.</i>	
37.	Modeling Trust in Wireless Ad-Hoc Networks	217
	<i>Tirthankar Ghosh, Hui Xu</i>	
38.	Address Management in MANETs Using an Ant Colony Metaphor	223
	<i>A. Pachón et al.</i>	
39.	Elitism Between Populations for the Improvement of the Fitness of a Genetic Algorithm Solution	229
	<i>Dr. Justin Champion</i>	
40.	Adaptive Genetic Algorithm for Neural Network Retraining.....	235
	<i>C.I. Bauer et al.</i>	
41.	A New Collaborative Approach for Intrusion Detection System on Wireless Sensor Networks	239
	<i>Marcus Vinícius de Sousa Lemos et al.</i>	
42.	A Dynamic Scheme for Authenticated Group Key Agreement Protocol	245
	<i>Yang Yu et al.</i>	
43.	Performance Evaluation of TCP Congestion Control Mechanisms.....	251
	<i>Eman Abdelfattah</i>	
44.	Optimization and Job Scheduling in Heterogeneous Networks.....	257
	<i>Abdelrahman Elleithy et al.</i>	
45.	A New Methodology for Self Localization in Wireless Sensor Networks	263
	<i>Allon Rai et al.</i>	
46.	A Novel Optimization of the Distance Source Routing (DSR) Protocol for the Mobile Ad Hoc Networks (MANET)	269
	<i>Syed S. Rizvi et al.</i>	

47.	A New Analytical Model for Maximizing the Capacity and Minimizing the Transmission Delay for MANET	275
	<i>Syed S. Rizvi et al.</i>	
48.	Faulty Links Optimization for Hypercube Networks via Stored and Forward One-Bit Round Robin Routing Algorithm	281
	<i>Syed S. Rizvi et al.</i>	
49.	Improving the Data Rate in Wireless Mesh Networks Using Orthogonal Frequency Code Division (OFCD).....	287
	<i>Jaiminkumar Gorasia et al.</i>	
50.	A Novel Encrypted Database Technique to Develop a Secure Application for an Academic Institution.....	293
	<i>Syed S. Rizvi et al.</i>	
51.	A Mathematical Model for Reducing Handover Time at MAC Layer for Wireless Networks	299
	<i>Syed S. Rizvi et al.</i>	
52.	A Software Solution for Mobile Context Handoff in WLANs	305
	<i>H. Gümuşkaya et al.</i>	
53.	Robust Transmission of Video Stream over Fading Channels	311
	<i>Mao-Quan Li et al.</i>	
54.	An Attack Classification Tool Based On Traffic Properties and Machine Learning.....	317
	<i>Victor Pasknel de Alencar Ribeiro and Raimir Holanda Filho</i>	
55.	Browser based Communications Integration Using Representational State Transfer.....	323
	<i>Keith Griffin and Colin Flanagan</i>	
56.	Security Aspects of Internet based Voting.....	329
	<i>Md. Abdul Base</i>	
57.	Middleware-based Distributed Heterogeneous Simulation	333
	<i>Cecil Bruce-Boye et al.</i>	
58.	Analysis of the Flooding Search Algorithm with OPNET.....	339
	<i>Arkadiusz Biernacki</i>	
59.	Efficient Self-Localization and Data Gathering Architecture for Wireless Sensor Networks	343
	<i>Milan Simek et al.</i>	
60.	Two Cross-Coupled H_∞ Filters for Fading Channel Estimation in OFDM Systems	349
	<i>Ali Jamoos et al.</i>	
61.	An Architecture for Wireless Intrusion Detection Systems Using Artificial Neural Networks.....	355
	<i>Ricardo Luis da Rocha Ataide & Zair Abdelouahab</i>	
62.	A Highly Parallel Scheduling Model for IT Change Management.....	361
	<i>Denilson Cursino Oliveira, Raimir Holanda Filho</i>	
63.	Design and Implementation of a Multi-sensor Mobile Platform	367
	<i>Ayssam Elkady and Tarek Sobh</i>	

64.	Methods Based on Fuzzy Sets to Solve Problems of Safe Ship Control	373
	<i>Mostefa Mohamed-Seghir</i>	
65.	Network Topology Impact on Influence Spreading.....	379
	<i>Sasho Gramatikov et al.</i>	
66.	An Adaptive Combiner-Equalizer for Multiple-Input Receivers.....	385
	<i>Ligia Chira Cremene et al.</i>	
67.	KSAM – An Improved RC4 Key-Scheduling Algorithm for Securing WEP	391
	<i>Bogdan Crainicu and Florian Mircea Boian</i>	
68.	Ubiquitous Media Communication Algorithms.....	397
	<i>Kostas E. Psannis</i>	
69.	Balancing Streaming and Demand Accesses in a Network Based Storage Environment.....	403
	<i>Dhawal N. Thakker et al.</i>	
70.	An Energy and Distance Based Clustering Protocol for Wireless Sensor Networks.....	409
	<i>Xu Wang et al.</i>	
71.	Encoding Forensic Multimedia Evidence from MARF Applications as Forensic Lucid Expressions.....	413
	<i>Serguei A. Mokhov</i>	
72.	Distributed Modular Audio Recognition Framework (DMARF) and its Applications Over Web Services	417
	<i>Serguei A. Mokhov and Rajagopalan Jayakumar</i>	
73.	The Authentication Framework within the Java Data Security Framework (JDSF): Design and Implementation Refinement	423
	<i>Serguei A. Mokhov et al.</i>	
74.	Performance Evaluation of MPLS Path Restoration Schemes Using OMNET++	431
	<i>Marcelino Minero-Muñoz et al.</i>	
75.	FM Transmitter System for Telemetrized Temperature Sensing Project.....	437
	<i>Saeid Moslehpoour et al.</i>	
76.	Enhancing Sensor Network Security with RSL Codes	443
	<i>Chunyan Bai and Guiliang Feng</i>	
77.	The Integrity Framework within the Java Data Security Framework (JDSF): Design and Implementation Refinement.....	449
	<i>Serguei A. Mokhov et al.</i>	
78.	A Multi-layer GSM Network Design Model	457
	<i>Alexei Barbosa de Aguiar et al.</i>	
79.	Performance Analysis of Multi Carrier CDMA and DS-CDMA on the Basis of Different Users and Modulation Scheme.....	461
	<i>Khalida Noori and Sami Ahmed Haider</i>	
80.	Scalability Analysis of a Model for GSM Mobile Network Design	465
	<i>Rebecca F. Pinheiro et al.</i>	

81. Location Management in 4G Wireless Heterogeneous Networks Using Mobile Data Mining Techniques	471
<i>Sherif Rashad</i>	
82. A new clustered Directed Diffusion Algorithm Based on Credit of Nodes for Wireless Sensor Networks.....	477
<i>Farnaz Dargahi et al.</i>	
83. Multiview Media Transmission Algorithm for Next Generation Networks	483
<i>Kostas E. Psannis</i>	
84. A 4GHz Clock Synchronized Non Coherent Energy Collection UWB Transceiver	489
<i>U Bala Maheshwaran et al.</i>	
85. Comparison of Cascaded LMS-RLS, LMS and RLS Adaptive Filters in Non-Stationary Environments	495
<i>Bharath Sridhar et al.</i>	
86. Data Mining Based Network Intrusion Detection System: A Survey.....	501
<i>Rasha G. Mohammed Helali</i>	
87. VDisaster Recovery with the Help of Real Time Video Streaming Using MANET Support	507
<i>Abdelshakour Abuzneid et al.</i>	
Index	513

Acknowledgements

The 2008 International Conferences on Telecommunications and Networking (TeNe) and the resulting proceedings could not have been organized without the assistance of a large number of individuals. TeNe is 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 including: Abdelshakour Abuzneid, Nirwan Ansari, Hesham El-Sayed, Hakan Ferhatosmanoglu, Ahmed Hambaba, Abdelsalam Helal, Gonhsin Liu, Torleiv Maseng, Anatoly Sachenko, Paul P. Wang, and Habib Youssef.

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, I want to acknowledge the contributions of all the reviewers. A complete list of reviewers is given in page XV.

Tarek Sobh, Ph.D., P.E.

Khaled Elleithy, Ph.D.

Ausif Mahmood, Ph.D.

Bridgeport, Connecticut

April 2009

List of Reviewers

- Aixin, Zhang, 245
Alexei, Barbosa de Aguiar, 457, 465
Ali, Jamoos, 349
Alvaro, Pachon, 223
Arkadiusz, Biernacki, 339
Ausif, Mahmood
Ayodeji, Oluwatope
Bharath, Sridhar, 495
Biju, Issac
Bogdan, Crainicu, 391
Carolin, Bauer, 235
Chunyan, Bai, 443
David, Wyld, 29
Dhawal, Thakker, 403
DOOKEE, Padaruth
Enda, Fallon, 81
Fatima, Yousaf, 149
Igor, Miskovski
Jizhi, Wang
John, Richter
Justin, Champion, 229
Keith, Griffin, 323
Khalida, Noori, 461
Laura, Vallone
Ligia, Chira Cremene, 385, 117
Mahabubuzzaman, A.K.M.
Marco, Zappatore, 189
Marcus, Lemos, 239
Md. Abdul, Based, 195
Mihail, Iliev, 161
Milan, Simek, 343
Mohammed, Abuhelaleh, 123
Morteza, Sargolzaei Javan
Nitin, Sharma
Osama, Rayis, 71
Padmakar, Deshmukh
Prashanth, Pai
Rahil, Zargarinejad
Randy, Maule
Rashed, Mustafa, 139
Raveendranathan, Kalathil Chellappan
Reza, Vahidnia, 93
Saloua, Chettibi
Santosh, Singh
Sasho, Gramatikov, 211, 379
Serguei, Mokhov, 413, 417, 423, 449
Sindhu, Tharangini.S, 489
Syed Sajjad, Rizvi, 257, 263, 269, 275, 281,
287, 293, 299
Teodor, Iliev, 161
Tirthankar, Ghosh, 217
Turki, Al-Somani
Vicente, Alarcon-Aquino, 431, 129
Victor, Ribeiro
Xu, Wang, 409
Ying-ying, Shan, 173
Yonggang, Wang, 135
Zhengping, Wu, 65
Zheng-Quan, Xu, 311

IP Application Test Framework

IPAT Framework

Michael Sauer

Department of Computer Science and Sensor Technology
HTW - University of Applied Sciences
Saarbrücken, Germany
michael.sauer@htw-saarland.de

Abstract—*Simulated use of IP applications on hosts spread on the internet is expensive, which leads already in simple use cases to an enormous amount of time for setting up and carrying out an experiment. Complex scenarios are only possible with an additional infrastructure.*

This document describes a framework with which a needed infrastructure can be implemented. This infrastructure allows an efficient use of the IP applications, even if their hosts are spread all over the WAN.

Due to the most different kinds of use cases a general solution is necessary. This solution is to meet any requirements so that all necessary IP applications can be integrated. Integration means that any application has a remote control feature. This feature is accessible from a special host, which also offers a comfortable remote desktop service on the internet. Supported by this remote desktop service an indirect remote control of applications in a test field is possible.

Target audience for the IP application test framework, briefly IPAT framework, are groups, institutes or companies engaged in pre-development research or pre-deployment activities of distributed IP applications. (Abstract)

Keywords: Computer Networks, Access Technologies, Modeling and Simulation, Wireless Networks

I. INTRODUCTION

The rollout of Apples iPhone shows clearly the trend of using IP applications on mobile internet hosts. Those IP applications communicate via different access networks with other IP applications, possibly also on mobile hosts. Availability of cheap standardized hardware leads to new markets with new challenges for application developers and service providers.

The application becomes aware of a network in which its local position, and thus also the underlying infrastructure, can be varied. The precondition for the application to work, however, is that it does transmit the IP protocol.

The products and tools used for the implementation of pre-development and field trials in spread networks need to meet special requirements, even if OSI-Level 1 and OSI-Level 2 are well known. In addition, a mobile internet host has changing IP quality parameters, depending on the current location.

Furthermore it is expected that the classical, simply-structured client / server portals, with their single-service offer will acquire a less important role. It is also expected that new offers will be combined by more services. Examples are the so called mash-ups of geographical data, photos and videos. The significance of peer-to-peer applications will also increase with the evolving social networks.

Realistic field trial with such basic conditions need a central remote control for the involved applications, no matter where they are carried out and whatever access net is used.

II. METHODOLOGY

An internet host with an exclusively executed application is defined by RFC 1122 [1] as single-purpose host. Example given is a special embedded measurement device for IP parameters. Executing more applications simultaneously, e. g. ping and ttcp, defines this host as a full-service host.

tool: A tool is an IP application which is executed on a single-purpose or a full-service host.

remote control: A remote control allows remote administration and operation of a tool.

integration: A tool is integrated into test field by a remote control.

Four requirements allow efficient work in a test field:

1. remote control of tools
2. measurement uninfluenced by 1.
3. integrate different kinds of tools
4. security considerations against misused resources

These requirements can be specified for one certain purpose. That leads to inflexible implementations. Then the usual changing requirements cause high expenses. General solutions are preferred regarding changing requirements that have to be implemented. A framework shaped solution is here offered. It's a general solution, so that tools are integrated in a test field, regarding security considerations.

A. Remote control and integration

The following classification takes in account the integration requirements:

1. Unix and Windows applications
 - a. GUI
 - b. Command line (also Webinterfaces)
2. Embedded Devices
 - a. GUI
 - b. Command line (also Webinterfaces)
 - c. proprietary

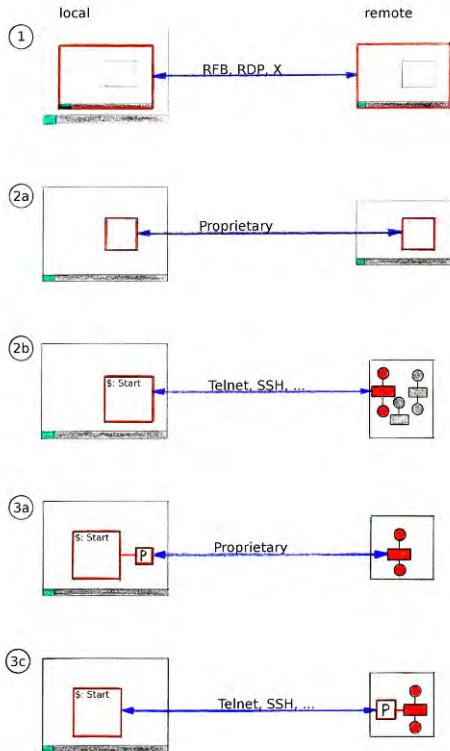


Figure 1. Remote control options

The possibilities for remote control are different, depending on the available user interfaces. Tools without any network interface can't be integrated. All other kinds of tools can be integrated in the framework with more or less effort. The different integration methods can be demonstrated by using the Unix operating system as example:

local: A host that does remote control something.

remote: A host on that something is remote controlled.

1. remote control the remote desktop
2. direct remote control a remote application
 - a. remote control by network interface

- b. execute locally a remote console
3. indirect control a remote application
 - a. local proxy uses 2.a
 - b. remote proxy uses 2.b

The following scenarios show different demands and its possible solutions to meet these. All scenarios should follow the baseline: Efficient work with geographically spread applications in field tests needs the ability to remote control any application, no matter where and when it is carried out.

1) Remote control the desktop

One or more hosts have to execute applications with a graphical user interface on the desktop.

Example: A peer-to-peer video chat application has to be examined. Therefore applications are carried out by the remote controlled desktop on several hosts [see figure 1]. Concurrently produce some other tools a defined traffic so that the behavior of the network and the video-chat-application could be observed.

Use case: This method could be used for tools which needs a desktop. The user behavior could be simulated in that way, perhaps with a desktop automation tool. This offers the advantage of reproducibility.

2) Remote control an application

One or more hosts have to carry out applications with a command line interface in order to simulate http download [see figure 1].

Example: A script initiate sequential downloads.

Use case: The applications should produce a representative traffic load. No user behavior is necessary for the simulation. There isn't the remote controlled desktop needed.

3) Remote control a proxy

One or more hosts have to carry out time coordinated actions with different applications.

Example: Remote proxies carry out applications like iperf or tcpp in order to send data packets from one host to another [see figure 1 (3b)].

Use case: The applications should produce a representative traffic load.

TABLE I. OPTIONS REMOTE CONTROL , PLATFORM AND OPERATING SYSTEM

Rem. control:	Desktop	Application		Proxy	
		GUI	TXT	Local	Remote
FSH+GUI	+	+	+	+	+
FSH+CON	-	+	+	+	+
SPH+GUI	-	0	0	-	+
SPH+CON	-	-	-	+	+
SPH+PUI	-	-	-	0	+

Available: + : yes, 0 : perhaps, - : no

FSH: full-service host with standard operating system

SPH: single-purpose host with other operating system

GUI: Graphical user interface (Win, CDE, KDE)

CON: Text console (CMD, bash)

PUI: Proprietary user interface

B. Security

A real network needs security arrangements. They can be classified:

1. Net security: Sniffing, Worms, Spoofing, Denial-of-Service
2. Local security: Viruses, Trojans, user privileges

Worms, Viruses and Trojans exploit inexperienced user and are therefore meaningless in the framework:

- users skill level is high
- installed Software is patched up to date
- single-purpose hosts operating systems are very prop

One the other side is it necessary to regard Sniffing, Spoofing and Denial-of-Service because these methods are used to get illegal user privileges in order to do some damage or misuse.

strong: A host in the frameworks sense is strong, if the hosts keeps undamaged and do not allow misuse

Strong means that a host may be attacked, but could not be compromised. During the attack working can be difficult or impossible but when the attack has finished, work could be continued without any repair task. In addition do production systems like the Google portal ensure that the service quality isn't reduced during an attack. The framework doesn't take any arrangements for that purpose because the necessary efforts. Building on the idea that a difficult target is an uninteresting target does the framework policy tolerate attacks that prevent working. Become strong requires to avoid any exchange of useable login information along an unsecured path between the involved hosts. With these assumptions a host has to options to become strong:

1. full-service hosts implements the well known IT rules
2. single-purpose host are inherently safe, because they offer no useable services

Beside that are the following rules important:

1. Any full-service host needs a host based firewall, which only opens necessary ports.
2. Remote login is only allowed by Unix hosts with a public key method.
3. Remote login on other (Windows) hosts is only allowed from 2.

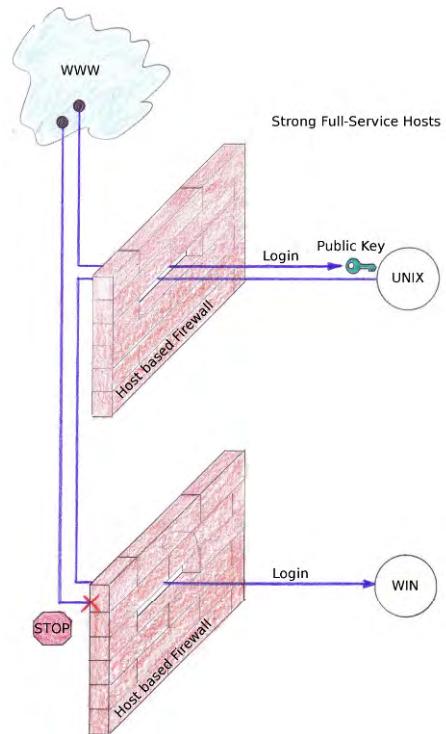


Figure 2. Unix and Windows strong full service hosts

III. TECHNOLOGY

For implement the outlined method are the open source projects OpenSSH and FreeNX used. FreeNX is a GPL implementation similar to the NX-Server of NoMachine, based on the NX core libraries. The NX core libraries are kindly offered from NoMachine to the community under the GPL. OpenSSH offers a tunnel especially for the desktop protocols X, RFB and RDP. The tunnel is used to transmit any protocol along any path between two hosts. The simplest case is the possibility to use a login shell through the tunnel [see figure 2].

A. OpenSSH

The use of OpenSSH with public keys is a fundamental principle for all login shells on strong full-service hosts. Only strong full-service hosts can be accessible in the internet, because they are protected against the usually automated attacks. All other hosts offer a login shell only to full-service hosts. That could be realized with ssh service configuration or with firewall rules.

B. FreeNX

The FreeNX-Server is used to virtualize desktops using a OpenSSH tunnel between the desktop serving host and the client host. NoMachines free NX-Clients are available for the marketable operating systems. There are beside the X

component additional components build in for the RFB and the RDP protocol. Using public keys allows no one to spy out information in order to get improperly login access. The FreeNX-Server acts as proxy for hosts, that offers MS Terminal Services or VNC services. It is possible to configure FreeNX-Server for more or less compression in order to reduce the necessary transmission bandwidth. In extreme cases may someone use 2 bundled ISDN channels for a remote controlled desktop.

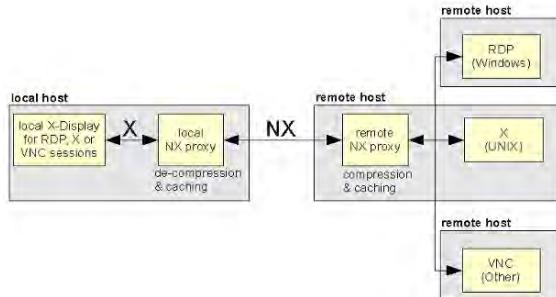


Figure 3. FreeNX function principle

I) Desktop protocols

The marketable protocols with free available implementations are RDP, RFB and X. ICA (Citrics) and AIP (Sun) are also marketable, but there are no free implementations and there are no additional features at the moment. So they are not regarded in the IPAT framework.

a) RFB

A generic solution is developed by the Olivetti Research Laboratory (ORL). Due to the simple functional principle – transmit the desktop image – fast ports to other platforms are possible. The simple functional principle supported the fast spreading in IT administration issues. Optimizing measures improve the performance extensively.

b) RDP

Microsoft's Remote Desktop Protocol offers since NT4 Server concurrent access on the users desktops. Since Windows XP Professional the desktop version of the OS allows also the remote access to the desktop, but only sequentially. The necessary client software is include or free of charge available. Unix can use the open source implementation rdesktop.

c) X

The X protocol is the oldest, still in use remote desktop protocol, but it is only useable in a LAN, because high requirements in small round trip times between the involved hosts. NoMachines proxy solution shows impressively how this disadvantage could be compensated. The FreeNX-Server plays an important role in the IPAT framework. Additional to the improvements on the X protocol acts the FreeNX-Server as an proxy agent for incoming connections, authenticate and forward them to the desired desktop server [see figure 3].

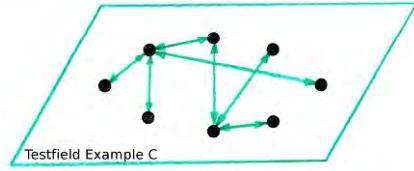
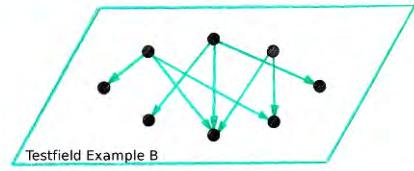
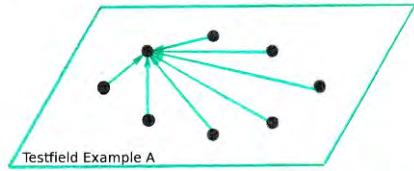
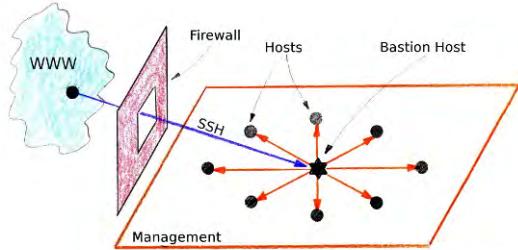


Figure 4. IPAT framework system levels

IV. ARCHITECTURE

The IPAT framework describes a system with two independent levels, an administration level and a test field level. The levels logical topology is defined by their functional requirements.

A bastion host [3] is a particularly secured full-service host. The term bastion is borrowed from medieval fortress concepts and describes especially well-fortified porches of a fortress. Porches protect the fortress walls and also the fortress inner infrastructure.

A multi homed host has more than one network interface, which connect the host to more networks. A multi homed host can or can't route the IP packets between the networks, depending its configuration.

A. Administration

The administration topology is a star with a bastion host acting as a hub. All other hosts are remote controlled by the bastion host. For administration purpose offers the bastion host a remote login and desktop service in the internet.

Regarding security considerations doesn't the multi homed bastion host IP forwarding between its network interfaces. Additional does the bastion host offers only access from the internet via the ssh protocol, the other network interfaces are used to access the hosts in the test field. The test field hosts allows only administration access for the bastion host.



Figure 5. Vauban fortress Saarlouis with bastions at the edges

Using further the fortress metaphor hosts in the internet are fortress walls which may be attacked, but grant only to the bastion host access. Sensitive inner environment are hosts, which are not visible in the internet, but the bastion host can control them also.

B. Test field

The test field topology is application specific, e. g. a peer-to-peer, a mash-up or some complete new concepts. The test field is implemented close to reality, which includes also connections to the internet.

1) Test field example A: Client/Server

A web application on a host offers its content to web browsers. Many clients may use the service. It's the classic client / server concept.

2) Test field example B: Mash up

An application aggregates something with more services to a new service. These stands for the upcoming service oriented architectures – SOA.

3) Test field example C: Peer-to-Peer

In a peer-to-peer network all involved applications are service provider and consumer. Think about Gnutella or something similar.

V. EXAMPLE OF USE

The IPAT framework was inspired by the WiMAX field trial, located in Saarbrücken [4], a city in the southwest of Germany. The WiMAX field trial is used to examine the WiMAX access technology. Therefore a WiMAX access net was installed and set in use. Test clients ensure realistic operation in the access network. The offer to the test clients is comparable to the corresponding DSL offers from Vodafone, Telekom or VSENet.

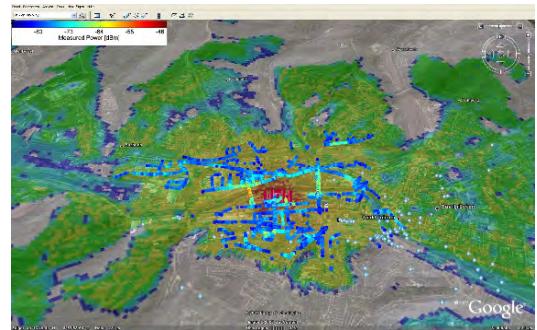


Figure 6. WiMAX prediction model vs. measurement points

The field trial is a permanent construction and is operated by the WiSAAR consortium. It is used by the computer science and communication engineering students as research object.

There are two base stations from different hardware providers, both works like the 802.16d standard (fixed wireless).

Doing research work shows clearly, that applications could not be integrated in a WAN on the fly. In other words, the effort becomes very high and efficient work is no longer possible. The researchers solve infrastructure problems, rather than their research themes. Figure 6 shows calculated WiMAX SNR predictions (coloured area) for Saarbrücken in contrast to measurement points (coloured points) with the measured SNR. The picture shows obviously that efficient work in a WAN needs particular infrastructure. In that case we use a converted car, equipped with measurement devices, its high voltage power supply and the also necessary antennas. All the experience collected by the operation of the research object are flown in the IPAT framework.

A. Components

The WiMAX field trial needs the following components. They are used to operate the WiMAX access net itself to offer internet access to test clients.

WiMAX: WiMAX access network like 802.16d standard

AN: Access Network – public subnet, connected to local provider VSENet, with WiMAX base station and test client hosts

BSM: Base station management hosts for the basestations Airspan MacroMAX and NSN WayMAX

First research themes deal only about the physical layer. So the above described components are sufficient to do the work. Experiments in higher protocol layers, like IP, shows very quickly handling problems. Problems arose especially because applications need to be executed on hosts which can be located at the most different positions in the propagation area.

Additionally needs physical layer measurements a few seconds, but IP measurements consume sometimes hours or days. To ease the work some available and some new components are integrated in the field trial:

TN: Test net - private secure IP network for get familiar with experiments and develop measurement templates.

LN: Lab net - privat IP network with workstations that can access all tools in the test field.

FW: Firewall

BH: Bastion host (multi homed)

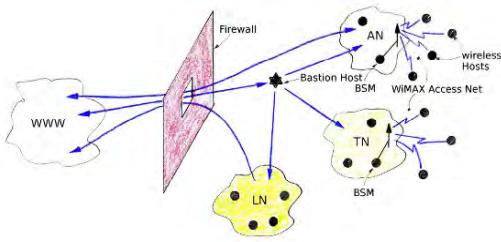


Figure 7. WiMAX field trial network configuration

The efficient improvements were achieved mainly by the following facts:

1. integration strategy available for new experiments
2. remote access from each internet host
3. focus on research theme due to given infrastructure

The interconnection to the research object in the test field is offered by the described multi homed bastion host and a standalone firewall [see figure 7].

B. Tools

Test field trials need usually two different kinds of tools. On one side there are prototypes or marketable applications in order to proof the usability under defined circumstances. These tools are used to give go/no go answers from the end users perspective. Perhaps someone wants to know, if an IP camera could be used. Test persons therefore evaluate these by watching the video stream.

Measurement applications are used to quantify quality parameters in a test field. The free available tools ping, ttcp and iperf are examples for measurement applications. With these tools one could examine long time connection behavior, bandwidth capacity or round trip times. But there are also more special tasks which may not be solved with free available applications. Devices from special measurement providers are necessary, or perhaps a self developed tool. Most of such tools could not implement the comfortable Windows- or UNIX-based user interfaces due to the lack of operating system resources. As example for that kind of tools stands synchronQoS, a self developed tool from the research group RI-ComET [5]. The consequences for the framework are demonstrated with synchronQoS:

1) synchronQoS



Figure 8. synchronQoS board

Under the project name synchronQoS [see figure 8] was a prototype for a measurement tool developed with the real time operating system PXROS-HR TriCore System Development Platform v3.4.5 of Firma HighTec EDV-System GmbH, Saarbrücken (www.hightec-rt.com). In that project GPS is used to measure quality criteria in IP based networks. There are one-way delay and one way delay variation options implemented. The tool was developed for VoIP in WiMAX, but may be used in all IP networks. The accuracy is better than 0.5 µs, independent from the global distribution of the two involved hosts. synchronQoS will be used where one-way measurement with high accuracy is needed. The user interface is a telnet session, similar to many other network measurement devices.

a) Interface implementation

Other marketable tools had comparable interfaces, sometimes there are also web interfaces, but the nature of telnet sessions and web interfaces is a command line like behavior: The user defines parameters, carried out something and gets the result.

The adaptation of such interface is only possible with changes in software. This may be possible by self developed tools, but not by third party tools. Therefore integration could not mean interface adaptation in the tool software. An alternative option is the development of a proxy application [see figure 1, (3a and 3b)] so that a tool can be integrated in a test field.

b) Interface diversity

The more tools, the more user interfaces are there. The experience shows, that a system consisting of men and many different tools scales not very well. The obviously visible failures by execution are much less dangerous than hidden failures, which lead to improper measurements results. Such mistakes are often caused by choosing not appropriate program parameters.

C. Metrics

Theoretical basics for solving the above problem with the interface diversity may be the work of the IPPM Workgroup [6]. The IPPM Workgroup examines application scenarios with application specific metrics. The RFCs shows how to define the metrics, but tells not which tools to use for implement the

metrics according your application. Developer needs high skills to use a certain tool or device in order to implement application specific metrics correctly. A reasonable approach is a generalization. The before mentioned proxy applications could be used in order to develop a standardized interface for use in metrics implementation. The following ongoing project MADIP shows such requirements:

1) MADIP

MADIP is a software system that carried out IP based measurements in a network. The measurements will be carried out on hosts with tools like ping, ttcp or iperf. Different measurements are collected in measurement orders. The measurement orders are designed by a graphical user interface [see figure 9]. The graphical user interface does seamless tool integration according to the metric issues. Distribution, supervision, call and processing happens automatically, according the defined parameters.

A backend component carried out the desired measurements orders. Therefore distributes the backend component the scheduled measurements at the hosts with the according tool. The measurements will be executed by time. The system architecture follows the client/server principle. The measurement order dispatcher acts as client of the tools. Each tool has to act for the measurement order dispatcher as a server. A generic server standardized the different tool interfaces in order to present a unified interface for the measurement order dispatcher. Each server takes its measurement order, executes it and stores the results for the dispatcher. The server acts as proxy [see figure 1, (3a and 3b)] for the tools. The measurement order dispatcher collect the measurement results of the involved tool servers, does a post processing and produce a measurement report.

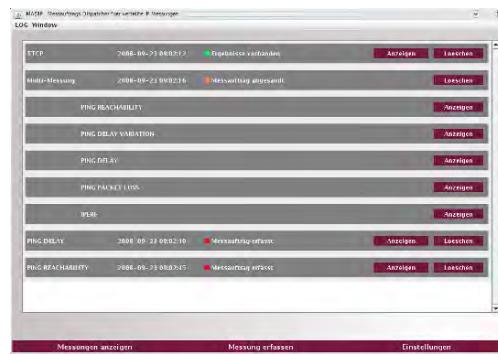


Figure 9. MADIP screenshot

2) Special case single-purpose hosts

synchronQoS prototype now offers a telnet interface, which is not very handy. This is similar to other special tools. Unlike self developed tools isn't there the possibility to change the interface in order to adapt it to MADIP. Such tools usually are closed source and may not be changed. This is the point were a proxy offers MADIP a unified interface. That means only a

proxy have to be rewritten, if there is special case device that has to be integrated in the test field. The proxy may be executed remote or local, depending on the tool.

VI. CONCLUSION

A field trial has been used to develop the best practice IPAT framework. The IPAT framework can be used to carry out measurements and experiments in IP-based WANs. The IPAT framework facilitates research activities, pre-development, and the operation of application scenarios in WANs. It is also useful for test field scenarios in the pre-deployment phase.

Especially trends to mobile ubiquitous internet use with a combination of whatever services, and their most different quality requirements, will lead to situations where just the knowledge of the up- and download speed does not suffice anymore. To verify their requirements application developers need test fields so as to implement, and test, metrics. This is necessary because the increasingly heterogeneous and numerous access networks do not allow for problems to be solved from the OSI-level 0 up. All this has become topical because of the new Google patent *Flexible Communication Systems and Methods* [7]. The objectives and the technology described in this patent make an automatic, seamless handover between access networks possible, regardless of what access technology - e.g. GSM, GPRS, UMTS, WLAN, WiMAX - or what provider is used. What is especially important in this scenario is that users may lose their interest in those services which cannot be used in all places at the same quality. This is due to the varying IP quality parameters of the used access technology. It is therefore vital for application developers and service providers to offer tools that help the users to check for themselves whether or not a certain quality of service is available. Moreover, in our mobile internet world, these tools are supposed to report the check results to the service providers, according to the defined IPPM metrics. The IPAT framework, and especially the *MADIP* tool, are conceived to support this new trend due to the easy implementation of metrics in WANs.

VII. LITERATUR

- [1] R. Braden, "Requirements for internet hosts – communication layers," RFC, no. 1122, 1989. [Online]. Available: <http://www.faqs.org/rfcs/rfc1122.html>
- [2] "Nomachine," Website. [Online]. Available: <http://www.nomachine.com/>
- [3] B. Fraser, "Site security handbook," RFC, no. 2196, 1997. [Online]. Available: <http://www.faqs.org/rfcs/rfc2196.html>
- [4] "WiSAAR-Konsortium," Website. [Online]. Available: <http://www.wisaar.de>
- [5] "RI-ComET-Forschungsgruppe Breitbandnetze," Website. [Online]. Available: <http://www.ri-comet.de>
- [6] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis, "Framework for ip performance metrics" RFC, no. 2330, 1998. [Online]. Available: <http://www.ietf.org/rfc/rfc2330.txt>
- [7] S. Baluja, M. Chu, and M. Matsuno, "Flexible Communication Systems and Methods" United States Patent Application 20080232574, filed March 19, 2007

CROSS-LAYER BASED APPROACH TO DETECT IDLE CHANNELS AND ALLOCATE THEM EFFICIENTLY USING MARKOV MODELS

Y. B. Reddy

Grambling State University, Grambling, LA 71245, USA; ybreddy@gram.edu

Abstract - Cross-layer based approach is used in cognitive wireless networks for efficient utilization of unused spectrum by quick and correct detection of primary signals. In the current research, Su's algorithm was modified and the RASH (Random Access by Sequential search and Hash organization) algorithm was proposed for quick detection of idle spectrum. Once the idle spectrum is detected, the Hidden Markov Model (HMM) is used to help the analysis of efficient utilization of the idle spectrum. The simulation results show that the proposed model will be helpful for better utilization of the idle spectrum.

KEYWORDS

Power consumption, cross-layer, game theory, cognitive networks, dynamic spectrum allocation, Markov Model

I. INTRODUCTION

The existing dynamic spectrum allocation (DSA) models work for enhancing the overall spectrum allocation and network efficiency. Furthermore, these models allow imbalance spectrum utilization. The imbalanced allocation may allocate more resources than the node requires (more resources to the needed with a low transmission rate), which falls into wastage of resources. Therefore, optimum resource allocation and Quality of Service (QoS) became an important research issue [1, 2, 3].

To meet the demands of wireless communications customers worldwide, the researchers proposed various models to improve the efficiency of power and bandwidth [4]. The cross layer design (CLD) model was one of the models used to achieve optimum resource allocation. The CLD focuses on exploring the dependencies and interactions between layers, by sharing information across layers of the protocol stack. Furthermore, the CLD models focus on adaptive waveform design (power, modulation, coding, and interleaving) to maintain consistent link performance across a range of channel conditions, channel traffic conditions, and Media Access Control (MAC) parameters to maintain higher throughput. Stable condition at the cognitive node may be achieved by radio adaptive behavior (e.g. transmission characteristics). Further optimum allocation of bandwidth to achieve QoS is very important.

Concepts in CLD are similar to software process model design. One of the CLD approach in wireless communications proposes to integrate all seven layers and optimize (eliminate layer approach), which is not practical. However, knowledge sharing between layers is practical.

Hence by keeping the layered approach and design violations minimal, one must allow the interactions between non-adjacent layers.

The cross-layer approach violates the traditional layered architecture since it requires new interfaces, merge adjacent layers, and share key variables among multiple layers. Therefore, we must select the CLD approach without modifying the current status of the traditional layered architecture. But, the CLD without solid architectural guidelines leads a spaghetti-design. Furthermore, different kinds of CLD design proposals raise different implementation concerns. In wireless communications, the first implementation concern is direct communication between layers through the creation of new interfaces for information sharing. The second concern proposes a common entity acting as a mediator between layers. The third depicts completely new abstractions.

Unutilized spectrum can be detected by using multiple sensors at each secondary user. Ma et al. [5] proposed dynamic open spectrum sharing MAC protocol by using separate set of transceivers to operate on the control channel, data channel, and busy-time channel, respectively. Hsu et al. [6] proposed the cognitive MAC with statistical channel allocation. In their approach, the secondary users select the highest successful transmission probability channel to send the packets based on channel statistics. They further identify the unused spectrum and highest successful transmission statistics with higher computational complexity. All these approaches require more computational time and resources. Alternatively, unutilized spectrum can be identified by tuning the transceivers through special algorithm (s) and allocating the spectrum without interfering with the primary user (PU). Su and Zhang [7] proposed algorithms for random sensing and negotiation-based channel sensing policies without centralized controllers. Su claimed their proposal performs better in identifying unused spectrum.

The new wireless networks are using the standard protocol stacks (TCP/IP) to ensure interoperability. These stacks are designed and implemented in a layered manner. Recent work focuses on the cross-layer design of cognitive network, which is essential in future wireless communication architecture [8, 9, 10]. The cross-layer is to adopt the data rate, power, coding at the physical layer to meet the requirements of the applications for a given channel and network conditions, and to share the knowledge between layers to obtain the highest possible adaptability. It is necessary to implement new and efficient algorithms to make use of multiuser diversity gain and similarly the

efficient algorithms for multi-cell cases. The cross-layer design may have the following possible designs:

- Interfaces to layers (upward, downward, and both ways): Keeping in view of architectural violations, and the new interface design (upward, downward, and both ways), which helps to share the information between the layers.
- Merging adjacent layers and making a super layer: The concept destroys the independence of data flow and data transportation.
- Interface the super layers: Merging two or more layers may not require a new interface. But it is suggested that a higher level interface for these merged layers will help to improve the performance with overheads.
- Coupling two or more layers without extra layers: This facility improves the performance without an interface. For example, design the MAC layer for the uplink of a wireless local area network (LAN) when the Physical layer (PHY) is capable of providing multiple packet reception capability. This changes the role of MAC layer with the new design, but there is no interaction with other layers. Sometimes this may hinder the overall performance.
- Tuning the parameters of each layer by looking at the performance of each layer: Joint tuning of parameters and keeping some metric in mind during design time will help more than tuning of individual parameters. Joint tuning is more useful in dynamic channel allocation.

Keeping in view of these design options, there are various issues in the cross-layer design activity. The design issues include:

- the cross-layer (CL) proposals in the current research and suitable cost-benefit network implementation
- the roles of layers at individual node and global parameter settings of layers
- the role of the cross-layer design in future networks and this will be different in cognitive network design

CLD in the cognitive networks is an interaction interface between non-adjacent nodes to increase the detection rate of the presence of the primary signal [11-16]. It allows exploring flexibility in the cognitive nodes by using them to enable adaptability and controlling specific features jointly across multiple nodes. The CLD extends the traditional network topology architecture by providing communication between non-adjacent nodes. Hence the CLD design became an important part in relation to flexibility and adaptability of the cognitive network nodes. One of the efficient CLD architecture for cognitive networks includes the following components:

- Cross-layer manager and scheduler of nodes
- Cross-layer interface to nodes
- Cross-layer module of single node
- Inter-node (network) cross-layer module

The CLD using these components needs more care because CLD nodes interact with other CLD which would generate interference. Furthermore, the interaction of CLDs influences not only the layers concerned, but also the parts of the system. It may be unrelated at the remote site but unintended overhead may effect on the overall performance.

The rest of this paper is organized as follows: i) Section 2 discusses concepts of cognitive networks and cross-layer design ii) Section 3 discusses the possible models for cross-layer architecture iii) Section 4 discusses the problem formulation with improved performance algorithm, time duration for idle channel, channel utilization, Hidden Markov Model (HMM), and analysis of channel utilization using HMM iv) Section 5 and 6 discuss the simulations and the conclusions.

II. COGNITIVE NETWORKS AND CROSS-LAYER DESIGN

A cognitive infrastructure consists of intelligent management and reconfigurable elements that can progressively evolve the policies based on their past actions. The cognitive network is viewed as the topology of cognitive nodes that perceives the current network conditions, updates the current status plan, and schedules the activities suitable to current conditions. The cognitive networks include the cognitive property at each node and among the network of nodes. The cognitive wireless access networks interact and respond to requests of a specific user by dynamically altering their topologies and/or operational parameters to enforce regulatory policies and optimize overall performance. Furthermore, the CLD in cognitive networks includes the cross-layer property of participating layers and the network of cognitive nodes. The CLD does not have learning capabilities but keeps the current status of participating nodes and act accordingly to increase the overall throughput.

Most of the CLD researchers concentrate on MAC layer, which is one of the sub-layers that make up Data Link Layer (DLL) of OSI model. The MAC layer is responsible for moving data packets to and from one network interface card (NIC) to another across a shared channel. The MAC layer uses MAC protocols (such as Ethernets, Token Rings, Token Buses, and wide area networks) to ensure that signals sent from different stations across the same channel do not collide. The IEEE 802.11 standard specifies a common MAC layer that manages and maintains communications between 802.11 stations (radio network cards and access points) by coordinating access to a shared radio channel and utilizing protocols that enhance communications over a wireless medium [17]. The goal is to design a topology that can offer maximum network-wide throughput, best user performance, and minimum interference to primary users. The 802.11 MAC layer functions include: scanning, authentication, association, wired equivalent privacy (WEP), request-to-send and clear-to-send (RTS/CTS) function, power save mode (PSM), and fragmentation.

III. POSSIBLE MODELS FOR CROSS-LAYER ARCHITECTURE

CLD architecture is viewed at two places. First, at the node level where sharing of needed information among the layers to adjust the capacity of individual wireless links and to support delay-constrained traffic; dynamic capacity assignment in the MAC layer for optimum resource allocation among various traffic flows; and intelligent packet scheduling and error-resilient audio/video coding to optimize low latency delivery over ad-hoc wireless networks. Secondly, at the network level, where sharing of information among the nodes help to improve the QoS and efficient utilization of resources.

One of the important factors to consider for cross-layer approach is data rate control. The channel condition is normally decided by the data rate, information communicated across the layers, and delivery mechanisms. If we implement the cross-layer design over the existing layered model, it violates the basic layer structure. Our goal is to develop an architecture that can accommodate the proposed cross-layer property without disturbing the current layered architecture. To achieve this we must preserve the modularity of existing protocol modules to the greatest extent possible, the model must facilitate multiple adaptations in a flexible and extensible manner, and the model must be portable to a variety of protocol implementations.

Most of the cross-layer work focused on the MAC and Physical layer, but we need to focus on all five layer of TCP for wireless problems. So far there is no systematic way or general considerations for cross-layer adaptations. One of our goal is to introduce cross-layer structure at the node level and at the inter node level.

We propose the cross-layer design among the cognitive nodes for better quality of service and high throughput. Each cognitive node contains a network cross-layer (NCL) component to connect to other participating nodes. The interaction among the cognitive nodes will be done through NCL component. The interaction between the nodes will be selected as one of the following:

- a. One node to the next closest node (one-to-one one to many). Each node communicates to the next closest node. In this process each node communicates to the closest nodes (one or many). The communication multiplies and the information will be broadcasted to all nodes. It is possible for the nodes to receive redundant information (more duplication possible).
- b. each node to all other participating nodes (one-to-many which involves heavy load on each node)
- c. all nodes interact through a central node
- d. closest nodes form a cluster and the cluster heads uses cases (a) or (b) or (c)

Each design has its own merits, but (c) and (d) has better benefits. In (c), the central node possesses the current state of all nodes and act upon current state of information

received. For example, if the primary user enters into the network, then the central node gets updated and it takes appropriate action to move current existing secondary channel from the primary channel space. In (d), the closest nodes form a cluster and one of the cluster nodes acts as cluster head. The cluster head keeps the current state of all nodes within the cluster and appropriate interaction with other cluster heads, or creates a central node for the cluster heads and interacts with the central node. Each cluster head acts as central node to the cluster and collaborates with other cluster heads through the main central node.

IV. PROBLEM FORMULATION

In the proposed CLD, we assume that each cognitive user has control transceiver (CT) and software designed radio (SDR) transceiver. The control transceiver obtains information about the un-used licensed channels and negotiates with the other secondary users through the contention-based algorithms, such as the 802.11 distributed coordination function (DCF) and carrier sense multiple access (CSMA) protocols. The SDR transceiver tunes to any one of the n licensed channels to sense for free spectrum and receive/transmit the secondary users' packets. The SDR transceiver further uses carrier sense multiple access with collision detection (CSMA/CD) protocol to avoid the packet collisions.

We assumed that there are n channels in a licensed spectrum band. The control channel must find the unused channels among these channels at any given time. There are many ways to find the unused channels. The controller can poll randomly and find the unused channels. Probability of finding the unused channel is $1/n$. The secondary user may wait till the particular channel becomes available or alternatively, it can negotiate for free channel or combination of these methods. All these methods take time to find a free channel for cognitive user. If there are m cognitive users and number of trials equals m times n ($m \times n$). Therefore, an alternative approach faster than current models is needed to find free channel for cognitive user to transmit the packets.

The proposed approach has two steps. In the first step, secondary users sense the primary channels and send the beacons about channel state. The control transceiver then negotiates with other secondary users to avoid the collision before sending the packets. Since each secondary user is equipped with one SDR, it can sense one channel at a time and it does not know the status of all channels. The goal is to show the status of all licensed channels. So we propose an algorithm called Random Access by Sequential search and Hash organization (RASH). RASH is similar to sequence search and alignment by hashing algorithm (SSAHA) approach [18] for faster search and identification of the idle channel. Using RASH, the primary channels are hashed into G groups with a tag bit as part of the hash head (bucket address). The flag bit (bucket bit) is in on/off state depending on if any channel in the group is idle (bit is on) or if all channels are busy (bit is off). The value of G is

calculated as $G = n/m$. Now, each secondary user uses its SDR transceiver to sense one hashed head to find the idle channel. If the flag bit is off, then there is no need to search the bucket for free channel. If the flag bit is on the sequential search continues to find the free channel or channels (if the bucket size is chosen very large, alternative search methods are required). The RASH algorithm is in two parts and given below:

IV.1.Pseudo code for cognitive user to identify idle channel at MAC protocol

The report part of the algorithm developed by su [7] is modified for faster access. The Negotiation phase is not modified. The modified report part is given below:

Report the idle channel

G =Bucket Number; m=hash factor (prime number);
 ICN= Idle channel number;
 LIC = List of idle channels; BCN=Channel number in the bucket;
 A. Control transceiver – listens on control channel
 Upon receive on Kth mini-slot (bucket number) Store
 the bucket number G = bn;
 //update the number of unused channels (List of available
 channels) in the bucket
 C=0; //counter
 BCBN=0;
 While (BCN != EOL) do //end of list
 {
 If BCBN is idle then {
 ICN (C)=BCN; //store idle channel available in bucket
 LIC (C)= G*m + ICN(C);
 //Slot number or channel number
 ++C;
 }
 }

B. SDR transceiver –Receive the list of idle channels
 Send the beacon to each idle channel in LIC using
 sensing policy
 Confirm and report the idle channels to control
 transceiver

See reference [7] for Negotiating Phase.

IV.2.Time Duration to Identify an Idle Channel

The time duration of the time slot in the proposed RASH algorithm is calculated as follows:

Let T_d be the time duration of the time slot, T_{rp} be reporting phase, and T_{np} be negotiation phase. The time duration is given by [7]

$$T_d = T_{rp} + T_{np}$$

The reporting phase is divided into bucket report and identification of idle channel or channels. Therefore, time reporting phase is written as

$$T_{rp} = B_{rp} + C_{rp}$$

// B_{rp} = bucket report and C_{rp} = channel report

For example, if there are 1000 channels and each bucket contains 11 channels, the probability of finding the bucket is 1/11, and probability of finding the channel in the bucket is 1/11. Therefore, the probability of finding the idle channel is 102/1001 or 102/1000 (approximately) whereas; the probability of finding the idle channel in random selection [7] is 1/1000. The results show RASH can find idle channels faster than random selection. Similarly, we can calculate the probability of channel utilization.

IV.3.Channel Utilization

It is important for cognitive user to calculate the idle time of the channel utilized by the primary signal. The idle time will be better utilized by the cognitive user during the absence of primary user. Assuming that the number of times channel is *on* is the same as number of times the channel is *off*, and then the total time utilization by any channel is calculated as:

$$T_{tct} = C_{it} + C_{ut} + C_{nc} \times (T_{on} + T_{off}) \quad \dots \dots \quad (1)$$

Where

T_{tct} = Total channel time

C_{it} = channel idle time

C_{ut} = channel utilization time

C_{nc} = number of times position change
 (on to off or off to on)

T_{on} = time taken to bring channel to on state

T_{off} = time take to bring the channel to off state

If the channel is on completely in a given time slot then the probability of channel utilization is 1, otherwise the probability of channel utilization time is

$$P_{cut} = \frac{1 - P_{cit} - \delta}{T_{tct}} \quad \dots \dots \quad (2)$$

Where

P_{cut} = probability of channel utilization

P_{cit} = probability of channel idle time

δ = channel on/of time which is very small and a constant

The value of P_{cut} is ≤ 1 . Similarly, we can find for all channels the utilization time at any given time. The total idle time of all channels for any licensed spectrum band of n channels is sum of idle time of n channels. If we assume the probability of a channel utilization is average channel utilization time, then the probability of presence of any primary signal P_{ps} at any given time slot is

$$P_{ps} = \frac{P_{cut}}{P_{tct}} \quad \dots \dots \quad (3)$$

Where

P_{tct} is the probability of total channel time (time slot that channel can have).

Using the equations (1), (2) and (3), we derive the probability of channel idle time P_{cit}

$$P_{cit} = 1 - \delta - P_{cut} \times T_{tct} \quad \text{--- (4)}$$

The efficient use and analysis of the available time slot (idle time) of primary channel will be done by Hidden Markov Model (HMM).

IV.4. Markov Model

The Markov model is used for the analysis of the efficient use of the available time slot (idle time) of primary channel. A Markov model is a probabilistic process over a finite set, $S = \{S_0, S_1, \dots, S_{k-1}\}$, usually called its *states*.

Transmissions among the states are governed by a set of probabilities called transition probabilities. Associated to a particular probability an observation (outcome) will be generated by keeping the state not visible to an external observer. Since the states are hidden to the outside, the model is called Hidden Markov Model (HMM). Mathematically, HMM is defined using the number of states N, the number of observations M, and set of state probabilities $A = \{a_{i,j}\}$, where

$$a_{i,j} = p\{q_{t+1} = S_j | q_t = S_i\}, \quad 1 \leq i, j \leq N \quad \text{--- (5)}$$

q_i is the current state. The transition probabilities should satisfy the normal stochastic constraints to reach any state to any other state

$$a_{i,j} \geq 0, \quad 1 \leq i, j \leq N \quad \text{--- (6)}$$

Otherwise $a_{i,j} = 0$

The observation $B = \{b_j(k)\}$, with probability distribution P, observation symbol v_k and initial state distribution $\pi = \{\pi_i\}$ is

$$b_j(k) = P[v_k \text{ at } t | q_t = S_j], \quad 1 \leq j \leq N \quad \text{--- (7)}$$

$$1 \leq k \leq M$$

$$\pi_i = P[q_t = S_i], \quad 1 \leq i \leq N \quad \text{--- (8)}$$

For any given values of $N, M, A, B, \text{and } \pi$, the HMM can be used to give an observation sequence

$$O = O_1 O_2 \dots O_t \quad \text{--- (9)}$$

where O_i is the i^{th} observation. The current problem is to adjust the model parameters $\lambda = \{A, B, \pi\}$ to maximize $P(O | \lambda)$. That is, to maximize the utilization of

channel idle time P_{cit} using the current model λ . The most likely associated problem is, for a given observation sequence O_i , find the most likely set of appropriate idle channel or channels. This problem is close to ‘Baum-Welch algorithm’ [19, 20], to find *hidden Markov model* parameters A, B , and π with the maximum likelihood of generating the given symbol sequence in the observation vector. We will find the probability of observing sequence O as

$$P(O) = \sum_S P(O | S)P(S) \quad \text{--- (10)}$$

where the sum runs over all the hidden node sequences $S = \{S_0, S_1, \dots, S_{k-1}\}$; Since the hidden nodes (channels) are very high in number, it is very difficult to track the $P(O)$ in real life, unless we use some special programming techniques like dynamic programming.

V.DISCSSION OF THE RESULTS

In the equation (10), the $P(O|S)$ is the channel available to cognitive users and $P(S)$ is the probability of primary user presence. The equation (10) can be rewritten as

$$P(O) = \sum_N P_{cit} \times P_{cut}$$

$$P(O) = \sum_N (1 - \delta - P_{cut} \times T_{tct}) \times \left(\frac{1 - \delta - P_{cit}}{T_{tct}} \right) \quad \text{--- (11)}$$

Let us assume the total channel time (T_{tct}) is 0.9, channel on/off time (δ) is 0.0001, and number of channels=64. The probability of channel utilization time (P_{cut}) and probability of channel idle time (P_{cit}) can be calculated using equations (1), (2), and (4). Since the probability of observing sequence P(O) depends upon the probability of channel available to cognitive users and probability of primary users presence, we calculate the probability of observing sequence for availability of variable number of channels.

Figure 1 shows the probability of observing sequence over 64 channels. The graph concludes that more than 50% of the channels have better performance level or above the average performance. The better performance channels are more available to cognitive user. The Figures 2a and 2b shows that the channel idle time directly may not be available to the cognitive user due to problems of detection of primary user. The Figures 2a and 2b further concludes that the detection of primary user is very important to utilize the channel idle time.

VI.CONCLUSIONS

In this research we have modified the Su’s algorithm to identify the unused channel so that cognitive user will be able to use the spectrum efficiently. The simulations show

that the presence of primary signals is important to detect without fail for better utilization of the spectrum. The Markov model helps to recognize the better channels for cognitive user. The simulations further conclude that we need alternative techniques to detect the primary signals when their presence is marginal.

ACKNOWLEDGEMENT

The research work was supported by Air Force Research Laboratory/Clarkson Minority Leaders Program through contract No: FA8650-05-D-1912. The author wishes to express appreciation to Dr. Connie Walton, Dean, College of Arts and Sciences, Grambling State University for her continuous support.

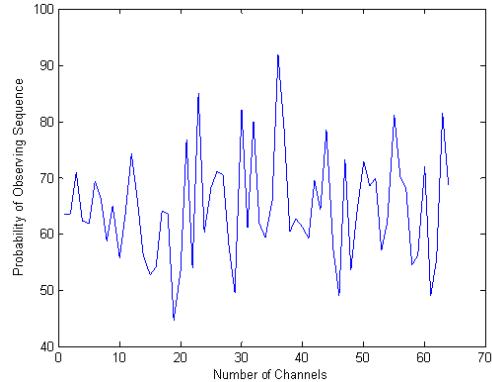


Figure1: Probability of Observing Sequence with 64 channels

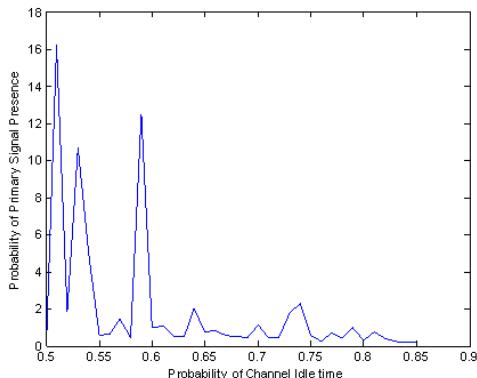


Figure 2a: Probability of Channel Idle Time

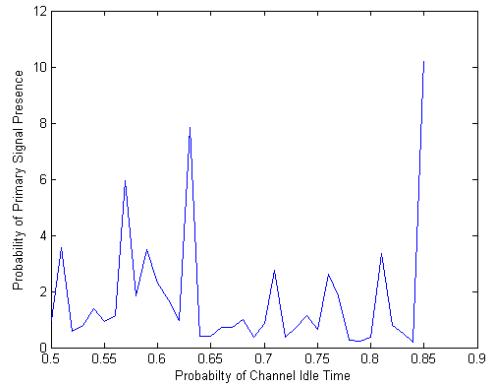


Figure 2b: Probability of Channel Idle Time

REFERENCES

- [1] G. Ganesan and Y. Li, "New Frontiers in Dynamic Spectrum Access Networks", First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. (DySPAN 2005), Volume, Issue, 8-11 Nov. 2005 Page(s):137 – 143.
- [2] I. Baldine, M. Vellala, A. Wang, G. Rouskas, R. Dutta, and D. Stevenson, "A Unified Software Architecture to Enable Cross-layer Design in the Future Internet", IEEE 2007.
- [3] C. Ghosh, B.Xie, and D.P. Agarwal, "ROPAS: Cross-layer Cognitive Architecture for Mobile UWB Networks", J. of Computer Science and Technology, 23 (3), pp 413-425, 2008.
- [4] A. J. Goldsmith and S. Chua., "Variable-rate variable-power MQAM for fading channels", IEEE Trans. Commun., Vol. 45, no. 10, pp 1218-1230, 1997.
- [5] L. Ma, X. Han, and C. Shen., "Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks", Proc. IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks", 2005.
- [6] A. Hsu, D. Wei, and C. Kuo., "A cognitive MAC protocol using statistical channel allocation for wireless ad-hoc networks", Proc IEEE WCNC, 2007.
- [7] H. Su and X Zhang., "Cross-layer Based Opportunistic MAC Protocols for QoS Provisionings Over Cognitive Radio Wireless Networks", IEEE Jr. on selected areas in communications, vol. 26, no. 1, 2008.
- [8] J. L. Burbank and W. T. Kasch. Cross-layer Design for Military Networks. IEEE Military Communications Conference, (MILCOM 2005). Vol 3, 2005, 1912 – 1918.
- [9] S. Khan, S. Duhovnikov, et al. Application-driven Cross-layer Optimization for Mobile Multimedia Communication using a Common Application Layer

- Quality Metric. 2nd International Symposium on Multimedia
- [10] A. Saul, S. Khan, G. Auer, W. Kellerer, and E. Steinbach. Cross-layer optimization with Model-Based Parameter exchange. The IEEE International Conference on Communications 2007.
- [11] K. Hamdi and K. Lataief, "Cooperative Communications for Cognitive Radio Networks", The 8th Annual Post Graduate Symposium on the Conference of Telecommunications, Networking, and Broad Casting (PG Net 2007), June 2007.
- [12] J. Unnikrishnan and V. Veeravalli, "Cooperative Spectrum Sensing and Detection for Cognitive Radio", IEEE Global Telecommunications Conference (GLOBECOM '07) 2007.
- [13] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative Sensing Among Cognitive Radios", IEEE International Conference on Communications (ICC '06) 2006.
- [14] Betran-Martinez, O.simeone, and Y. Bar-Ness, "Detecting Primary Transmitters via Cooperation and memory in Cognitive Radio", 41st Annual Conference on Information Sciences and Systems (CISS apos 07), 14-16 March 2007 Pp 369 – 369, 2007.
- [15] M. Gudmundson., "Correlation Model for Shadow Fading in Mobile Radio Systems", Electronics Letters, vol. 27, No. 3, 1991.
- [16] A. H. Abdallah and M. S. Beattie., "Technique for signal detection using adaptive filtering in mud pulse telemetry", US Patent 6308562.
- [17] N. Han, S. Shon, J. H. Chung, J. M. Kim, "Spectral Correlation Based Signal Detection Method for Spectrum Sensing in IEEE 802.22 WRAN Systems", ICACT, 2006.
- [18] Z. Ning, A. J. Cox , J. C. Mullikin., "SSAHA: a fast search method for large DNA databases", Genome Res. 2001 Oct;11(10):1725-9.
- [19] L. E. Baum, T. Petrie, G. Soules, and N. Weiss, "A maximization technique occurring in the statistical analysis of probabilistic functions of Markov chains", Ann. Math. Statist., vol. 41, no. 1, pp. 164--171, 1970
- [20] Paul E. Black, "Baum Welch algorithm", in Dictionary of Algorithms and Data Structures [online], Paul E. Black, ed., U.S. National Institute of Standards and Technology. 7 July 20.

Threshold Based Call Admission Control for QoS Provisioning in Cellular Wireless Networks with Spectrum Renting

Show-Shiow Tzeng and Ching-Wen Huang

Department of Optoelectronics and Communication Engineering
National Kaohsiung Normal University
Kaohsiung, 802 Taiwan, R.O.C.

Abstract- Radio spectrum is scarce and precious resource in wireless networks. To efficiently utilize radio spectrum, idle radio channels can be rented between various wireless networks and a wireless network renting out its idle channels can withdraw its radio channels when requiring its channels. However, the rental and withdrawal of radio channels result in two phenomena. One is the variation in the number of available channels in a wireless network, and the other is that a mobile user may be dropped due to the withdrawal. Threshold based call admission control, which uses an admission threshold to provide quality-of-service (QoS) guarantees for mobile users and maximize throughput, should include the two phenomena to select the optimal value of the admission threshold. In this paper, we study two call admission control schemes, namely, single-threshold call admission control and multiple-threshold call admission control, in a cellular wireless network with spectrum renting. We develop numerical analyses to analyze the performances of the two call admission control schemes, and apply the numerical analyses to select the optimal values of the admission thresholds in the two call admission control schemes such that the quality-of-services (in terms of hand-off dropping and withdrawal dropping probabilities) of mobile users are satisfied while throughput is maximized. Numerical results show that the multiple-threshold call admission control scheme outperforms the single-threshold call admission control scheme.

I. INTRODUCTION

Radio spectrum can be divided into radio channels by means of multiple access methods, such as Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) etc. Mobile users then use radio channels to access wireless services. Since radio spectrum is scarce and precious, radio spectrum should be efficiently utilized in order to allow more mobile users to access diverse wireless services in a limited radio spectrum. In the past, a large amount of radio spectrum has been statically assigned to various radio systems. However, Federal Communications Commission (FCC) indicated that most of the radio spectrum in the radio systems is underutilized [1]. One possible way to efficiently utilize the radio spectrum is to allow spectrum sharing between various radio systems [2]. One radio system can rent idle radio spectrum from (or out to) other radio systems. Then, mobile users in one radio system can dynamically access the radio spectrum in other radio systems. That is, when mobile users suffer insufficient channels in one radio system, mobile users can attempt to use idle channels in other radio systems.

Service areas in cellular wireless networks consist of cells, each of which is usually in the coverage of a base station. When a new mobile user arrives at a cell, a call admission control procedure is initiated to determine whether or not to admit the mobile user. If there are sufficient channels in the cell to satisfy the channel requirement of the mobile user, the mobile user is admitted; otherwise, the mobile user is blocked. The probability that a new mobile user seeking admission into a cell is blocked is called new call blocking probability. From the viewpoint of system providers, the new call blocking probability should be as low as possible such that more mobile users are accommodated in wireless systems and channels are utilized efficiently.

Due to the mobility of mobile users, mobile users may move from one cell to a neighbor cell. When a mobile user moves from one cell to a neighbor cell, a hand-off procedure is enabled to maintain the mobile user's communication. If the neighbor cell can provide sufficient channels to satisfy the channel requirement of the mobile user, the mobile user continues its communication; otherwise, the mobile user is dropped. The probability that a hand-off call attempt is dropped is called hand-off dropping probability. The hand-off dropping probability is an important metric of quality-of-service (QoS) in wireless networks. From the perspective of mobile users, the hand-off dropping probability should be as low as possible. To provide low hand-off dropping probability for mobile users, threshold based call admission control schemes have been discussed in [3], [4]. The basic idea of the threshold based call admission control is that new mobile users are admitted into a cell only when the number of mobile users in the cell is below a threshold (called admission threshold). Hand-off users are admitted into a cell until there is no free channel in the cell. In the other words, when the traffic load in a cell increases to a certain threshold, the remaining free channels in the cell are merely allocated to hand-off users. The smaller value of the admission threshold means more radio channels will be reserved for hand-off users; on the other hand, fewer channels are provided for new mobile users, which leads to that fewer mobile users are accommodated in a cell and that channel utilization is reduced. Therefore, the value of the admission threshold should be carefully selected such that the QoS requirement (i.e. hand-off

dropping probability) of mobile users is satisfied while throughput is maximized. The papers [3]-[4] consider an environment in which mobile users merely use channels that are statically assigned to one system.

This paper considers a cellular wireless network which allows mobile users to use idle channels in another wireless network. In such an environment, a wireless network that rents radio channels out to other wireless networks always has the first priority to use its radio channels; that is, the wireless network can withdraw its radio channels from the other wireless networks when the wireless network requires the radio channels. A mobile user is forcibly dropped when the radio channel occupied to the mobile user is withdrawn. The probability that a mobile user is dropped when the withdrawal occurs is called withdrawal dropping probability in this paper. To reduce the number of dropped calls due to the withdrawal, a wireless network does not rent all idle channels out to other wireless networks [6]; that is, partial idle channels are reserved for the wireless network. When the wireless network requires idle channels, the wireless network first uses the reserved idle channels instead of performing the operation of channel withdrawal.

According to the description in the previous paragraph, we observe that the channel rental and channel withdrawal result in two phenomena: one is the variable number of radio channels in a wireless network; the other is the call dropping due to channel withdrawal. The aforementioned papers [3], [4] discuss threshold based call admission control schemes in an environment without the two phenomena. However, it is more complicated to find the optimal value of an admission threshold in a cellular wireless network with the variable number of channels than that in a cellular wireless network with the fixed number of channels. In addition, the value of an admission threshold affects the probability that all radio channels in a cell are occupied, and as mentioned before, a channel withdrawal causes one or more dropped calls when all radio channels are occupied. Therefore, the value of admission threshold also impacts the withdrawal dropping probability. Due to the above reasons, we re-consider the threshold based call admission control schemes in a cellular wireless network with spectrum renting.

In this paper, we study threshold based call admission control in a cellular wireless network which allows mobile users to access idle radio channels in another wireless network. To adapt the characteristic of the variable available number of radio channels, this paper presents a call admission control scheme, namely, multiple-threshold call admission control, which uses multiple thresholds to determine whether or not to admit new mobile users. The multiple-threshold call admission control scheme can use different thresholds in different cases in each of which the total number of channels available for mobile users in a cell is different. For performance comparison, we also study another call admission control scheme, namely, single-threshold call admission control, which merely employs a single threshold to determine

whether or not to accept new mobile users. Numerical analyses are developed to analyze the performances of the two call admission control schemes. Using the numerical analyses, we can select the optimal values of the admission thresholds in the single-threshold and multiple-threshold call admission control schemes such that the hand-off dropping and withdrawal dropping probabilities of mobile users are satisfied while throughput is maximized. Numerical results show that the multiple-threshold call admission control scheme produces higher throughput than the single-threshold call admission control scheme.

The rest of this paper is organized as follows. Section II describes an environment of spectrum renting. The single-threshold call admission control and multiple-threshold call admission control schemes then are described in Section III. Section IV describes our numerical analyses of the two call admission control schemes. Subsequently, numerical results are described in Section V. Finally, some concluding remarks are presented in Section VI.

II. THE ENVIRONMENT OF SPECTRUM RENTING

In this section, we describe a cellular environment of spectrum renting, in which a cellular wireless network can rent idle radio channels from or out to one or more cellular wireless networks.

A cellular wireless network may be licensed for holding a radio spectrum over a long period of time. The licensed radio spectrum can be further divided into radio channels. The licensed radio channels in a cellular wireless network are called “licensed channels” herein. After mobile users register in a cellular wireless network, the mobile users can use the licensed channels in the cellular wireless network. In addition, when the mobile users are using the licensed channels in the cellular wireless network, the cellular network does not forcibly withdraw the licensed channels from the mobile users. Although a mobile user may request one or more channels, we assume, for simplicity, that a mobile user merely requires one channel in this paper.

A cellular wireless network can rent its idle licensed channels out to one or more wireless networks. In this paper, a wireless network that rents out its idle licensed channels is referred to as “channel owner”. A cellular network can also rent idle radio channels from one or more channel owners. A cellular network that rents idle radio channels from channel owners is referred to as “channel renter”. For a channel renter, the radio channels that are rented from channel owners are called “rented channels”. A channel owner can immediately withdraw its licensed channel from a channel renter when the channel owner requires the licensed channel.

In a channel renter, a rented channel can be allocated to a mobile user that registers in the channel renter. However, a rented channel may be withdrawn by a channel owner. Once this channel withdrawal occurs, the mobile user using the rented channel will be dropped. In this paper, we allow the mobile user to seek remaining idle radio channels in the

channel renter in order to continue its communication [6]. If there is at least one idle radio channel, the mobile user is allocated an idle channel and then continues its communication; otherwise, the mobile user is dropped.

III. THRESHOLD BASED CALL ADMISSION CONTROL SCHEMES

When a new mobile user arrives at a cell, a call admission control (CAC) procedure is initiated to determine whether or not to accept the new mobile user. In this section, we describe two call admission control schemes, single-threshold call admission control and multiple-threshold call admission control, in a cellular wireless network with spectrum renting.

The single-threshold call admission control scheme uses (i) a pre-determined threshold and (ii) the number of mobile users in a cell to determine whether or not to admit new mobile users. When a new mobile user arrives at a cell, the single-threshold call admission control scheme exams the above two conditions. If the number of mobile users in a cell is less than a threshold, the new mobile user is admitted; otherwise, the new mobile user is blocked. In the single-threshold call admission control scheme, the total number of channels reserved for hand-off users in a cell is equal to the total number of channels in a cell minus the threshold. The total channels in a cell include both licensed channels and rented channels. However, rented channels are opportunistically available by other wireless networks. Therefore, the number of channels reserved for hand-off users is not fixed. System providers can select the optimal value of the threshold such that the QoS requirement of mobile users is satisfied while throughput is maximized. In this paper, we would like to study the performance of the single-threshold call admission control scheme in a cellular wireless network with spectrum renting. Besides, we use the single-threshold call admission control scheme for performance comparison with the other call admission control scheme, called multiple-threshold call admission control, which is described as follows.

In cellular wireless networks with spectrum renting, the total number of channels that are available for mobile users in a network is variable. To adapt the characteristic of variable number of channels, this paper presents another call admission control scheme, namely, multiple-threshold call admission control, that uses multiple thresholds to determine whether or not to admit new mobile users. The multiple-threshold call admission control scheme can use different thresholds in different cases in each of which the total number of channels available for mobile users in a cell is different. For example, given two thresholds t and \tilde{t} which are respectively used in the conditions that the total numbers of channels in a cell are n and \tilde{n} , the multiple-threshold call admission control scheme operates as follows. When a new mobile user arrives at a cell, the multiple-threshold call admission control procedure is initiated. The multiple-threshold call admission control procedure first exams the total number of channels in a cell. If the total number of channels in a cell is equal to n , a

threshold t is selected; if the total number of channels is equal to \tilde{n} , the other threshold \tilde{t} is selected. Next, the multiple-threshold call admission control procedure uses (i) the selected threshold and (ii) the number of mobile users in a cell to determine whether or not to admit the new mobile user. If the number of mobile uses in a cell is less than the selected threshold, the new mobile user is admitted; otherwise, the new mobile user is blocked. In order to provide mobile users with satisfactory quality-of-service while maximize throughput, it is essential to select the optimal values of the multiple thresholds.

IV. NUMERICAL ANALYSES

In this section, we analyze the performances of the cellular wireless networks with the single-threshold and multiple-threshold call admission control schemes. This section first describes the assumptions in our analyses. Subsequently, we describe the Markov chains of the cellular wireless networks with the two call admission control schemes.

A. Assumptions

In this paper, we consider a homogeneous cellular wireless network. In the cellular wireless network, radio channels consist of licensed channels and rented channels. The number of licensed channels in a cell is denoted by N_l , and the number of rented channels in a cell is denoted by N_r . New mobile users arrive at a cell according to a Poisson process with mean rate λ_l^n . The lifetime which mobile users experience is assumed to be exponentially distributed with mean $1/\mu_l^n$. The duration that mobile users sojourn in a cell is exponentially distributed with mean $1/\mu_l^h$. When a mobile user attempts to hand-off to neighbor cells, the mobile user hand-offs to each of the neighbor cells with equal probability. We also assume that channel withdrawal requests arrive at a cell according to a Poisson process with mean rate λ_r . The duration that rented channels are withdrawn is exponentially distributed with mean $1/\mu_r$.

B. Single-threshold call admission control

We use a two-dimensional Markov chain, which is shown in Fig. 1, to analyze the performance of the single-threshold call admission control in a cellular wireless network with spectrum renting. Each of the states in the Markov chain is denoted by (i, j) , where i denotes the number of mobile users in a cell and j denotes the number of radio channels withdrawn from a cell. The possible value of j is an integer which is greater than or equal to 0 but is less than or equal to N_r , and the possible value of i is an integer which is greater than or equal to 0 but is less than or equal to $N_l + N_r - j$.

In Fig. 1, the value of the threshold t is a positive integer that is greater than or equal to 1 but is less than or equal to

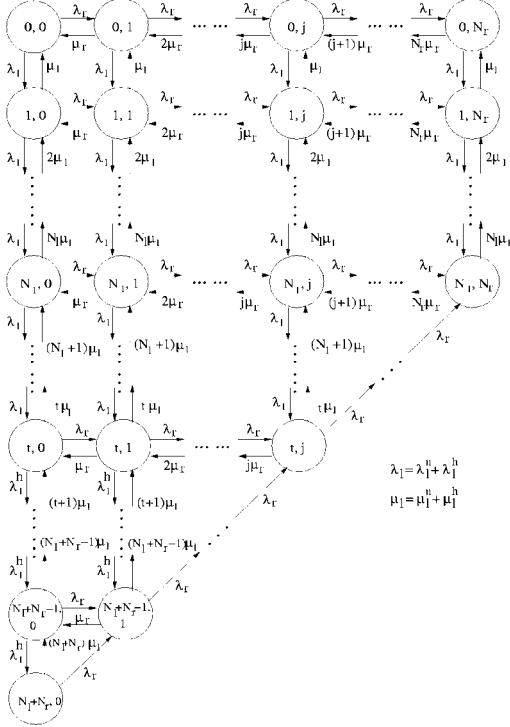


Fig. 1. Single-threshold call admission control scheme: a state transition rate diagram for mobile users in a cell.

$N_l + N_r$. λ_l^h denotes the total rate at which mobile users move from neighbor cells to a cell. If there are i mobile users in a cell, the rate at which mobile users hand-off out of the cell is $i\mu_l^h$. The mean rate at which mobile users hand-off out a cell is $\sum_{j=0}^{N_r} \sum_{i=0}^{N_l+N_r-j} i\mu_l^h \times p(i, j)$. Hand-off calls from a cell will move to each neighbor cell with equal probability. Moreover, the total rate at which hand-off calls arrive at a cell is the sum of the rates that hand-off calls move from neighbor cells. Hence, λ_l^h can be written as follows:

$$\lambda_l^h = \sum_{j=0}^{N_r} \sum_{i=0}^{N_l+N_r-j} i\mu_l^h \times p(i, j). \quad (1)$$

According to the above description of the two-dimensional Markov chain in Fig. 1, it is obvious that the Markov chain is of finite state space, irreducible and homogeneous [5]. There is a unique equilibrium probability solution for the Markov chain. We can use an iterative procedure to obtain the value of the equilibrium probability of state (i, j) , where $0 \leq j \leq N_r$ and $0 \leq i \leq N_l + N_r - j$. Then, we use the equilibrium probability to calculate new call blocking probability, hand-off dropping probability, withdrawal dropping probability and throughput as follows.

A new call arrival is blocked from entering into a cell when the number of mobile users in the cell is greater than or equal to threshold t . Hence, the new call blocking probability, P_b^s , is the sum of the probabilities of the states (i, j) , where $0 \leq j \leq N_r$ and $t \leq i \leq N_l + N_r - j$, which is given as follows:

$$P_b^s = \sum_{j=0}^{N_r} \sum_{i=t}^{N_l + N_r - j} p(i, j). \quad (2)$$

A hand-off call arrival is rejected from moving into a cell when there is no idle channel in the cell. When a hand-off call arrives in a situation that j rented channels have been withdrawn, the hand-off call is dropped if the number of mobile users in a cell is equal to $N_l + N_r - j$ (i.e. there is no idle channel). Therefore, the hand-off dropping probability in a situation that j rented channels have been withdrawn, $P_{d,j}^s$, where $j = 0, 1, \dots, N_r$, is given as follows:

$$P_{d,j}^s = \frac{p(N_l + N_r - j, j)}{\sum_{i=0}^{N_l + N_r - j} p(i, j)}. \quad (3)$$

It is necessary to keep the hand-off dropping probability below a certain value in various situations that different rented channels have been withdrawn. In this paper, we attempt to keep the hand-off dropping probabilities, $P_{d,j}^s$ where $j = 0, 1, 2, \dots, N_r$, below a certain value in all situations.

When an operation of channel withdrawal is involved in a situation that all rented channels are occupied, a mobile user will be forcibly dropped in order to withdraw a rented channel. Since an operation of channel withdrawal will not occur in the case that all rented channels have been withdrawn, a channel withdrawal will merely occur in the states (i, j) , where $0 \leq j \leq N_r - 1$ and $0 \leq i \leq N_l + N_r - j$. Once a channel withdrawal occurs, a withdrawal dropping will occur in the situation that all radio channels are busy. Hence, the withdrawal dropping probability, P_w^s , can be calculated as follows:

$$P_w^s = \frac{\sum_{i+j=N_l+N_r} p(i, j)}{\sum_j \sum_i p(i, j)}, \quad (4)$$

where $0 \leq i \leq N_l + N_r - j$ and $0 \leq j \leq N_r - 1$.

The throughput produced in the system with the single-threshold call admission control scheme, U^s , can be calculated as follows:

$$U^s = \sum_{j=0}^{N_r} \sum_{i=0}^{N_l + N_r - j} i\mu_l^n \times p(i, j). \quad (5)$$

In order to guarantee the quality-of-service metrics (in terms of hand-off dropping probability and withdrawal dropping probability) below a certain value at any load, we consider a load condition where the new call arrival rate per cell, λ_l^n , approaches infinity. Consider the Markov chain in Fig. 1 under an infinite load, we can further derive the asymptotic values of the hand-off dropping probability $P_{d,j,\infty}^s$, where

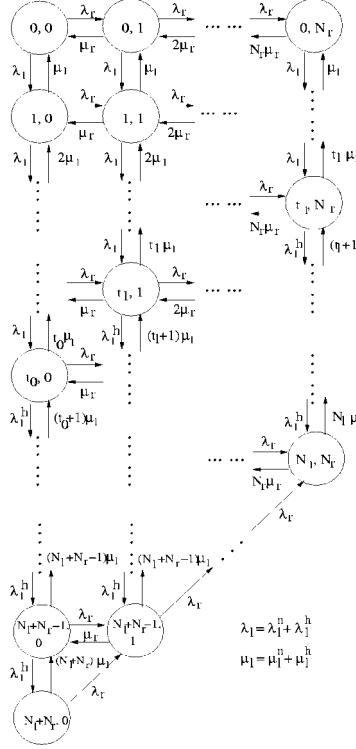


Fig. 2. Multiple threshold call admission control scheme: a state transition rate diagram for mobile users

$0 \leq j \leq N_r$, and the withdrawal dropping probability $P_{w,\infty}^s$ as follows:

$$P_{d,j,\infty}^s = \frac{p_\infty(N_l + N_r - j, j)}{\sum_{i=\min(t, N_l + N_r - j)}^{N_l + N_r - j} p_\infty(i, j)}, \text{ where } 0 \leq j \leq N_r. \quad (8)$$

$$P_{w,\infty}^s = \frac{\sum_{i+j=N_l+N_r} P_\infty(i, j)}{\sum_j \sum_i p_\infty(i, j)}, \quad (9)$$

where $0 \leq j \leq N_r - 1$ and $\min(t, N_l + N_r - j) \leq i \leq N_l + N_r - j$.

C. Multiple-threshold call admission control

A two-dimensional Markov chain, as shown in Fig. 2, is used to analyze the performance of the multiple-threshold call admission control in a cellular wireless network with spectrum renting. The Markov chain in Fig. 2 has the same states as the Markov chain in Fig. 1, but the transition rates in the two Markov chains are partially different.

The multiple-threshold call admission control scheme uses different thresholds in different cases in each of which the number of rented channels available for mobile users in a cell is different. In Fig. 2, the admission threshold used in a

situation that j rented channels have been withdrawn is denoted by t_j , where $0 \leq j \leq N_r$.

It is obvious that the Markov chain in Fig. 2 is ergodic [5]. There is a unique equilibrium probability solution for the Markov chain. We use the equilibrium probability to derive new call blocking probability P_b^m , hand-off dropping probability $P_{d,j}^m$, withdrawal dropping probability P_w^m and throughput U^m as follows.

$$P_b^m = \sum_{j=0}^{N_r} \sum_{i=t_j}^{N_l + N_r - j} p(i, j). \quad (10)$$

$$P_{d,j}^m = \frac{p(N_l + N_r - j, j)}{\sum_{i=0}^{N_l + N_r - j} p(i, j)}, \quad \text{where } 0 \leq j \leq N_r - 1. \quad (11)$$

$$P_w^m = \frac{\sum_{i+j=N_l+N_r} p(i, j)}{\sum_j \sum_i p(i, j)}, \quad (12)$$

where $0 \leq i \leq N_l + N_r - j$ and $0 \leq j \leq N_r - 1$.

$$U^m = \sum_{j=0}^{N_r} \sum_{i=0}^{N_l + N_r - j} i \mu_l^i \times p(i, j). \quad (13)$$

For the multiple-threshold call admission control scheme, we also consider a load condition where the new call arrival rate per cell, λ_l^n , approaches infinity. Consider the Markov chain in Fig. 2 under an infinite load, the asymptotic values of the hand-off dropping probability $P_{d,j,\infty}^m$, where $0 \leq j \leq N_r$, and the withdrawal dropping probability $P_{w,\infty}^m$ can be derived as follows:

$$P_{d,j,\infty}^m = \frac{p_\infty(N_l + N_r - j, j)}{\sum_{i=t_j}^{N_l + N_r - j} p_\infty(i, j)}, \quad \text{where } 0 \leq j \leq N_r. \quad (15)$$

$$P_{w,\infty}^m = \frac{\sum_{i+j=N_l+N_r} p_\infty(i, j)}{\sum_j \sum_i p_\infty(i, j)}, \quad (16)$$

where $0 \leq j \leq N_r - 1$ and $t_j \leq i \leq N_l + N_r - j$.

V. NUMERICAL RESULTS

In this section, numerical results are presented to study the performances of the single-threshold and multiple-threshold call admission control schemes. The parameters used in numerical results are described as follows. The number of licensed channels in a cell is 10. The maximum number of rented channels in a cell is equal to 4. The mean lifetime of mobile users, $1/\mu_l^n$, is equal to 120 seconds. The mean duration that mobile users sojourn in a cell, $1/\mu_l^h$, is 60 seconds. The mean duration that rented channels are withdrawn, $1/\mu_r$, is equal to 40 seconds. The channel withdrawn rate, λ_r , is equal to 1/300.

To fairly compare the performances of the two call admission control schemes, each of the call admission control schemes will select its optimal threshold(s) from a wide range of possible thresholds such that the quality of services are

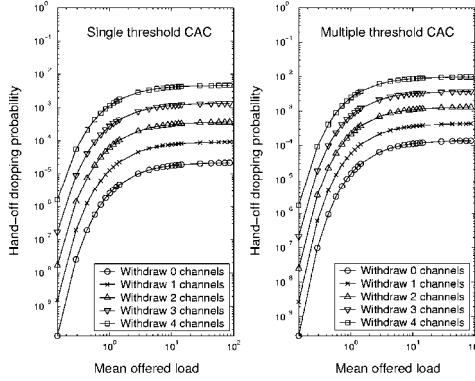


Fig. 3. Hand-off dropping probabilities of single-threshold and multiple-threshold call admission control

satisfied while throughput is maximized. In the single-threshold call admission control scheme, the possible value of the admission threshold t in a cell ranges from 1 to 14. In the multiple-threshold call admission control scheme, the possible values of admission thresholds t_j , where $0 \leq j \leq 4$, range between 1 and $14 - j$. QoS metrics herein are the hand-off dropping and withdrawal dropping probabilities. The hand-off dropping probabilities in various situations, in each of which the number of withdrawn rented channels is different, will be kept below 10^{-2} . The withdrawal dropping probability is also kept below 10^{-2} . Using the numerical analyses, the optimal value of the admission threshold in the single-threshold call admission control scheme is 4, and the optimal values of the admission thresholds, t_0 , t_1 , t_2 , t_3 , t_4 , in the multiple-threshold call admission control scheme are 5, 3, 2, 3 and 3. Fig. 3 shows the hand-off dropping probabilities of the single-threshold and multiple-threshold call admission control schemes in various situations in each of which the number of withdrawn rented channels is different. In order to observe whether the hand-off dropping probabilities of the two call admission control schemes can be kept below 10^{-2} in heavy load, the maximum value of the offered load is up to 100. From the figure, we can observe that the two call admission control schemes keep their hand-off dropping probabilities below 10^{-2} in various situations at different loads.

Fig. 4 shows the withdrawal dropping probabilities and throughputs of the single-threshold and multiple-threshold call admission control schemes at different loads. From the figure, we can observe that the two call admission control schemes keep their withdrawal dropping probabilities below 10^{-2} . From the figure, we can also observe that the multiple-threshold call admission control produces higher throughput than the single-threshold call admission control scheme. This is because the multiple-threshold call admission control scheme uses appropriate thresholds in different situations in each of which the number of rented channels available for mobile users is different. On the contrary, the single-threshold

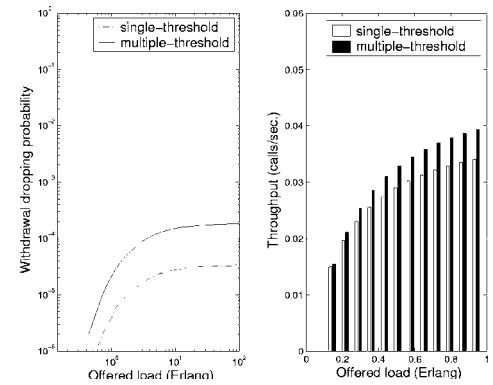


Fig. 4. Withdrawal dropping probability and throughput call admission control scheme uses the same threshold in the different situations.

VI. CONCLUSIONS

In this paper, we study threshold based call admission schemes for QoS provisioning in cellular wireless networks with spectrum renting. Two call admission control schemes, namely, single-threshold call admission control and multiple-threshold call admission control, are presented. We employ two-dimensional Markov chains to analyze the two call admission control schemes. Based on the analyses, we can select optimal thresholds for the two call admission control schemes such that the hand-off dropping and withdrawal dropping probabilities are kept below a certain value while throughput is maximized. Numerical results show that multiple-threshold call admission control scheme yields higher throughput than the single-threshold call admission control scheme in the constraint that the hand-off dropping and withdrawal dropping probabilities of the two call admission control schemes are kept below a certain value.

ACKNOWLEDGMENTS

This research was partially supported by the National Science Council, Taiwan, under grant NSC97-2622-E-017-001-CC3.

REFERENCES

- [1] FCC, "ET Docket No 03-222 Notice of proposed rule making and order," December 2003.
- [2] I.F. Akyildiz, W.-Y. Lee, M.C. Vuran, S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, Sep. 2006, pp. 2127-2159.
- [3] B. Gavish and S. Sridhar, "Threshold priority policy for channel assignment in cellular networks," *IEEE Transactions on Computers*, vol. 46, no. 3, March 1997.
- [4] X. Chen, B. Li, and Y. Fang, "A dynamic multiple-threshold bandwidth reservation (DMTBR) scheme for QoS provisioning in multimedia wireless networks," *IEEE Transactions on Wireless Communications*, vol. 4, no. 2, pp. 583-592, March 2005.
- [5] B. Bolch et al. *Queueing Networks and Markov Chains: Modeling and Performance Evaluation with Computer Science Applications*, John Wiley and Sons 1998.
- [6] X. Zhu, L. Shen, and T.-S.P. Yum, "Analysis of cognitive radio spectrum access with optimal channel reservation," *IEEE Communications Letters*, vol. 11, no. 4, pp. 304-306, April 2007.

Ontology-Based Web Application Testing

Samad Paydar, Mohsen Kahani
Computer Engineering Department, Ferdowsi University of Mashhad
samad.paydar@stu-mail.um.ac.ir, kahani@um.ac.ir

Abstract- Testing Web applications is still a challenging work which can greatly benefit from test automation techniques. In this paper, we focus on using ontologies as a means of test automation. Current works that use ontologies for software testing are discussed. Further a theoretical roadmap is presented, with some examples, on ontology-based web application testing.

Keywords: Ontology, Software testing, Web application, test automation.

I. INTRODUCTION

Web applications possess special characteristics, such as multi-tiered nature, multiple technologies and programming languages being involved in their development, highly dynamic behavior and lack of full control on user's interaction. This makes the analysis and verification of such systems more challenging than traditional software. Therefore, Web application testing is a labor-intensive and expensive process. In many cases, new testing methods and techniques are required, or at least some adaptations must be applied to testing methods targeted at traditional software [1][2]. Further, with the new trend in web based systems, i.e. using Web Services and SOA-based systems which lead to highly-dynamic and more loosely-coupled distributed systems, the situation gets even more challenging [1].

Test automation, that is, automating the activities involved in testing process, leads to more cost-effective, labor-saving and time-preserving methods. Using methods and techniques for automated testing of web applications can reduce the above mentioned costs and complexities [1].

Generally speaking, there are three main types of automation in software test domain.

1. Writing programs that perform some type of tests on systems. Unit testing is a good example of such automation. In order to test a unit of a system, e.g. a method, a program is written to execute the required tests on the test target. Of course, this is not limited only to unit testing, and for instance, it is possible to write a program to perform functional tests on a Web application using HTTPUnit [3]. This kind of automation, despite its great value, may be expensive for testing web applications, because such systems always grow in size and frequency of modification. We call this type, *manual test generation, automatic test execution*.
2. The second type of automation usually deals with coarse-grained goals, such as functionality testing and acceptance testing. The automation is mainly performed by capture/replay methods [3], relying heavily on human involvement and user interaction. Capture/replay methods, being not real automated methods, are not so cost-effective and scalable, because the capturing phase, which is the main part of the test, needs human intervention and it might be expensive or very hard to

capture all interactions and user scenarios [4]. We call this type, *manual test case generation, automatic test execution*.

3. The third type of automations is automatic test generation based on some formal model or specification of the system. This kind of automation, which is called model-based testing, is nearer to real automation. Many works in the literature have been reported using this type of automation [1]. We call this type, *automatic test generation, automatic test execution*.

Beside this categorization, there are some other technologies that can be used for web application testing. For instance, intelligent agents are autonomous and able to live and migrate across the network and adapt to the dynamic and loosely-coupled nature of web applications. Therefore as suggested in [1], they fit better for automating web application testing. Web services can also be considered as another example of such enabler technologies, especially for testing of highly-dynamic and loosely-coupled systems like service-oriented systems [5].

Ideally, to fully automate the testing process, i.e. replacing the human tester with a computer and remove all dependencies on human, all kinds of knowledge that is required for the test process, must be acquired from the human tester and transferred to the computer in a formal and machine understandable format. Ontologies, as a powerful tool for capturing domain knowledge in a machine understandable format, show great potentials for being used to move toward this way.

In our view, ontologies can be assumed as a very powerful infrastructure for real automation of web application testing. Therefore they can be considered in the third category of automation types.

In this paper, we first present current works that have used ontologies in software testing process, and then discuss their benefits, capabilities and potential uses for automating web application testing.

II. CURRENT WORKS

An ontology is an explicit and formal specification of a conceptualization of a domain of interest [6]. To state it simpler, an ontology defines the basic terms and relations comprising the vocabulary of a topic area as well as the rules for combining terms and relations to define extensions to the vocabulary [7]. The main point about the ontology is its formality and therefore machine-processable format. Ontologies can be used in different phases of software development [8]. Here we are concentrated on current works that have used ontologies for software testing process.

In [9], an agent-based environment for software testing is proposed with the goal of minimizing the tester interferences. There are different kinds of agents in the system, such as interface agent, execution agent, and oracle

agent. Each kind of agent is responsible for one part of the testing process. For example, TCG (Test Case Generator) agent has the role of test case generation. In order to enable agents to communicate and understand each others' messages, and also share a common knowledge of the test process, an ontology for software testing is developed and used. This ontology contains concepts like activities, stages, purposes, contexts, methods, artifacts, etc.

TestLixis a project with the goal of developing necessary ontologies for Linux test domains. It focuses on 3 ontologies: OSOnto (Operating System Ontology), SwTO (Software Test Ontology), SwTOi (Software Test Ontology Integrated). This project is registered in 2007/4/14, but there is no information or documentation available on the project homepage [10].

In [11], a work is introduced which is about development and use of ontologies of the fault and failure domains of distributed systems, such as SOA-based system and Grids. The work is said to be in the early stages of the ontology development. It is hoped that in future, this ontology can be used to guide and discover novel testing and evaluation methods for complex systems such as Grids and SOA-based systems. In this work, ontologies are viewed as an intelligent communication media for machines, and also as a means for enabling machines to acquire knowledge necessary to develop their own strategies for testing and evaluating systems.

In [12], ontologies have been used to model Web service composition logics, Web service operational semantics, and test case generation for testing Web services. OWL-S is used to describe the semantic and application logic of the composite Web service process. Then, using the Petri-Net ontology, developed by the authors, a Petri-Net model is constructed to depict the structure and behavior of the target composite service. Then, using the Petri-Net model of the composite service, and the ontology, test cases are generated for testing the service.

In [13], an ontology is developed for software metrics and indicators. ISO standards, for instance ISO/IEC 15939 standard[14], and ISO/IEC 9126-1 standard[15], have been used as the main source for development of the ontology. The authors have described the application of this ontology in a cataloging system. This system provides a collaborative mechanism for discussing, agreeing, and adding approved metrics and indicators to a repository. In addition, the system provides semantic-based query functionality, which can be utilized for consultation and reuse. Similar work is also presented in [16].

A SOA-based framework is proposed for automated web service testing in [17] and [18]. The authors have mentioned some technical issues that have to be addressed in order to enable automated online test of web services. For instance, issues like how to describe, publish, and register a testing service in a machine understandable encoding, or how to retrieve a testing service. To resolve these issues, a software testing ontology named STOW (Software Testing Ontology for Web Services) was developed.

In addition to categorization of terms and concepts, they have defined appropriate relations, which can be used to do

some reasoning in the testing process. For instance, when a testing service with the capability of testing Java applets is requested, and there is a testing service capable of testing Java programs, it can be reasoned that the later can be used for the required task.

In [8], some examples of ontology applications throughout the whole software development lifecycle are presented. It is claimed that in the testing phase, a non-trivial and expensive task, which demands some degree of domain knowledge, is the task of writing suitable test cases. They propose to use ontologies to encode domain knowledge in a machine processable format. Using ontologies for equivalence partitioning of test data is mentioned as an example. In addition, by storing the domain knowledge in an ontology, it will be possible to reuse this knowledge.

In [19] the main focus is to use ontologies in early software design phases, i.e. specifications, with emphasis on detecting conceptual errors, such as mismatches between system behavior and system specifications. In addition, an architecture and some required tools are presented to support such conceptual error checking.

In [20] it is suggested that ontologies can be used as semantic formal models, and hence MDA (Model-Driven Architecture) can be extended to ODA (Ontology-Driven Architecture). Using ontologies, it will be possible to represent unambiguous domain vocabularies, perform model consistency checking, validation and some levels of functionality testing.

III. ONTOLOGY-BASED SOFTWARE TESTING REQUIREMENTS

In this section we discuss the required steps to reach the goal of ontology-based web application testing.

The process of using ontologies in software testing can be divided into two phases or activities.

1. The first one is developing the required ontology which captures an appropriate level of required knowledge to perform the testing process. By 'required knowledge' and hence 'required ontology', we mean two different kinds of knowledge and hence ontology:
 - The first kind of knowledge required is the knowledge of the testing process, i.e. different types of tests, their goals, limitations and capabilities, the activities involved in testing, their order and relation. Obviously this kind of knowledge is vital for automating web application testing. Therefore from the point of view of ontology-based software testing, it is required to develop an ontology which captures an appropriate level of this knowledge in a machine processable format.
 - The second kind of knowledge required is the application domain knowledge. It is required to know the concepts, possibilities, limitations, relations, and expected functionalities of the application under test. For instance, testing an online auction web application will require different knowledge from what is needed for testing an e-learning application. One simple reason is that to perform some tests, like functional test, it is required that expected functionalities be known. Therefore, to fully automate the test process, an appropriate level

- of application domain knowledge is required to be captured and formally expressed through an ontology.
2. The next phase is to develop procedures for utilizing the knowledge embedded in the ontology to automate different tasks in the testing process. Of course the two stages are not necessarily independent or completely sequential. It is possible to start second phase with a reasonable ontology and incrementally improve and enhance the ontology and the testing processes.

A. *Ontology developing for application testing*

Although development of a knowledge-rich ontology is a time-consuming and laborious activity, it seems that it does not possess serious technical problems that need innovative ideas. Currently there are numerous environments for ontology development and also tools and utilities to automate some activities of ontology development. For instance, there are tools that extract basic terms and concepts from a set of technical documents using text-mining methods, though their results need to be verified by an expert [21]. It is worth to note that once an ontology is developed for web application testing, it can be frequently reused and incrementally evolved and improved.

As stated before, an ontology defines the basic terms and relations comprising the vocabulary of a topic area, as well as the rules for combining terms and relations to define extensions to the vocabulary. So the main part of the ontology development is to extract the terms, concepts, relations and rules of the domain. Currently there are good sources available for this purpose. Here, we discuss some of them.

As stated in [22], The Guide to the Software Engineering Body of Knowledge (SWEBOK) is a project of IEEE Computer Society and Professional Practices Committee which aims at providing a consensually validated characterization of the bounds of the software engineering discipline and to provide a topical access to the Body of Knowledge supporting that discipline [23].

The Body of Knowledge is divided into ten software engineering Knowledge Areas (KA) (Fig. 1). To promote a consistent view of software engineering worldwide, the guide uses a hierarchical organization to decompose each KA into a set of topics with recognizable labels. A two- or three-level breakdown provides a reasonable way to find topics of interest. The breakdowns of topics do not presume particular application domains, business uses, management philosophies, development methods, and so forth. The extent of each topic's description is only that needed to understand the generally accepted nature of the topics and for the reader to successfully find reference material.

One of the KAs defined in SWEBOK, is the Software Testing KA. This KA is a useful source for developing ontology of software testing. As shown in Figure 2, the number of concepts and facts and relations in the Software Testing KA, is noticeable in comparison to other KAs. Chapter 5 of the guide, which is focused on Software Testing, presents a breakdown of the topics and related concepts in a manner that can be helpful for developing the ontology. Although it does not mainly focus on web

application testing, but it can be used as a useful guide to manage and organize the concepts and relations.

In addition, there are ISO and IEEE standards that can be used to extract the main terminology, concepts, and their relations[14], [15], [24].

Therefore we believe that the first phase, that is, the development of an ontology for web application testing is not theoretically so challenging.

Software requirements
Software design
Software construction
Software testing
Software maintenance
Software configuration management
Software engineering management
Software engineering process
Software engineering tools and methods
Software quality

Fig. 1. SWEBOK knowledge areas (KAs)

B. *Ontology developing for application domain*

It is not a good idea to first develop the system completely and then start to develop its ontology separately from the scratch; rather it is desirable to somehow synchronize the development of the system with the development of its ontology. We see two approaches for reaching to this goal.

One approach is to develop the application domain ontology and then start to develop the application. In this approach, supporting tools and environments are required to help the developer use and communicate with the developed ontology, while developing the application. For instance, when designing a HTML form containing a text field, the designer can annotate the text field with the term 'emailAddress' defined in the ontology of the application previously designed. The main difficulty of this approach is of course the development of the application domain ontology. It is worth to note that although it may seem that postponing the development of the system to the completion of the development of the ontology will lengthen the development lifecycle, but it undoubtedly will shorten the testing time and therefore this drawback can be somehow remedied.

The second approach is to use ODA, as to some extent suggested in [20]. In this case, it is required to develop the semantically-rich formal models of the system using ontologies. Then, automatically extract the executables of the system from these models. Although this approach is an open field for future research, but it is worth noting that currently it is possible to use UML and OCL as a language for designing ontologies of the system and then from UML, get executable code, though not 100% complete. Using UML for developing ontologies is used in [18] [25] for example, and significant work has been done to bring together Software Engineering languages and methodologies such as the UML with Semantic Web technologies such as RDF and OWL,

exemplified by the OMG's Ontology Definition Metamodel (ODM) [20].

	Relationships	Concepts	Facts	Principles
Software Requirements	24	240	72	0
Software Design	44	307	211	2
Software Construction	21	214	63	0
Software Testing	96	1001	165	7
Software Maintenance	44	706	140	0
Software Configuration Management	31	85	46	0
Software Engineering Management	33	72	46	0
Software Engineering Process	45	587	134	1
Software Engineering Tools and Methods	19	263	62	0
Software Quality	34	447	61	5
TOTAL	407	4141	1087	15

Figure 2- Overview of quantity of elements in the SWEBOk

C. Developing intelligent methods to utilize the ontology

Once the required ontologies, whether ontology of the testing process or ontology of the application domain, are developed, the main part of the job can be started. That is, to develop intelligent methods and procedures that utilize the available ontologies to minimize the human intervention in the testing process.

Although some works in this direction, has been reported in the literature ([12], [18]), but this is still an open research area and the methods of using ontologies, needs to be improved. For instance, in [9], which is an agent-based testing framework, ontology is used only as a communication media between the agents. Agents run procedures that are exactly hardwired in them, and there is no inference or adaptation.

To further move in this area, it is required to utilize ontologies to enable agents dynamically devise their plans and procedures. This is needed because it can eliminate the need to hardwire all procedures within the agents.

IV. POTENTIAL APPLICATIONS OF ONTOLOGIES IN WEB APPLICATION TESTING

Ontologies are a means of capturing knowledge of a domain in a machine understandable manner. Therefore by using well-developed ontologies, we would be able to write intelligent methods that automate different tasks and activities of the testing process. In this section, we present some examples to show potentials of using ontologies to automate web application testing:

1. Using ontologies for test planning and Test specification: Using an ontology that provides the knowledge of different testing activities and their order and relationships, it is possible to specify the test plan in a machine understandable language. For instance, in the presence of such ontology, by specifying that "system X must be tested using black-box strategy", it

can be inferred that what type of tests, in what order, must be performed on this system, and which test criteria and test case generation method should be used.

2. Using ontologies for semantic querying: Using ontology in different testing activities, such as test planning, test specification, test execution and result evaluation, enable automatic generation of the whole test process documents in a machine-understandable format. Therefore it will be possible to retrieve test process information using semantic queries. For instance, after performing code coverage on an application, it would be possible to ask the system which classes or methods have nor been sufficiently tested.
3. Using Ontology as an enabler: Using web services for testing web based application, especially large, distributed ones, seems a good idea because of the interesting properties that they have, such as being loosely coupled, dynamic, and interoperable. In such cases, i.e. using web services for different activities in the testing process, there is a potential for ontology to be utilized for service definition, publication, registration, advertisement and retrieval. In addition to web services, agents are also a good candidate for automating the test process. In this view, ontologies can be used more than just as a communication media, making it possible to share the domain knowledge between agents and make them cooperate with each other. In addition, agents can utilize the ontology to perform their tasks more intelligently.
4. Using Ontology for test case generation: Ontologies show great potentials to be used for test case generation. Here, we just mention some examples. These potentials can be divided into two categories:
 - a. *Test case generation based on the software test ontology.* For instance, based on the test type that is to be performed, it might be necessary to use different test generation methods. E.g. when

performing security tests on a web application, it is better to use SQL injection or cross site scripting techniques to generate test data, which is used to fill form fields. However, when performing functional testing, other techniques are more appropriate.

- b. *Test case generation based on the domain ontology of the application under test.* For instance, while testing the registration page of a web forum application, ontology of the application domain- in this case a web forum- can be used to generate appropriate test data for registration form fields. As an example, if a form field is properly annotated with the term “User.Age”, it can be used for equivalence partitioning of candidate test data for entering in this field. If a form field is annotated with “Pass.MinLen=6”, this information can be used to infer border values for password length, so generating good set of test data. As another example, annotating a form field with term “EmailAddress” and another field with “CountryName”, enables generation of different and specific test data.
- 5. *Ontologies for test oracle:* One of the main obstacles in really and fully automating software test process is the test oracle. As mentioned in [26], “*It is little use to execute a test automatically if execution results must be manually inspected to apply a pass/fail criterion. Relying on human intervention to judge test outcomes is not merely expensive, but also unreliable*”. Ontologies can be used for test oracle automation. An oracle must judge on the result of a test execution, deciding whether the test is passed or failed. This judgment is based on a set of criteria, which can be categorized and defined formally, and hence can be to some extent embedded in ontologies. Therefore, it is possible to specify the evaluation criteria of each test type in the ontology in order to be used by the automated oracle to judge the test results. For instance, while performing load or performance test on a web application, test results can be judged based on the delay of the HTTP responses. Or, in some cases, test results can be judged by inspecting absence or presence of a special term in the HTTP response. Also, HTTP status codes can be used for this purpose. More complicated judgments may also be automated. For instance, it may be possible to specify in a test specification, that if the test runs successfully, a new record must be inserted [deleted, or changed] in [from, in] table X of database D. Of course, there may be some cases which cannot be satisfied by a non-human oracle, e.g. verifying how user-friendly a system is.

V. CONCLUSION

In this paper we first presented a brief survey of current works that have used ontology in the software testing process. Then, the possible applications of using ontologies in web application testing were investigated.

It can be concluded that the full potential of using ontologies for web application testing has yet to be explored and it is an open area for research and innovation to develop intelligent methods and procedures for maximize the automation of different activities involved in software testing process.

ACKNOWLEDGMENT

This work has been supported by a grant by Iran’s Telecommunication Research Center (ITRC), which is hereby acknowledged.

REFERENCES

- [1]. G.A. Di Lucca, A.R. Fasolino, “Testing web-based applications: The state of the art and future trends”, Information and Software Technology 48:1172-1186, 2006.
- [2]. Y. Wu, J. Offutt, “Modeling and testing web-based applications”, GMU ISE Technical Report, ISE-TR-02-08, 2002.
- [3]. F. Ricca, P. Tonella, “Web Testing: a Roadmap for the Empirical Research”, WSE:63-70, 2005.
- [4]. K. Li, M. Wu, “Effective GUI Test Automation: Developing an Automated GUI testing Tool”, Sybex publications, p20, 2005.
- [5]. H. Zhu, “A Framework for Service-Oriented Testing of Web Services”, COMPSAC, 2006.
- [6]. T.R. Gruber, “A translation approach to portable ontologies”, Knowledge Acquisition, 5(2):199-220, 1993.
- [7]. R. Neches, R.E. Fikes, T. Finin, T.R. Gruber, T. Senator, and W.R. Swartout, “Enabling technology for knowledge sharing”, AI Magazine, 12(3):36-56, 1991.
- [8]. H. J. Happel, S. Seedorf, “Applications of Ontologies in Software Engineering”, 2nd Int. Workshop on Semantic Web Enabled Software Engineering (SWESE 2006).
- [9]. R. Maamri, Z. Sahnoun, “MAEST: Multi-Agent Environment for Software Testing”, Journal of Computer Science, April, 2007.
- [10]. TestLix Project: <http://projects.semwebcentral.org/projects/testlix/>
- [11]. The White Rose Grid e-Science Centre, “Developing a Fault Ontology Engine for the Testing and Evaluation of Service-Oriented Architectures”, September, 2006.
- [12]. Y. Wang, X. Bai, J. Li, R. Huang, “Ontology-Based Test Case Generation for Testing Web Services”, ISADS, March 2007.
- [13]. M. de los Angeles Martin, L. Olsina, “Towards an ontology for software metrics and indicators as the foundation for a cataloging web system”, LA-WEB, 2003.
- [14]. ISO/IEC 15939:2007 – “Systems and Software Engineering - Measurement Process”, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44344
- [15]. ISO/IEC 9126-1:2001 – “Software Engineering – Product Quality - Part 1: Quality Model”, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22749
- [16]. M. Genero, F. Ruiz, M. Piattini, C. Calero, “Towards an Ontology for Software Measurement”, SEKE 2003.
- [17]. H. Zhu, “A Framework for Service-Oriented Testing of Web Services”, COMPSAC 2006.
- [18]. H. Zhu et al, “Developing A Software Testing Ontology in UML for A Software Growth Environment of Web-Based Applications”, “Software Evolution with UML and XML”, 2004, chapter 9.
- [19]. Y. Kalfovglou, “Deploying ontologies in Software Design”, Ph.D. thesis, Dept. of Artificial Intelligence, University of Edinburgh, 2000.
- [20]. W3C Semantic Web Best Practices & Deployment Working Group, “Ontology Driven Architectures and Potential Uses of the Semantic Web in Systems and Software Engineering”, 2006.
- [21]. C. Calero, F. Ruiz, M. Piattini, “Ontologies for Software Engineering and Software Technology”, Springer, 2006, chapter 1.
- [22]. “Guide to the Software Engineering Body of Knowledge”, www.swebok.org/ironman/pdf/SWEBOK_Guide_2004.pdf
- [23]. Guide to the SWEBOK, <http://www.swebok.org/>
- [24]. IEEE Standard for Software Test Documentation, 1998.
- [25]. S. Cranfield, “UML and the semantic web”, proceedings of International Semantic Web Working Symposium (SWWS), 2001.
- [26]. M. Pezz, M. Young, “Software Testing and Analysis: Process, Principles and Techniques”, 2008, section 17.5.

Preventing the “Worst Case Scenario:” Combating the Lost Laptop Epidemic with RFID Technology

David C. Wyld
Southeastern Louisiana University
Department of Management – Box 10350
Hammond, LA 70402-0350

Abstract- This paper examines the most frequent cause of data breach today – that of stolen or lost laptops. Over one million laptops go missing each year in the U.S., creating tremendous problems and exposure for American companies, universities, government agencies, and individuals. This paper first looks at the size and scope of the laptop theft problem and the ramifications of the loss of the hardware and data contained on the device. Then, the paper examines new developments in the use of RFID (radio frequency identification) technology as a potential deterrent and detection device for laptop security. It concludes with an analysis of the impact of the application of RFID in this area, looking at the legal, IT, and financial aspects of the issues involved in enhancing laptop security. With laptop sales far-outpacing those of PCs and with form-factors shrinking, the issues involved with laptop security will only increase in coming years.

I. INTRODUCTION

The airport security line. All of us dread the now familiar ritual. Shoes off, belts off, jackets off, jewelry off, drinks thrown away, and of course, laptops out of their cases. We always see the unknowing – the grandmother from Poughkeepsie who hasn’t flown since the days of propellers and flight attendants offering real meals with actual silverware en route – and the tremendously inconvenienced – the gentleman in a wheelchair and the mother with three kids struggling to comply. Still, we Americans who travel routinely comply with the airport security drill knowing that it is now just part of life in a post 9/11 world, and airports are even trying to make the process faster – by adding more lanes – and – dare we say – a bit fun, as anyone who has seen the video instructions at Las Vegas’ McCarran International Airport, which features noted entertainers from the Las Vegas Strip, including the Blue Man Group and Cirque du Soleil acrobats, trying to comply with TSA (Transportation Security Administration) guidelines [1].

Still, there is that moment of fear when one places your laptop – laden with your work, your iTunes™, your copy of The Matrix, and in most cases, valuable corporate data and client info – on the screening belt. What if you get distracted by other passengers and their travails? What if you get selected for the special, more intense screening? What if your carry-on has to be hand-inspected for having too big a bottle of shampoo? What if you shouldn’t have had that last overpriced beer in the airport bar? The “what if” question

lingers in the mind of every business traveler – what if I lose my laptop?

II. THE LOST LAPTOP PROBLEM

The Ponemon Institute, an independent information technology research organization, recently released an astonishing report detailing the extent of the problem of lost laptops in the airport environment – answering the “what if” question with data suggesting that the problem of lost – and most commonly, stolen – laptops is reaching epidemic proportions at U.S. airports. They found that, on average, at the nation’s largest 106 commercial airports, over 12,000 laptops are lost or stolen each week – a staggering 600,000 laptops annually [2]! While some have criticized the Ponemon Institute’s study for extrapolating figures to overestimate the size of the laptop security issue, the findings have found support from a variety of computer security and airport industry experts [3,4]. For instance, Charles Chambers, Senior Vice President of Security for the Airports Council International North America, believes the loss of 12,000 laptops per week is very plausible, considering that there are 3.5 million business travelers flying each week [5].

As can be seen in Table 1, an analysis shows that there is not a direct correlation between the size of the airport and the rate of laptop losses [2]. In fact, while Atlanta’s airport is the busiest in the nation – and indeed the entire world, it is tied for eighth overall in the rate of laptop disappearances. In fact, the rate of laptop losses in Atlanta is equal to that of Ronald Reagan Washington National Airport, the 29th busiest in the nation, an airport that handles less than a quarter of the passengers traveling through Hartsfield-Jackson Atlanta International.

As can be seen in Figure 1, not surprisingly, fully 40% of all airport laptop losses take place at the security checkpoint, where by design, a traveler must be separated from his or her laptop [2]. Earlier this spring, the Transportation Security Administration announced that it was working with laptop bag manufacturers to create designs that would allow for full scanning without the owner needing to remove the laptop from its case at security checkpoints. It is expected that by 2009, we will see the introduction of “checkpoint-friendly” laptop cases to the market [6]. This could indeed work to greatly lessen the problem of laptops being lost, stolen, or just forgotten at airport security lines. Still, for the vast majority of all air travelers, for the next few years until such

approved laptop cases become commonplace, the airport security line may be the place where one's corporate laptop – and thus the valuable corporate data contained inside – is most vulnerable.

Airport	Airport Traffic Ranking	Number of Lost Laptops per Week
Los Angeles International (LAX)	3	1200
Miami International (MIA)	16	1000
New York John F. Kennedy International (JFK)	6	900
Chicago O'Hare International (ORD)	2	825
Newark Liberty International (EWR)	10	750
New York La Guardia (LGA)	20	630
Detroit Metropolitan Wayne County (DTW)	12	575
Ronald Reagan Washington National (DCA)	29	450
Hartsfield-Jackson Atlanta International (ATL)	1	450
Washington Dulles International (IAD)	21	400

Tab. 1. The Top Ten U.S. Airports for Laptop Loss.
Source Data: The Ponemon Institute, July 2008.

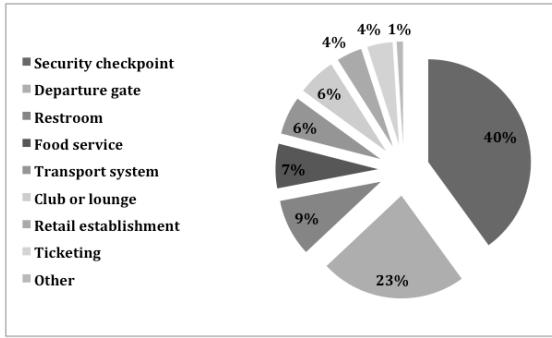


Fig. 1. Laptop Losses by Location in Airports.
Source Data: The Ponemon Institute, July 2008.

Perhaps the most astonishing statistics in the Ponemon Institute's study concern what happens after the traveler discovers that his or her laptop has went missing. Quite concerning for corporate IT managers is the fact that in over two-thirds of all loss cases – fully 69% of the time, the laptop is not reunited with its owner. What was even more surprising perhaps was the fact that of the business travelers surveyed by the Ponemon Institute for the report, when asked what they would do when they discovered their laptop was missing, 16% responded that they would do nothing, and over half would contact their company for help or instructions before seeking to find the laptop themselves [2]!

III. THE HIGH COST OF LAPTOP LOSSES

Of course, unfortunately, laptops are lost or stolen not just in airports, but everywhere and anywhere. In fact, in the U.S.,

it has been estimated that upwards of a million laptops are stolen annually, with an estimated hardware loss alone totaling over a billion dollars [7]. And it is not just companies that are affected. Indeed, across federal agencies, leading universities, and all facets of healthcare and education, there is increasing focus on laptop theft, as surveys of IT executives across organizations of all types show such occurrences happening on a routine basis – often with dire consequences potentially impacting thousands of employees, customers, patients, and students [8].

Until recently, a common misconception was that the impact of a lost or stolen laptop was merely the cost a replacing the hardware – the laptop itself, a replacement cost that could be assumed to continue decline over time [9]. However, in 2001, the respected Rand Corporation released a study that pegged the actual replacement cost of a lost laptop and found the average value to be over \$6,000. The Rand researchers included not just the replacement cost for a new unit plus any payments owed on the missing item, but the data and software lost on the laptop, as well as the added costs to the organization in terms of procuring and setting-up the replacement computer [10]. When including potential loss of corporate data and legal liability, the dollar loss can be quite high. There are wide variances in the estimates of the financial losses stemming from laptop theft, with losses ranging from simple replacement costs of a few thousand dollars to estimates ranging into the millions. Beyond replacement costs, there may be far greater – and more costly impacts – from loss of customer information and records to loss of confidential business information and intellectual property, such as marketing plans, software code and product renderings.

In 2004, a joint study issued by the Computer Security Institute and the Federal Bureau of Investigation (FBI) estimated the cost per incident to be approximately \$48,000 [11]. iBahn, a leading provider of secure broadband services to hotels and conference centers, found that the average business traveler has over \$330,000 worth of personal information on their laptop [12]. In a white paper entitled, *Datagate: The Next Inevitable Corporate Disaster?*, the value of a lost notebook computer, in terms of confidential consumer information and company data, was pegged at almost \$9 million [13]. In fact, a recent study has projected that when confidential personal information is lost or stolen, the average cost to a company is \$197 per record [14]! Overall, the National Hi-Tech Crime Unit has pegged stolen laptops as having a greater impact on organizations than any other computer threat, including viruses and hackers [15]. Finally, in today's 24/7 media environment, there is also a "hit" on the company's name brand and image from the negative public relations garnered from such cases, which can translate into declining consumer trust in doing business with the firm and actual negative impact on sales and revenue, at least in the short-term, and in some extreme cases, with long-term impact. The FBI itself is not immune from the problem, for it has been estimated that the agency loses 3-4 laptops each month [16]!

IV. AN EXAMINATION OF RFID SOLUTIONS FOR LAPTOP SECURITY

There is a wide array of data protection measures available today for laptops, from physical locks to data backups to password protection to encryption and even biometrics [17]. There are also software-based products, most notably Vancouver, BC-based Absolute Software's Computrace® Agent that can be built into BIOS of the machine at the factory [18]. However, RFID-based solutions are just now beginning to enter the marketplace.

In the U.S., corporate and governmental interest in acquiring RFID-based laptop security systems is indeed accelerating. In the private sector, clients range from Fortune 500 companies to even smaller businesses [11]. Across higher education, colleges and universities are seeking to replace their laborious paper and bar-code based systems for inventorying laptops and other IT assets with RFID installations [19]. In the federal government, a number of Cabinet-level agencies have begun looking to RFID solutions. Carrollton, Texas-based Axcess International, Inc. is working with three federal agencies on RFID tracking of their laptop assets within their facilities with their ActiveTag™ solution [20]. This spring, Profitable Inventory Control Systems, Inc. (PICS), based in Bogart, Georgia, began an installation of their AssetTrakker system for the headquarters building of the U.S. Army National Guard in Washington, DC. The National Guard has approximately ten thousand electronic assets – with up to 8 per employee - that will be tagged as part of the PICS installation, which will begin with the use of hand-held readers for inventory purposes and expand to include readers at building doorways and the parking garage to track movements and send alerts for unauthorized movements [21].

There are other new U.S.-based entrants in the emerging RFID laptop protection market. Cognizant Technology Solutions' RFID Center of Excellence recently reported that it has developed and implemented an RFID-based laptop tracking system for internal use with its over 45,000 employees who use more than 10,000 laptops at its locations around the world which could serve as the basis for a commercially-available solution [22]. Saratoga, California-based AssetPulse, Inc. recently introduced its AssetGather solution for tracking laptops and other electronic equipment with RFID. The AssetGather system is designed to work with any type or brand of tags (passive, semi-passive or active) and various forms of readers. The AssetGather software is web-based, and it can provide dashboard controls and real-time visibility on a client's IT assets across multiple locations, including map, graph and list views, based on user preferences. AssetGather can also provide IT managers with reporting and audit controls. It can also provide users with programmed alerts on specific suspect laptop movements, including:

- Perimeter Alerts: Alert when an asset goes outside its permitted “home” zone

- Delinquency Alert: An alert is raised when an asset is not seen back within configured time
- Serial Number Alert: An alert action is triggered when a specific asset is seen [23].

And interest in laptop security is quickly becoming a global marketplace. In India, Orizin Technologies has recently introduced a system for laptop tracking. Using active RFID tags, capable of tracking laptops and other IT assets in an organization's premises with a range of up to 20 meters [24]. Finally, perhaps the most innovative RFID solution to date comes from the United Kingdom. Sheffield, England-based Virtuity, Ltd. has introduced a data protection solution under the brand name BackStopp. In short, the BackStopp solution uses RFID tags to ensure that laptops are securely maintained within the allowable range of a client's facilities. So, as long as the laptop is within range, it operates normally. However, if it is removed on an unauthorized basis from the permitted range, the BackStopp server attempts to locate the laptop, using both the Internet and the internal GSM card on the laptop [25]. Protection goes beyond that though, as BackStopp immediately blocks any unauthorized user from accessing the computer and sends out a “self-destruct” message to the laptop to securely and permanently delete the data on the hard drive of the computer [26]. BackStopp also has what Virtuity terms a “culprit identification capability” in that the built-in webcam capabilities found in many laptops today are prompted to take and transmit digital images that might very well capture the laptop thief [27].

V. ANALYSIS

Much of IT security is based on knowing that a threat is foreseeable, and unfortunately, corporate expenditures against known and continuing threats, from spyware, computer virus, hackers, denial of service attacks, and other cyber threats are just a cost of doing business in the Internet Age. And today, laptop theft is a similar foreseeable, ongoing threat. Experts have pegged the probability of a given laptop being lost or stolen at between 1 and 4%. Using the FBI's \$48,000 laptop loss estimate, and assuming just a 1% loss probability, the expected loss per laptop – each year - is \$480. If one uses higher probabilities in the range – between 3 and 4%, the expected loss would easily equal or exceed the actual hardware replacement costs of 95% of all laptops on the market [11]! Thus, even with significant investments for hardware and software to implement an RFID-based security, when considering the potential demonstrated costs of the loss of even a single laptop, the ROI equation for RFID protection is clearly demonstrable. And, as we have seen in cases involving companies like IBM, The Gap, and Pfizer and governmental agencies ranging from the U.S. military to leading universities, the larger the organization, the larger the potential vulnerability [28]. Indeed, according to a report from the U.S. House of Representatives' Committee on Government Reform, the theft of a single laptop from a Department of Veterans Affairs employee exposed personal

information on 2.5 million active and retired military personnel [29]!

Finally, a basic understanding of statistics shows that the chance of a laptop loss occurring for any one company or one individual goes up over time! So, to guard against this foreseeable threat is not just being proactive, it may even be a necessity in today's legal environment. Courts are increasingly looking at steps that a company has taken to better secure its data in case of a security breach as a mitigating factor in cases stemming from such data loss. Further, legal analysts believe that the much-discussed Sarbanes-Oxley Act (SOX) may indeed impose new legal requirements on corporate IT departments to safeguard its mobile devices as part of its fiduciary duty to maintain a system of adequate internal controls [11].

Today's concerns over laptop security may indeed be just the tip of an data security iceberg, when one considers the panoply of mobile devices used in business today – cell phones, PDA's, Blackberry devices, etc., especially as form factors across the board for all such electronics shrink [15]. While fixed computers still outsell laptops (with just over 150 million desktops sold in 2007), laptop sales are themselves surging, with approximately 110 million units shipped worldwide last year. In fact, global laptop shipments grew by 33% between 2006 and 2007, while PC shipments grew just 4% year over year during the same time period [30]. So, there will be no abating the challenge – and market prospects – for laptop security. The challenge will be to move beyond the closed-loop, four wall-delimited solutions being introduced and marketed today to more open systems solutions that would enable tracking and location of laptops on a global basis. Let's face it, we have RFID-based systems on the market today for finding lost luggage in an airport [31], lost medical equipment in a hospital [32], and even for tracking down golf balls lost in the woods [33], but if you lose your laptop in an airport, hotel, restaurant today, you have no way to remotely locate it today, simply because it is a location outside the closed-loop of protection. The company that can find a way to create such location systems in high traffic areas – such as airports - that can be available "on demand" will find significant interest worldwide. With scary statistics such as those conveyed in this report, the marketing should be an easy sell – namely to take away the very real fears of traveling executives and their IT managers.

REFERENCES

- [1] B. Wilson, "TSA pilot would offer ads at airport security checkpoints," *Aviation Week*, January 4, 2007. Retrieved July 6, 2008, from http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=omm&id=news/ADS01047.xml.
- [2] The Ponemon Institute, *White Paper - Airport insecurity: The case of lost laptops*, June 30, 2008. Retrieved July 2, 2008, from http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf.
- [3] P. Seitz, "New Dell services help users hunt down missing laptops," *Investors Business Daily*, June 30, 2008. Retrieved July 4, 2008, from <http://investors.com/editorial/IBDArticles.asp?artsec=17&issue=20080630>.
- [4] T. Wilson, "Laptop losses total 12,000 per week at US airports: Nearly 70% are never recovered, many go unreported," *Dark Reading*, July 2, 2008. Retrieved July 13, 2008, from http://www.darkreading.com/document.asp?doc_id=158099&f_src=dr
- [5] D. Hughes, "12,000 laptops lost weekly at U.S. airports," *Aviation Week*, July 3, 2008. Retrieved July 10, 2008, from http://www.aviationnow.com/aw/generic/story_channel.jsp?channel=omm&id=news/LAP07038.xml&headline=12,000%20Laptops%20Los%20Weekly%20At%20U.S.%20Airports.
- [6] T. Frank, "TSA takes steps toward speedier laptop X-rays," *USA Today*, July 6, 2008. Retrieved September 13, 2008, from http://www.usatoday.com/travel/flights/2008-07-06-laptops_N.htm.
- [7] Identity Theft Daily Staff, "Costs attributable to laptop theft are projected to exceed \$1 billion," *Identity Theft Daily*, July 16, 2008. Retrieved AUgust 20, 2008, from [http://www.identitythetfdaily.com/index.php/20080714370/Latest/Costs-Attributable-to-Laptop-Theft-Are-Projected-to-Exceed-\\$1-Billion.html](http://www.identitythetfdaily.com/index.php/20080714370/Latest/Costs-Attributable-to-Laptop-Theft-Are-Projected-to-Exceed-$1-Billion.html).
- [8] J. Ryder, "Laptop security, part one: Preventing laptop theft," *Security Focus*, July 30, 2001. Retrieved May 28, 2008, from <http://www.securityfocus.com/infocus/1186>.
- [9] A. Sacco, "Lax laptop security can be dangerous ... and expensive," *Network World*, November 12, 2007. Retrieved June 11, 2008, from <http://www.networkworld.com/news/2007/111207-lax-laptop-security-can-be.html>.
- [10] J. Arquilla, *Networks and netwars: The future of terror, crime, and militancy*. Santa Monica, CA: RAND Corporation, 2001.
- [11] A. Griebenow, *White Paper: RFID as mandatory protection for laptops*, March 2008. Retrieved September 22, 2008, from <http://www.mediarecovery.com/library/AxcessLaptopWhitePaper.pdf>.
- [12] A. Sacco, "Study: Average value of business info on travelers' laptops equals \$525K - The average value of personal information on travelers' laptop computers is \$330,000, according to iBahn," *Network World*, October 17, 2007. Retrieved August 14, 2008, from http://www.cio.com/article/147000/Study_Average_Value_of_Business_Info_on_Travelers_Laptops_Equals_K.
- [13] McAfee and Datamonitor, *White Paper - Datagate: The Next Inevitable Corporate Disaster?*, April 2007. Retrieved October 2, 2008, from http://www.mcafee.com/us/local_content/misc/dlp_datagate_research.pdf.
- [14] The Ponemon Institute, *2007 Annual Study: Cost of a data breach*. Retrieved July 28, 2008, from http://www.ponemon.org/press/PR_Ponemon_2007-COB_071126_F.pdf.
- [15] G. Gruman, "How to lock up laptop security," *CIO Magazine*, October 22, 2007. Retrieved June 27, 2008, from http://www.cio.com/article/147900/How_to_Lock_Up_Laptop_Security/.
- [16] M.O. Foley, "New technologies to thwart laptop theft." *Inc.*, August 2007. Retrieved September 22, 2008, from <http://technology.inc.com/hardware/articles/200708/theft.html>.
- [17] R.K. Raghavan, "Protect your laptop," *The Hindu Business Line*, June 18, 2007. Retrieved August 14, 2008, from <http://www.thehindubusinessline.com/ew/2007/06/18/stories/2007061850010200.htm>.
- [18] G. Gruman, "ABC: An introduction to mobile security," *CIO Magazine*, March 8, 2007. Retrieved June 27, 2008, from http://www.cio.com/article/40360/ABC_An_Introduction_to_Mobile_Security/.
- [19] A. Foster, "Increase in stolen laptops endangers data security," *The Chronicle of Higher Education*. Retrieved July 25, 2008, from <http://chronicle.com/free/v54/i43/43a00103.htm>.
- [20] Anonymous, "Dallas-based AXCESS' RFID technology used by U.S.government to stop laptop theft," *Pegasus News*, April 17, 2007. Retrieved September 29, 2008, from <http://www.pegasusnews.com/news/2007/apr/17/dallas-based-axcess-rfid-technology-used-us-govern/>.
- [21] C. Swedberg, "Army National Guard tracks assets: A PICS RFID system enables U.S. Army National Guard divisions to locate laptop computers and other electronics as they are moved in and out of their Washington, D.C., headquarters," *RFID Journal*, March 3, 2008.

- Retrieved July 22, 2008, from
<http://www.rfidjournal.com/article/articleview/3951/1/1/>.
- [22] B. Violino, “Eating your own dog food: Cognizant Uses RFID to Track Laptops - The global technology solutions company is currently deploying an asset-tracking system throughout its development facilities worldwide,” *RFID Journal*, January 21, 2008. Retrieved August 22, 2008, from
<http://www.rfidjournal.com/article/articleview/3857/>.
- [23] AssetPulse, Inc., *Fact Sheet: AssetGather for laptop tracking - RFID-based solution for tracking laptops and IT assets*, July 2008. Retrieved September 8, 2008, from
<http://www.assetpulse.com/solutions/AssetGatherForLaptopTracking.pdf>.
- [24] Anonymous, “Orizin Technologies launches active RFID system for laptop tracking,” *Newswire Today*, September 3, 2007. Retrieved July 19, 2008, from <http://www.newswiretoday.com/news/23006/>.
- [25] Virtuity, Ltd., *Fact Sheet: What is BackStopp?*, February 2008. Retrieved May 27, 2008, from
http://www.backstopp.com/what_is_backstopp.aspx.
- [26] G. Dixon, “Self-destruct laptops foil thieves: Wi-Fi and RFID system destroys sensitive data,” *Vnunet.com*, February 19, 2008. Retrieved July 17, 2008, from
<http://www.vnunet.com/vnunet/news/2209973/laptops-set-self-destruct>.
- [27] J.E. Dunn, “Laptop wipes own hard drive to beat thieves: A new laptop protection system can automatically wipe hard disk data on machines taken from authorized locations,” *PC World*, February 19, 2008. Retrieved July 17, 2008, from
<http://www.pcworld.com/printable/article/id,142631/printable.html>.
- [28] D. Goodin, “Mind the gap: Data for 800,000 job applicants stolen. The Register, September 28, 2007. Retrieved July 28, 2008, from
http://www.theregister.co.uk/2007/09/28/gap_data_breach/.
- [29] U.S. House of Representatives, Committee on Government Reform, *Staff Report: Agency data breaches since January 1, 2003*, October 13, 2006. Retrieved September 19, 2006, from
<http://oversight.house.gov/documents/20061013145352-82231.pdf>.
- [30] Y. Ting and J. Tsai, “Worldwide notebook shipments grow 33% on year in 2007, says IDC,” *DigiTimes*, January 31, 2008. Retrieved June 29, 2008, from
<http://www.digitimes.com/NewsShow/MailHome.asp?datePublish=2008/1/31&pages=PD&seq=209>.
- [31] D.C. Wyld, M.A. Jones, and J.W. Totten, “Where is my suitcase?: RFID and airline customer service,” *Marketing Intelligence & Planning*, vol. 23, no. 4, pp. 382-394.
- [32] B. Bachelder, “Medical distributor puts RFID tags on equipment,” *RFID Journal*, July 25, 2006. Retrieved September 20, 2008, from
[http://www.rfidjournal.com/article/articleview/2513/1/1/](http://www.rfidjournal.com/article/articleview/2513/1/1).
- [33] D.C. Wyld, “Sports 2.0: A look at the future of sports in the context of RFID’s ‘weird new media revolution,’” *The Sport Journal*, October 2006. Retrieved October 26, 2006, from
<http://www.thesportjournal.org/article/sports-20-look-future-sports-context-rfid-s-weird-new-media-revolution>.

Information Security and System Development

Dr. PhD Margareth Stoll Margareth.stoll@dnet.it
Dr. Dietmar Laner dlaner@eurac.edu
EURAC Research, Drususallee, 1
39100 Bozen, South Tyrol, Italy

Abstract-Due to globalization, stronger competition, increased complexity, information explosion, interconnection and extensive use of IT data and information management are main performance driver and key differentiator for sustainable organization success. Long time organizations had developed IT systems regarding overall access rights. Due to stronger requirements of data protection code and increased requirements for data integrity, availability and confidentiality information security is a key requirement for system development. Many organizations of different sizes are implementing standard based management systems, such as quality ISO9001, environmental ISO14001 or others, which are based on common principles: objectives and strategies, business processes, resource management and continuously optimization. Due to this situation we used in different case studies as basis for system development a the organization adapted, holistic, standard based management system to analyze the system requirements. This promotes legal conformity, information security awareness, effectiveness and information security improvement for sustainable organization success.

Keywords: information security, management system, system development, data protection, system integrity

I. INTRODUCTION

A Starting Situation

Due to globalization and the distribution of organization units over all the world, ever stronger competition, information explosion, increasing interconnection, extensive use of IT-systems and increased complexity the need for continually improvement data and information management for knowledge generation and continual improvement are main performance driver and key differentiator for competitive advantages and sustainable organization success. Data, information and knowledge are exposed to most different threats, such as physical and environmental threats, technical threats and organizational and human related threats. Long time organizations had developed IT applications regarding overall access rights. In the last years the data protection law requirements are sharpened, the IT governance requirements and thereby the data integrity requirements are increased and based on the main role of data, information and knowledge the requirements for confidentiality and availability are increased.

Many organizations of different size and scopes are implementing already for several years process oriented management system as quality ISO9001, environmental ISO14001,

IT service ISO/IEC 20000-1, hygiene management systems ISO 22000 or others or others. These systems are implemented more frequently holistic, whereby are integrated according with the organizational purpose and objectives different aspects, like quality, environment, hygiene, occupational health and safety, as well as human resource development, resource management, IT - management, communication management, controlling and also knowledge management. The established management system must be documented, communicated, implemented and continuously improved. Thereby the system documentation contains the entire actual explicit knowledge and supports individual and thus organizational learning, whereby management systems push constantly the knowledge and learning spiral, change organizational knowledge and promote sustainable the organizational development.

B Purpose of the article

The increased requirements for information security including availability, confidentiality and integrity, international standards such as ISO/IEC 27001, ISO/IEC 20000-1, Sarbanes-Oxley and others requires a holistic information security oriented system development approach.

Organizations commit a radical error and analyze their organization by the lens of their lived processes. They ask themselves "how can we use new technology to optimize our processes" instead of, "how we can do something new with the technology automation instead innovation" [1]. IT objective must be to promote in the best way possible the organization objectives.

Thus we need a holistic, systematic approach, which is oriented to the organization objectives and promote a constantly development to fulfill stakeholder requirements including information security requirements, to guarantee a sustainable organizational development by increased information security, efficiently and effectiveness and reduced costs.

C Research Approach

The always stronger requests for stakeholder orientation, information security, efficiency, effectiveness, innovation, shorter change cycles, process orientation, process and service improvement, cost reduction and the increasing implementation of holistic, process oriented management systems, the great importance of the continually organization optimization, the individual and organizational learning and the IT

involvement leaded us to introduce as basis for system development a the organization adapted, holistic, interdisciplinary, integrated, standard based management system to analyze security and stakeholder requirements, integrate, optimize and harmonize processes, services, documents and concepts to promote legal conformity, information security awareness, effectiveness and information security improvement as part of organizational development to guarantee sustainable organization success.

D Structure of the article

Firstly we describe based on the starting situation the project objectives [II] and illustrate the common requirements of international standards for management systems [III]. Afterwards we explain our approach [IV]. Finally we document the project experiences and results of the implementation in different organizations with distinct management systems [V] including the achievement of the project principles [V A] and a reflection about success factors [V B] and at the end we express an outlook [VI] and our conclusion [VII].

II. PROJECT OBJECTIVES

Due to this starting situation we have to resolve following questions in order to contribute to organization success by using IT security:

- How we can establish organization objectives and strategies and thereby information security requirements regarding the requirements of all stakeholders (shareholder, customer, collaborators, supplier, environment and society)?
- How can we promote sustainable continually information security improvement and optimization of the organization in accordance to stakeholder requirements and established organization objectives?

By implementing a holistic, interdisciplinary, integrated, information security oriented standard based management system for IT system development we expect to foster:

- Legal conformity: data protection and information security laws will be respected
- Information security awareness: the collaborators awareness for information security will increase
- Effectiveness: the whole organization will be managed by figures to fulfil effectively the established objectives including information security objectives
- Information security improvement by employee involvement and knowledge generation.

Continually organization development promotes sustainable stakeholder orientation, information security, quality and cost effectiveness.

III. MAIN REQUIREMENTS OF STANDARD BASED MANAGEMENT SYSTEMS



Fig. 1. Main requirements of standard based management systems

The standards for management systems have different specialized focuses, but are all based on common principles [2], [3], [4]:

- Organizations objectives and strategies must be established regarding stakeholder requirements.
- All business processes including management process, support processes, resource processes and optimization processes must be defined and promote the optimized fulfilment of the organization objectives under the focus of the respective standard.
- Process oriented resource management must be promoted including human resource development, IT – management and other infrastructures, tools and instruments.
- The organization, their objectives and strategies, services/ products and processes must be continually optimized according to established processes in sense of a PDCA cycle (plan, do, check, act).

The established management system must be structured and systematically documented and communicated within the organization and the collaborators must be continually motivated for implementing the system and for recommending improvements.

These standard based management systems are implemented more frequently in a holistic way. In accordance with the organizational purposes and objectives are integrated in a management system different aspects like quality, environment, hygiene, occupational health and safety, as well as human resource development, resource management, IT - management, communication management, controlling and also knowledge management.

IV. APPROACH

Due to large relevance and range of a project for implementing a holistic, interdisciplinary, integrated, process oriented, standard based management system as basis for IT system development should be used project management methods

for planning, adapting optimally to customer requirements, implementing and the objective fulfillment should be controlled constantly by concrete figures deduced from the stakeholder requirements.

A Stakeholder oriented organization objectives

For establishing the vision, organization objectives and strategies we use quality function deployment [5]. With the concerned collaborators including management we define and prioritize the stakeholders. Due to experiences from intensive contact between stakeholder and collaborators and / or due to interviews, literature research, market research stakeholder's requirements and expectations are identified. Subsequently they are prioritized and thus vision, policy and organization objectives are deduced from them. Establishing the policy, objectives and strategies we consider also the information security objectives and determine therefore security strategies [6]. Due to standard requirements we deduce from defined vision, policy and organization objectives longer-term strategic objectives and concrete full year objectives with appropriate programs and projects, figures, responsible, deadlines and necessary resources. Thus the entire organization is focused on stakeholder requirements including information security.

B Process analysis and process improvement

The process steps are analyzed with associated responsible persons "bottom up" including the necessary information, data and documents [1]. Thereby we consider all organizational processes: beginning from the management process, all business processes including the development and design process, as well all supporting processes, resources processes and optimization processes. In accordance with the organizational purposes and objectives are also considered information security aspects regarding availability, confidentiality and integrity and data protection in accordance to established information security objectives, as well as different other aspects like quality, environment, hygiene, occupational health and safety, human resource development, resource management, IT - management, communication management, controlling and also knowledge management and integrated into a holistic model. All processes are analyzed, optimized regarding the established organization objectives and this aspects, as well efficiency, effectiveness, harmonized regulations, legal and regulatory interpretations, information flow, collection and passing necessary knowledge by checklist, regulations, forms and workflow based databases and optimized, if possible [7]. Thereby implicit knowledge is externalized, knowledge identified and possible optimizations (knowledge generation) are discussed.

Analyzing the process steps we recognize these, in which experiences and special legal or regulation interpretations (lessons learned) are developed and these experiences will be documented for later use [8], [9], [10]. Thus for all necessary documents and forms e.g. grant application forms, tem-

plates are developed, whereby these must be examined e.g. for fulfilling the relevant data protection code, only once by specialized experts and afterwards every collaborator is able to fill them with the personal data of applicant. Appropriate applies to checklists, into which the specialized knowledge of the experts is integrated and thereby implicit knowledge is externalized. Further these checklists are continually extended or changed regarding the defined optimization processes according to the experiences during the application in the work everyday life or if special cases appears, which are not clearly regulated until now. Also experiences and necessary interpretations of data protection laws and regulations are integrated and the knowledge base and processes changed flexible. In the same way knowledge, which is no more needed, is removed in time. Thereby we integrate optimal information security with process modeling, process standardization, transparency and need and objective oriented flexible process implementation.

Accordingly also the necessary information regarding data protection about customer/citizen should be analyzed and their collection and processing should be planed and implemented systematically and structured. In the public administration can be integrated directly into the workflow a user-oriented, context sensitive interface to the legal requirements and regulations, which are relevant for the single process step including data protection and other information security regulations. Thereby a need oriented, context sensitive knowledge source for information security is integrated directly into the working process. It is also integrated by input of personal notes into auxiliary systems.

For the process documentation we use a very simple form of flow charts, which is modeled by graphic support tools [Fig.2.]. By process modeling for all process steps the responsible functions, as well as documents, information, tools, IT - applications including the observing information security laws and regulations are defined. For all documents we deduce from the process model the responsible persons for establishing, generating, changing, handling, as well as the read entitled functions, also possible external information sources or receiver (document logistic), the data protection class in accordance to the data protection law and further the required archiving methods (for current, intermediate and historical archiving). Thereby we define necessary and licit access rights, archiving procedures, information security requirements regarding confidentiality, availability and integrity, signature rights and signature procedures as basis for the implementation of the signature regulations and required data encryption with necessary encryption procedures. Thereby all information security requirements and necessary treatments in accordance to a holistic information security management system regarding ISO/IEC 27001 information security management are established and afterwards implemented systematically and optimized constantly. Due to establish external sources and receivers and the necessary data exchange between the different IT - applications are defined also all required interfaces. All treated data are examined for it necessity and lawfulness.

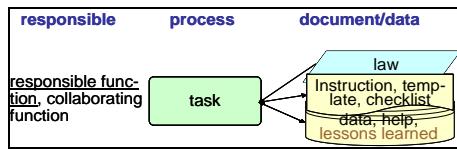


Fig. 2. Applied process documentation method

Based on the established processes we conduct an information security risk assessment to reduce risks to acceptable levels of risk. Therefore we identify the asset, define the required levels of confidentiality, integrity and availability for the assets, identify the potential threats to those assets, define the realistic likelihood of security failures, the impacts that losses of confidentiality, integrity and availability may have on the assets, the controls currently implemented, estimate the levels of risks regarding the implemented controls and elaborate for the higher risk options for the treatment of risks. The management approve whether the risks are acceptable or further risk treatments are to implement. For the treatment of risks control objectives and controls are selected and approved. This risk treatment plan is integrated into the operational processes. For the identified remaining risk is developed a business continuity plan to maintain or restore operations and ensure availability at the required level and in the required time scale following interruption to, or failure of, critical business processes. Also this business continuity plan is integrated into the operational processes and thereby implemented, maintained, tested and updated regularly to ensure its effectiveness.

To promote efficiency already existing customer data should be accessed regarding data protection law and not collected another time. If there are changes, the data must be changed immediately in all applications and all necessary subsequent procedures must be taken. To guarantee the necessary data integrity we need clear harmonized regulations.

Function profiles and competences are deduced from the definition of the responsible persons for the single process steps. Thus knowledge carriers are specified and knowledge maps - yellow pages- are constructed. For all function profiles the necessary requirement profiles can be intended due to the posed process steps and the necessary knowledge [9], [11], [12].

C Resource management

The organization must determine and provide due to standard requirements necessary resources, tools and instruments to obtain the established objectives and to continually improve the organization. Therefore also optimal IT – systems are promoted.

In the resource management also training and competence objectives must be planned, realized according to defined processes and their effectiveness has to be evaluated. Thus the continual improvement of information security is promoted systematically and structured, their effectiveness evaluated and possibly necessary corrective actions are taken. The strengthened IT – applications effect task modifications, redistribution of responsibilities, job enlargement, stronger

customer orientation, increased service quality and service orientation and this requires self and social competencies, communication skills, media competences, IT – competences, information security awareness, interest in new knowledge, change and learning willingness, team ability, openness and tolerance, empathy, as well as autonomous, entrepreneurial spirit, self-driven, objective oriented acting and strategic thinking in accordance to established regulations and also system and process oriented thinking. Therefore suitable human resource development projects must be developed, implemented and their effectiveness evaluated. Further usually the personnel order (like career profiles, requirement profiles, selective procedures) must be changed.

D Continually improvement

In management systems the ability to achieve planned objectives are evaluated periodically in base of established measurements (process and organization measurements including customers satisfaction) and consequently determined, implemented and evaluated necessary corrective, optimization or preventive actions. Integrating information security objectives and strategies into the objectives and strategies of the whole organization also the information security is thereby constantly evaluated and if necessary changed and optimized. For problem solving, the implementation of recognized optimizations and for preventive actions must be determined and implemented appropriate systematically and structured problem solving, optimization, change and documentation processes. Other optimizations and / or preventive actions are introduced by means of collaborators ideas and suggestions and systematically handled. Also periodically internal and external audits, feedbacks from stakeholders, the collaboration with supplier and praxis experiences promote possible optimizations, which are handled systematically. These promotes a systematically organization development, service, product and process innovations and a continually information security and organization improvement in accordance to established objectives and stakeholder requirements. Therefore the organization and information security are continuously coordinated optimized according to organization objectives and experiences. Theoretical considerations are tested in practice. Thereby we integrate also optimal process modeling, process standardization and transparency with need and objective oriented flexible process implementation. Changing organizational knowledge new individual learning becomes possible. Thus new knowledge will be generated, represented, discussed, communicated and implemented. Thereby the knowledge and learning spiral is constantly pushed again and the organizational knowledge base is extended continually [13].

E IT Implementation

A established, implemented and optimized, standard based, the organization optimally adapted management system regarding information security requirements and data protection offers by its strong stakeholder and objective orienta-

tion, the systematically, structured and holistic approach, the collaborator involvement, the harmonized, simplified, in the practice “tested” and optimized processes and forms an optimal basis for a stakeholder and objective oriented, efficiently, effectively, holistic and lower-cost IT system using workflow based database. By strong and early user involvement and a systematically, holistic, information security regarding requirement analysis the IT will best adapted to the organization, information security and stakeholder requirements and promotes a sustainable organization optimization.

V. PROJECT EXPERIENCES AND RESULTS

This concept for establishing and implementing a holistic, integrated, information security oriented standard based management system for IT system development is implemented successfully in several organizations with different management systems. Thereby implementing information security and process thinking, harmonizing and simplifying processes and process and information security controlling were great challenges.

A Achieving the project objectives

The described concept leads the following case study results collected by measuring the established process and system measurements and interviewing the managers and collaborators:

- Legal conformity: Due to accurate analysis of data protection and information security law requirements and there implementation by IT system development the legal conformity is increased and legal changes are implemented systematically and structured following established procedures.
- Information security awareness: Due to discussion during elaborating the system requirements the collaborators awareness for information security increased and due to effectively trainings maintained. Also constantly information security discussions and the whole improvement process promote continually information security.
- Effectiveness: the fulfilment of the established objectives including information security objectives is periodically evaluated by defined measurements. The customer satisfaction and the fulfilment of the objectives were increased constantly over more years. By an optimal IT support the measurements can be continually evaluated with no additional expenditure. Many collaborators and specially managers felt the clear definition of objectives and aligned measurements as a great help and assistance.
- Information security improvement by employee involvement and knowledge generation: Prior to introducing the management system the collaborators ideas and suggestions were occasionally missing on the way through the different decision levels. Now all ideas are documented, handle in accordance to established processes and all col-

laborators receive a reliable answer. The collaborators appreciate it and bring in a lot of ideas and suggestions.

-

Establishing and optimizing an business processes in accordance with the defined organization objectives including information security and involving early the collaborators and the following IT implementation using workflow based systems of the optimized processes promotes the user system acceptance and they feel it as helpful tool and instrument to mange their job. Thereby are realized optimal starting conditions for holistic system development to promote organization success.

Standard based, holistic management systems are by there clear structured, holistic, systemic approach, there strong orientation to stakeholders, there systematic process approach and the continually optimization through measurement and facts an excellent reference models for a holistic development and implementation of IT systems regarding also information security.

By optimizing information and communication flows, the organizational relationship promoted by process thinking, the implemented human resource development, the increased system availability, knowledge exchange and knowledge generation and the improved collaborators involvement increased the collaborators satisfaction.

The new IT system is felt from the collaborators not as the introduction of something new one, but seen as a helpful, useful, best need adapted, powerful tool to accomplish their job efficiently and effective.

Developing an IT system by this approach the IT system is adapted optimal to the requirements of the user and the organization, fulfills all legal requirements regarding information security and can contribute thereby in the best way possible also to the stakeholder required information security and continually optimization of the organization.

Changes and planned actions must be communicated and implemented systematically and constantly by all collaborators. Therefore the continually information security awareness and a constantly improvement are very strongly promoted.

In the periodically internal and external audits the compliance between lived practice and the system documentation is examined. This supports also the constantly check of information security requirements, updating and change of the system documentation and thereby we integrate optimal information security, process modeling, process standardization and transparency with need and objective oriented flexible process implementation.

B Success factors

Corporate culture processes and IT technologies must be integrated optimally according to the organization objectives and to collaborators needs and requirements in order a to successfully system development based on holistic, integrated standard based management system. The system is thereby only a tool, which supports the optimization of the

organization so far as this is also admitted by the culture. Therefore we need an open, confident based, fault-tolerant, objective oriented, innovative, flexible, cooperative, participative, esteeming, stakeholder, customer, service oriented corporate and learning culture with criticism and change readiness, which promotes self organizing units, autonomous, objectives oriented acting, as well as personality development of all collaborators regarding self, learn and social competences. The collaborators should be interested in new knowledge, have personal employment, team ability and change and learning willingness apart from necessary IT-competences. All managers must use constantly and actively the system and motivate their collaborators in following these principles. A strengthening point for achieving this is maintaining an optimal communication internally as well as with external partners.

Introducing holistic standard based management systems as basis for system development requires the organization best adapted systems, which is impossible buying external sample manuals, which do not correspond with the lived processes and objectives. The management systems must be continually best implemented and lived and can not be only an alibi for the auditor for maintaining the certificate.

By introducing this concept for system development the system manager and/or IT analyst extend their own job, needing apart from the technical skills also the necessary skills about information security, legal requirements, necessary technical skills, standard requirements, organizational development, change management, business process management, business reengineering, organizational learning, knowledge management, controlling , as well as experience in information technology (system manager), information management and IT – service management.

Sufficient IT-infrastructure and IT-support are also very important for the project success. Only by promoting a need and objective oriented workflow based integrated, holistic database supported system a continuously optimization of the organization, in accordance with its objectives, and a sustainable organization success are secured.

VI. OUTLOOK

Due to these excellent project experiences in several organizations with different management systems there should be used enhanced a holistic, integrated, standard based management systems regarding all success factors [V B] as basis for system development.

IT analyst trainings should inform about the principles of standard based management systems and information security and management system training should inform also about the workflow based database systems.

The management systems standards should emphasize the importance of information security and IT support and an open, confident based, fault tolerant corporate and learning culture with criticism and change readiness.

VII. CONCLUSION

Establishing and implementing a holistic, integrated, standard based, individual, the organization best adapted management system as basis for system development to analyze customer requirements, integrate and optimize information security promotes legal conformity, information security awareness, effectiveness, information security improvement and the continually organizational development by means of collaborators ideas and suggestions to guarantee sustainable stakeholder orientation, information security, quality, profitability and sustainable organization success.

REFERENCES

- [1] M. Hammer, *Beyond reengineering*, HarperCollins Business, London, 1996.
- [2] ISO/IEC 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements*, 5.10.2005.
- [3] EN/ISO 9001:2000 *Quality Management Systems – requirements*, ISO 17.12.2000.
- [4] P. Osanna, M. Durakbasa and A. Afjehi-Sada, *Quality in Industry*, Vienna University of Technology, 2004.
- [5] Y. Akao, *Quality Function Deployment*, integrating customer requirements into product design, Productivity Press, Portland, 1990.
- [6] M. Stoll, *Workplace Process Integrated Learning and Knowledge Organization*, in H. Maurer and K. Tochtermann Eds. Proc. I-Know 07, 7th International Conference on Knowledge Management, J.UCS Journal of Universal Computer Science, Graz, 2007.
- [7] T. Davenport and L. Prusak, *Working Knowledge*, Harvard Business School Press, Boston, 1998.
- [8] R. Maier, *Knowledge management systems*, Springer, Berlin, 2002.
- [9] G. Riempp, *Integrierte Wissensmanagementsysteme: Architektur und praktische Anwendung*, Springer, Berlin, 2004.
- [10] G. Probst, S. Raub and K. Romhardt, *Wissen managen*, Gabler, Wiesbaden, 1999.
- [11] F. Lehner, *Wissensmanagement: Grundlagen Methoden und technische Unterstützung*, Hanser, München, 2006.
- [12] S. Güldenberg, *Wissensmanagement und Wissenscontrolling in lernenden Organisationen*. Deutscher Universitäts-Verlag, Wiesbaden, 1997.
- [13] P. Pawlowsky, *Wissensmanagement*, Erfahrungen und Perspektiven. Gabler, Wiesbaden, 1998.

A Survey of Wireless Sensor Network Interconnection to External Networks

Agnius Liutkevicius^{#1}, Arunas Vrubliauskas^{#2}, Egidijus Kazanavicius^{#3}

[#]Real Time Computing Systems Centre, Kaunas University of Technology
Studentu St. 50-213, Kaunas, Lithuania

¹agnius@ifko.ktu.lt, ²aras@ifko.ktu.lt, ³ekaza@ifko.ktu.lt

Abstract— This paper aims at investigating the WSN (wireless sensor network) connectivity to external networks and infrastructures. It addresses research regarding existing techniques, mechanisms and devices that will provide connectivity of WSNs to external networks.

I. INTRODUCTION

Power limitations are a major constraint of WSNs and are considered as a restricting factor of the interconnection functionality. These limitations must be formulated as a complete set of WSN capabilities that will be used as restrictions to the interconnection requirements and specification. In this context, the architecture and protocol particularities of the interconnected networks are studied. Alternative network structures and interconnection architectures including gateways, brokers, and distributed middleware are discussed. The evaluation procedure is based on criteria like energy efficiency, coverage, network connectivity, fault tolerance and network performance.

This paper organized as follows: In chapter 2 the WSN interconnection to external networks approaches are presented. In chapter 3 the WSN topologies and interconnection architectures are discussed. Chapter 4 contains information about middleware and brokers, which are used to access, control and develop WSN. The recommendations for WSN interconnection to external networks are presented in the last chapter.

II. WSN INTERCONNECTION TO EXTERNAL NETWORKS TECHNIQUES

Most sensor network applications aim at monitoring or detection of phenomena (e.g. health monitoring, office building environment control, wild-life habitat monitoring, forest fire detection, etc.). There must be a way for a monitoring entity to gain access to the data produced by the sensor network. By connecting the sensor network to an existing network infrastructure such as the global Internet, a local-area network, or a private intranet, remote access to the sensor network can be achieved.

A. Interconnection techniques

Basically, interconnection techniques can be categorized into two different approaches:

1) Gateway-based approach;

This research has been supported by the EU funded project FP6-2005-IST-034642

2) Overlay-based approach.

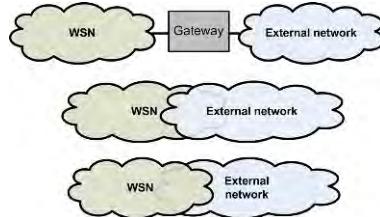


Fig. 1. WSN interconnection to external networks techniques.

B. Gateway-based approach

Sensor networks often are intended to run specialized communication protocols, thereby making it impossible to directly connect the sensor network with other network (e.g. TCP/IP). The most commonly suggested way to get the sensor network to communicate with other network is to deploy a gateway between the sensor network and the other network.

Gateway – “In a communications network, a network node equipped for interfacing with another network that uses different protocols.” [19].

The gateway is able to communicate both with the sensors in the sensor network and hosts on the other network, and is thereby able to either relay the information gathered by the sensors, or to act as a front-end for the sensor network. Gateway node is the central node in a sensor network responsible for establishment and maintenance of the network and is the only access point to its network [20]. Unlike conventional wireless sensor networks where self-organization algorithms are executed by all sensor nodes, here that responsibility lies solely on the gateway nodes. It, in general, does not take part in sensing tasks, but is a dedicated control node, more powerful than regular sensor nodes, responsible for communication with users, as well as data collection and processing [20].

This is the common solution to integrate sensor networks with an external network by using *Application-level Gateways* [21] as the interface. Different protocols in both networks are translated in the application layer. The advantage is: the communication protocol used in the sensor networks may be chosen freely. However, the drawbacks are:

- External network users may not directly access any special sensor node – it depends on protocol or gateway implementation;

- Gateway approach creates a single point of failure. If the gateway fails, all communication to and from the sensor network is effectively made impossible;
- Gateway implementation usually is specialized for a specific task or a particular set of protocols.

Another research work, DTN (Delay Tolerant Network [22]), also follows this *Gateway-based approach*. The *Bundle Layer* is deployed in both TCP/IP network and non-TCP/IP network protocol stacks to store and forward packets. It is very easy to integrate with different heterogeneous wireless networks by deploying this *Bundler Layer* into their protocol stacks. But the drawback also comes from the deployment of *Bundle Layer* into existing protocols, which is a costly job.

In general case the gateways can operate at any layer of the OSI model, not only in application layer [21], [23].

C. Overlay-based approach

There are two kinds of overlay-based approaches for connecting sensor network with other network:

- 1) *External network overlay sensor network*;
- 2) *Sensor network overlay external network*.

There are number of researches [24]-[27] to implement TCP/IP protocol stack on sensor nodes. The key advantage is: internet host can directly send commands to some particular nodes in sensor networks via IP address. However, TCP/IP protocol can only be deployed on some sensor nodes which have enough processing capabilities.

Other problems are:

- The addressing and routing schemes of IP are host-centric.
- The header overhead in TCP/IP is very large for small packets.
- TCP does not perform well over links with high bit-error rates, such as wireless links.
- The end-to-end retransmissions used by TCP consume energy at every hop of the retransmission path.

The *sensor networks overlay TCP/IP* has also been proposed in [28], where sensor networks protocol stack is deployed over the TCP/IP and each Internet host is considered as a virtual sensor node. The problem of [28] is: it brings more protocol header overhead to TCP/IP network and loses the consistency with current IP based working model.

D. Summary

Most of the gateway approach drawbacks mentioned above can be solved using multi-gateway solutions and cluster-based approach [5], [6]. According to latest research the gateway solution is most suitable for power-aware wireless sensor networks. It is more complex than overlay approach, because requires additional hardware and software to be developed (gateway, middleware). However, gateway-based approach allows developers to create custom WSN protocol with required characteristics. Hence, in the following chapters the gateway approach will be assumed.

III. WSN INTERCONNECTION ARCHITECTURES

The sensor network is more application specific than traditional networks and organization and architecture of a

sensor network should be designed or adapted to suit a special task so as to optimize the system performance, maximize the operation lifetime (save energy), and minimize the cost.

With respect to the communication mechanism adopted, four basic architectures of sensor networks exist [8]: *direct connected*, *flat ad hoc*, *peer-to-peer multihop*, and *cluster-based multihop*, as shown in Fig. 2 - Fig. 5. It is crucial to select the optimal architecture, because the communication energy dominates, by more than two orders of magnitude, computation, storage and sensing requirements for a majority of common applications and data aggregation comprises more than 99% of communication and therefore energy in sensor networks [4],[30]. The mentioned architectures belong to the few topologies: *star topology* (Fig 2), *mesh topology* (Fig. 3) and *hybrid topology* (Fig. 4 - Fig. 5).

The direct connected mode (Fig. 2) is not suitable for large-scale deployed sensor networks, because it is impossible, for each small sensor to communicate directly with the collector (gateway) and the transmit range of sensor nodes may be limited due to the battery capacity limitations.

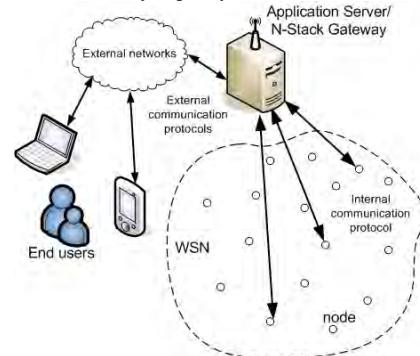


Fig. 2. Direct connected WSN.

Multihop mode (Fig. 3) is more energy efficient than direct connected mode. Multihop short-range transmission usually consumes less power than the power required by one large-hop transmission for a given pair of source and destination because, in general, the average received signal power is inversely proportional to the n th power of the distance, (usually $2 < n \leq 4$) [8]. This mode is flexible and energy efficient, however scalability is still a problem. The nodes closer to the collection and processing centre (gateway) will be primarily used to route data packets from other nodes to the processing centre; if the network size is large, these nodes will relay a large number of data and their energy will be exhausted very fast, resulting finally in disconnection of the network.

To reduce the amount of power spent on long distance radio transmissions, the sensor nodes can be aggregated into clusters. This concept is especially useful when the ranges of the sensors are relatively short. Cluster-based multihop sensor networks attempt to address the scalability issues. In a cluster-based system [5], [6], [9], sensor nodes form clusters; a cluster head for each cluster is selected according to some negotiated rules [31].

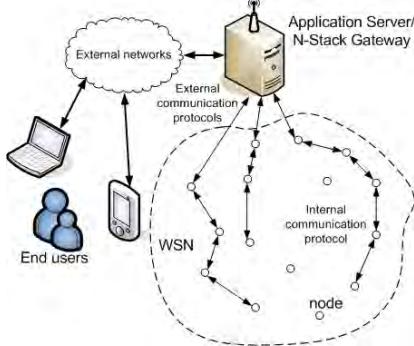


Fig. 3. Multihop WSN.

Sensor nodes only transmit their data to their immediate local cluster head (Fig. 4). Local data fusion and classification at cluster heads may be used to reduce the amount of information that must be transmitted to the collection centre, thereby reducing the overall energy consumed for transmission.

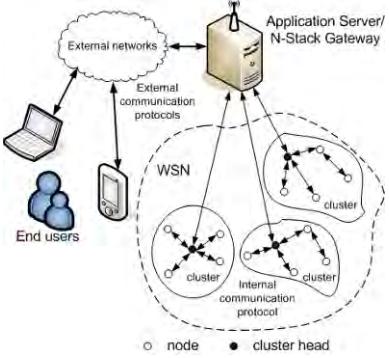


Fig. 4. Cluster-based multihop WSN.

The main disadvantages of this mode of operation are that the communication relies highly on the cluster head and energy depletion of cluster heads is faster than that of other nodes. If cluster head is exhausted, then the cluster stops functioning. But such solutions as dynamic cluster head election [31] or even placing cluster heads with permanent power supplies solves this problem. Cluster-based architectures can be fault-tolerant as well. In [11] the mechanism of fault detection and recovery for the cluster based system is proposed, where the cluster head failure leads to the re-clustering of network. Node redundancy also is a solution for the fault tolerant system.

However, organizing nodes into a hierarchy typically introduces overhead into the network. This is particularly true of clustering algorithms. For instance, the algorithm described in Banerjee and Khuller [32] first requires that a spanning tree be identified, followed by the execution of the clustering algorithm. If node mobility results in frequent re-clustering, the overhead may outweigh the benefit.

In some scenarios the gateway could be mobile, e.g., on a battlefield [33]. By relocating the gateway towards highly active sensors, the packets will be routed directly to the

gateway instead of using along-the-path sensors as a bridge to reach the gateway.

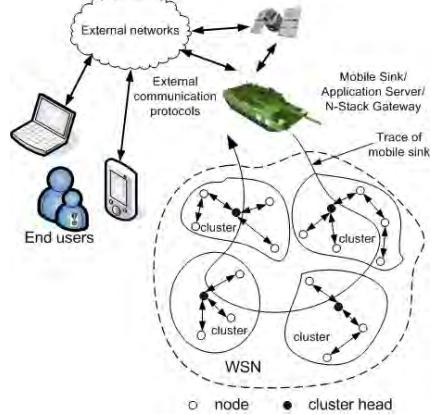


Fig. 5. WSN architecture with mobile gateway(s).

Moving the gateway towards highly loaded nodes would have the potential for enhancing network performance in terms of energy consumption, throughput and delay [33]. On the other hand, when gateway changes its location the network topology changes too and the network control message flow can take too much energy. Therefore, the gateway mobility requires careful handling to limit the overhead of excessive topology management, maintain low packet loss ratio and still thrive to achieve efficient network operation [2]. Some of mobile gateway solutions are presented in [35], [36], [37].

A. Gateway role in WSN security

As stated in [29] the security researches concentrates on the securing sensor-to-sensor communications which is very important. But security is also associated with WSN interconnection to external networks and infrastructures.

The WSN-gateway usually has a connection to the Internet or a dedicated network such as satellite network for remote data access and monitoring control. Hence, gateway is a single point of failure and is vulnerable to the attacks from the external network. The experiments with commercial grade wireless sensor network with PC-based gateway showed that in case of Distributed Denial of Service (DDoS) attack against a WSN-gateway it stop collection, recording, and reporting of the sensor data [29]. Hence it is very important to pay attention to the external threats and use solutions (e.g. firewalls, authentication) to minimize them. The multiple base station and multiple routing paths to base station solutions addresses this problem [12].

B. Multi-gateway architectures

Single gateway architectures have drawbacks: single point of failure (low fault-tolerance) and low scalability. On the other hand, proposals exist where these problems are solved using *multi-gateway* architectures. In applications in which the multiplicity of gateway nodes is not restrained, it would be beneficial to increase the number of deployed gateways in

order to extend the lifetime of sensors and provide a more predictable sensor-to-gateway transmission times [6].

The fault tolerant and scalable multi-gateway system is described in [5], [11]. The authors of [11] use clustering approach, where gateways are the cluster heads. Similar multi-gateway architecture is discussed in [9] and results are rather optimistic.

An adaptive and fault tolerant protocol for multiple gateways is presented in [38]. It is highly scalable, because uses clustering and allows network to recover from gateway failure using neighbour gateways as backup. Security issues are also addressed in [12] there multiple base stations (gateways) provide tolerance against individual base station attacks.

Finally, as mentioned above, the gateway (sink) can be mobile. Some papers describe multi-gateway systems, where gateways are mobile (e.g. PDA devices) [35], [37], [10], [7]. Authors of [37] use a personal digital assistant (PDA) with a custom wireless interface module as a mobile gateway to collect data from individual monitors during periodic visits to the training facility. Reliable data transmission is based on error detection and retransmissions. System can be wirelessly connected to the Internet, using add-in PDA cards for WAN connectivity, creating a true real-time telemedical system.

IV. MIDDLEWARE AND BROKERS IN WSN

A wireless sensor networks have been developed for a wide range of applications (healthcare, military, environment monitoring etc.). Middleware systems have also been proposed to facilitate both the development of these applications and provide common application services. Traditional middleware systems such as Java RMI (Remote Method Invocation) [39], EJB (Enterprise JavaBeans) [40] and CORBA (Common Object Request Broker Architecture) [41] are normally heavyweight in terms of memory and computation and therefore not suitable for WSNs [42].

A middleware for WSN should facilitate development, maintenance, deployment and execution of sensing-based applications and provide appropriate abstractions and mechanisms for dealing with the heterogeneity of sensor nodes [43]. All mechanisms provided by a middleware system should respect the restrictions involved in WSN systems, which are mostly energy efficiency, robustness and scalability [44], [45]. Most of researches in this field are directed to development of new power-aware, resource efficient protocols [1]. To make these protocols more useful, application designers would benefit from a middleware layer that hides details of communication protocols, while providing an API (Application Programming Interface) that reduces the cost of developing applications [34], [43].

The interactions between applications and WSN are done via one or several nodes of the WSN, which act as gateway(s) [46], [47]. Apart from providing communication interfaces, the most important role a gateway has is the one of a sensor network representative. In other words, each gateway has the full knowledge of its network: what types of sensors are available, what services are offered, who can access sensor information, how to communicate with sensors, how to control them, collect

data, etc. and is responsible for presenting these capabilities in a structured and logical manner to interested external parties [20].

The authors of [46] groups existing middleware into four groups: low-level APIs, databases, agents and Web Services. The low level APIs come as low level commands and in specialized languages or in high level languages like C/C++ or Java, exposing the sensor capabilities to programmers [48]-[51]. The database approach allows to look at the WSN as a distributed database [52], where applications use SQL-like queries to the sensor network via the gateway and get the results back [53]-[56]. In agent-based approach, the specialized scripts or programs inside sensor networks collect data and send them back via the gateway whenever certain phenomenon is detected or an application asks for that data [17], [18], [57]. Web Services [14], [15], [16] usually are placed at the gateway and provide the services of the sensor networks.

In [13] an interesting new approach to Application Programming Interface for Wireless Sensor Networks (WSN API) is presented. The WSN API consists of a client-side API (Gateway API) and a sensor-side API (Node API). WSN API provides a well-defined and easy-to-use way to collect data from WSN nodes, and give commands to them as well as service discovery mechanisms and attribute based queries. According to [13] WSN applications can be divided into two groups, external and internal. External applications execute on remote devices that are not WSN nodes and internal applications execute on the WSN nodes. Since users communicate with the WSN through gateway nodes, they are the logical architectural location for the API for external applications (Gateway API). The API for internal applications is in the WSN nodes (Node API).

Since middleware abstract low level APIs, the middleware has to support mapping between services at application level to services called on the sensor layer as presented in a Service Oriented Approach, which has been proposed in [3].

According to [17] there are many middleware systems that increase WSN flexibility by enabling in-network reprogramming: XNP, Deluge, Mat'e, SensorWare, Impala, and Smart Messages. There are also coordination middleware like Lime and MARS that are designed for IP networks. These middleware systems are either targeted for WSNs, or IP networks, but not the integration of both. In [17] the WSN integration to the IP networks is presented as well as overview of similar projects (including Hourglass, SBONs, Tenet, SERUN and IrisNET).

V. RECOMMENDATIONS FOR WSN INTERCONNECTION IMPLEMENTATION

As mentioned previously, there are two basic approaches to connect WSN to external network: gateway approach and overlay approach. Gateway approach is better in terms of power efficiency and allows integrating custom made WSNs to external networks. Cluster-based architecture (topology) is more power-efficient and scalable than others architectures for WSNs. To best suit the application scenario requirements and meet the criteria such as energy efficiency, coverage, network

connectivity, fault tolerance and network performance, the recommendation is to employ the cluster-based architecture of the wireless sensor network.

Several alternative architectures with cluster-based approach can be proposed: single-gateway architecture, architecture using mobile sinks, architecture using mote-gateways (Fig. 6). The single-gateway architecture has low fault-tolerance, because there is a single point of failure at gateway. On the other hand, this architecture is relatively easy to implement. The architecture using multiple mobile sinks still has the fault-tolerance problem, if gateway (application server) is down. However the network can be functional and send data directly to the mobile sinks (PDA with interface to the WSN mote). Normally two data paths exist: from the WSN nodes to the gateway (application server), and from the WSN nodes to the mobile sinks (PDAs).

The architecture using multiple mote-gateways (Fig. 6) is the best in terms of very high level of scalability, energy efficiency and fault-tolerance. In this case, the gateways are placed statically and have Wi-Fi interface to communicate with PDAs or other end-user devices.

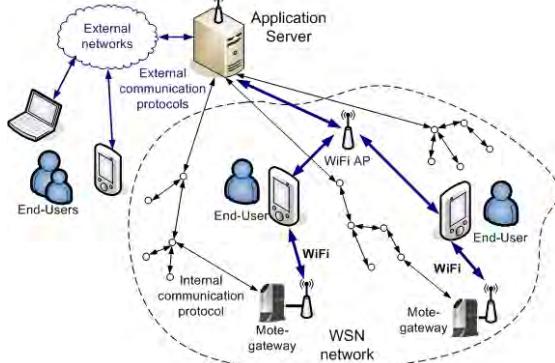


Fig. 6. WSN architecture using mote-gateways.

Power aware internal communication protocol to be developed is the key issue. As for external network protocol, TCP/IP based network like Internet are most preferred, because it is the most widely spread across the world, and the application services could be reached from anywhere. Other network technologies, such as Wi-Fi has to be taken into account, when WSN users are mobile, which imposes the need of mobile devices such as PDAs or smart phones having the necessary software to access WSN services, to be able to react as soon as possible.

VI. CONCLUSIONS

This paper researches available techniques and methods to connect wireless sensor network with external networks (usually TCP/IP based). The gateway approach for interconnection is considered better in terms of power efficiency and allows integrating custom made WSN protocol to external networks. Basic WSN topologies and architectures are discussed and compared, including multi-gateway architectures, in terms of energy efficiency, robustness, and

scalability. The middleware and its main functionalities for interacting with WSN presented in paper as well. Finally, the recommendations for interconnection implementation between wireless sensor network and external networks using gateways are proposed in last section.

REFERENCES

- [1] K. Akkaya and M. Younis, "A Survey of Routing Protocols in Wireless Sensor Networks," in *Elsevier Ad Hoc Network Journal*, Vol. 3/3 pp. 325-349, 2005.
- [2] K. Akkaya and M. Younis, "Energy-Aware Routing to a Mobile Gateway in Wireless Sensor Networks," in the *Proceedings of the IEEE Globecom Wireless Ad Hoc and Sensor Networks Workshop*, Dallas, TX, November, 2004.
- [3] Xingchen Chu, Tom Kobialka, Bohdan Durnota, and Rajkumar Buyya, "Open Sensor Web Architecture: Core Services," *Proceedings of the 4th International Conference on Intelligent Sensing and Information Processing 2006*, Dec. 15-18, 2006, Bangalore, India.
- [4] J. Wong, R. Jafari, and M. Potkonjak, "Gateway placement for latency and energy efficient data aggregation," in *29th Annual IEEE International Conference on Local Computer Networks*, November 2004, pp. 490-497.
- [5] G. Gupta and M. Younis, "Load-balanced clustering of wireless sensor networks," in *Proc. IEEE International Conference on Communications (ICC'03)*, vol. 3, pp. 1848--1852, May 2003.
- [6] Mohamed Younis, Poonam Munshi, Gaurav Gupta, and Sameh M. Elsharkawy, "On Efficient Clustering of Wireless Sensor Networks", *Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems (DSSNS 2006)*, Columbia, MD, April 2006.
- [7] H.M. Ammari, S.K. Das, "Data dissemination to mobile sinks in wireless sensor networks: an information theoretic approach," *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 2005, November 2005.
- [8] Ilyas, Mohammad, *Handbook of sensor networks: compact wireless and wired sensing systems*, CRC Press, 2005, ISBN: 0849319684.
- [9] Prabal Dutta, Jonathan Hui, Jaemin Jeong, Sukun Kim, Cory Sharp, Jay Tanuja, Gilman Tolle, Kamin Whitehouse, and David Culler, "Trio: Enabling Sustainable and Scalable Outdoor Wireless Sensor Network Deployments," In Proceedings of the Fifth International Conference on Information Processing in Sensor Networks Special track on Platform Tools and Design Methods for Network Embedded Sensors (IPSN/SPOTS'06), Apr, 2006.
- [10] Kim, H. S., Abdelzaher, T. F., and Kwon, W. H. "Minimum-energy Asynchronous Dissemination to Mobile Sinks in Wireless Sensor Networks," *Sensys 2003*, pp. 193-204.
- [11] G. Gupta and M. Younis, "Fault-Tolerant Clustering of Wireless Sensor Networks," *Wireless Communications and Networking (WCNC'03)*, March 2003.
- [12] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," *Technical Report CU-CS 951-03*, Department of Computer Science, University of Colorado, Boulder, CO, November 2002.
- [13] Jari Junutunen, Mauri Kuorilehto, Mikko Kohvakka, Ville Kaseva, Marko Hännikäinen, Timo D. Hämäläinen, "WSN API: Application Programming Interface For Wireless Sensor Networks", *17th Annual IEEE International Symposium on Personal Indoor and Mobile Radio communications (PIMRC'06)*, Helsinki, Finland, September 11-14, 2006.
- [14] Kwang-il Hwang, Jeongsik In, NhoKyung Park, Doo-seop Eom, "A Design and Implementation of Wireless Sensor Gateway for Efficient Querying and Managing through World Wide Web", *IEEE Transactions on Consumer Electronics*, November 2003, Volume: 49, Issue: 4.
- [15] J. Blumenthal, M. Handy, F. Golatowski, M. Haase, D. Timmermann, "Wireless Sensor Networks - New Challenges in Software Engineering," *Proceedings of 9th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Lissabon, Portugal, September 2003.
- [16] F. Curbera et al., "Unraveling the Web services Web: An Introduction to SOAP, WSDL and UDDI," *IEEE Internet Computing*, Vol. 6, No2 (March-April 2002), p.p. 86-93.

- [17] Gregory Hackmann, Chien-Liang Fok, Gruia-Catalin Roman, and Chenyang Lu, "Agimone: Middleware Support for Seamless Integration of Sensor and IP Networks", *Proceedings of 2006 International Conference on Distributed Computing in Sensor Systems (DCOSS '06)*, November 2005.
- [18] A. Boulis and M. B. Srivastava, "A Framework for Efficient and Programmable Sensor Networks," In *proceedings of OPENARCH 2002*, New York, June, 2002.
- [19] Federal Standard 1037C, available at [<http://www.its.blrdoc.gov/fs-1037c.htm>].
- [20] S. Kroo, D. Cleary, and D. Parker, "P2P mobile sensor networks," in *Proc. 38th IEEE Hawaii Int. Conference on System Sciences (HICSS 2005)*, Hawaii, Jan. 03–06, 2005, pp. 324c–324c.
- [21] Z. Z. Marco, K. Bhaskar, "Integrating Future Large-scale Wireless Sensor Networks with the Internet", *USC Computer Science Technical Report CS 03-792*, 2003.
- [22] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets", In *Proceedings of the SIGCOMM 2003 Conference*, 2003.
- [23] Lei Shu, Wu Xiaoling, Xu Hui, Yang Jie, Jinsung Cho, and Sungyoung Lee, "Connecting Heterogeneous Sensor Networks with IP Based Wire/Wireless Networks," *Proc. of IEEE International Workshop on Software Technologies for Future Embedded & Ubiquitous Systems (SEUS2006)*, 127-132, Gyeongju, Korea, April, 2006.
- [24] A. Dunkels, J. Alonso, T. Voigt, H. Ritter, J. Schiller, "Connecting Wireless Sensors with TCP/IP Networks", In *Proceedings of the Second International Conference on Wired/Wireless Internet Communications (WWIC2004)*, Frankfurt (Oder), Germany, February 2004.
- [25] A. Dunkels, J. Alonso, and T. Voigt, "Making TCP/IP Viable for Wireless Sensor Networks," In *Proceedings of the Work-in-Progress Session of the 1st European Workshop on Wireless Sensor Networks (EWSN)*, Technical Report TKN-04-001 of Technical University Berlin, Telecommunication Networks Group, Berlin, Germany, January 2004.
- [26] Mauri Kuorilehto, Jukka Suonen, Mikko Kohvakka, Marko Hännikäinen, Timo D. Härmäläinen, "Experimenting TCP/IP for Low-Power Wireless Sensor Networks," *17th Annual IEEE International Symposium on Personal Indoor and Mobile Radio communications (PIMRC'06)*, Helsinki, Finland, September 11-14, 2006.
- [27] K. Mayer and W. Fritzsche, "IP-enabled Wireless Sensor Networks and their integration into the Internet," *Proc. of the First International Conference on Integrated Internet Ad-Hoc and Sensor Networks (INTERSENSE06)*, Nice, France, May 2006.
- [28] H. Dai, R. Han, "Unifying Micro Sensor Networks with the Internet via Overlay Networking," in *Proc. IEEE Emmets-I*, Nov. 2004.
- [29] S. Kumar and R. Valdez and O. Gomez and S. Bose, "Survivability Evaluation of Wireless Sensor Network under DDoS Attack," *ICN/ICONS/MCL 2006*, p. 82.
- [30] V. Raghunathan et al., "Energy-Aware Wireless Microsensor Networks," *IEEE Sig. Proc. Mag.*, vol. 1, no. 2, March 2002, pp. 40-50.
- [31] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," *HICSS 2000*, Maui, 8020–8029, January 2000.
- [32] S. Banerjee and S. Khuller, "A clustering scheme for hierarchical control in multi-hop wireless networks," *IEEE INFOCOM 2001*, Anchorage, AK, April 2001.
- [33] W. Youssef, M. Younis and K. Akkaya, "An Intelligent Safety-Aware Gateway Relocation Scheme for Wireless Sensor Networks", in the *Proceedings of the IEEE International Conference on Communications (ICC) 2006*, June 2006, Istanbul, Turkey.
- [34] W. Heinzelman, A. Murphy, H. Carvalho, M. Perillo, "Middleware to support sensor network applications," *IEEE Network Magazine Special Issue*, pp 6–14, January 2004.
- [35] Canfeng Chen, Jian Ma, "Mobile Enabled Large Scale Wireless Sensor Networks," *The 8th International Conference Advanced Communication Technology 2006*, 20-22 Feb. 2006.
- [36] K. Akkaya and M. Younis, "Sink Repositioning for Enhanced Performance in Wireless Sensor Networks," in *Elsevier Computer Networks Journal*, Vol. 49/4, pp. 512-534, 2005.
- [37] E. Jovanov, D. Raskovic, A.O. Lords, P. Cox, R. Adhami, F. Andrasik, "Synchronized Physiological Monitoring Using a Distributed Wireless Intelligent Sensor System," *Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Cancun, Mexico, 17-21 Sept. 2003, Vol. 2, pp. 1368 - 1371.
- [38] W. Su, "An adaptive and fault-tolerant scheme for gateway assignment in sensor networks," In *IEEE Military Communications Conference, 2004, MILCOM 2004*, Nov. 2004.
- [39] A. Wollrath, R. Riggs, J. Waldo, "A distributed object model for the Java system," *Usenix conference on object oriented technologies and systems*, May 1996.
- [40] A. Thomas, P. Seybold, Enterprise JavaBeans Technology, available at <http://www.cs.indiana.edu/classes/b649-gann/ejb-white-paper.pdf>, December 1998.
- [41] Object Management Group (OMG), The common object request broker: architecture and specification. Published by the Object Management Group (OMG), Revision 2.3, June 1999.
- [42] Y. Yu, B. Krishnamachari, V.K. Prasanna, "Issues in designing middleware for wireless sensor networks," *IEEE Network Magazine Special Issue* 18(1):15–21, 2004.
- [43] E. Souto , et al., "A Message-Oriented Middleware for Sensor Networks," *Proc. 2nd Int'l Workshop Middleware for Pervasive and Ad-Hoc Computing (MPAC 04)*, ACM Press, 2004, pp. 127-134.
- [44] K. Römer, O. Kasten, and F. Mattern, "Middleware Challenges for Wireless Sensor Networks," *ACM Mobile Communication and Communications Review*, 6(2): 59–61, 2002.
- [45] Mohsen Sharifi, Madjid Elkaee Taleghani and Amirhosein Taherkordi, "A Middleware Layer Mechanism for QoS Support in Wireless Sensor Networks", *The 4th IEEE International Conference on Networking (ICN'06)*, Mauritius, April 23-29, 2006.
- [46] T. Ta, N. Othman, R. Glitho and F. Khendek, "Using Web Services for Bridging End-User Applications and Wireless Sensor Networks," *IEEE International Symposium on Computers and Communications (ISCC'06)*, June 26-29, Sardinia, Italy.
- [47] Simeon Furrer, Wolfgang Schott, Hong Linh Truong, and Beat Weiss, "The IBM Wireless Sensor Networking Testbed," *2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, TRIDENTCOM 2006*, March 2006.
- [48] D. Gay, P. Lewis, R. von Behren, M. Welsh, E. Brewer, D. Culler, "The nesC Language: A Holistic Approach to Networked Embedded Systems," *Proceedings of the ACM SIGPLAN 2003*, San Diego, California, USA, (2003) 1–11.
- [49] E. Cheong, J. Liu, "galsC: A Language for Event-Driven Embedded Systems," *Design, Automation and Test in Europe (DATE'05)*, vol. 02, no. 2, Design (2005) 1050-1055.
- [50] Adam Smith, Hari Balakrishnan, Michel Goraczko, Nissanka Priyantha, "Tracking Moving Devices with the Cricket Location System," *Proc. 2nd USENIX/ACM MOBISYS Conf.*, Boston, MA, June 2004.
- [51] JSR 256 Mobile Sensor API Specification Version 0.27, Java Community Process, 2006.
- [52] R. Govindan, et al., "The Sensor Network as a Database," *Tech-Rep 02-771* CS Department, University of Southern California, September 2002.
- [53] Samuel R. Madden, Michael J. Franklin, Joseph M. Hellerstein, Wei Hong., "TinyDB: an acquisitional query processing system for sensor networks," *ACM Transactions on database systems (TODS)*, volume 30, Issue 1, March 2005, 122 – 173.
- [54] Phillip B. Gibbons, Brad Karp, Yan Ke, Suman Nath, Srinivasan Seshan, "IrisNet: An Architecture for a World-Wide Sensor Web," *IEEE Pervasive Computing*, Volume 2, Number 4, (October-December 2003).
- [55] Y. Yao and J. Gehrke, "The cougar approach to in-network query processing in sensor networks," *ACM SIGMOD Record*, vol. 31, no. 3, pp. 9–18, 2002.
- [56] C.-C. Chen, C. Srisathapornphat, and C. Jaikaeo, "Sensor information networking architecture and applications," *Personal communications, IEEE*, vol. 8, no. 4, pp. 42–59, 2001.
- [57] Chien-Liang Fok, Gruia-Catalin Roman, Chenyang Lu, "Rapid Development and Flexible Deployment of Adaptive Wireless Sensor Network Applications," In *Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS'05)*, Columbus, Ohio, June 6-10, 2005, pp. 653-662, available at [<http://mobilab.wustl.edu/projects/agilla/>].

Comparing the Performance of UMTS and Mobile WiMAX Convolutional Turbo Code

Ehab Ahmed Ibrahim, Mohamed Amr Mokhtar
Electrical Engineering Department, Faculty of Engineering, Alexandria University, Egypt
ehab_ahmed@aast.edu, amromokhtar@yahoo.com

Abstract – A useful tool in the design of reliable digital communication systems is channel coding. Turbo codes [1, 2] have been shown to yield an outstanding coding gain close to theoretical Shannon limit in the Additive White Gaussian Noise (AWGN) channel. This is due to relatively large coding gains that can be achieved. Turbo codes are widely used in many communication systems. In this paper, we chose two of them – Mobile WiMAX and UMTS – to study their convolutional turbo encoder's structure, and then compare their relative Bit Error Rate (BER) performance.

Keywords – WiMAX, UMTS, CTC, BWA, BER, AWGN

I. INTRODUCTION

After the installation of fixed Internet networks in many places all over the world and their now large expansion, the need is now becoming more important for wireless access.

There is no doubt that by the end of the first decade of this century, high-speed (Broadband) wireless data access will be largely deployed worldwide. A Broadband Wireless Access (BWA) [3, 4] system is a high data rate Wireless Metropolitan Area Network (WMAN) or Wireless Wide Area Network (WWAN).

WiMAX, an acronym of Worldwide Interoperability for Microwave Access, is both a BWA standard, and a MAN technology which addresses to deliver high speed, cost-effective and high quality services for residential and enterprise customers with long distance broad coverage. It's a standard-based and well-defined wireless technology which could provide multiple access mode that includes fixed, nomadic, portable and mobile across wired and wireless connectivity. WiMAX is IEEE standard developed as IEEE 802.16 standard specification technology by founding member of WiMAX forum.

IEEE 802.16 standards has experienced a few phases of extension and amelioration, from initial 802.16 to 802.16a, c, d, e, then f, g, some of them (like 802.16a,c) are already completed, while some others are being developed (802.16e) and researched (802.16 f, g), here we only put our focus on version 802.16e, the Mobile WiMAX [5, 6].

Mobile WiMAX is based on the advanced technology OFDM which is considered as the core technology of fourth Generation (4G). It provides flexibility of network deployment and good service offerings.

WiMAX has some advantages to 3G e.g. Universal Mobile Telecommunication System (UMTS), such as the larger

coverage and higher transmission speed. The transmission coverage of a WiMAX base station is around ten times of the coverage as a 3G tower. It, also offers Quality of Service (QoS) control for each service flow over the air interface. QoS in 3G is limited to priority system on all the service flows. During heavy load period of network, high priority traffic might starve the low priority traffic in 3G.

The remainder of this paper is organized as follows: Section II and III provide an overview of the Mobile WiMAX Convolutional Turbo Code (WiMAX-CTC) and UMTS Convolutional Turbo Code (UMTS-CTC) structure, respectively. Simulation results are given in section IV. Finally, section V concludes the paper and suggests ideas as an area for future work.

II. WiMAX-CTC STRUCTURE

The mandatory channel coding scheme in IEEE 802.16e is based on binary nonrecursive convolutional coding. Several optional channel coding schemes such as block turbo codes, convolutional turbo codes, and Low Density Parity Check (LDPC) codes are, also defined in IEEE 802.16e. Among all of these schemes, we choose the CTC because of its superior performance and high popularity in other broadband wireless systems.

As shown in Fig. 1, WiMAX uses duobinary turbo codes with a constituent circular recursive systematic convolutional encoder of constraint length 4. In duobinary turbo codes two consecutive bits from the uncoded bit sequence are sent to the encoder simultaneously.

The bits of the data to be encoded are alternatively fed to A and B, starting with the MSB of the first byte being fed to A. The encoder is fed by blocks of k bits or N couples ($k = 2N$ bits). For all the frame sizes, k is a multiple of 8 and N is a multiple of 4. Further, N is limited to $8 \leq N/4 \leq 1024$.

The duobinary convolutional encoder has two generating polynomials, $1+D^2+D^3$ and $1+D^3$ for two parity bits Y and W, respectively and the generating polynomial $1+D+D^3$ for the feedback branch.

First, the encoder (after initialization by the circulation state Sc_1)¹) is fed by the N bits sequence in the natural order (position 1 in Fig.1). This first encoding is called C_1 encoding. Then the encoder (after initialization by the

¹ For details about the circulation states Sc_1 and Sc_2 , refer to Ref.[5]

circulation state S_{C_2}) is fed by the interleaved sequence (switch in position 2). This second encoding is called C_2 encoding. The order of the output (encoded) bit is: A, B, Y_1, Y_2, W_1 , and W_2

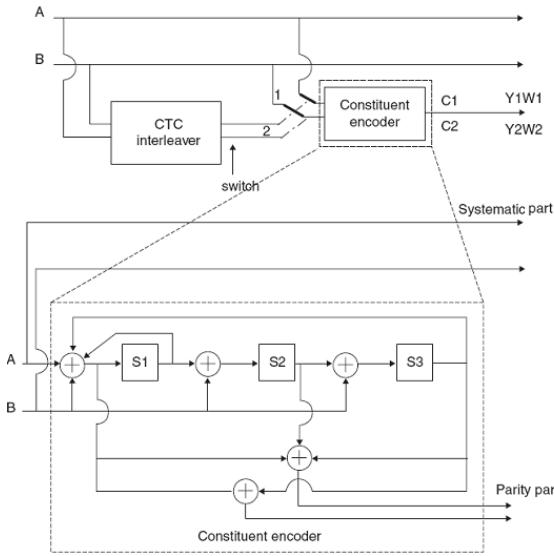


Fig. 1 Mobile WiMAX convolutional turbo encoder

A. Internal Interleaver

The internal interleaver consists of two stages:

- (1) The first stage of the interleaver flips bits contained in the alternating symbol (symbol refers to a pair of consecutive bits).
- (2) The second stage of the interleaver permutes the positions of the symbols. In order to achieve the target code rate, the interleaved couples Y_1, Y_2, W_1 , and W_2 are punctured using a specific puncturing pattern.

III. UMTS-CTC STRUCTURE

The scheme of UMTS convolutional turbo coder [7] is a Parallel Concatenated Convolutional Code (PCCC) with two 8-state constituent encoders and one Turbo code internal interleaver. Data is encoded by the first (upper) encoder in its natural order and by the second (lower) encoder after being interleaved. The coding rate of Turbo coder is 1/3. The structure of Turbo coder is illustrated in Fig. 2.

The transfer function of the 8-state constituent code for PCCC is:

$$G(D) = \begin{bmatrix} 1 & \frac{g_2(D)}{g_1(D)} \\ 0 & 1 \end{bmatrix}, \quad (1)$$

where

$$g_1(D) = 1 + D^2 + D^3 \quad (2)$$

$$g_2(D) = 1 + D + D^3 \quad (3)$$

The initial value of the shift registers of the 8-state constituent encoders shall be all zeros when starting to encode the input bits. The output from the Turbo coder is:

$$X_1, Z_1, Z'_1, X_2, Z_2, Z'_2, \dots, X_K, Z_K, Z'_K \quad (4)$$

where X_1, X_2, \dots, X_K are the bits input to the Turbo coder i.e. both first constituent encoder and Turbo code internal interleaver, and K is the number of bits and takes one value of $40 \leq K \leq 5114$, and Z_1, Z_2, \dots, Z_K and Z'_1, Z'_2, \dots, Z'_K are the bits output from first and second constituent encoders, respectively. The bits output from Turbo code internal interleaver are denoted by X'_1, X'_2, \dots, X'_K , and these bits are to be input to the second constituent encoder.

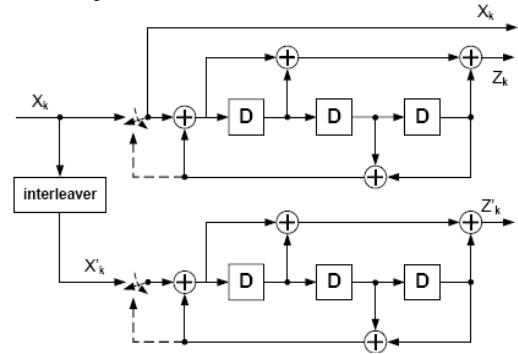


Fig. 2 UMTS convolutional turbo encoder

A. Internal Interleaver

The Turbo code internal interleaving is performed as follows:

1. The bits input to the interleaver are written into a rectangular matrix. Number of rows is 5, 10 or 20 according to the input data frame length, number of columns is calculated, also, according to the data frame Length. Data is written into the interleaver, in row wise from left to right and top to bottom.
2. Intra-row permutations on each row of the rectangular matrix are performed according to a relatively complex algorithm. This algorithm is completely described in the specification [7].
3. Inter-row permutations are performed to change the ordering of rows (without affecting the positions of elements within each row). When there are 5 or 10 rows, the inter-row permutation is simply a reflection about the center row (for the 5-row case, the rows {1, 2, 3, 4, 5} become rows {5, 4, 3, 2, 1}, respectively). When there are 20 rows, rows {1, ..., 20} become rows {20, 10, 15, 5, 1, 3, 6, 8, 13, 19, 17, 14, 18, 16, 4, 2, 7, 12, 9, 11}, respectively,

when the number of input bits satisfies either $2281 \leq K \leq 2480$ or $3161 \leq K \leq 3210$. Otherwise, they become rows $\{20, 10, 15, 5, 1, 3, 6, 8, 13, 19, 11, 9, 14, 18, 4, 2, 17, 7, 16, 12\}$, respectively.

4. Finally, the data is read out from the interleaver column wise from top to bottom and left to right.

After the K data bits have been encoded, the trellises of both encoders are terminated (forced back to the all-zeros state) Trellis termination is performed by taking the tail bits from the shift register feedback after all information bits are encoded. Tail bits are added after the encoding of information bits. The first three tail bits shall be used to terminate the first constituent encoder (upper switch of Fig.2 in lower position) while the second constituent encoder is disabled. The last three tail bits shall be used to terminate the second constituent encoder (lower switch of Fig.2 in lower position) while the first constituent encoder is disabled.

IV. SIMULATION RESULTS

In this section the BER performance of both Mobile WiMAX and UMTS turbo code is compared. The simulation is carried out for different Frame Sizes (FS) 240, 960 and 1920 bits, different code rates (1/2 and 1/3) and different channel models (AWGN and Rayleigh fading channel [8]). The modulation technique used is Quadrature Phase Shift Keying (QPSK), the decoding algorithm is Log-MAP [9] and number of iterations is 10.

Fig.3 to 5 draw the BER versus average bit energy-to-noise power spectral density ratio (E_b/N_0) plot for code rates 1/2 and 1/3 and for FS 240, 960 and 1920 bits transmitted in AWGN.

In Fig.3, the FS 240 bits is selected for the comparison. The BER performance of WiMAX-CTC has shown to be better than the UMTS-CTC system for code rate 1/2.

In Fig.4 and as the selected frame size increases to 960 bits, the BER performance of WiMAX-CTC is better than the UMTS-CTC for code rate 1/2 and the opposite is correct for code rate 1/3.

In Fig.5, the selected FS is 1920 bits. It is clearly shown that the BER performance improvement increased compared with FS 960 bits for both code rates.

Fig.6 to 8 draw the BER versus E_b/N_0 plot for the same parameters, code rates 1/2 and 1/3 and frame sizes 240, 960 and 1920 bits, but here the channel model is Rayleigh fading channel. The simulated model is flat fading channel with uncorrelated coefficients; each coefficient is a complex Gaussian random variable.

In Fig 6, the comparison is held for FS 240 bits. It can be clearly shown that the BER performance for both WiMAX-CTC and UMTS-CTC is almost the same for the entire selected range of E_b/N_0 and for both code rates.

Fig.7, the FS increases to 960 bits, shows that the WiMAX-CTC is better than the UMTS-CTC for code rate 1/2. For code rate 1/3 the performance is almost the same for both systems.

Finally, in Fig 8 and compared with Fig.7, we can clearly see that the BER performance is better for values of E_b/N_0 in the interval from 2.5 to 3 dB.

V. CONCLUSION AND FUTURE WORK

From the simulation results we conclude that:

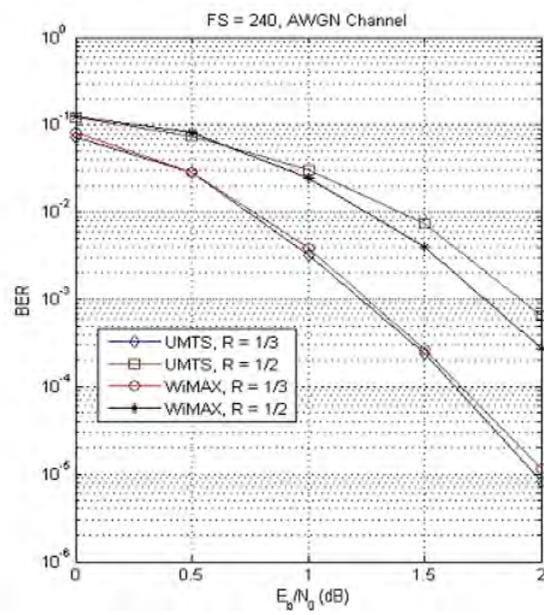
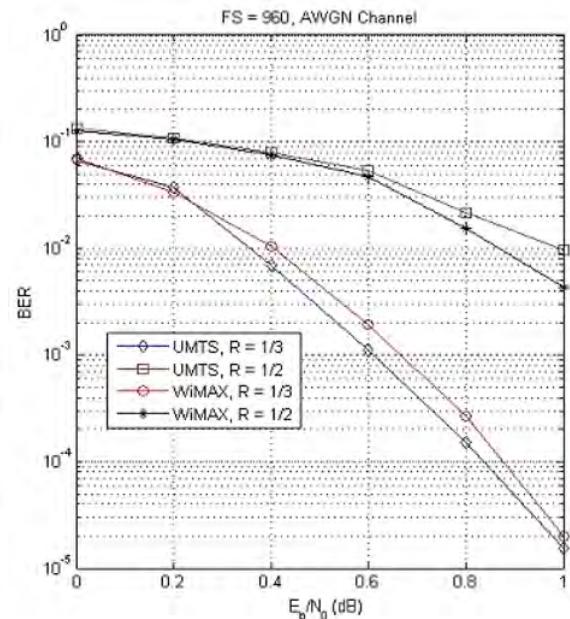
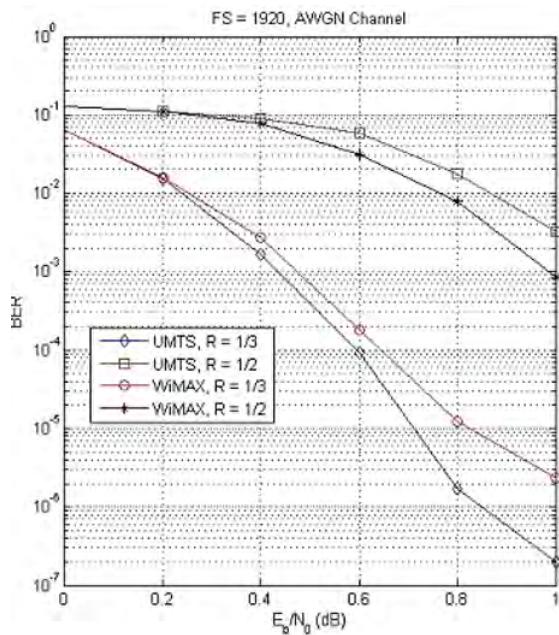
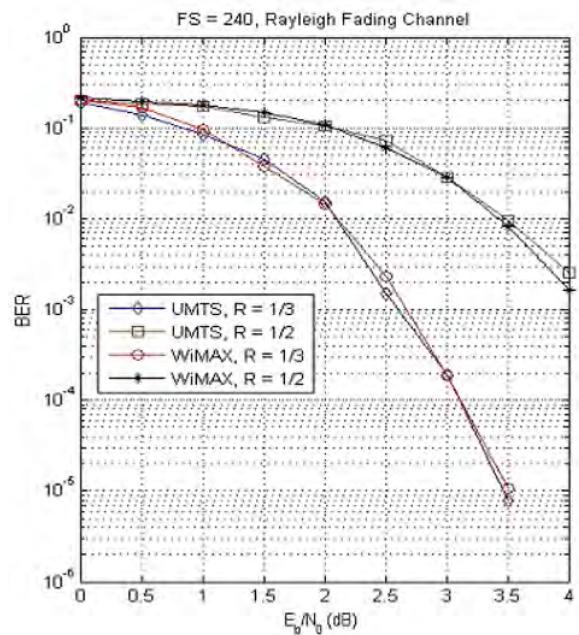
1. When dealing with AWGN channel and for code rate 1/2, WiMAX-CTC achieves better performance than the UMTS systems. This improvement is increased as the frame size (FS) increases. This is shown clearly in Fig.5 for FS 1920 bits. On the other hand, at code rate 1/3 (the standard UMTS code rate), the BER performance of both UMTS-CTC and WiMAX-CTC is almost the same for relatively small FS (240 bits) as shown in Fig. 3. As the FS increases (960 and 1920 bits), the BER performance for UMTS-CTC is improved over the WiMAX-CTC as shown in Fig.4 and Fig.5.
2. When dealing with Rayleigh fading channel and for code rate 1/2, the BER performance for WiMAX-CTC is slightly better than UMTS-CTC, especially for large FS (Fig.8). However, at code rate 1/3 the BER performance for both UMTS-CTC and WiMAX-CTC is almost the same for all selected FS.

Finally, we suggest the following as areas for future work:

- Implementing both UMTS-CTC and WiMAX-CTC on Hardware.
- Applying the LDPC code for both UMTS and Mobile WiMAX systems and study their BER performance.
- Comparing the results with the one obtained for CTC.

REFERENCES

- [1] Berrou, C., Glavieux, A. and Thitimajshima, P., "Near Shannon limit error-correcting coding and decoding: Turbo codes," Proc. 1993 IEEE International Conference on Communications, Geneva, Switzerland, pp. 1064-1070, 1993.
- [2] Berrou, C. and Glavieux, A., "Near Optimum Error Correcting Coding and Decoding: Turbo-Codes," IEEE Trans. On Communications, vol. 44, no. 10, pp. 1261-1271 October 1996.
- [3] Loutfi N., "WiMax-Technology for Broadband Wireless Access", Wiley, 2007.
- [4] Jeffrey G. A., Arunabha G., Rias., "Fundamentals of WiMAX", Prentice Hall, 2007
- [5] IEEE. Standard 802.16e-2005. Part16: Air interface for fixed and mobile broadband wireless access systems—Amendment for physical and medium access control layers for combined fixed and mobile operation in licensed band, December 2005.
- [6] IEEE. Standard 802.16-2004. Part16: Air interface for fixed broadband wireless access systems, October 2004.
- [7] European Telecommunications Standards Institute, Universal mobile telecommunications system (UMTS): Multiplexing and channel coding (FDD), 3GPP TS 25.212 version 5.0, 2002.
- [8] W. George, "Optimized Turbo Codes for Wireless Channels", Doctor of Philosophy (Ph.D.)Thesis, University of York, UK, October 2001
- [9] P. Robertson and E. Villebrun and P. H'ohler, "A Comparison of Optimal and Sub-Optimal MAP Decoding Algorithms Operating in the Log Domain," Proceedings of the International Conference on Communications, Seattle, United States, pp.1009-1013, 1995.

Fig. 3 BER performance comparison for $FS = 240$ and AWGN channelFig. 4 BER performance comparison for $FS = 960$ and AWGN channelFig. 5 BER performance comparison for $FS = 1920$ and AWGN channelFig. 6 BER performance comparison for $FS = 240$ and Rayleigh fading channel

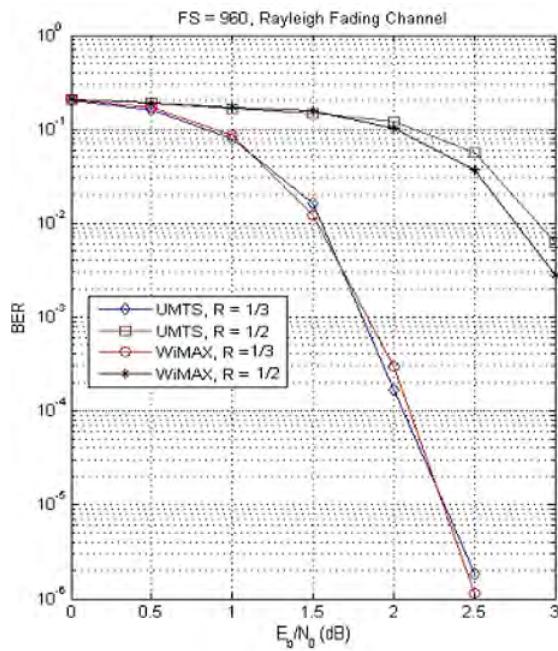


Fig. 7 BER performance comparison for FS = 960 and Rayleigh fading channel

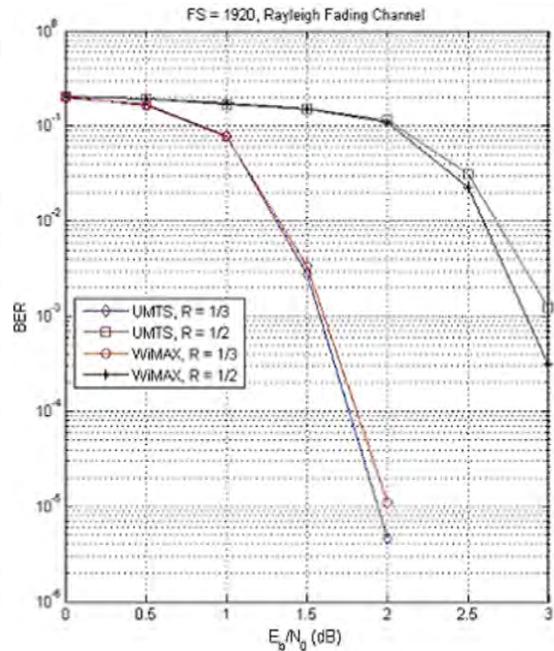


Fig. 8 BER performance comparison for FS = 1920 and Rayleigh fading channel

Performance of Interleaved Cipher Block Chaining in CCMP

Zadia Codabux-Rossan, M. Razvi Doomun
Computer Science Department, Faculty of Engineering
University of Mauritius
zadiac@gmail.com, r.doomun@uom.ac.mu

Abstract - Nowadays, the increased use of battery-powered mobile appliances and the urge to access sensitive data anywhere has fuelled the demand for wireless networks. However, wireless network is susceptible to intrusion and security problems. There is an inherent need to secure the wireless data communication to ensure the confidentiality, authenticity, integrity and non repudiation of the data being exchanged. On the other hand, the computation and energy cost to achieve security can be high as encryption algorithms are generally computationally intensive, thus consuming a significant amount of computing resources such as CPU time, memory, and battery power. Considering the very limited resources on wireless devices, it is crucial implement security protocols efficiently. This work focuses on how the energy consumption of execution is impacted by the use of unoptimized AES-CCMP algorithm and optimized AES CCMP Algorithm using 2-Way Interleaving, without compromising the security of the session. We also analyze the performance of AES (Rijndael) and AES-CCMP. Two-way interleaving technique as an optimization of the CBC MAC is investigated using two performance metrics, namely encryption time and throughput.

Keywords: Wireless Security, CCMP, IEEE 802.11i, Interleaved Cipher Block Chaining

I. Introduction

With the maturing of industry standards and the deployment of lightweight wireless hardware across a broad market section, wireless technology has come of age. Recent advances in wireless network technologies are growing fast, evidenced by vast number of publications in the field of IEEE 802.11 Wireless Local Area Networks (WLANs), Mobile Ad Hoc networks and wireless sensor networks [8]. Deployment wireless networks are rapidly expanding due to their ability to provide communications with ubiquity and mobility. Due to the broadcast nature of the wireless radio signals, wireless networks are inherently vulnerable to several network attacks. Anyone within the wireless transmission range of a device is able to passively listen to or eavesdrop on the signals and could potentially access information from the signals. It is also possible to actively transmit

signals that can attack the network. Wireless networks are therefore extremely vulnerable to many kinds of security threats and they essentially need strong countermeasures to overcome those threats.

It is imperative to provide adequate security services to wireless networks, but providing security for wireless devices is a more challenging research topic because of very limited resources such as low-speed CPUs, small-sized memory, and importantly limited battery power. Designing efficient security services in battery-powered devices is a challenging research problem because security services rely on cryptographic and mathematical functions that are known to be computationally intensive. Therefore, innovative techniques are required to find the best trade-off between optimizing security strength to thwart existing security attacks and conserving maximum battery power to expand the operational lifetime of these devices.

The structure of the paper is organised as follows: We explain AES and AES-CCMP in section II and give a review of related works in section III. The Interleaved CBC technique is proposed in section IV. The experimental set and Results & Discussions follow in section V and VI, respectively. Finally, we conclude the work in section VII.

II. AES Overview

A. Advanced Encryption Standard (AES)

AES is a symmetric iterated block cipher, meaning that the same key is used for both encryption and decryption, with multiple passes made over the data for encryption, and the clear text is encrypted in discrete fixed length blocks. AES processing in CCMP use AES 128-bit key and 128-bit block size. Per FIPS 197 standard [6], the AES algorithm (a block cipher) uses blocks of 128 bits, cipher keys with lengths of 128, 192 and 256 bits, as well as a number of rounds 10, 12 and 14 respectively. The security of the AES algorithm depends on the number of “Rijndael” rounds. The more the number of rounds, the more the security

strength will be [23]. Each Rijndael round is composed of four stages: Byte Substitution, Shift Rows, Mix Columns, and Add Round Key with some exceptions for the last round [2].

B. AES CCMP

The 802.11i defines a new encryption method based on the AES-CCM. CCM Protocol provides data-confidentiality (AES in counter mode) and for authentication and integrity, CCMP uses CBC-MAC. In IEEE 802.11i, CCMP uses a 128-bit key and protects some fields that are not encrypted. The additional parts of the IEEE 802.11 frame that get protected (AAD) includes the packets source and destination and protects against attackers replaying packets to different destinations. CCM is intended for use in a packet environment, i.e., when all of the data is available in storage before CCM is applied; It is not designed to support partial processing or stream processing. The input to CCM, as shown in **Figure I**, includes three elements: 1) data that will be both authenticated and encrypted, called the payload; 2) associated data, e.g., a header, that will be authenticated but not encrypted; and 3) a unique value, called a nonce, that is assigned to the payload and the associated data [13].

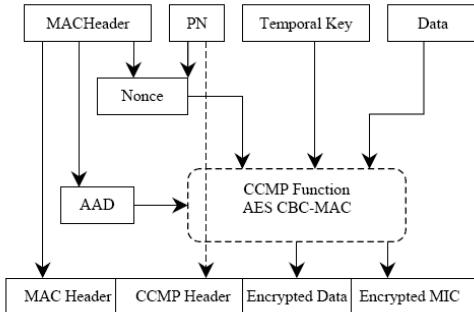


Figure 1: AES-CCMP [21]

C. AES-CCMP in Wireless Network Security

Many wireless devices have limited resources such as low-speed CPUs, small-sized memory, and importantly limited battery power. The pace of advancements in battery technologies has not kept up with that of wireless technologies. This implies that mobile devices typically operate on a meagre power budget and therefore computationally intensive encryption/decryption algorithms and the related security parameters may not be supported. We also note that there are several areas such as wireless sensor networks where the battery power limitation is extreme and re-charging or changing drained batteries may be impossible. Therefore, the primary challenge in providing security in low power mobile wireless devices lies in the conflicting interest between minimizing power

consumption and maximizing security. In general, it is assumed that by doing more computations one can achieve a higher amount of security. For example, the strength of encryption schemes depend on the size of the key and the number of encryption rounds [10]. Larger key sizes/more rounds produce higher levels of security (or less security vulnerabilities) at the cost of additional power consumption [20].

III. Related Work

Due to the efficiency and performance of Rijndael, AES-CCMP is a good candidate for wireless network devices but there are many previous works [2] regarding hardware and software implementations of AES-CCMP that have been carried out in order to optimize the AES-CCMP encryption algorithm to reduce power consumption. In this section, a review of recent related work concerning energy consumption of cryptographic mechanisms is presented and the researches carried out by other authors are critically discussed.

The main sources of energy consumption during a secure wireless transaction are: (i) cryptographic computations used to establish secure sessions and for encryption and authentication (ii) for performing secure data transactions [22]. Security in wireless networks is achieved by security protocols at different levels of the protocol stack, for example WEP at the Link Layer, IPSec at the Network Layer, TLS/SSL and WTLS at the Transport Layer and so on. Security protocols are made up of cryptographic algorithms which can be categorized as asymmetric and symmetric algorithms for authentication and privacy purposes and hash algorithms for message integrity [14]. One of the main challenges of mobile wireless systems is the mismatch between security requirements and available battery capabilities. A number of research publications [14][15][23] have focused on analyzing the energy consumption of different encryption algorithms rather than finding ways to optimize battery life.

There are some works which have compared the energy consumption of AES/Rijndael with other algorithms. In ref. [19], the authors compared AES and RC4 and proved that AES is more suitable for devices with low processing power such as wireless devices. Performance and energy consumption of the following block ciphers Rijndael (AES), RC6, Serpent, Twofish and XTEA were evaluated by [9] with lightweight software implementations. In [5], the author describes a study that compared encryption algorithms namely RC2, BLOWFISH, XTEA and AES to investigate the performance in terms of latency and throughput and energy consumption of block ciphers on a resource limited handheld device, the PDA.

Research has also been carried out with protocols and algorithms other than AES, to investigate their energy-efficiency and propose ways to optimize them to minimize their energy consumption. The work [18] reviewed the energy consumption of IPsec. The papers by [14] and [15] compared the energy consumption among the three types of cryptographic algorithms namely symmetric, asymmetric and hash algorithm. Ref [22] conducted a study for the energy cost of session negotiation protocols used by IPsec and WTLS protocols and proposed techniques to optimize the energy consumption during the session negotiation. Ref [16] conducted a study of the energy savings at some levels of the protocol stack for wireless systems. There are also numerous software strategies to optimize energy consumption in wireless networks that have been proposed by different academia and researches. According to [19], a common way to minimize wasted transmission energy in communication protocol is to send a short probe first to determine if conditions for data transfer are optimum and then send data. The probes are encrypted with an encryption algorithm which doesn't consume much energy. A proposal by [4] consisted of proposing a novel block cipher, HD Cipher to replace AES in the CCMP. HD Cipher has a 288-bit keystream and therefore has fewer encryptions per frame. Energy savings realized by HD Cipher were of the order of 40% over the use of AES. Computation offloading on a handheld in a wireless LAN secured by IPsec was investigated by [24]. In [14] and [21] both studied the use of an adaptive resource-aware security protocol which alters its behavior based on the operating environment. Ref. [15] mentioned that there are 2 software techniques for improving performance namely table look-ups and loop unrolling. The NOVSF code hopping technique was proposed by [7]. NOVSF takes advantage of the time slots and assigns data blocks to different time slots in every session and therefore increases communication security without additional energy.

In addition to the software approaches proposed earlier, there exists many hardware schemes to optimize power-security efficiency. Ref [1] implements a fast, efficient, low-power FPGA of AES-CCM whereby the computational intensive cryptographic processes are offloaded from the main processor. The authors in [11] proposed an implementation which uses the ARM core architecture and a new implementation for the new Mix Column implementation. Ref. [3] demonstrates the implementation of the AES/Rijndael algorithm on the DREAM architecture which is a dynamically reconfigurable architecture. The work in [17] presents the design and implementation of a compact 8-bit AES ASIC encryption core suitable for low-cost and low-power devices.

IV. Interleaved Cipher Block Chaining

Interleaved encryption is the processing of the encryption of a message as multiple independent messages block of known size, with N different IVs, generally treating every n th block as part of a single message. CBC is difficult to parallelize, which leads to the development of Interleaved CBC (ICBC), in which multiple streams of CBC encryption are interleaved [12]. The encryption of the next block of data can start as soon as the block N positions earlier have been encrypted. For this work, we are proposing the software implementation of two-way CBC interleaving as an optimisation in the AES CCMP encryption. In two-way interleaved chaining, the first, third and every two block thereafter is encrypted in CBC mode. The second, fourth and every two block thereafter is encrypted as another stream. An example of such mode is the interleaved CBC mode shown in **Figure II**. The benefits of interleaved modes, such as the interleaved CBC mode is that they have a potential to offer security of feedback modes combined with the performance of non-feedback modes. Interleaving allows delivering of high performance mainly in terms of gain in speed while maintaining level of security.

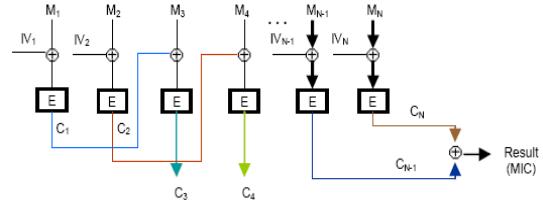


Figure II: Interleaved CBC Mode

However, as shown in **Figure II**, for the ICBC, 2 IVs are required to be transmitted to receiver. Moreover, more than 1 result is obtained as the outcome of ICBC. An additional computation is required to merge the multiple results into 1. The two-way interleaved chaining will produce 2 results at the end. The multiple results will be XORED to produce a single MIC as the outcome. Such modes are likely to be considered by NIST for standardization as future AES operating modes and become a part of other standardization efforts.

V. Experimental Setup

Experimental tests have been performed on an HP Compaq Presario V2000, which is equipped with an Intel Pentium Mobile Processor Centrino 1.6 GHz CPU working at a (constant) clock rate of 598.5 MHz and a physical RAM of 512 MB. The operating system was Microsoft Windows XP Professional Version 2002. During the simulations, there were no other tasks running on the system except the system tasks. The coding of the program is in the C++ language, which is a high-level

language defined at higher abstract levels and is programmer-friendly. For obtaining the energy consumption of the encryption algorithm it was necessary to determine several factors, which can be used for a general comparison. In our experiment, the performance metrics measured are encryption time and throughput. The encryption time is the time that an encryption algorithm takes to produce a ciphertext from a plaintext. It is calculated as the total of CBC MAC encryption time and Counter mode encryption time. Encryption time is used to calculate the throughput of an encryption scheme that indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time.

VI. Results & Discussions

A. Unoptimized AES CCMP

AES CCMP has been implemented by calculating the MIC tag and then encrypting the plaintext and MIC tag in counter mode to get the cipher text. For increasing text size, the encryption time and throughput is measured to encrypt plaintext to cipher text using the unoptimized version of the AES CCMP software.

- **Encryption Time Measurement**

The encryption time measured is the total time of the CBC MAC time summed with the Counter mode encryption time. The CBC MAC encryption time is the total time of the MIC IV calculation time added with the headers calculation time and the MIC tag calculation time.

CBC MAC encryption time = `construct_mic_iv()` time + `construct_mic_header1()` time + `construct_mic_header2()` time + `calculate_mic()` time

The Counter mode encryption time is the total time of the Counter calculation time and the data and MIC tag encrypted in counter mode time.

Counter mode encryption time = `construct_ctr_preload()` time + `encrypt_mpdu()` time

The results of these measurements were averaged to get the encryption time for blocks of plaintext and the results are presented in **Figure III**. With an increasing plaintext data size (in bytes), the encryption time increases. When the plaintext data size quadruples, it results in an increase in encryption performance time by 340.7%.

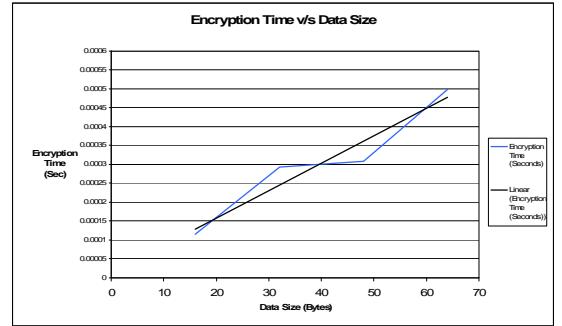


Fig III: Encryption Time v/s Data Size for unoptimized AES CCMP

- **Throughput Measurement**

The throughput was measured by dividing the length of the data size by the encryption time. An increase in the plaintext data size will cause a decrease in the throughput. When the plaintext data size quadruples, it leads to a decrease in the encryption time by 331.7%, shown in **Figure IV**.

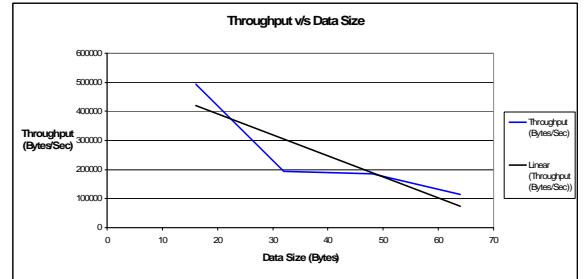


Fig IV: Throughput v/s Data Size for unoptimized AES CCMP

B.2 Way Interleaved ICBC

AES CCMP has been optimized using 2-way interleaving. For increasing text size, the encryption time and throughput is measured to encrypt plaintext to cipher text using the 2-way interleaved version of the AES CCMP software.

It should be noted that the CBC MAC encryption time takes up to 80% of the total encryption time and according to the equation for the CBC MAC encryption time, the IV and headers take up to about 3% and the MIC tag calculation takes up 97% of the total time respectively. With the 2 way ICBC optimization, the encryption time for the IV and headers will remain similar as for the unoptimized AES CCMP and the Counter mode time also will be same as no modifications have been made to that part of the design. However, as the encryption of the plaintext will be done in parallel, the MIC tag calculation time is expected to decrease by approximately 50%. **Figure V** shows that the general trend is an increase as the data size in bytes increases.

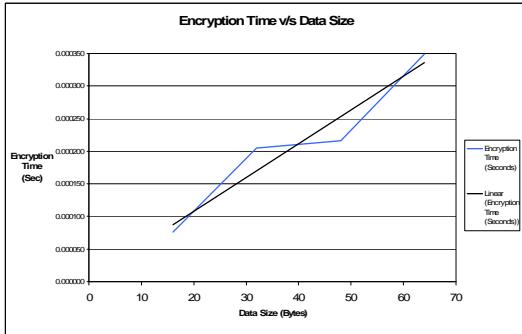


Fig V: Encryption Time v/s Data Size for 2 Way Interleaved AES CCMP

The throughput for the 2 Way Interleaved AES CCMP is as shown in **Figure VII**:

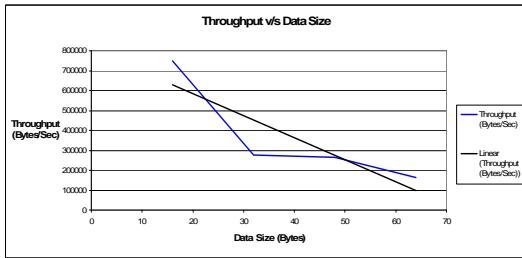


Fig VI: Throughput v/s Data Size for 2 Way Interleaved AES CCMP

C. Unoptimized AES CCMP and 2-Way ICBC

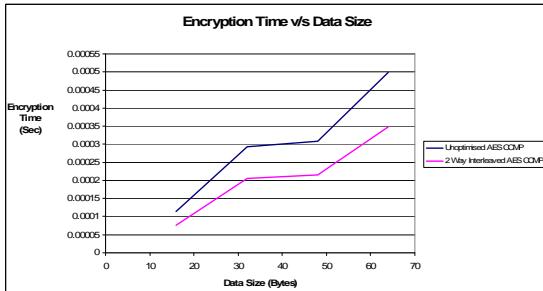


Fig VII: Unoptimized AES CCMP v/s 2 Way Interleaved AES CCMP for encryption time metric

The results in **Figure VII** confirms that it takes less time to encrypt the same amount of data with the 2 way interleaved CBC algorithms rather than the unoptimized AES CCMP. The approximate percentage decrease in time taken is roughly 30%.

With increasing data size, the throughput decreases. The 2 way interleaved CBC algorithms encrypt more data per unit time rather than the unoptimized AES CCMP. More data is encrypted for 2 way interleaved CBC algorithm rather than unoptimized AES CCMP during the same lapse of time, as shown in **Figure VIII**.

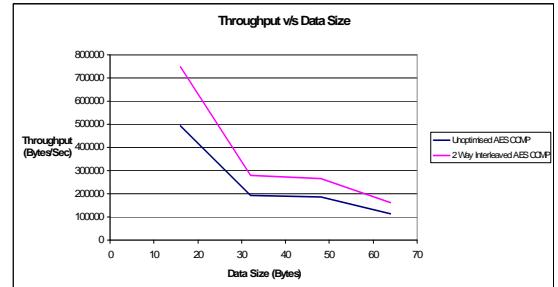


Fig VIII: Unoptimized AES CCMP v/s 2 Way Interleaved AES CCMP for throughput metric

VII. Conclusion & Future Works

The AES CCMP, referred to as the “unoptimized AES CCMP” was implemented and performance metrics like encryption time and throughput were evaluated for increasing number of data blocks. It was noted that with an increasing plaintext data size, the general trend for the encryption time is a linear increase. As the throughput is inversely proportional to the data size, an increase in the plaintext data size will cause a decrease in the throughput. Increasing the plaintext data by a factor of 4, increases the encryption time increases by a factor of **4.33** and decreases the throughput by a factor of **4.31**.

An optimized AES CCMP, with interleaved CBC-MAC, was then implemented and the performance gain compared with the unoptimized version of AES CCMP. The enhanced AES CCMP is the combination of an optimized CBC MAC, while the Counter mode is unchanged. The Interleaved CBC (ICBC) in which multiple streams of CBC encryption are interleaved is motivated from the work in reference by [12] which proposes the concept of parallel computation. With this method, the encryption of the next block of data can start as soon as the block N positions earlier have been encrypted. In two-way interleaved chaining, the first, third and every two block thereafter is encrypted in CBC mode. The second, fourth and every two block thereafter is encrypted separately as another CBC mode stream. The simulation scenarios clearly demonstrate for the 2-Way Interleaved AES CCMP that as the plaintext increases, the encryption time increases and the throughput decreases.

VIII. References

- [1] A. Aziz and N. Ikram, “An FPGA- based AES-CCM Crypto Core for IEEE 802.11i Architecture”, International Journal of Network Security, Vol5, No2, Sept 2007
- [2] A. Samiah, A. Aziz and N. Ikram, “An Efficient Software Implementation of AES-CCM for IEEE 802.11i Wireless Standard”, 31st Annual International Computer Software and Applications Conference - Vol. 2- pp. 689-694, COMPSAC 2007

- [3] C.Mucci, L.Vanzolini, F.Campi, A. Lodi, A. Deledda, M. Toma and R. Guerrieri, "Implementation Of AES/Rijndael On A Dynamically Reconfigurable Architecture", Design, Automation & Test in Europe Conference & Exhibition, 2007
- [4] C.N.Mathur and K.P. Subbalakshmi, "Energy efficient wireless encryption", IEEE Global Telecommunications Conference, 2006.
- [5] C.T.R. Hager, S.F. Midkiff, J.-M Park, T.L. Martin, "Performance and Energy Efficiency of Block Ciphers in Personal Digital Assistants", In proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (Percom 2005), IEEE Computer Society Press, 2005
- [6] Federal Information Processing Standards Publication (FIPS) 197, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", November 26, 2001
- [7] H. Cam. S. Ozdemir, D. Muthuavinashiappan, P. Nair, "Energy efficient security protocol for wireless sensor networks", VTC 2003-Fall. 2003 IEEE 58th, Vehicular Technology Conference, 2003.
- [8] H. Yang, F. Ricciato, S. Lu, L. Zhang, "Securing a Wireless World", Computer. Sci. Dept., Univ. of California, Los Angeles, CA, USA, Proceedings of the IEEE, Feb. 2006 Volume: 94, Issue: 2
- [9] J. Großschädl, S. Tillich, C. Rechberger, M. Hofmann, and M. Medwed, "Energy evaluation of software implementations of block ciphers under memory constraints", Design, Automation & Test in Europe Conference & Exhibition, 2007.
- [10] J. Nechvatal, E. Barker, D. Dodson, M. Dworkin, J. Foti, E. Roback, "Status Report on the First Round of the Development of the Advanced Encryption Standard", Journal of Research of the National Institute of Standards and Technology, Volume 104, Number 5, September–October 1999
- [11] K. Atasu , L. Breveglieri , M. Macchetti, "Efficient AES Implementations For ARM Based Platforms", Proceedings of the 2004 ACM symposium on Applied computing, 2004
- [12] K. Gaj, P. Chodowiec, "Hardware performance of the AES finalists - survey and analysis of results", Technical Report, George Mason University, Sep 2000, http://ece.gmu.edu/crypto/AES_survey.pdf
- [13] M Dworkin, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, NIST Special Publication 800-38C, May 2004
- [14] N.R. Potlapally, S. Ravi, A. Raghunathan, N.K.Jha, "Analyzing the energy consumption of security protocols, Proceedings of 8th International Symposium on Low Power Electronics and Design", ISLPED '03, ACM Press 2003
- [15] N.R. Potlapally, S. Ravi, A. Raghunathan, N.K.Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols", IEEE Transactions on Mobile Computing, Vol 5, No 2, February 2006
- [16] P Agrawal, "Energy efficient protocols for wireless systems", IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Vol 2, Boston , USA, 1998
- [17] P. Hamalainen, M. Hannikainen, T.D. Hamalainen, "Efficient Hardware Implementation of Security Processing For IEEE 802.15.4 Wireless Networks", 48th Midwest Symposium on Circuits and Systems, 2005.
- [18] P. Ni and Z. Li, "Energy cost analysis of IPsec on handheld devices", Microprocessors and Microsystems, Special Issue on Secure Computing Platform, 2004.
- [19] P. Prasithsangaree, P. Krishnamurthy, "Analysis of energy consumption of RC4 & AES algorithms in wireless LANs", Global Telecommunications Conference, GLOBECOM IEEE, 2003
- [20] R. Chandramouli, S. Bapatla, K. P. Subbalakshmi, R. N. Uma, "Battery Power-aware Encryption", ACM Journal Name, Vol. V, No. N, February 2005.
- [21] M.R. Doomun, K.M.S Soyjaudah, "Adaptive IEEE 802.11i security for energy security optimization", The Third Advanced International Conference on Telecommunications, 2007. AICT 2007.
- [22] R. Karri and P. Mishra, "Analysis of energy consumed by secure session negotiation protocols in wireless networks", International Workshop on Power and Timing Modeling, Optimization and Simulation, Torino, Italy, Sep 2003
- [23] W Roche, "The Advanced Encryption Standard, The Process, Its Strengths and Weaknesses", University of Colorado, Denver, Spring 2006 Computer Security Class, CSC 7002, Final Paper, May 6, 2006
- [24] Z. Li. R. Xu, "Energy Impact of Secure Computation on a Handheld Device", IEEE 5th International Workshop on Workload Characterization, 2002.

Localization and Frequency of Packet Retransmission as Criteria for Successful Message Propagation in Vehicular Ad Hoc Networks

Andriy Shpylchyn, Abdelshakour Abuzneid

University of Bridgeport

ashpylech@bridgeport.edu, abuzneid@bridgeport.edu

Abstract – As the field of the wired networking communications developed, so did the mechanisms for the reliable delivery of messages from one user to another. With the advance of the wireless communications, these mechanisms had to be adjusted, or sometimes developed anew. Vehicular ad hoc networks present themselves as a specific example, where the mechanisms, which are in use in the Wireless LANs and mobile ad hoc networks, are not enough. This paper will discuss, in particular, the range of the message propagation and frequency of the message re-broadcasts by nodes that received it. As these factors are adjusted, they will produce higher throughput and lesser packet loss. The latter factor is of prime importance for the vehicular ad hoc networks, due to the fact that there is no process of packet reception acknowledgment as it exists in typical Wireless LANs. The concept of a single broadcast is of the utmost importance in the case of a vehicle sending a warning message, where the neighboring vehicles could benefit greatly from the information received. These abovementioned aspects will be shown through the simulation of the vehicular ad hoc network.

I. INTRODUCTION

The area of vehicular ad hoc networks can still be thought of as being in its early stages of development. In the last few years there has been an increased interest in this field. VANETs are different from the traditional Wireless LANs, MANETs and cellular networks. Even though the basic concepts are the same, their actual physical representation is significantly different.

In the WLAN environment there are mechanisms to ensure the integrity of the message and the confirmation of its delivery. In case of the packet loss, the packet, which has not been confirmed as received, will once again be transmitted. In the vehicular networks, sending acknowledgment would add more packets to already congested network. This acknowledgment mechanism could certainly be used in case of the applications that maintain their state, multimedia downloads, and for security purposes.

The VANET, being subclass of MANETs, exhibits the behavior of the mobile nodes connected via an ad hoc network. However, the most distinguishing characteristic is the speed of the nodes that are part of the network. In the vehicular ad hoc networks the nodes operate at high speeds as the vehicles move along the highway. Here the vehicles can still participate in the same ad hoc network; however, with the change of node's

speed in relation to the VANET the vehicle will not be able to be a part of the network. The vehicles can also be part of the ad hoc network in a big city. They will not move with high speeds. The nodes will belong to a particular VANET for some time. However, their location in regard to each other will constantly be changing as the drivers change the course of their route or stop at the red light. Therefore, in both cases the frequent, and at times even radical, changes in network topology should be expected.



Figure 1: Instance of VANET at intersection

Figure 1 depicts the event of formation of small-sized VANET in an urban environment. A vehicle at the intersection, the green auto, sends out a warning packet to the vehicles in the vicinity. It takes only one hop to reach these nodes. This packet is, in turn, retransmitted by the red vehicle to the vehicle near by, the other red vehicle. Hence the packet reaches the second red vehicle in two hops.

The mobile nodes in the vehicular ad hoc network can also communicate with the infrastructure nodes. The existence of the infrastructure helps the message propagation over large distances. It is also important for the possible future use with multimedia applications. Current trends in this area are described in [1]. At the present time, however, building an infrastructure would be an enormous task which would involve careful planning and tradeoffs between the density of infrastructure nodes and their costs.

This brief overview of VANETs and their place among the array of mobile communication technologies brings us to the statement regarding the scope of this research. This paper will center on the communication between the vehicles in the urban environment. A particular emphasis of this research is on the propagation of the emergency and warning messages over the neighborhood area of the sender. In addition to this, the impact of the transmission distance and frequency of the message

rebroadcast by the receivers on the network congestion and packet loss will be discussed.

The following is the structure of this paper. First, the brief background of the research in the area of vehicular ad hoc networks will be presented. Next section will convey the state of the available simulators for VANETs. This will show the way to the presentation of the possible environments that can be simulated for the vehicle-to-vehicle communication. The experimental section will present the setting of the research and discuss ways of mitigating the packet collisions. Finally, the results of the simulation experiment will be analyzed and the significance of this research for the future developments in VANETs will be discussed.

II. VEHICULAR AD HOC NETWORKS

As mentioned before, the field of vehicular ad hoc networks is a relatively new one. At the present time, there has been no extensive research conducted in this field. This is why the VANETs have been perceived by the research community as an important area. For this cause, FCC has allocated a bandwidth of 75 MHz on the licensed ITS band of 5.9 GHz, so that the possibilities of car-to-car communication applications could be further researched. In regard to the protocol stack, a customized version of protocol for wireless communication between vehicles, IEEE802.11p, has been developed. There has been made a significant progress on the definitions of physical and MAC protocol layers by IEEE P1609.2 Working Group [10]. In the US, the range of applications for the 802.11p (WAVE) protocol is addressed by the Federal Intelligence Systems Program [9]. In Europe, Car 2 Car Communication Consortium has been established for the leading car makers to implement the new technology [8]. Since the establishment of these research consortiums many aspects of vehicular communication has been researched [11-14]. The research included not only the work on the protocol itself, but also on the numerous applications of this new way of communication. As the standardization of the WAVE protocol progressed, new groups appeared that centered on the specific applications of vehicular ad hoc network. European industry activity, PReVENT is working on the project WILLWARN, the system that aims to help drivers to avoid potential accidents [15]. Project SEVECOM is centered on the issue of providing secure communication between the vehicles [16]. Another project, Network On Wheels, focuses on the area of infotainment and safety applications [17].

III. VEHICULAR NETWORK SIMULATORS

The research conducted by the abovementioned consortiums and groups is very costly. The vehicles and the equipment constitute the major portion of the expense. In addition, it is time-consuming to perform a particular experiment a number of times. Also in many experiments there are large numbers of vehicles tested.

The best option for the small research groups is to use well-developed vehicular network simulator, which would be able to simulate the realistic vehicular models.

A vehicular network simulator required for this research is the simulator that contains models of ad hoc communication and variety of mobility options. On one hand, there are number of generic simulators, like OPNET [20], NS-2 [21] and QualNet, which include a range of wireless traces. These three, however, do not have models for the vehicular traffic. On the other hand, there are simulators that created for the sole purpose of generating the vehicular traces. The traffic simulators like SUMO [27] and VISSIM are able to create very close imitation of the real world traffic activity. However, they do not include models for communication between the vehicles.

In the last two years there have been attempts on the part of number of simulator developers to create additional models in ns-2 that would simulate vehicle-to-vehicle communication. The result of one such attempts is TraNS, joint traffic and network simulation environment [18]. The main purpose of this tool is to take the mobility traces from vehicular simulator SUMO and make them available for ns-2. In this way, TraNS was the first open-source project aimed at providing environment that would provide the results very close to those in the real-world environment [22].

In addition to TraNS there have been developed several simulators focusing on different mobility traces. The STRAW, simulator created by AquaLab project, concentrates mostly on the communication of the vehicles that move randomly along the streets of a city [23]. The University of Düsseldorf has developed simulation environment [25] that interlinks network simulator ns-2, traffic simulator PTV Vissim, Matlab/Simulink and Click [24] modular router.

The simulators and the simulation environments that have been mentioned up to this point have helped the research community to focus on the particular aspects of the vehicular ad hoc networks. The simulator that will be used in this research paper is GrooveNet [19]. This project was a joint effort of Carnegie Mellon University and General Motors Corporation. This is an example of a hybrid simulator which enables use of the real and simulated vehicles [4]. Moreover, this simulator includes a number of different vehicular mobility models. The availability of such models allows for a variety of simulation tests and comparison of the performance of VANETs in different environments, like city streets, highways or roads in the countryside. The GrooveNet also includes the Visual Display. This enables user to see what is happening in the network "in real-time". One can observe number of nodes that received any give packet and the area of message propagation. In order to enable the realistic representation of vehicular motion, the map database is included. It uses US Census Bureau's TIGER/Line files, which include selected geographic and cartographic information about particular area [26].

IV. MOBILITY MODELS IN GROOVENET

In order to study the network activity in the vehicular environment the behavior of the vehicles has to be taken into account. When we look at vehicular activity in a big city, for example, Manhattan, the vehicles do not always move in one

particular direction for a long time. The speed of the vehicles constantly changes in reference to each other.

GrooveNet includes Street Speed Model, where the vehicles move according to the speed limit set for a particular street. It is easy to work with this particular model because most of the vehicles will be approximately at the same distance from each other. Also there will not be drastic changes in the network topology for some time.

Another available model, Uniform Speed, is very similar to the Street Speed Model. This model allows for the distribution of the speed about the speed limit. With vehicles moving at different speeds and following their own path there will be more changes to the network topology than with Street Speed Model. One has to keep in mind that the vehicles still will not be moving at very high speeds due to the fact that the trip takes place in a busy city. They will also be constrained by the topology of the streets and activity of the traffic controllers.

It might happen on the single lane street that a vehicle could restrict the movement of other vehicles that follow it. In this situation the vehicles will not exceed the speed of the vehicle in front. In this case, a new VANET could originate and its topology, probably, would not change until the next intersection, where the drivers willing to proceed with greater speeds will be compelled to choose another route.

The notion of a vehicle having a particular route further extends the concept vehicular activity. In the recent years the GPS navigation systems have become extremely popular. The newer car models include these systems as a built in component. As a result, if a driver has a set destination, the shortest route will be selected.

The route of a vehicle could also consist of random “walking” for a certain distance and then taking a shortcut back home. The vehicle might exhibit an activity of randomly choosing where to go whenever it approaches an intersection. A glimpse at the network topology through the prism of such random activity makes one realize that the transmission of the warning packet will be an arduous task for the nodes of a particular ad hoc network.

At the time of transmission of a packet, the vehicles might be either at the close vicinity of the transmitting vehicle, or outside of the area of signal propagation. This situation leads to the next question: Should the transmitting node take into account the possibility of packet collision, in case of highly dense area of vehicles sending messages? If the network congestion is to be taken into account, then the transmitting vehicle has to sense the network state and wait to certain period of time and then transmit.

In addition to the network state, the message priority should be considered. If there is a certain warning message that has to be conveyed to a certain area, there might be a need to rebroadcast it without sensing the state of the ad hoc network. In this case, this particular message might cause enormity of packet collisions. Hence a few unimportant informational messages would give way to a priority message.

V. SETTING THE SIMULATION

The examination of various mobility and communication models available brings us to the experimental part of this paper. In order to evaluate the propagation of warning messages in the urban settings, the city that has been chosen for the simulation is Manhattan, NY. It is a very good example of a busy city due to a large amount of traffic throughout the day. In addition, the presence of one way streets further constrains the ability of vehicles to navigate freely.

For this given simulation 100 vehicles have been randomly placed over the area of 4 km². The duration of the simulation is 20 seconds. The model used for the simulation of the vehicular activity is the Uniform Speed Model. The speed of the vehicles is randomly distributed between 20 and 30 km/hour. The route for each vehicle is set up according to the Sightseeing Trip Model; the vehicles randomly “walk” along the streets of Manhattan for a period of time and then return to their starting point. The traffic lights have been added to the simulation, in order to make the conditions closer to those in a real city. The range of transmission of any given message is fixed to 200 meters.

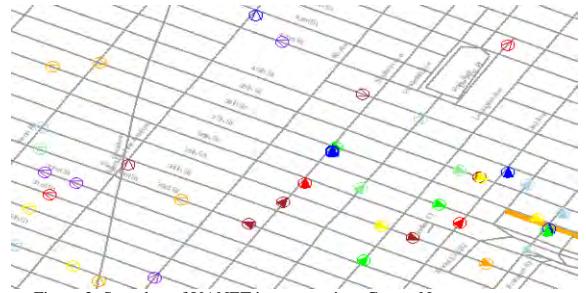


Figure 2: Snapshot of VANET instance using GrooveNet

The map of Manhattan with sending and receiving nodes is depicted by Figure 2. The blue node in the middle of the map transmits an emergency packet. This packet is received and then retransmitted by the nodes in the vicinity, marked by solid color. The nodes that have not received the emergency packet are marked by empty triangles. These nodes are beyond the range of transmission of the original sender of the packet. If the packet does not collide with other packets and the nodes move closer to the area of transmission, they will be able to receive it.

A. Rate of Message Retransmission

The simplest model for packet retransmission by the nodes that received it would be to wait a set period of time and then retransmit this packet to other nodes in the area. This model does not require complex calculations on the part of the node that performs the retransmission. With this model all messages will be considered as having equal priority.

In contrast to “receive-wait-retransmit” model, the real world situations might require more complex retransmission models. Due to the fact that some of the messages could be of greater priority, they would have to be retransmitted at a higher rate. This can be achieved through the adaptive broadcasting. At the beginning the rate of the retransmissions by nodes is set to be very high. With each subsequent retransmission, the time between each retransmission will grow exponentially. As a result, the nodes closer to the epicenter of the message will be

transmitting the message at a much higher rate than those far away from the epicenter.

In addition to the higher broadcast rate, the sensing mechanism can be added. Thus, if the node overhears that nearby the same packet has been transmitted, it does not take the action to retransmit the packet. As a result, the network will not be as congested as it would be with all duplicate messages.

In addition to the warning and emergency messages, the vehicles used in this simulation will be sending the information about their speed and direction to neighbors around them. This information will be sent on a channel different from that of the warning messages. Hence the informational packets will not collide with the important emergency packets.

B. Results of the Simulation

The simulation that is the center of interest for this paper consists of 5 warning/emergency packets sent by the randomly chosen nodes at the beginning of the simulation. The throughput, number of collisions and broadcast latency will be evaluated in case of the three retransmission methods described above.

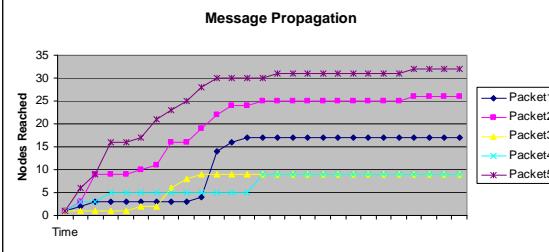


Figure 3: Throughput in case of “receive - wait 1 second - retransmit” retransmission

The Figure 3 reflects the propagation of the message through the midtown area of Manhattan. In the course of the first 10 to 12 seconds the packets have reached 95 percent of nodes. These figures when looked at under the normal conditions would satisfy the needs or the network. However, if a warning message has to reach the vehicles in a much shorter time of about 2 to 3 seconds, this method does not really perform well.

In order to be able to achieve a higher throughput, the time the node waits before retransmitting the packet should be much less than 1 second. In order to lower the possible congestion in the network, the rate of transmission should be lowered with time. The adaptive broadcast has the features needed to perform the abovementioned operations. At the start of transmission the rate will be set to less than half of a second. With each subsequent retransmission the time period to “wait” will be increased.

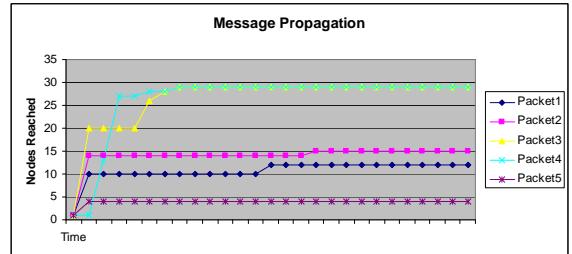


Figure 4: Throughput using adaptive broadcast method

The rate of packet propagation with the adaptive broadcast method is represented by Figure 4. Here something very different can be observed. 90 to 95 percent of nodes have received the message 3 to 4 seconds after the initial transmission. This clearly shows the advantage of the adaptive broadcast method. The delay of 4 seconds maximum should be acceptable the nodes that are further away from the epicenter of the message. The vehicles that are within 200 meters will be receiving the emergency packet with the delay up to 2 seconds. The drivers can make a decision based on the information delivered as to whether they should lower their speed, change a route, or continue along the previously chosen path.

Another metric that could be useful in evaluating the activity of the vehicular ad hoc network is the correlation between the number of packets and number of collisions. In case of the transmission with the steady rate of every 1 second, this relationship is 6 to 1. However, it has to be mentioned that most of collisions occur after the packet has been retransmitted for 7 to 10 seconds. In regard to the adaptive broadcast method, the packets to collisions ratio is 5 to 1. Here the collisions occur closer to the start of the transmission of the packet. Most of the collisions occur due to the network congestion at the initial stages of message propagation. The adaptive method still shows a higher performance rate simply because the packet was initially retransmitted at a much higher rate than that in case of regular retransmitting.

From the close observation of the Figure 4 it can be clearly seen that two of the packets, namely 3 and 4, have a much higher throughput than that of the remaining three. These two packets were transmitted in the area beyond the transmission range of the other packets. For this particular reason, the speed of packet propagation and the number of nodes that received it is much higher than the throughput of the remaining three packets. In addition, the vicinity of these packets was not as congested as the area of packets 1, 2, and 5. Thus, localization of a warning packet can be viewed as a way of increasing the throughput of the vehicular ad hoc network. And the way to further safeguard the priority messages, the separate channels could be used for priority messages, low priority warning messages and messages containing the speed of the neighboring vehicles.

To help lower the congestion of the network the nodes could sense the transmission channel before transmitting the emergency message. For this purpose, the Adaptive Broadcasting Model with sensing has been used in the simulation. In order to keep the speed of packet propagation,

the speed of rebroadcasting at the start of transmission will be high and decrease with each subsequent retransmission. If the node “overhears” that the same message is being retransmitted in the vicinity, it will stop sending the packet.

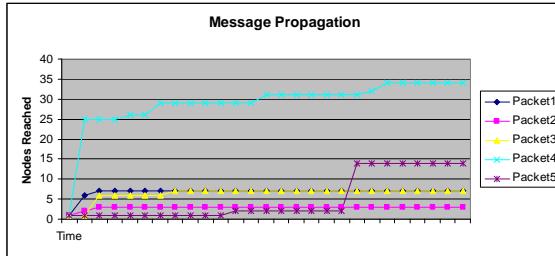


Figure 5: Throughput using adaptive broadcasting with sensing

The results of the simulation using this method are represented by Figure 5. Except for packets 4 and 5, the remaining three have reached the neighboring nodes with the rate very close to the regular adaptive broadcast method. This figure also shows that as there is a possibility for retransmitting without collision with the same packet, a high number of nodes received the packet.

The success of the adaptive broadcasting method with sensing is also supported with another metric. The number of collisions is very low in comparison to the previous two methods. Also the relationship between the number of packets on the network and the collisions is 8.6 to 1. This value is higher than that of the retransmission with the rate of retransmission being 1 second. Thus, the high throughput for the first few seconds after the initial transmission is achieved with this method.

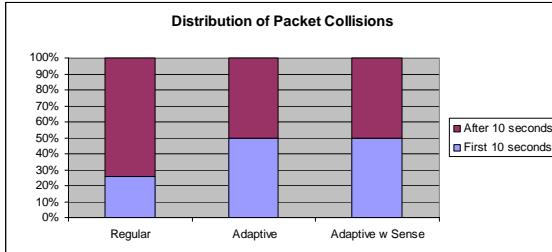


Figure 6: Distribution of Packet collisions over 20 seconds per Propagation Model

The correlation between the number of packets and number of the collisions indicates that by using the adaptive broadcasting method with sensing we will achieve the best results. However, what about the relationship between the collisions in the first 10 seconds after the initial transmission and after? The Figure 6 compares the percentages of packet collisions resulting with using a particular method. While using the Model with regular retransmission of 1 second, in the first 10 seconds since the initial message transmission the network experienced 26% of total collisions. By using the packet propagation method with retransmission rate of 1 second, the congestion state of the network is low. Most of the collisions will occur as more and more messages are propagated on the network. The bar number 2 in the Figure 6 depicts the distribution of collisions over time for the adaptive

broadcasting method. The amount of collisions is evenly distributed between the first half and second half of the 20 second period of packets transmission. The same appears to happen in case of adaptive broadcasting with sensing. In order to further examine the apparent similarities between the last two message propagation methods we have to examine the correspondence of the actual number of collisions when using each of the methods.

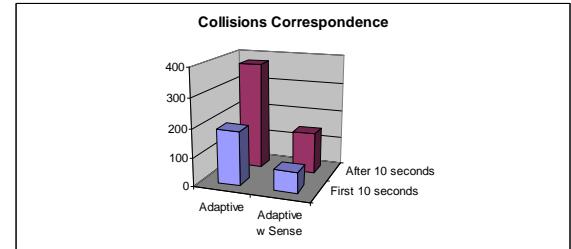


Figure 7: Correspondence of collisions when using Adaptive Method and Adaptive Method with Sensing

The Figure 7 sheds more light on the apparent resemblance of both methods. In fact, according to this Figure, the total number of collisions that occur when using the Adaptive Method is two times higher than in case of the same method that uses sensing. The nodes continue retransmitting the packet despite the fact that the same packet might already be circulating in their vicinity. As a result the possibility of transmitting additional packets becomes more limited.

C. Summation of the Results

In the process of simulating the vehicular ad hoc network the following assumptions have been proved true. By localizing a specific packet from other packets in the network (this can be done by limiting the area of packet propagation), more nodes in the vicinity will receive it. Moreover, less packet collisions happen.

The rate of packet propagation, which is the most important in case of the emergency packets, can be improved by using adaptive broadcasting. It is very important for the emergency packets to be transmitted to nodes in the vicinity in the first few seconds after the first transmission of the message appears on the network. This can be achieved with the retransmission rate which starts high and slows down over time. As a result the neighboring nodes receive the packet very quickly. By using such a retransmission rate, the network becomes congested from the high number of packets in the small area. Hence there is a need to maintain the congestion level in the network low. This can be achieved with adaptive broadcasting with sensing. Before transmitting the emergency packet, the node senses the network for the availability of the same packet. The packet will only be retransmitted if the given emergency packet is not being retransmitted in the vicinity of the retransmitting node. This method helps to lower the congestion rate, which the throughput of the packets remains relatively the same.

VI. THE FUTURE WORK

The work presented in this paper is related to the area of propagation of small-sized emergency packets. This research

shows that the high amount of these packets in a particular area results in collisions. In case of the emergency packets, the time for propagation could be lowered to 10 or 15 seconds since the first transmission. For emergency packets the broadcast latency is important. The packet should be delivered in a very short time to the nodes in vicinity. The nodes that are far away would not need to receive packets with information irrelevant to them. It is of the most importance for the nodes in vicinity to receive the given emergency packet. Lowering the total packet existence time will in turn lead to fewer collisions with other safety packets on the network.

In the recent years there has been a lot of talk regarding the multimedia applications over the network. Such applications would require higher bandwidth than regular safety packets. The network could be still sensed for congestion. And, in addition, the packets could be stored on the nodes themselves. The vehicles have the available space to store the information and power to continue retransmitting without need to charge as is the case of mobile laptops. As the network becomes less congested, the cached packets could be further retransmitted.

Different channels could be used for various applications. In the research conducted for this paper, the informational messages from neighboring nodes were sent on a channel different from the one that emergency and safety packets were sent. This method could be adapted for larger scale applications.

The security of the vehicular ad hoc network is as important as it is in any Wireless LAN. The fact that the infrastructure is absent makes the situation complicated. For the purposes of security, public-private key certificates can be used. More information on the use of certificates and security architecture could be found in [3].

VII. CONCLUSIONS

The center of attention for this paper is the localization of emergency packets and the frequency of retransmission. The simulation of the vehicular ad hoc network using GrooveNet VANET simulator showed that using these methods the given packet will be delivered to vehicles in the vicinity in much shorter time. This gives the driver an opportunity to make a decision about following a particular route. The faster the packet is delivered, the better chance for the driver to avoid the obstacle and safely continue to the destination. The methods of packet retransmission described before, in particular Adaptive Broadcasting with Sensing, together with separating the packets over the several channels (which is of great importance for infotainment and multimedia applications) will provide a solid foundation for stable network operations. The addition of the several infrastructure nodes evenly distributed over the area will ensure that the future applications for the vehicular networks will further enhance the meaning of the vehicular ad hoc networks.

REFERENCES

- [1] M. Gerla, B. Zhou, Y-Z. Lee, F. Soldo, L. Lee, G. Marfia. Vehicular Grid Communications: The Role of Internet Infrastructure. In *WICON '06*, Boston, MA. Aug. 2006.

- [2] S. Yousefi, S. Bastani, M. Fathy. On the Performance of Safety Message Dissemination in Vehicular Ad Hoc Networks. In *ECUMN'07*, 2007.
- [3] M. Raya, P. Papadimitratos, J.-P. Hubaux. Securing Vehicular Communications. In *IEEE Wireless Communications*. Volume 13, Issue 5, October 2006.
- [4] R. Mangharam, D. S. Weller, R. Rajkumar, P. Mudalige and Fan Bai. GrooveNet: A Hybrid Simulator for Vehicle-to-Vehicle Networks. *Second International Workshop on Vehicle-to-Vehicle Communications (V2VCOM)*, San Jose, USA. July 2006.
- [5] <http://vanet.info/projects>
- [6] <http://trans.epfl.ch/>
- [7] M. Artimy, W. Robertson, W. Phillips. Assignment of Dynamic Transmission Range Based on Estimation of Vehicle Density. In *VANET'05*, Sept. 2005.
- [8] <http://www.car-to-car.org/index.php?id=129>
- [9] <http://www.itsoverview.its.dot.gov/>
- [10] http://www.standards.its.dot.gov/fact_sheet.asp?f=80
- [11] J. Blum, A. Eskandarian. Threat of Intelligent Collisions. In *IT Professional 6(1)*, 2004, 24-29.
- [12] L. Gollan, C. Meinel. Digital Signatures for Automobiles. In *Proceedings of Systemics, Cybernetics and Informatics (SCI)'02*, 2002.
- [13] J.-P. Hubaux, S. Capkun, J. Luo. The Security and Privacy of Smart Vehicles. In *IEEE Security and Privacy Magazine* 2(3) 2004, 49-55.
- [14] Q. Xu, T. Mak, J. Ko and R. Sengupta, Vehicle to Vehicle Safety Messaging in DSRC. In *Proceedings of VANET'04*, 2004.
- [15] <http://www.prevent-ip.org/en/home.htm>
- [16] <http://www.sevecom.org/>
- [17] <http://www.network-on-wheels.de/documents.html>
- [18] <http://trans.epfl.ch/>
- [19] <http://www.seas.upenn.edu/~rahulm/Research/GrooveNet>
- [20] http://www.opnet.com/solutions/network_rd/index.html
- [21] <http://nsnam.isi.edu/nsnam/ns/>
- [22] M. Piorkowski, M. Raya, A. Lugo, P. Papadimitratos, M. Grossglauser, J.-P. Hubaux. TraNS: Realistic Joint Traffic and Network Simulator for VANETs. Accepted In *ACM SIGMOBILE Mobile Computing and Communications Review*.
- [23] <http://www.aqualab.cs.northwestern.edu/projects/STRAW>
- [24] <http://www.read.cs.ucla.edu/click/>
- [25] <http://www.cn.uni-duesseldorf.de/projects/MSIE>
- [26] <http://www.census.gov/geo/www/tiger/>
- [27] <http://sumo.sourceforge.net/index.shtml>

Authentication Information Alignment for Cross-Domain Federations

Zhengping Wu

Department of Computer Science and Engineering,
University of Bridgeport
221 University Avenue
Bridgeport, CT 06604 USA

Alfred C. Weaver

Department of Computer Science
University of Virginia
151 Engineer's Way
Charlottesville, VA 22904 USA

Abstract-With the rapid deployment of distributed systems and the Internet, federation activities such as online collaboration and information sharing become pervasive. Trust is a big issue in these federation activities. To manage trust in federation activities, authentication information needs flexible manipulation to accommodate technical and managerial requirements. To achieve identity federation across domains, authentication information must sometimes be adjusted, transformed, augmented, or substituted during the authorization and verification operations. In this paper, we propose a plug-in style alignment using a wavelet transformation to manipulate authentication information for verification and authentication. We incorporate BioAPI in our implementation to extend the capability of our system to adapt to different authentication models and technologies. Experimental results show that the overhead of this plug-in alignment is negligible.

1. INTRODUCTION

Federation activities become more and more pervasive with the development of network infrastructures. When different organizations or trust domains control different computing resources for federation activities, trust management plays a critical role to smooth security and privacy issues in collaboration and information sharing among these domains. Representation of trust-related information is important for federated trust management [1]. Trust representation needs to express various factors in federated trust management and a set of protocols to make different languages interoperable.

Factual trust information includes those objectively measurable elements, which can be classified into three categories: identity information, privilege information and trust knowledge. Identity information includes a representative element (identification number or name) and other credential information. Privilege information describes allowable actions and behaviors in a system. Trust knowledge covers other supportive information for establishment, monitoring and enforcement of trust. Trust credentials are used to attest their owners' identifications. Representation of trust should provide ways to express these credentials from emerging biometric authentication technologies such as fingerprints, iris patterns, voice patterns, signatures, etc. These biometric authentication technologies have different ratings for social acceptance and system effectiveness [3]. Table 1 ranks some example

biometric authentication technologies and their ratings. With more and more authentication technologies being used in enterprise computing, we need representations of trust credentials to be flexible enough to accommodate theoretical levels of reliability as well as practical managerial manipulations for federation activities.

TABLE 1. COMPARISON OF AUTHENTICATION TECHNOLOGIES

Techniques in order of effectiveness (highest to lowest)	Techniques in order of social acceptance (highest to lowest)
Iris Scan Fingerprint Hand Geometry Voice Print Face Geometry	Face Geometry Voice Print Fingerprint Hand Geometry Iris Scan

Since trust management for federation activities deals with different trust factors across trust domains, such a system should provide flexibility to allow subjective adjustments to objective trust factors. For example, within one trust domain, different authentication technology representations should comply with the accepted or theoretical rankings of the reliabilities of the authentication technologies (e.g., in general, iris scans are more reliable than fingerprints because they exhibit more degrees of freedom, but actual reliability can only be determined by false-acceptance and false-rejection experiments on specific technologies). But for inter-domain federation, special purpose exceptions should be allowed. More concretely, if a hospital needs to share with pharmacies for patients' prescription information, any authentication technologies and their representations used within the pharmacies' domains may be only mapped to some authentication technology with a lower reliability (e.g., password) in the hospital domain. In other words, the reliability of the information in an external authentication token might be downgraded when imported if the importer has insufficient knowledge about the token or the technology or entity that produced it. This is a typical operational or managerial decision when handling information from an unfamiliar organization, and it is subjective.

As authentication technology has developed, biometrics has become popular with its promise of no

more calls to the IT helpdesk complaining of forgotten passwords or lost hardware tokens. Biometric authentication technologies are used to measure certain features a person has. They can compare a physical (fingerprint/voice) or behavioral (keystrokes/signature) trait with a stored value. Combine this with something a person knows such as a PIN or a password and it forms a strong two-factor authentication method. Recently researchers, hardware engineers and product developers have been looking at ways to bring these technologies into our daily lives in a form such that their speed, accuracy, reliability and user acceptability are all adequate for daily use. But as people's business and social relationships expand, management systems also need to be extended to accommodate new requirements for these authentication technologies for purposes of federation. This paper describes a flexible alignment mechanism to make different authentication information from different authentication technologies or methods efficiently and effectively fit into the needs of federation for cross-domain activities. Section 2 describes the design of this alignment mechanism. Section 3 illustrates the detailed implementation, system architecture, and a case study in a healthcare environment. Section 4 evaluates the alignment mechanism from theoretical and practical aspects. Section 5 concludes with some summary remarks.

2. AUTHENTICATION INFORMATION ALIGNMENT

2.1. *Performance Modeling of Authentication Technologies*

A password is a common form of secret authentication data that is used to control access to a resource (service, information, etc.). The password is kept secret from those not allowed access, and those wishing to gain access are verified based upon whether or not they know the password and are then granted or denied access accordingly. Used in many secure communication systems, encryption keys (symmetric key, public/private key) are also forms of secret authentication data distinguishing authentic users/identities. Both plain passwords and encryption keys can be treated as one-dimensional signals with unique texts or transformed texts to distinguish the authenticity of identities.

As for biometric authentication, one of the most fundamental questions one would like to ask about any practical biometric authentication system is: what is the inherent distinguishable information available in the input signal? Unfortunately, this question has only been answered in a very limited setting for most biometric modalities. The inherent signal capacity is of enormous complexity as it involves modeling both the composition of the population as well as the interaction between the behavioral and physiological attributes at different scales

of time and space. Nevertheless, a first-order approximation to the answers to these questions will have a significant bearing on the acceptance of (biometric-based) personal identification systems in our society as well as determining the upper bound on scalability of deployment of such systems. As mentioned earlier, regardless of whether we are using two-dimensional images or three-dimensional voice patterns, a system's acceptance is significantly impacted by its false-rejection rate and false-acceptance rate.

2.2. *Signal Quality and Enhancement*

For a particular biometric measurement to be effective, it should be universal: every individual in the target population should possess the biometric and every acquisition of the biometric from an individual should provide useful information for personal identity recognition. In practice, adverse signal acquisition conditions and inconsistent presentations of the signal often can result in unusable biometric signals (biometric samples). This is confounded by the problem that the underlying individual biometric signal can vary over time due to some natural human process (e.g., aging). Hence, the most common cause of poor matching accuracy is the collection of poor quality biometric samples. Therefore, it is important to quantify the quality of the signal for either seeking a better representation of the signal or for adjusting a poor signal to achieve better levels of reliability. In situations involving non-cooperative individuals, where it may not be feasible to acquire a good quality biometric signal, it is critical that either (a) the procured signal be suitably enhanced in order to permit accurate processing of the data or (b) the trust level associated with the sample be lowered to reduce the risk level inherent in the procured signal. Indeed, biometric signal enhancement is an important research problem that has to be pursued in a systematic manner, which is not within the scope of this paper. Secondly, flexible adjustment is an important alternative to allow information management systems and trust management systems to adapt to unanticipated behavior and unknown trustworthiness from federated partners.

2.3. *Alignment of Authentication Information*

2.3.1. *Requirements from Federation*

The first step toward trusting an entity is identification of the entity. Identity information can be verified by authentication systems, where the system authenticates a person's claimed identity from his/her previously enrolled identification data or credential. The reliability of identity information is significantly impacted by the reliability of the authentication system and deployed authentication technologies [2]. Tokens, such as smart cards, magnetic stripe cards, physical keys, and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be

forgotten, shared, or copied. Biometric authentication bases identification on an intrinsic part of a human being, but it still has practical usability issues with authentication technologies and false-acceptance rate and false-rejection rate choices.

Meanwhile, federation imposes new requirements on authentication information management. As used in many extant trust management systems, authentication information management or certain central authentication servers are responsible for identity verification and management. Federation requires that these servers take care of not only pre-enrolled authentication information but also identity information and authentication tokens from other trust domains. If the reliability of the identity information or authentication tokens is unknown, or if a local domain's policies or user's trust intentions have specified foreign information or tokens' trust levels, flexible adjustment needs to be provided to incorporate foreign information and tokens into local authentication information management without compromising its consistency. This adjustment or manipulation should not change the original management framework.

Alignment of different authentication information provides a way to adjust or manipulate trust levels without interfering with extant system design and operations. This alignment is to incorporate dynamic trust levels into authentication information management as well as to adjust authentication technologies' reliability according to users' intentions or application requirements for further verification and authorization. The core idea is to align the reliabilities of authentication technologies and their resultant identity information's reliabilities or trust levels to users' intentions or application requirements. For example, if a user from a foreign trust domain seeks to access a medical record with an authentication token from that foreign domain and its authentication technology is unknown, the local authentication management system may enforce a policy to set the trust level of the foreign identity equal to that derived from password verification within the local domain.

2.3.2. Application of Wavelet Transformation

To minimize the impact of adjustment and manipulation on system design and operation, we propose a modular transformation (or an embedded transformation) to serve this purpose. We introduce wavelet transformation into the authentication information management to offer flexible manipulation. Wavelet transformation [4] is a relatively new approach used in the analysis of sounds and images, as well as in many other applications. For images the wavelet transformation allows one to first describe the coarse features with a broad brush, and then later fill in details. This is similar to zooming in with a camera: first you can see a scene consisting of shrubs in a garden; then you concentrate on one shrub and see that it

bears berries; then, by zooming in on one branch, you find that this is a raspberry bush. Because wavelet transformation allows you to do a similar thing in more mathematical terms, it is called a mathematical microscope. A wavelet-transformed password is a binary string in a transformed format with a required length for a certain trust level. It is like an encrypted version with its unique coarse pattern. A wavelet-transformed biometric template is a binary string containing resized patterns with a required length for a certain trust level. For image- or voice-based biometric authentication templates, it is more natural to use wavelet transformations to reduce or magnify the scales of the unique patterns in them. Below is an application of wavelet transformation on a fingerprint pattern. The wavelet-transformed fingerprint contains only one forty-eighth of the distinguishable information of the original fingerprint (one sixteenth the size and one third the bit-rate of each color channel), and the amount of information can be reduced more according to length and trust level requirements.

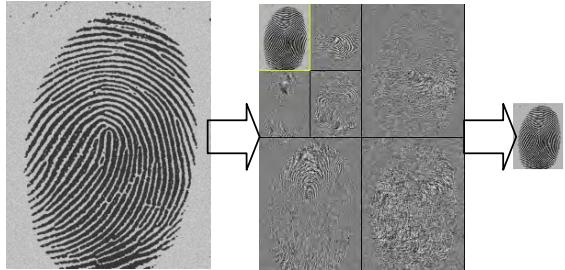


Fig. 1. Example application of wavelet transformation on fingerprint patterns

No matter what protocol, technology or architecture is used, the procedure of authentication can be modeled as signal matching. The original signal of a user (password or biometric template) is stored securely after enrollment. Then the user provides a signal to match the stored signal in order to authenticate its identity. Meanwhile, according to the requirements imposed by federated management of trust, flexible manipulation of the reliabilities of different authentication information is needed when trust levels are associated with those reliabilities.

In our design, the wavelet transformation is incorporated as an embedded module to provide flexible manipulation of authentication information. Thus, existing applications do not need to change their authentication architectures or procedures. They only need to add a "filter" to process the authentication information one more time at run time.

2.3.3. Alignment Framework

As mentioned before, high levels of trust require highly reliable identity information. As everyone has seen in movies, access to a high security place or document

requires reliable identity information. High reliability results from high complexity within the authentication technology. But federation introduces new concerns. When you authenticate yourself within one trust domain using a highly reliable authentication technology, you will get a high trust level. According to the negotiated contract between your own trust domain and a federated trust domain, you may not have the same level of trust in the other domain. For example, even if you use a fingerprint scanner to authenticate yourself in your own trust domain, the federated domain may grant your security token a lower level of trust. For the purpose of single sign-on, a federated trust domain does not need to enroll you again. It can authenticate you by matching your fingerprint with the template enrolled in your own domain. Since the federated domain only requires a template with a lower level of reliability, we provide an alignment operation to reduce the reliability by providing a wavelet-transformed template with equivalent lower-level reliability (the same as a password). Figure 2 illustrates the procedure.

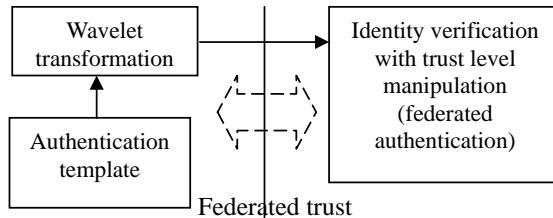


Fig. 2. Alignment using wavelet transformation

Thus, federations between trust domains can accommodate dynamic trust relationships by dynamically aligning the reliability of identity information using a wavelet transformation. The dynamic alignment can be achieved through assigning a proper wavelet transformation dynamically in federation activities such as verification and authorization, which need authentication templates.

3. IMPLEMENTATION

We implement authentication information alignment in a federated management system of cyber trust for a healthcare environment. Figure 3 illustrates interactions between a number of trust domains – billing, insurance, pharmacy and hospital (dash line rectangles) involving several modules with grey rectangles to handle federated authentication and verification. Alignment operations are required in these federated activities if trust levels need to be adjusted according to trust intentions (policies).

For example, if a pharmacist in the pharmacy domain needs to access a patient's medical record, the hospital domain requires the pharmacist to provide some authentication credential with a trust level equivalent to password authentication. But the pharmacist only has a

fingerprint authentication credential in his own security domain. So the authentication service in the pharmacy domain will apply a wavelet transformation to dynamically align the pharmacist's authentication template to accommodate the requirement from the hospital security domain. Figure 4 depicts the detailed architecture of alignment.

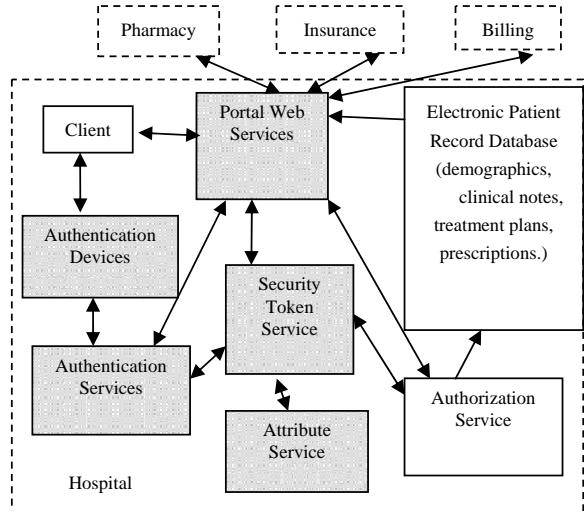


Fig. 3. Federated management system of cyber trust for a healthcare environment

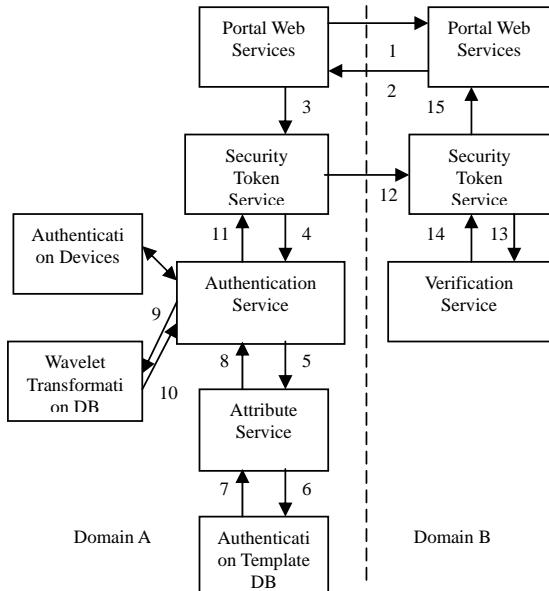


Fig. 4. Detailed alignment architecture for federated authentication

The steps described below correspond to the arrow numbers in figure 4.

- (1) An access request from an entity in domain A is sent to the portal service in domain B.
- (2) The portal service in domain B challenges with a requirement of certain authentication credentials including a password equivalent authentication credential.
- (3) The portal service forwards the challenge to the security token service in domain A, which handles all meta information related to security, privacy and trust.
- (4) When the security token service identifies the challenge about its authentication credential, it forwards the challenge to an authentication service.
- (5) Since we treat authentication templates as attributes, the challenge is further forwarded to an attribute service.
- (6) The attribute service tries to retrieve the authentication template from an authentication template database.
- (7) If the authentication template is found, the template will be returned to the attribute service.
- (8) The template will be further returned to the authentication service. (If no required authentication template is found, the authentication service will ask the entity to do a first-time enrollment of his/her authentication template.)
- (9) Here we assume the template is found, but it is not exactly matched with the requirement. For example, domain B requires a password-equivalent authentication credential. But the entity in domain A has only a fingerprint template. The authentication service will find a proper wavelet transformation from a wavelet transformation database.
- (10) The proper wavelet transformation is returned to the authentication service and applied to the found authentication template. The authentication template is transformed to the required trust level, and the required authentication credential is formed.
- (11) The authentication credential is returned to the security token service.
- (12) Then the authentication credential is embedded into a security token and sent to domain B's security token service.
- (13) The security token service in domain B extracts the authentication credential and forwards it to a verification service in domain B.
- (14) After verification, the result is sent to security token service in domain B.
- (15) If it is a positive result, the security token service will allow the portal web service to grant the access request in step one; otherwise, the request will be denied.

After describing the detailed architecture of alignment, we illustrate its usage with some practical examples. Here are several examples of authentication templates used in a healthcare environment. The most frequently used authentication mechanisms are password and fingerprint authentication. The templates stored in authentication

template database are created in the enrollment process. A password template is a string of plain text; a fingerprint template is a string of binary data representing the image obtained from a fingerprint scanner.

The templates used for verification with a certain trust level requirement after alignment (using wavelet transformation to adjust the trust level of the fingerprint template to make it equivalent to the password template) are illustrated below. (In this example, the password template is not necessarily aligned.)

- Password template before alignment: “TestPassword”
- Fingerprint template before alignment (from the fingerprint scanner on an HP iPAQ H5455):

```
"a[Qf@ Íep a r °ÉcùŠ>°ÉpôNµÖ‡\ECµV¶$... .
FÍ+,,hµ ZPV úÓÁ=UQ+OLÓ ...x T,ZdÉ& jæx
D.' . #@®' ,@'Ü'É CäÔ úo<%'§ÁyÖHþTþ y,®{
½1yw >fúfÝQÖVD}qxº%4+ &E TM>%âß\`Fµ ZK
TM<@kµ G:*<iöY ³eØ®(C©D"r= Jšæ,T¶|çë= ½eV
Øý/a ¾...ý#G¾§ý VÍ†ókba:...r?o4J Q i "PøøF]
ÖE÷Æ"om (E2èxJG³=cÃæ» ü ùO°É ÄfCöJ ß‡
>íÚ f< ÍO<>YòL2(J tœé'Gž×P>S 3Cír€Ø-ÍNÆrPÍ7
> ý"‰ °×©-T½Jžâ'ö1×}'ëÆ 8 ¶ ÜyžÝ
20 " öùDåTM.T .ëDç Šb±,±ùÐvjk|Li.*Nâ<á5. \
¶t8.:=\$ÑqìÖ"ZýLJŽ Áí¶U YO!4/qNQNbÓFA {n!¡(ü
Z'V,,d+pdOMµ*! î ÷T:åšO"v6'çñŒäÈ-ö>å ûlNö6p"8
ØNKÿÄT'Ý éå+ÌÉQøþ ^fÔ|Rµ"O ' X TùYa§býu~t
e¶ØÅ¶Øoi@$ hž³ öcx;øs-Dù iÈ 1æ X"
```

- Password template after alignment: “-#Ø:å1;:r”
 - Fingerprint template after alignment: “[jg¹ wzâ_XÛ9”
- Meanwhile, to promote modularity and exchangeability in our implementation, we choose four primitive functions from BioAPI [5]: Capture(), Process(), VerifyMatch(), and CreateTemplate(), to construct the basic interfaces (APIs) for authentication data exchange in the workflow of alignment.

4. DISCUSSION

For federation, management of trust needs to handle trust level adjustment within the authentication operations. We achieve trust level manipulation for this purpose via an alignment mechanism via a plug-in wavelet transformation module. This alignment mechanism also provides formal representations of different authentication technologies under the BioAPI interface. The proposed alignment mechanism does not change the structure of authentication-related operations, such as enrollment and verification. It uses APIs described in the BioAPI standard to accommodate various authentication device vendors. It can also be easily embedded into four authentication service models described in BioAPI.

Since wavelet transformation keeps the most distinguishable feature information in biometrics, fundamentally, this alignment mechanism does not

change the basic assumptions on biometrics: (1) for each individual with a biometric b with feature information $fb(t)$ at time t , and for any times $t1, t2$, it holds that $d(fb(t1), fb(t2)) < \delta$; (2) for any two individuals with biometrics $b1, b2$, with feature information $fb1(t), fb2(t)$ at time t , respectively, and for any times $t1, t2$, it holds that $d(fb(t1), fb(t2)) > \gamma$ ($\delta < \gamma$, d is a distance function). Since this alignment mechanism uses an embedded style, it only plugs in wavelet transformations for the workflows of the authentication processes. The only difference is extra time consumed in wavelet transformations. We compared the performance of the original authentication operation (verification only) without steps 9 and 10 and the alignment-enabled authentication operation described in figure 4. We randomly choose authentication operations conducted by patients and doctors using password and fingerprint authentications. We measured the time used for authentication operations (see Figure 5). The blue (black) series is authentication with wavelet-based alignment; the red (grey) series is without alignment. Although the difference of the time used for a single authentication operation varies from 1ms to 158ms, the mean value of the authentication time with wavelet-based alignment is 437ms and the mean value of the authentication time without alignment is 432ms (a 1.16% difference). We found the degradation of performance is almost unnoticeable.

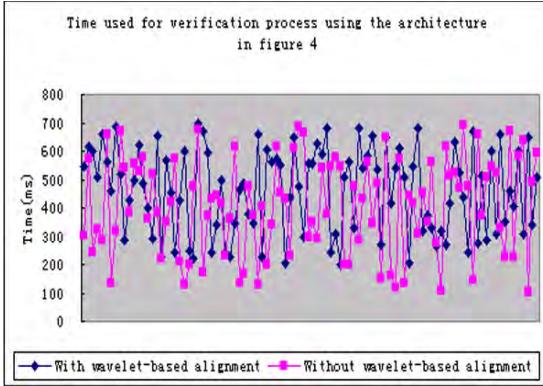


Fig. 5. Comparison of authentication operations' performance (with and without alignment)

Since users may impose additional overhead to the authentication operation, we also ran a script-driven single round verification with and without alignment, illustrated in figure 6. The performance overhead (in terms of time) of wavelet-based alignment is only 2.20% for passwords and 2.46% for fingerprints.

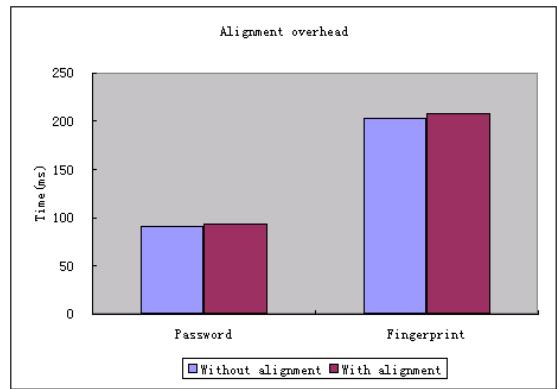


Fig. 6. Overhead of plug-in alignment

5. CONCLUSION

To accommodate the requirements of authentication information's reliability level or trust level manipulation for enforcement of trust in federation activities, we propose an alignment mechanism using wavelet transformation to provide plug-in authentication information manipulation for authentication, verification, and authentication operations. It provides flexible trust level manipulation via a wavelet transformation for user-defined adjustment requirements for different authentication technologies and authentication models from different trust domains. Our implementation incorporates BioAPI to provide the most capability to adapt to different authentication workflow models and different authentication technologies. Our performance measurements show that the resulting time overhead is negligible.

REFERENCES

- [1] Z. Wu, A.C. Weaver, "Requirements of federated trust management for service-oriented architectures," *International Journal of Information Security*, Vol. 6(5), 2007, pp. 287 – 296.
- [2] P. Beynon-Davies, "Personal identity management and electronic government," *Journal of Enterprise Information Management*, Vol. 20(3), 2007, pp. 244 – 270.
- [3] J. Wayman, A. Jain, D. Maltoni, and D. Maio, *Biometric Systems: Technology, Design and Performance Evaluation*, Springer, 2005.
- [4] P. S. Addison, *The Illustrated Wavelet Transform Handbook*, Institute of Physics Publishing, 2002.
- [5] The BioAPI Consortium, "the BioAPI 2.0 standard," ISO/IEC 19784, 2005.

Formally Specifying Linux Protection

Osama A. Rayis

Sudan University of Science & Technology

rayis@sustech.edu

Abstract

Authorization and protection deal with the problem of the control of access to resources. A key aspect of modern computing systems is resource sharing, so a need arose to govern access to these resources only to authorized users. In multi-user operating systems (such as Linux) authorization is of great interest. Computer security and authorization as a subset is characterized by the fact that a security fault or hole can be very costly. It is of great interest therefore to formalize and reason about security. Z notation is a powerful well-known formal notation based on set theory and predicate calculus which provides both abstraction and formalism. This work reports a formal expression in the Z notation for the basic protection (authorization) system of the Linux operating system.

Key words:

Authorization, Linux Security, Access Control, Protection, Z notation, Formal Modeling, Reasoning.

I- INTRODUCTION

Modern operating systems like Linux came with many capabilities like multiple user support, remote access, networking, resource sharing and many other useful functions. Despite of its usefulness such facilities give rise to the risks of unauthorized access, thus processes and resources in operating systems must be protected (Johnson & Troan 2005), (Silberschatz *et al* 2002). Protection is an important quality for Linux to have and this quality should be rendered proven formally so that the operating system can be trusted.

Proving system conformance by formal means (if feasible at all) is expensive and rarely cost-effective; one area in which it is cost-effective is computer security (Mclean 1990).

Authorization can be defined as the problem governing subject's accesses to objects according to some rights theses subjects have permission to perform on the objects, where subjects in this context can be any computing element. Lampson (1971) gave a model for authorization known now as access matrix model which was further refined and improved in (Graham & Denning 1972) and in (Harrison, *et al* 1976). The model expressed here follows Harrison *et al* (1976) model. The security kernel mechanism introduced by Schell is based on defining a small subset of the system to be responsible for the system's security and this subset would monitor all accesses, would be correct and it would be isolated and tamper-proof. The lattice security model which extends the access matrix model with classification, clearances and rules is found in the Bell and LaPPadula (1973) famous article. Denning (1976) introduced the information flow model which is based on the lattice security model but requires that the flow of information is subject to the flow of relation among security classes.

Again in the 90th due to the large implementation of networking and distribution, authorization had gained lot of interest in many specialized area. In 1990 Glenn *et al* extended the distributed model given by Akyildiz *et al* (1989) and reported a formal model in centralized, parallel and

distributed systems. Glenn *et al* reduced the problem of proving security for concurrent model to proving security for sequential model. Protection in embedded systems was studied in (Rayis 1996). Glasgow *et al* (1992) presented a logic for reasoning about security which is based on a modal logic framework.

Time, roles, constraints, events were motivation to extend classical models to new application areas as in distributed databases and workflow management systems by Sandhu *et al* (1994, 1996), Atluri and Huang (1996), Elisa Bertino *et al* (1996a, 1996b, 1997a and 1997b), (Rayis 1997), (Tomur & Erten, 2006), (Kwon & Moon, 2007) and (Peleg *et al.* 2008). Thorough surveys on the subject of authorization can be found in (Denning 1982), (Sandhu *et al.* 1994), (Sandhu *et al.* 1996), (Goscinski 1991), (Pfleeger 1989), (Boyd 1993), (Leiss 1982), (Landwehr 1981) (Stallings, 2007) and (Stallings & Brown , 2007). Computer Security is characterized by the fact that a single mistake can cost billions. Authorization deals with threats and risks and involves requirements that are considered of supreme importance, thus high level of assurance is needed, and testing alone is insufficient to establish the required level of confidence. Z notation developed at Oxford is a powerful tool for formal expression and reasoning. It is intended to be used here because we think that the development of security systems should follow a process models as information systems development and use similar tools and methodologies.

The Z language is a powerful formal tool for specification and it is proposed to be used to specify the above mentioned problem formally. Snekkenes in [29] had expresses some authentication procedures of X.509 (which is a joint ISO and CCITT specifications) in Z. There he noted the benefits of Z to make compact specifications through the reuse of schemas. Through the

use of Z he reported also some weaknesses of the X.509. Boyd (1993) had also specified the authentication in Z, he developed some secure communication architectures using Z. Boswell (1995) presented a formal development of security policy model in Z for the NATO Air Command Control System. He described Mandatory and discretionary access control rules and integrity control. He concluded the capacity of Z to be used in such field, the modularity provided by it and the help it provides for informal validation. Further information about Z notation is found in many references one of them is (Potter *et al.* 1996).

The system to be modeled is a standard Linux protection system. A simplified description of a Linux protection system consists of a finite number of objects of different types. The n types are processes and files and they are related by rights which some object (process) may have over some other object (file). The number of objects is not fixed but is finite. Rights may be “read”, “write”, “execute”, “delete”, “update” and “own”. A Z specification of the system will first define given sets, definitions and initial conditions. The second thing to be specified is the system state or the configuration. Third is the modeling of primitive operations and last is modeling commands.

II- THE PROTECTION SYSTEM

The model adapted to Linux core protection system presented here was developed using features described in (Johnson & Troan 2005), (Silberschatz *et al* 2002) (Torvalds, 2008) and the model originally developed by Harrison, et al (1976) was used as a core model. Yet new extensions to model extra security features in Linux can be augmented. An example is the support of role based security authorization, where the model presented in (Sandhu *et al.* 1996) can be of much help.

Given X_1, \dots, X_k are formal parameters for objects, r_1, \dots, r_m are generic rights, R is a finite set of generic rights and C is a finite set of commands. The authorization system then consists of R and C. Formal parameters are identifiers used as place holders for concrete values. Later in the formalism formal parameters will be replaced with the set of objects {processes X_{si} , files X_{oj} }, $k=i+j$.

Commands c in C are of the following form:

command c(X_1, \dots, X_k):

if

r_1 is in (X_{s1}, \dots, X_{o1}) **and**

r_2 is in (X_{s2}, \dots, X_{o2}) **and**

...

r_m is in (X_{sm}, \dots, X_{om})

then

op_1

...

op_n

end

Where each op_i is one of the following six primitive operations:

enter r into (X_s, X_o),

delete r from (X_s, X_o),

create subject X_s ,

destroy subject X_s ,

create object X_o or

destroy object X_o .

Where

$X_s = \{x_{s0}, x_{s1}, \dots, x_{si}\}$ is the set of processes,

$X_o = \{x_{o0}, x_{o1}, \dots, x_{oj}\}$ is the set of files and $1 \leq s, s_1, \dots, s_i, o, o_1, \dots, o_j \leq k$

2.2- A Configuration

Given such a system (R,C) an instantaneous description of it will be a configuration which is triple (S,O,P) where O is the set of objects, S is a subset of it denoting the set of current processes and P is the access matrix with a row for every s in S and a column for every o in O. The entry $p[s,o]$ defines the set of rights in R which the process s has to the object o.

Then the system comprises a collection of processes and files. Each file is owned by a process. At every time processes are related to files by sets of generic rights. At the initial condition there is only one process named Super and no file exists.

2.3- Commands

Like what had been described in 2 above commands in the context commands can be thought of as formal procedures affecting the access matrix using primitive operations, the following commands are needed to be modeled:

2.3.1- ADD process

At any time the process Super may add a new process (or new user).

2.3.2- MAKE file

At any time any process may make a new file. The process making the file owns it a.

2.3.3- CONFER right

The owner of a file may confer any right other than own to a friendly process. Friendliness is not to be specified.

2.3.4- REMOVE right

The owner of a file may revoke any right from an X-friendly process to which he had previously conferred this right. X-friendliness is not to be specified.

III- A Z SPECIFICATION OF THE SYSTEM

A Z specification of the system will first define given sets, definitions and initial conditions. The second thing to be specified is the system state or the configuration. Third is the modeling of primitive operations and last is modeling commands.

3.1- Given Sets and Definitions

Three sets are assumed:

{objects, rights, message}, which are the sets of all possible objects (which is (processes U files)) generic rights as described in section 1 and message ={error, OK}. Further it will be derived from the basic given sets the sets of users and files.

3.2- Initial Conditions

Initial conditions are enforced with the following schemas Fig. 1 and Fig. 2.

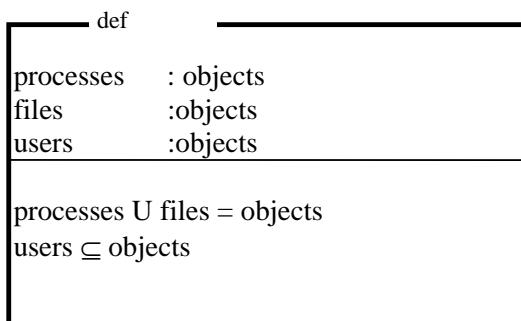


Fig. 1 Given Sets and Definitions

Schema of Fig.1.1 state, the fact that both processes and files are objects, which is then used in the schema of fig1.2 which is the one to enforce initial conditions. The initial conditions says that at the beginning the set current processes (cprocesses) contains only the super user and no file existed at that moment.

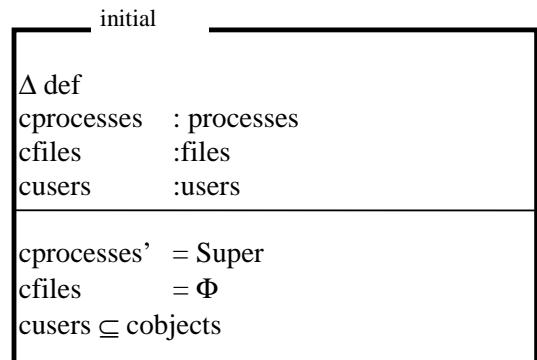


Fig. 2 Initial State

3.3- System State

System state is the configuration defined earlier. System state is represented as shown in Fig.3. The notion of access matrix is modeled as a two-dimensional array, and relating the array valid sets of indexes to entries of the access matrix, which are the set of valid rights relating the specific process CP to the specific object CO.

$$((CP, CO) \leftrightarrow P(CP, CO)).$$

System state is enforced with the following schema in Fig. 3

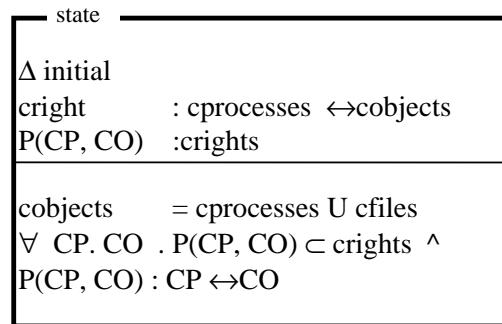


Fig. 3 System State

3.4- Primitive Operations

Primitive operations mentioned earlier in section 2 represent the primitive alteration to the system state by adding or removing rights (to the set of rights a subject can perform on objects), processes, or files. Primitive operations are enforced with the following schemas:

3.4.1 enter r?

This operation specifies the system state after adding a right to the set of rights a process have over another object, where $r \in \{R - \text{own}\}$ we write it with r and is shown in Fig. 4

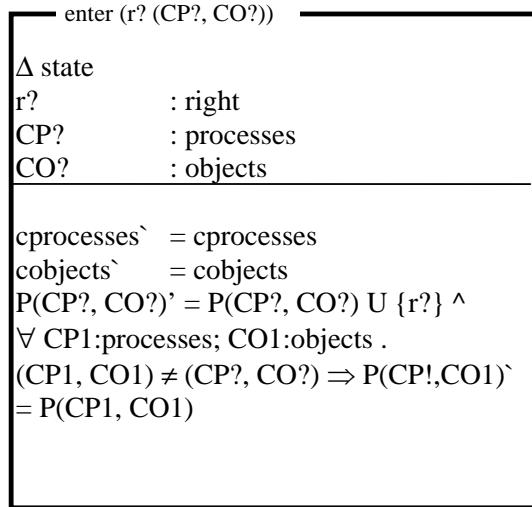


Fig. 4 Primitive Operation **enter r?**

3.4.2 delete r?

This is the opposite operation to enter $r?$ (described above). The Schema for delete $r?$ is shown in Fig. 5.

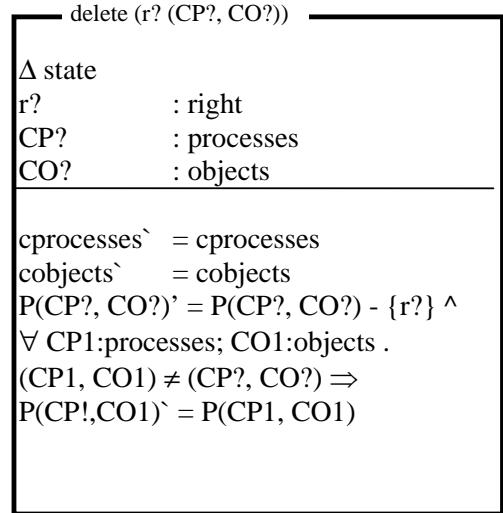


Fig. 5 Primitive Operation **delete r?**

3.5.3- create CP

Creates a new process and is shown in Fig. 6 (the same schema can be for create new user with the addition of $\text{cusers}' = \text{cusers} \cup \{CP?\}$).

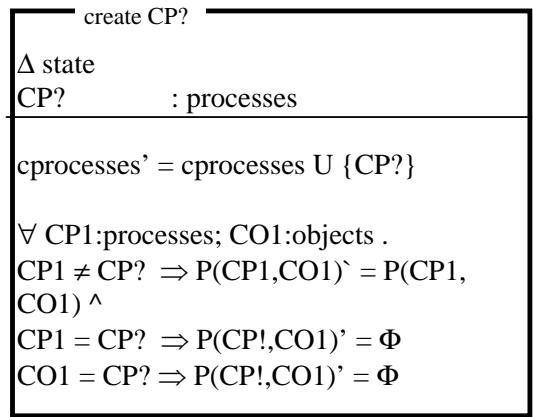
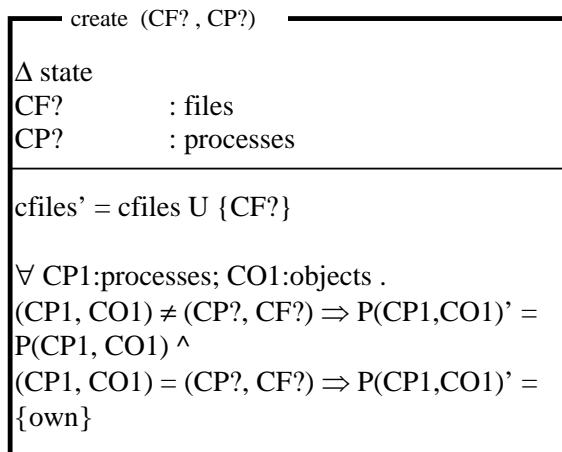


Fig. 6 Primitive Operation **create CP?**

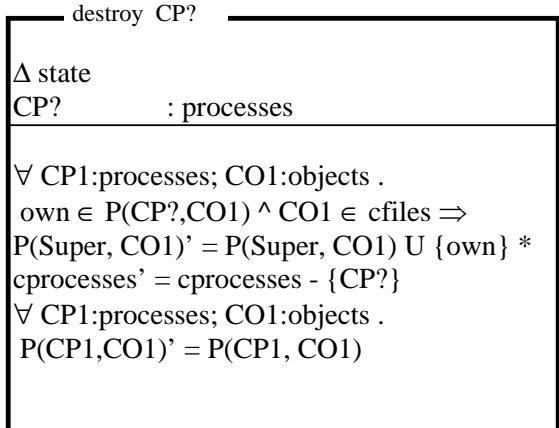
3.5.4- create (CF?, CP?)

Creates a new file CF owned by a process CP and is shown in Fig. 7

Fig. 7 Primitive Operation **create (CF?, CP?)**

3.5.5- destroy CP

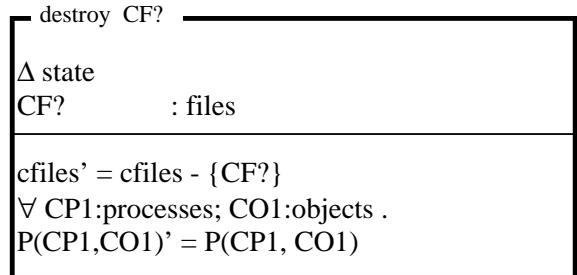
Destroys a current process and is shown in Fig 8

Fig. 8 Primitive Operation **destroy CP?**

* This was not specified in the original specification presented in (Harrison, *et al* 1976).

3.5.6- destroy CF

Destroys a current file and is shown in Fig. 9

Fig. 9 Primitive Operation **destroy CF?**

3.6- Commands

Commands are in the higher level abstraction of the system and are enforced with the following schemas:

3.6.1 Mechanisms and State Schema

Shown in Fig. 10

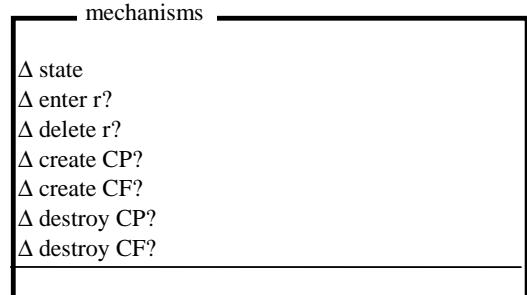
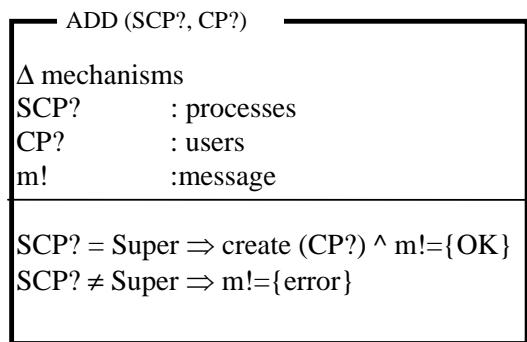


Fig. 10 Mechanisms and State

3.6.2 ADD CP?

Corresponds to 2.3.1 and is shown in Fig. 11

Fig. 11 Command **ADD CP?**

3.6.2 MAKE CF?

Corresponds to 2.3.2 and is shown in Fig 12

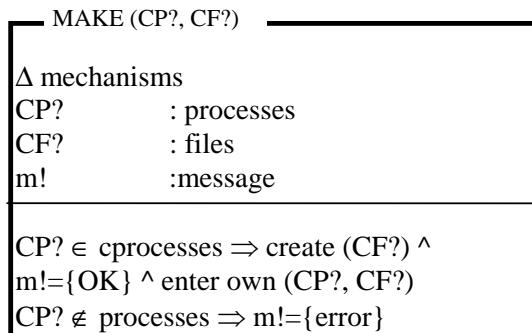


Fig. 12 Command **MAKE (CP? , CF?)**

3.6.3 CONFER

Corresponds to 2.3.3 and is shown in Fig. 13

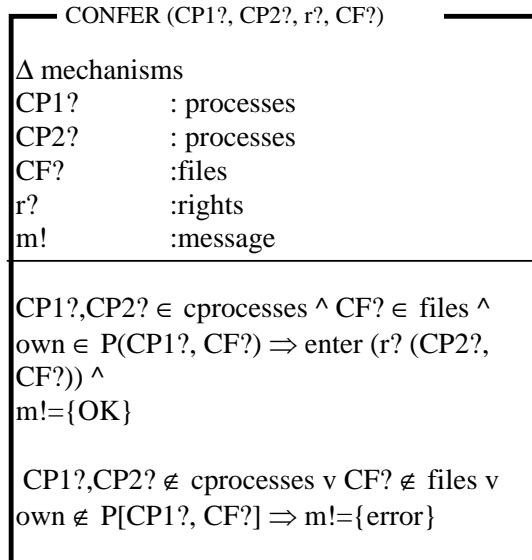


Fig.13Command **CONFER (CP1?, CP2?, r?, CF?)**

3.6.4 REMOVE

Corresponds to 2.3.4 and is shown in Fig. 14

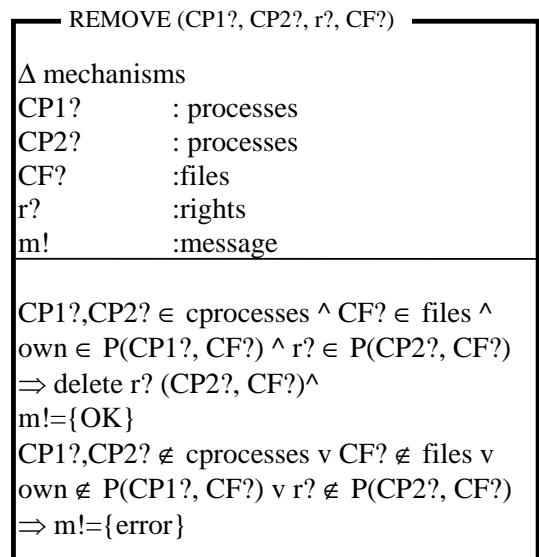


Fig.14Command **REMOVE(CP1?, CP2?, r?, CF?)**

IV-CONCLUSIONS

In this paper a *z* representation of the protection in Linux operating systems is presented. The model presented here is the access matrix model, which is one of the classical authorization models. This work represents the core of the Linux protection system. Future work to augment extended authorization mechanisms to the model is required; namely the role-based access control feature. Also other security features of Linux like authentication mechanisms can be represented and integrated. The use of *Z* gave insight in the subject matter of the problem and helped in the validation of the specifications where some ambiguities were discovered in the original specifications (e.g. it was not specified what to do with objects owned by a destroyed process). The work reported here can be extended in the direction of writing other specialized models (e.g. For Databases or Workflow M. S.) in *Z* and reason about security in them,

or in the direction of writing other formal models of authorization in Z.

REFERENCES

- Akyildiz, I. And Benson G., 1989, "Security Models of Distributed Systems". In Proceedings of the 4th International Symposium on Computer and Information Sciences, A. Dogacand E. Gelenbe, Eds.Turkey.
- Bell and LaPadula, 1973, "Secure Computer Systems : Mathematical Foundations". ESD-TR-278, 1 , ESD/AFSC, Hanscom AFB, Bedford, Ma.
- Bertino Elisa et al, 1996, "A Temporal Access Control Mechanism for Database Systems", IEEE Transactions on Knowledge and Data Engineering Vol. 8, No. 1.
- Bertino Elisa et al, 1996, "Supporting Periodic Authorization and Temporal Reasoning in Database Access Control," Proceeding of the 22nd VLDB conference Mumbai, India.
- Bertino Elisa, P. Sammarati and S. Jajodia, 1997, "An Extended Authorization Model for Relational Databases." IEEE Transactions on Knowledge and Data Engineering.
- Bertino Elisa et al, 1997, "A Flexible model for the Specification and Enforcement of Authorizations in Workflow Management Systems" Technical Report, University of Milano.
- Boswell A., 1995, "Specification and Validation of a Security Policy Model," in IEEE Transactions on Software Engineering, Vol. 21, No.2
- Benson G., I. Akyildiz and W. Applebe, 1990, "A Formal Protection Model of Security in Centralized, Parallel and Distributed Systems." ACM Transaction on Computer Systems.
- Boyd Colin, 1993, "Security Architectures Using Formal Methods," IEEE Journal On Selected Areas In Communications.
- Charles P. Pfleeger, 1989, "Security In Computing," Prentice Hall.
- Denning D.E., 1976, "A Lattice Model of Secure Information Flow". Communications of the ACM.
- Denning Dorothy, 1982, "Cryptography and Data Security," Addison-Wesley.
- Glasgow J., G.MacEwen and P. Panangaden, 1992, "A Logic for Reasoning About Security," ACM Transaction on Computer Systems.
- Goscinski A. G., 1991 "Distributed Operating Systems The Logical Design," Adison-Wesly.
- Graham and Denning, 1972, "Protection Principles and practices." Proceedings of the AFIPS Spring Joint Computer Conference.
- Harrison, Ruzzo and Ullman, 1976, "Protection in operating system," Communications of the ACM.
- Johnson Michael & Troan Erik, 2005, "Linux Application Development", 2nd edition, Pearson Education.
- Kwon J., Chang-Joo Moon, 2007, "Visual Modeling and Formal Specification of Constraints of RBAC Using Semantic Web Technology," Knowledge-Based System, Volume 20, Issue 4.
- Lampson B. W., 1971, "Protection". Fifth Princeton Conference on Information and Systems Sciences.
- Landwehr C.E., 1981, "Formal Models for Computer Security." ACM Computing Surveys 13(3).
- Leiss Ernst, 1982, "Principles of Data Security," Plenum Press.
- Mclean John, 1990, "The Specification And Modeling Of Computer Security." IEEE Computer, Volume 23, Issue 1.
- Peleg M., Dizza Beimel, Dov Dori, Yaron Denekamp, 2008, "Situation -Based Access Control: Privacy Management Via Modeling of Patient Data Access Scenarios" Journal of Biomedical Informatics.

- Potter B., Sinclair J. And Till D. 1996 “An Introduction to Formal Specification and Z,” 2nd edition, Prentice Hall.
- Rayis Osama, 1996, “Software Protection through dedicated Hardware. Ms Thesis Middle East Technical University.
- Rayis Osama, 1997, “An Adaptable Workflow Environment, Authorization Model Definition,” Technical Report SRDC - Middle East Technical University.
- Sandhu Ravi and Pierangela Samarati, 1994, “Access Control: Principles and Practice”. IEEE Communications, 32(9):40-48.
- Sandhu Ravi, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman, 1996 “Role-Based Access Control Models,” IEEE Computer, 29(2):38-47.
- Snekkenes E., 1990, “Authentication in Open Systems”, in Protocol Spec. Testing & Ver., Elsevier Science Publishers.
- Stallings B., 2007 “Role-Based Access Control in Computer Security” Prentice Hall.
- Stallings W., Brown L., 2007, “Computer Security: Principles and Practice,” Prentice Hall.
- Tomur E., Erten Y., 2006 “Application Of Temporal and Spatial Role Based Access Control In 802.11 Wireless Networks,” Computers & Security, Vol. 25, Issue 6.
- Vijayalakshmi Atluri and Wei-Kuang Huang, 1996, “An Authorization Model for Workflows”, Computer Security - ESORICS 96, Rome.
- Wordsworth J.B., 1992, “Software Development with Z”, Addison-Wesley.
- Torvalds L., 2008, “The Linux Kernel,” <http://www.kernel.org/>

Path Failure Effects on Video Quality in Multihomed Environments

Karena Stannett, Adomas Sutkevicius, Enda Fallon, Yuansong Qiao, Paul Jacob, Austin Hanley

Software Research Centre, Athlone Institute of Technology, Ireland

Email :{kstannett, asutkevicius, pjacob, efallon, ysqiao, ahanley}@ait.ie

Abstract—The networking capabilities of mobile devices have increased dramatically in recent years. A wide range of mobile devices now provide the capability to simultaneously connect to multiple underlying networks. The increasingly ubiquitous deployment of WLAN technologies, particularly in urban and campus scenarios, has allowed mobile developers to enhance their application functionality based on the characteristics of wireless rather than mobile networks. This increase in capability comes at a cost however as the provision of seamless mobility for wireless networks remains an open research area. Multi-homing technologies which exploit multiple underlying networks in an application transparent manner, have the potential to overcome many of the issues relating to wireless network mobility. There are a number of mechanisms through which a multi-homed session can be achieved. This paper compares two approaches to multi-homing support; transport layer multi-homing utilising the Stream Control Transmission Protocol (SCTP) and application layer multi-homing utilising the Session Initiation Protocol (SIP). Multimedia streaming experimental evaluations are undertaken which compare the performance of SCTP against a number of increasingly aggressive SIP based handover strategies in response to a path failure. Results indicate that the transport layer SCTP based strategy has significantly better performance within the handover period than the application layer SIP based strategies achieving up to 22.5% better performance than the SIP based strategies.

I. INTRODUCTION

Modern network technologies allow hosts to connect to multiple, diverse underlying physical networks concurrently. For example most laptops can now be equipped with both integrated and USB wireless local area network capabilities and recent growth in the availability of heterogeneous wireless networks has lead to overlapping coverage zones. A host with multiple IP addresses is known as a multi-homed node.

These developments provide an opportunity for developers to integrate multi-homing support into applications as the path redundancy offered with multi-homing can improve the quality of an end user's experience. Wireless networks are commonly subject to significant fluctuations and performance degradation can often result in disconnection from a network. Where multi-homing is supported a path handover to an alternate path can be performed and transmission continued rather than irretrievably terminated.

This paper outlines two different methods of achieving a multi-homing supportive multimedia application. Both methods employ prototype applications. One application employs the multi-homed transport layer Stream Control Transmission Protocol (SCTP) whilst the other is a Session Initiation Protocol (SIP) user agent that implements multi-

homing at the application layer. In particular this paper compares the quality of the data received by the user in a multi-homed environment under permanent network failure and path handover conditions.

Section 2 of this paper gives an overview of related work in this. Section 3 outlines the relevant technologies and prototype applications. Test conditions are explained in section 4 with section 5 detailing the results of the tests. Conclusions drawn from the results are given in section 6.

II. RELATED WORK

Recent research on use of SCTP for the transmission of multimedia content includes [1] which investigates the impact of path handover subsequent to a permanent network failure on the quality of a video file using SCTP. In [2] a mechanism for transmission of MPEG-4 video traffic over mobile networks is described with a comparison of the performance of SCTP, TCP and User Datagram Protocol (UDP) transport protocols. Enhancements to SCTP loss event detection are outlined in [3]. These aim to improve SCTP performance over wireless networks where mobility and higher bit rate errors are experienced. Throughput and robustness advantages of using SCTP within multi-access wireless scenarios are explored in [4].

Triangulation issues of using Mobile IP to support mobility in IP networks are discussed in [5] which proposes the use of SIP at the application layer to improve efficiency of support to real time communications. The authors of [6] propose a SIP mobility agent to facilitate network handover when TCP or UDP connections are employed. Possible handover scenarios, including multi-homing, are outlined in [7] with discussion about the arising issues for connection continuity of a SIP multimedia session. Work in progress under IETF documentation includes [8] which opens discussion on strategies to support multiple path routing in SIP based architectures.

III. TECHNOLOGY

A. SCTP

SCTP [9] is a connection-oriented, reliable transport protocol with message boundary preservation and TCP-friendly congestion control. The inbuilt multi-homing feature of SCTP enables multi-homed SCTP aware endpoints to communicate via multiple IP addresses within a single connection which is known as an association. During association initiation one path between the endpoints is

selected as the primary path and transmission occurs across this path. During the lifetime of the association all other paths are monitored for reachability and in the event of a primary path failure, a new primary path is selected from those available.

Path failure is detected when the number of consecutive retransmission attempts on a path exceeds the SCTP control parameter Path.Max.Retrans. Transmission timeout detection occurs when an acknowledgement for a transmitted SCTP chunk fails to arrive at the sender before the protocol parameter Retransmission Time-out (RTO) expires. RTO calculations are maintained in respect of each path in the association; being updated in respect of round trip time and doubled in the event of a transmission timeout. Therefore the speed of path failure detection and initiation of path handover is significantly dependent on the value of RTO.

Other protocol parameters that are instrumental in the handover process include; RTO.Initial – initial RTO value, RTO.Min – minimum RTO value allowed, RTO.Max – maximum RTO value allowed and Ack.Delay – time receiver can delay before sending acknowledgement. The IETF protocol specification [9] gives default values for these parameters.

B. SIP

SIP [10] is a signalling protocol used widely for the set up and tear down of communications involving multimedia content. It can be used to create, modify and terminate unicast or multicast sessions of one or more media streams. SIP operates at the session layer in the OSI model. It is designed to be transport layer independent and could use SCTP [11] as its transport mechanism.

C. Prototype Application Implementing SCTP

Figure 1 illustrates the architecture of the prototype application which implemented SCTP at the transport layer.

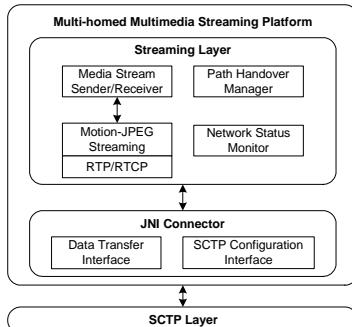


Fig. 1. SCTP based prototype application

The server consisted of an SCTP aware media stream sender which transmitted a short avi format video stream to an SCTP aware media stream receiver on the client side. The SCTP components include elements to monitor the status of the networks being used and to instigate path handover where required. The receiver displays the video in a media player and

saves it to a file in avi format. The SCTP Configuration interface can be used to adjust configurable SCTP parameters.

D. Prototype Application Implementing SIP User Agent

The SIP user agent architecture is shown in figure 2.

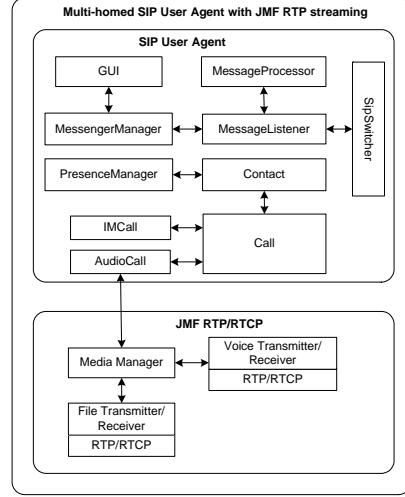


Fig. 2. SIP based prototype application

The application consists of two logical parts. The SIP user agent which supports multi-homing by creating multiple SIP dialogs for each possible end-to-end connection and a media part that makes multi-homing possible by utilizing the Java Media Framework (JMF) Real-time Transport Protocol (RTP) capabilities to create multiple media sessions with multiple destinations.

SIP user agents exchange information about their multiple IP addresses, by sending a SUBSCRIBE message to a SIP presence server containing list of addresses in the *Contact* field. The message is addressed to all SIP UAs from which it expects to get notifications about IP changes. When another SIP UA registers to SIP proxy/registrar server, the presence server sends SUBSCRIBE message containing IP addresses and UA responds with NOTIFY message that includes its IP addresses in the *Contact* field.

Each SIP UA scans for local and remote IP failure. The remote addresses are constantly monitored by sending UDP heartbeats with three user adjustable parameters. Initial timeout is used to block and wait for heartbeat response, timeout increment value indicates how the next timeout value will be modified and number of heartbeat retries determine how many times a heartbeat is resent before the remote node is considered unreachable. When a local or remote network failure is detected the application is notified about this event in order that it may take the necessary actions. The SIP UA searches for next available SIP *Dialog* in order to continue the signalling session. If there is any media session active, the appropriate transmitter and receiver are started to continue the media flow as seamlessly as possible.

IV. TEST ENVIRONMENT

E. Network Apparatus

A desktop PC with two Ethernet network interfaces was designated to act as a server. Each network interface was connected by an Ethernet cable to two separate LAN's and hence to two separate Linksys wireless 802.11g routers. A laptop with dual wireless interface cards acted as the client. Each wireless interface was configured to connect to one of the Linksys wireless routers. This configuration, figure 3, was implemented for both the SCTP and SIP evaluations.

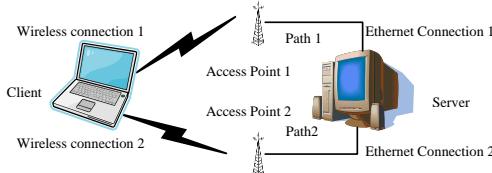


Fig. 3. Network Configuration

This created two separate server-to-client paths and avoided a single point of path failure between the nodes.

F. SCTP Configuration

Previous research [12] has demonstrated that implementation of configurable SCTP parameters at their recommended values results in a minimum handover delay of 63 seconds following a primary path failure. This is unacceptably large for many applications, especially multimedia content. The following adjustments to SCTP parameters were made based on research such as that undertaken in [13] and [14] that has optimised these parameters and pre-test trials. These values lead to more aggressive handover responses.

In order to prevent the RTO value from growing too large and delaying handover Path.Max.Retrans was reduced to a single retransmission. Based on previous research [15] RTO.min was shortened to 400 milliseconds to avoid unnecessary retransmission as it remains shorter than most round trip times but also low enough to reduce retransmission delays.

G. SIP User Agent Configuration

Configurable SIP user agent parameters were adjusted during the course of the test as per table 1 and as discussed in H. This was to evaluate handover performance according to 3 different levels of aggression in respect of handover strategies, with less aggressive handover implying a longer handover delay.

SIP does not generically support multi-homing therefore these parameters are part of the prototype application development and have not been optimised by previous research. The most aggressive setting gives the total of 500ms delay for handover, whereas least aggressive setting gives 7200ms delay for handover. The given parameters were selected in order to compare the changes in quality during transmission as more and more packets are lost and due to RTP running over

unreliable UDP protocol, all the packets during handover period are lost.

TABLE I
SIP PATH HANDOVER CONTROL VALUES

Handover sample (sets of 10 files)	Timeout (ms)	Timeout Increase (ms)	Path Retries
Least Aggressive	2000	400	3
Aggressive	1000	200	2
Most Aggressive	500	0	1

H. Video Transmission

The SCTP and SIP user agent multi-homed implementations both transmitted the same 150 second video file from the server application to the client application. To initiate permanent path failure during selected transmissions an Ethernet cable was explicitly removed from the server machine.

For the SCTP implementation the file was transmitted a total of 50 times. For the first 25 transmissions the full transmission occurred over primary path 1 and no path failure was initiated. The following 25 transmissions each experienced an initiated primary path failure at approximately $t=60$ seconds. Transmission of the remainder of the file continued over path 2.

For the SIP user agent implementation the file was transmitted a total of 40 times. The first 10 transmissions occurred over path 1 with no path failures initiated. The remaining 30 transmissions experienced an initiated path failure on path 1 at approximately $t=60$ seconds followed by a handover and transmission completion on path 2. These 30 transmissions were grouped into three sets of 10 transmissions each, with switchover related parameters adjusted for each set of ten as detailed in table 1.

V. RESULTS

Using a video quality measurement tool developed by Moscow State University [16], each video file received by the client was compared to the original file sent by the server. Two sets of metric values, peak signal to noise ratio (PSNR) and video quality metric (VQM) were obtained in respect of each comparison. These are both objective evaluation methods. PSNR is a mathematically based model that calculates the ratio between the maximum possible energy of a signal and the energy of noise related to it. VQM is modelled on human visual perception and has a discrete cosine transform basis with filters to detect differences and distortion. Better quality is indicated by a higher result for the PSNR metric and a lower value for the VQM metric.

These values were firstly collated by metric type and handover status and the results for the SIP based experiment were further grouped by handover aggression parameters. Average metric values across commonly collated files were calculated and graphed.

Averaged PSNR metric results for complete file transmissions are illustrated by Figures 4 in respect of the SCTP implementation and figure 5 in respect of the SIP implementation.

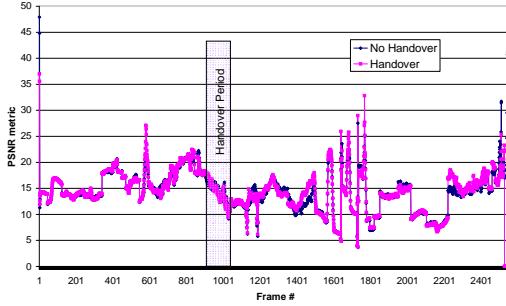


Fig. 4. SCTP – Averaged Complete File PSNR

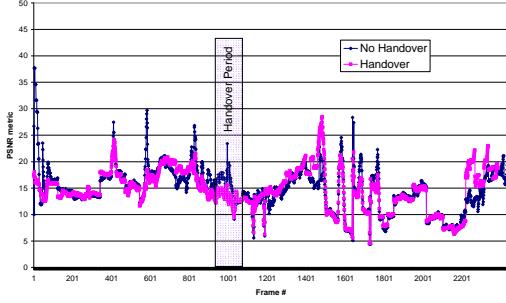


Fig. 5. SIP - Averaged Complete File PSNR

Transmissions that experienced no path failure are grouped under the label “No Handover” and those that had path handover are grouped as “Handover”. The bar towards the centre of the graphs represents the approximate portion of the results that would have been impacted by the path failure and subsequent handover for all “Handover” files. In figure 5 the averages across all 30 SIP based “Handover” files have been grouped together irrespective of handover aggression.

While both figures 4 and 5 show that the averaged metric outputs for “Handover” files are similar to the averaged metric outputs for “No Handover”, it is clear that the SIP implementation suffers a greater divergence. In particular, for the SCTP implementation, the differences between the two series of values appear to be no greater during the approximate handover period than during any other part of the transmission. The differences between the two series of metrics during the handover period are more pronounced within the SIP implementation.

Figures 6 and 7 show PSNR metrics for the handover period, as shown by the shaded sections of figures 4 and 5, for the SCTP and SIP based implementations respectively.

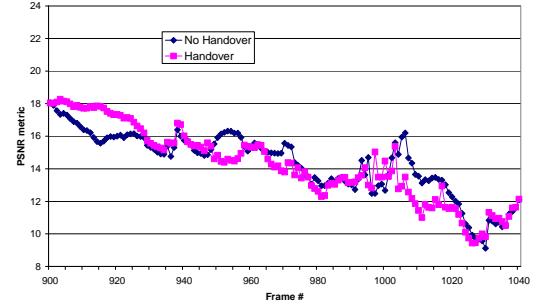


Fig. 6. SCTP - Averaged Handover Period PSNR

The PSNR metrics for the SCTP “Handover” files are similar in value to the metrics for the “No Handover” files as shown in figure 6. In figure 7 the averaged “Handover” file results of figure 5 are replaced with three series giving metrics for the three sub-groups of “Handover” files as detailed in *H* and *G*.

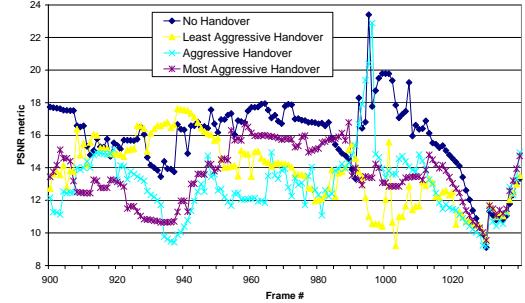


Fig. 7. SIP - Averaged Handover Period PSNR

However figure 7 clearly shows the larger deviation between “Handover” and “No Handover” metrics for the SIP implementation. The SIP “Handover” files achieve lower metrics across almost the entire handover period. These graphs indicate that the SCTP implementation gives a better quality performance during the handover period.

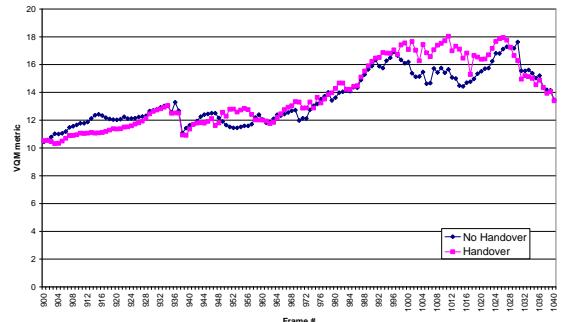


Fig. 8. SCTP - Averaged Handover Period VQM

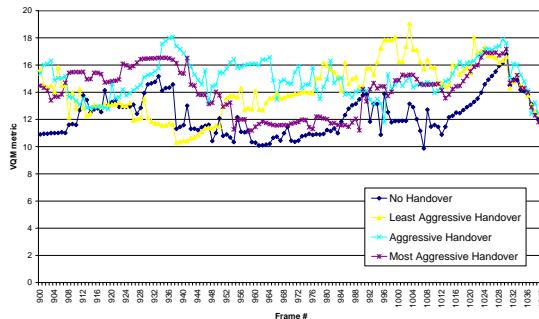


Fig. 9. SIP - Averaged Handover Period VQM

Similar inferences can be drawn from the graphical representation of the VQM metrics in figure 8 and 9 as have been stated in respect of the PSNR metrics. The key inference with both metrics is that the SCTP implementation maintains a better quality during the handover period.

Further examination of the metric data supports this finding. Tables 2 and 3 give the overall PSNR average metrics for the SCTP and SIP implementations respectively in respect of complete received files and the handover periods of those files. Each table gives the percentage and metric difference between the “Handover” and “No Handover” files and table 3 gives the differences for each set of “Handover” files.

TABLE 2
SCTP OVERALL PSNR METRICS

SCTP	PSNR results (complete file)	PSNR results (handover period)
No handover	14.40	14.34
Handover	14.45	14.24
Difference	(0.37%)	0.05

TABLE 3
SIP OVERALL PSNR METRICS

SIP	PSNR results (complete file)	PSNR results (handover period)
No handover	14.83	15.82
Least Aggressive	14.81	13.74
Difference	(0.16%)	0.02

SIP	PSNR results (complete file)	PSNR results (handover period)
No handover	14.83	15.82
Least Aggressive	14.81	13.74
Difference	(0.16%)	0.02
Aggressive	14.52	12.91
Difference	(2.14%)	0.31
Most Aggressive	14.42	13.51
Difference	(2.84%)	0.41

From the tables it can be seen that the SIP implementations mid-level aggression setting achieved the closest metric results to the SCTP implementation in respect of the “No Handover”

files yet suffered the biggest difference in quality between “Handover” and “No Handover” files.

Similarly tables 4 and 5 give the overall VQM metrics for the same files and both implementations.

TABLE 4
SCTP VQM OVERALL VQM METRICS

SCTP	VQM results (complete file)	VQM results (handover period)
No handover	13.49	13.57
Handover	13.48	13.83
Difference	(0.12%)	0.02

TABLE 5
SIP OVERALL VQM METRICS

SIP	VQM results (complete file)	VQM results (handover period)
No handover	13.31	12.3
Least Aggressive	13.41	14.15
Difference	(0.75%)	0.10
Aggressive	13.49	14.98
Difference	(1.35%)	0.18
Most Aggressive	13.54	14.09
Difference	(1.72%)	0.23

The magnitude of the complete file metric difference between the “Handover” and “No Handover” files is relatively small for both the SCTP and SIP based implementations over both metrics. Furthermore the SCTP metrics have a difference of less than 2% between “Handover” and “No Handover” files over the handover period. In contrast the SIP implementation metrics for the “Handover” and “No Handover” files for the same period differ significantly by between 14.5% and 22.5% over the two metrics.

It could be expected that increasingly aggressive handover SIP strategies which produce incrementally faster path handovers would lead to improving performance from least to most aggressive handover policy. The results do not show this to be the case, as can be seen across tables 3 and 5.

VI. CONCLUSIONS

This paper compared transport layer SCTP based and application layer SIP based approaches to providing multi-homing support. The simulation included transmissions of multimedia data between two multi-homed endpoints, during which selected transmissions suffered a permanent path failure and subsequent path handover. Objective quality metrics were used to evaluate the performance of the SCTP based approach against a number of increasingly aggressive handover strategies in the SIP based approach.

The results show that the SCTP based implementation’s performance is generally more consistent irrespective of whether a handover occurs than the SIP based implementation. Most significantly the SCTP based implementation has notably better performance over the handover period than the SIP based approach. Whilst the SCTP based approach

experienced no greater than a 2% difference between the “Handover” and “No Handover” files over the handover period, the SIP based implementation suffered differences as high as 22.5%.

Interestingly the metrics obtained for the SIP based implementation “Handover” files have not displayed the correlation between performance and level of handover aggressiveness that might have been expected and this will be subject to further analysis as part of future work.

SCTP has been designed to support multi-homing on an end-to-end basis between two endpoints. Implementation of multi-homing at the application layer would be on a per application basis and would hence raise interoperability issues. SCTP aware applications could give better performance in multi-homed wireless environments where networks fluctuations and path failures may disrupt connections and degrade the end users experience.

REFERENCES

- [1] Stannett K. et al, “Assessing ELearning Application Multimedia Quality in a Multihomed Environment” in *Proc. IADIS Int. Conf. e-society ‘08*, Algarve, 2008, pp. 195-203.
- [2] Wang H. et al, “The Performance Comparison of PR-SCTP, TCP and UDP for MPEG-4 Multimedia Traffic in Mobile Network” in *Proc. Int. Conf. Communication Technology*, Beijing, 2003, pp. 403-406.
- [3] Wang J “Jitter-based SCTP: Improving SCTP performance by jitter-based congestion control over wired-wireless networks” M. Eng. Thesis, Nanchang University, China, July 2006
- [4] Shi J. et al, “Experimental Performance Studies of SCTP in Wireless Access Networks” in *Proc. Int Conf on Commun Tech (ICCT 2003)* Beijing, vol. 1, pp 392-395
- [5] Wedlund E., Schulzrinne H., “Mobility Support using SIP”, in *Proc. 2nd ACM Int. Workshop on Wireless Mobile Multimedia*, 1999, pp 76-82
- [6] Lee S.H., Lim J.S., “SIP Mobility Support Using SIP Mobility Agent in All-IP Networks”, in *Proc. IASTED Int. Conf. Parallel & Distributed Computing and Networks*, 2004, Innsbruck, Austria, pp 207-209
- [7] Dutta A. et al., “Multimedia SIP Sessions In a Mobile Heterogeneous Access Environment” in *Proc. 2002 Int. Conf. 3rd Generation Wireless & Beyond*, San Francisco
- [8] Worley D, “Supporting Multiple Path Routing in the Session Initiation Protocol”, IETF Internet Draft, 2007, <http://www.ietf.org/internet-drafts/draft-worley-redundancy-response-02.txt>, last viewed April 2008
- [9] *Stream Control Transmission Protocol*, IETF proposed standard RFC4960, 2007
- [10] *Session Initiation Protocol*, IETF proposed standard RRC3261, 2002
- [11] *The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)*, IETF proposed standard RFC4168, 2005
- [12] Caro A.L. et al., “End to End Failover Thresholds For Transport Layer Multihoming” in *Proc. MILCOM 2004*, California, vol. 1, pp 99-105
- [13] Caro A.L. et al., “Retransmission Schemes for End to End Failover with Transport Layer Multihoming”, in *Proc. GLOBECOM 2004*, Texas, Vol. 3 pp 1341-1347
- [14] Fallon S. et al., “SCTP Switchover Performance Issues in WLAN Environments”, in *Proc. Consumer Commun. & Networking Conf. 2008*, Nevada, pp 564-568
- [15] Jungmaier A. Rathgeb E.P. and Txen M. “On the Use of SCTP in Failover-Scenarios”. In *Proc. SCI 2002*, Volume X, Mobile/Wireless Computing and Communication Systems II, volume X, Orlando/U.S.A., Jul 2002.
- [16] Moskovin A. Petrov O. “MSU Video Quality Measurement Tool”. http://compression.ru/video/quality_measure/video_measurement_tool_en.html

Reconfigurable Implementation of Karatsuba Multiplier for Galois Field in Elliptic Curves

Ashraf B. El-sisi, Sameh M. Shohdy and Nabil Ismail
Computer Science Department, Faculty of Computers and Information,
Menoufiya University, Shebin Elkom 32511, Egypt,
ashrafelsisi@hotmail.com, s_mufic@yahoo.com , nabil_a_ismail@yahoo.com

Abstract: The efficiency of the core Galois field arithmetic improves the performance of elliptic curve based public key cryptosystem implementation. This paper describes the design and implementation of a reconfigurable Galois field multiplier, which is implemented using field programmable gate arrays (FPGAs). The multiplier of Galois field based on karatsuba's divide and conquer algorithm allows for reasonable speedup of the top-level public key algorithms. Binary Karatsuba multiplier is more efficient if it is truncated at n-bit multiplicand level and use an efficient classic multiplier algorithm. In these work three levels to truncate Binary karatsuba algorithm (4 bits, 8 bits and 16 bits) are chosen showing that 8 bits is the best level for minimum number of slices and time delay to truncate Binary karatsuba algorithm which is designed on a Xilinx VirtexE XCV2600 FPGA device. The VHDL hardware models are building using Xilinx ISE foundation software. This work is able to compute GF(2¹⁹¹) multiplication in 45.899 ns.

I. INTRODUCTION

During last decade cryptography took an important role in most of data exchange applications. Plain Data should be encrypted to cipher data before transferred to guarantee security necessities. On the other side the data decrypted to be ready to be processed in the main application. Cryptography algorithms divide in two categories: symmetric and asymmetric cryptosystems. In symmetric systems a single key is used to encrypt\decrypt the plain text to\ from cipher text but due to the complex task for sharing this key between sender and receiver it's not preferred in applications that's can't guaranteed secure key transferred. In asymmetric systems encryption and decryption operations done with two keys named private and public key. The private key owned by its owner and the public key is known for all other parties. When sender A needs to send data to receiver B, he encrypts his message with B's public key. This message will decrypted only with B's private key. So B only can read the message even if there is a third party spy on the channel.

Wireless Application Protocol (WAP) is a protocol for wireless devices. WAP contains many layers to complete its function. One of them is Wireless Transport Layer Security (WTLS) which is a security layer to ensure privacy, data integrity and authentication between communication parties. Secure transactions between client and server done by data encryption. But, first both parties

must be authenticated before the beginning of transaction. Secure connection establishment consists of several steps includes key exchange and authentication. Because of the nature of wireless transmissions correspond to low bandwidth, limited processing power and memory capacity we need to speed up the security operation and in the same time makes a balance between security needs and energy consumption and area. Hardware accelerators for any public key algorithm is reduce calculation time due to parallel processing rather than sequential processing in software, but in the same time with large area use.

Elliptic Curve Cryptography (ECC) preferred when compared with classical cryptosystems such as RSA because of higher speed and lower power consumption which are particularly useful for wireless applications. Because of ECC guarantees the same security level as RSA but with shorter key size [5] and [7].Elliptic curve used in many applications (e.g. Digital Signature, authentication protocols, etc.). But, the client and server authentication scenario illustrates how we can use it in *Elliptic curve Diffe-Hellman authentication algorithm* to authenticate client and server parties in WTLS layer at WAP protocol. Server and client should transfer cipher data using secret key to encrypt and decrypt the data. But, this is a problem for sharing this key between the two parties. So there are some protocols useful for this problem. *Diffe-Hellman key exchange protocol* is one of them. ECC can be used for this protocol. First, client and server choose two random integer numbers K_C and K_S . Second, client computes Q_C using ECC scalar multiplication by multiply ECC point (P) by K_C . Also, server does the same operation but multiply P by K_S producing Q_S . Now, client transfers Q_C to the server and server transfers Q_S to the Client. Client receives Q_S and using Scalar multiplication again multiplies Q_S by K_C . On the other hand, server multiplies Q_C by K_S . The result in both sides is the same key $K_C K_S P$ as shown in figure1. Now, the two parties have the same key which can be used as a secret key in the authentication process.

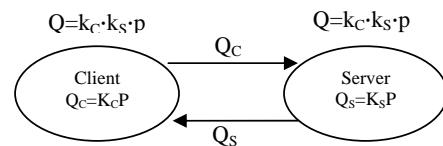


Figure 1: Elliptic curve Diffie-Hellman (ECDH)

Hardware implementation of ECC passes through 3 main levels. First, underlying *Galois field* arithmetic which includes four operations field multiplication, field addition, field squaring and field inversion. Second, elliptic curve preparation steps which includes Point doubling ($Q=2P$) and point addition ($R=P+Q$). Finally, elliptic curve main operation (scalar multiplication ($Q=K \cdot P$)) as shown in figure 2.

The long-term objective is to implement the first three levels layers to compute scalar multiplication for ECC using hardware to gain fast computation, reduce power and storage space. Many designs implement the scalar multiplication in hardware [2, 3, 4, 11, 13, and 16]. This work concerns in implement *Galois field* multiplication operation.

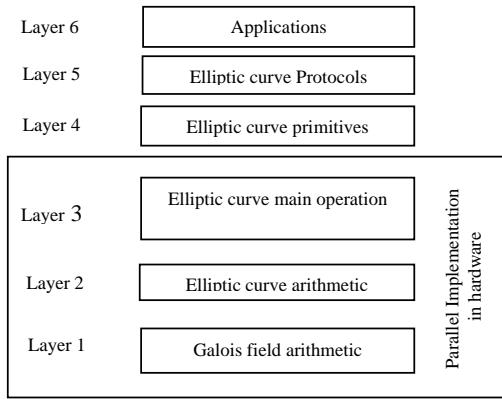


Fig. 2. Elliptic Curve Cryptography hierarchical model

The organization of this paper is as follows. In section 2 we describe mathematical background of elliptic curve cryptography and Galois field. Section 3 describes multiplication operation in $GF(2^m)$ and karatsuba-Ofman multiplier. In section 4 Architectural Design and Results for the implementation of karatsuba multiplier implementing finite field arithmetic in $GF(2^{191})$ is presented. Finally, in section 5 some conclusions remarks as well as future work are drawn.

II. MATHEMATICAL BACKGROUND

A. Galois Field Arithmetic

Galois field or *Finite field* (F) defines as $GF(p^m)$ which is a field with finite number of elements (p^m elements with p is a prime number called characteristic of field) and two binary operation addition and multiplication satisfy the following axioms: F is Abelian group with respect to '+', $F \setminus \{0\}$ is an abelian group with respect to 'x' and distributive. Furthermore, Order of Galois field is the number of elements on the Galois field [5, 10].

Galois field arithmetic plays a critical role in elliptic curve cryptography implementation because it's the core of ECC scalar multiplication. So, more efficient implementation of underlying field operations results

more efficient in the overall algorithm. *Galois fields* suitable for ECC implementation divides into two categories: prime field where $m=1$ and binary field where $p=2$ and $m>1$. *Binary Galois field* preferred in hardware because of free carry propagation property in hardware which make addition operation only done with one n-bit XOR operation (*equal to bit wise addition module 2*), square operation done with no hardware resource rather than in (F_p) is cost as a general multiplication and faster Inversion operation in $GF(2^m)$.

Next two subsections discuss needed operations (*addition, multiplication, squaring and inversion*) for binary field needed for ECC implementation in hardware.

B. Binary field

Finite field of order 2^m is called binary field. Suppose Binary field (F_2^m) and we have two elements $A, B \in F_2^m$. Addition does not have any carry propagation. It can be done only with one n-bit XOR operation (equal to bit wise addition module 2), multiplication done by ordinary multiplication ($a \cdot b$) modulo irreducible polynomial $P(x)$ in F_2^m , but does not have any carry propagation too in addition stage, squaring in F_2^m done only by change bits order modulo irreducible polynomial $P(x)$ and Inversion computed by calculate A^{-1} which prove $(A \cdot A^{-1} \bmod P(x) = 1)$. For example: F_2^4 is a Binary field with $m=4$. F_2^4 polynomial elements e {0, 1, x , $x+1$... x^3+x^2+x+1 }, suppose $A, B \in F_2^4$ and $p(x)=x^4+x+1$. The four mathematical operations are illustrated in table 1.

TABLE 1: BINARY FIELD F_2^4 ARITHMETIC OPERATIONS

Polynomial elements	Binary Form	Operation
$A = X^3 + X^2$ $B = X^2 + X + 1$	$A=1100$ $B=0111$	Addition $A+B=X^3+X^2+X^2+X+1$ $=X^3+X+1$ $A+B=1100@0111$ $=1011$
$A = X^3 + X^2$ $B = X^2 + X + 1$	$A=1100$ $B=0111$	Multiplication $A \cdot B = X^5 + X^4 + X^3 + X^4 + X^3 + X^2$ $= X^5 + X^2 \bmod X^4 + X + 1$ $= X^3 + X + 1$ $A \cdot B = 1100 \cdot 0111$ $=100100$ (reduction step) $100100 \bmod 10011=1011$
$A = X^3 + X^2$	$A=1100$	Squaring $A^{-1}=X^6+X^4$ $A^2=\sum a_i x^i = 1010000$
$A = X^3 + X^2 + 1$	$A=1101$	Inversion $A^{-1}=X^2$, Since $(X^3+X^2+1) \cdot (X^2) \bmod (X^4+X+1)=1$ $A^{-1}=00100$

C. Elliptic Curve Cryptography Arithmetic

Elliptic curves are defined over chosen finite field. For example, an elliptic curve defined over real numbers is a set of points (x, y) which satisfy the equation:

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5 \quad (1)$$

Where $a_1, a_2, a_3, a_4, a_5 \in \mathbb{R}$ and $a_1, a_2, a_3 = 0$. Different values of a_4, a_5 produce different curve defined over real numbers.

For example, Let $a_4 = -9, a_5 = 9$ the equation will be present as:

$$y^2 = x^3 - 9x + 9.$$

The elliptic curve is additive group (its main operation is the addition). Let A and B two points on the curve then $R=A+B$ can geometry represents by draw a line through the two points that will intersect the curve at another point, call $-R$. The point $-R$ is reflected in the x-axis to get a point R which is the required point as shown in figure 3.

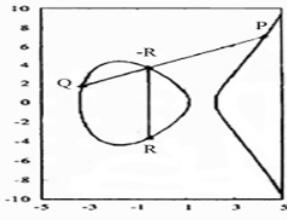


Fig. 3. Addition operation in $y^2 = x^3 - 9x + 9$

Elliptic curve cryptography (ECC) arithmetic: The main operation in ECC is the scalar multiplication operation ($Q=K \cdot P$, where k is integer and P is a point on the selected curve and Q is the scalar multiplication resulting from multiply K and P). There is no multiplication operation in elliptic curve groups. However, the scalar product KP can be obtained by adding k copies of the same point P . The security of elliptic curve systems is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). ECDLP define as : Given an elliptic curve E defined over a Galois field (F_p) and two points Q and P that belong to the curve, the trick is to find the integer k which if multiplies by P we get Q . Pollard's rho is one of the popular algorithms known for solving the ECDLP. The largest ECDLP instance solved with Pollard's rho algorithm is for an elliptic curve over a 109-bit prime field as illustrates in [14].

Different schemes exist for performing elliptic curve scalar multiplication operation as mentions in [9]. For example, *Montgomery algorithm* which calculates the KP multiplication using two main blocks *Point addition* and *Point doubling* [16].

III. MULTIPLICATION OPERATIONS IN $GF(2^m)$

Assume we have two elements $A(x), B(x)$ belongs to binary field $GF(2^m)$ with irreducible polynomial $P(x)$. Field multiplication done by two steps:

1. Polynomial multiplication of $A(x)$ and $B(x)$
 $C'(x) = A(x) \cdot B(x)$
2. Reduction using irreducible polynomial $p(x)$
 $C(x) = C'(x) \bmod p(x)$

A. Karatsuba-Ofman Multiplier

As we mention above there are two steps to compute the multiplication operation over $GF(2^m)$. A lot of multipliers addressed the problem of compute polynomial multiplication some suitable for hardware and some for software. We addressed here two algorithms one suitable for composite field (where $m=ns$, $s=2^t$, t integer) called *karatsuba multiplier* first proposed in [12] and it's modification-*Binary karatsuba multiplier*- proposed in [15] which is suitable for $GF(2^m)$ where m an arbitrary number. The two algorithms depend on splitting the two multiplied elements to two parts for provide a parallel computation in hardware.

Let A, B two elements in the *Galois field* $F(2^m)$ they can be represented as:

$$A = \sum_{i=0}^{m-1} a_i x^i = \sum_{i=0}^{m-1} a_i x^i + \sum_{i=0}^{\frac{m}{2}-1} a_i x^i \\ = X^{\frac{m}{2}} A^H + A^L \quad (2)$$

$$\text{Where } A^H = \sum_{i=0}^{\frac{m}{2}-1} a_{i+\frac{m}{2}} X^i, A^L = \sum_{i=0}^{\frac{m}{2}-1} a_i x^i$$

Also,

$$B = \sum_{i=0}^{m-1} b_i x^i = \sum_{i=0}^{m-1} b_i x^i + \sum_{i=0}^{\frac{m}{2}-1} b_i x^i \\ = X^{\frac{m}{2}} B^H + B^L \quad (3)$$

$$\text{Where } B^H = \sum_{i=0}^{\frac{m}{2}-1} b_{i+\frac{m}{2}} X^i, B^L = \sum_{i=0}^{\frac{m}{2}-1} b_i x^i$$

With some modifications we can say that:

$$C(x) = X^m A^H B^H + A^L B^L + (A^H B^H + A^L B^L + (A^H + A^L)(B^H + B^L)) X^{\frac{m}{2}} \quad (4)$$

According equation (4) Suppose $M_A = (A^H + A^L)$, $M_B = (B^H + B^L)$ then we need three polynomial multiplications: $(A^H B^H, A^L B^L \text{ and } M_A M_B)$ and four

polynomial additions: $(A^H + A^L, B^H + B^L, R = A^H B^H + A^L B^L \text{ and } R + M_A M_B)$.

Figure 4 shows the karatsuba algorithm. As seen in line 8, 9, 10 the algorithm called recursively to reduce the complexity of large size operand until an efficient point we can use classic algorithm- line 2 - to complete the multiplication process for small size operands[14].

```
Input: Two elements  $A, B \in GF(2^m)$  with  $m = rn = 2^t n$ , and where  $A$  and  $B$  can be expressed as  $A = X^{\frac{m}{2}} A^H + A^L$ ,  $B = X^{\frac{m}{2}} B^H + B^L$ 
Output: A polynomial  $C = AB$  with up to  $2m-1$  coordinates, where  $C = X^m C^H + C^L$ .
Procedure KmMul $^{2^t}(C, A, B)$ 
1. Begin
2. If ( $r == 1$ ) then
3.    $C = \text{classic\_mul}(A, B)$ 
4.   return;
5. for  $i$  from 0 to  $\frac{r}{n}-1$  do;
6.    $M_{Ai} = A_i^L + A_i^H$ 
7.    $M_{Bi} = B_i^L + B_i^H$ 
8. end;
9. KmMul $^t(C^L, A^L, B^L)$ ;
10. KmMul $^t(M, M_A, M_B)$ ;
11. KmMul $^t(C^H, A^H, B^H)$ ;
12. for  $i$  from 0 to  $r-1$  do
13.    $M_i = M_i + C_i^L + C_i^H$ 
14. end;
15. for  $i$  from 0 to  $r-1$  do
16.    $C_{\frac{r}{2}+i} = C_{\frac{r}{2}+i} + M_i$ 
17. end;
18. end;
```

Fig.4. karatsuba multiplier for composite fields

As mentioned in the algorithm each m bit polynomial multiplication divides into three $m/2$ bit polynomial multiplication and some polynomial additions which make a recursive methodology to compute polynomial multiplication [15]. It's recommended for $GF(2^m)$ to choose prime m values [6]. Now, we can say $m=2^t+d$. to use karatsuba multiplier we make $m=2^{t+1}$ for both elements and put $(2^{t+1}-d)$ most significant bits equal to zero. But, this operation waste arithmetic operation in multiply zero values.

In [15] an approach called *Binary karatsuba multiplier*

algorithm works using the same technique of karatsuba multiplier rather than it can use for arbitrary degree of m . This approach splits A, B many times as karatsuba multiplier but it cut off all complete zero operands from the computation as shown in figure 5.

Classic or Binary karatsuba multiplier is more efficient if we truncate them at n -bit multiplicand level and use an efficient classic algorithm which called hybrid karatsuba multiplier. In this work we design hybrid binary karatsuba multiplier for $GF(2^{191})$. Also we choose three levels to truncate binary karatsuba algorithm- (4, 8 and 16 bits) and making a comparison of the performance of three levels of hybrid karatsuba multiplier.

```
Input: Two elements  $A, B \in GF(2^m)$  with  $m$  an arbitrary number, and where  $A$  and  $B$  can be expressed as  $A = X^{\frac{m}{2}} A^H + A^L$ ,  $B = X^{\frac{m}{2}} B^H + B^L$ 
Output: A polynomial  $C = AB$  with up to  $2m-1$  coordinates, Where  $C = X^m C^H + C^L$ .
Procedure BK $(C, A, B)$ 
1. Begin
2.  $k = [\log_2 m]$ 
3.  $d = m - 2^k$ ;
4. If ( $d == 0$ ) then
5.    $C = \text{KmMul}^{2^k}(A, B)$ 
6.   return;
7. for  $i$  from 0 to  $d-1$  do;
8.    $M_{Ai} = A_i^L + A_i^H$ 
9.    $M_{Bi} = B_i^L + B_i^H$ 
10. end;
11. mul $^{2^k}(C^L, A^L, B^L)$ ;
12. mul $^k(M, M_A, M_B)$ ;
13. BK $(C^H, A^H, B^H)$ ;
14. for  $i$  from 0 to  $2^k-2$  do
15.    $M_i = M_i + C_i^L + C_i^H$ 
16. end;
17. for  $i$  from 0 to  $2^k-2$  do
18.    $C_{k+i} = C_{k+i} + M_i$ 
19. end;
20. end;
```

Fig.5. Binary karatsuba multiplier for arbitrary m

Figure 6 shows the architecture of *Binary Karatsuba multiplier* for $GF(2^{191})$ with the reduction Step demonstrates in next section

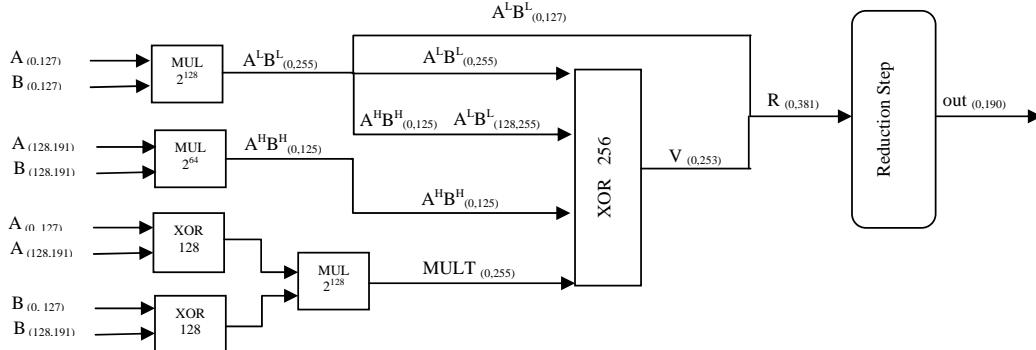


Fig.6. Karatsuba multiplier Architecture for $GF(2^{191})$

B. Reduction Step

After calculating $C'(x) = A(x) \cdot B(x)$ the next step to completely compute polynomial multiplication is the reduction process $C(x) = C'(x) \bmod P(x)$. Once the irreducible polynomial $P(x)$ has been selected, the reduction step can be complete by using XOR gates only [14].

$$C' = \sum_{i=0}^{2m-2} C_i$$

$$C = \sum_{i=0}^{m-1} C_i , \text{ where } C = C' \bmod P(x)$$

$$C(x) = C'_{[0, m-1]} + C'_{[m, 2m-1]} + C'_{[m, 2m-1-n]} X^n + (C'_{[2m-n, 2m-1]} + C'_{[2m-n, 2m-1]} X^n) \quad (5)$$

We select the irreducible polynomial $P(x) = X^{191} + X^9 + 1$ in the form $X^m + X^n + 1$ for this work.

Figure 7 illustrates the reduction step in GF(2¹⁹¹).

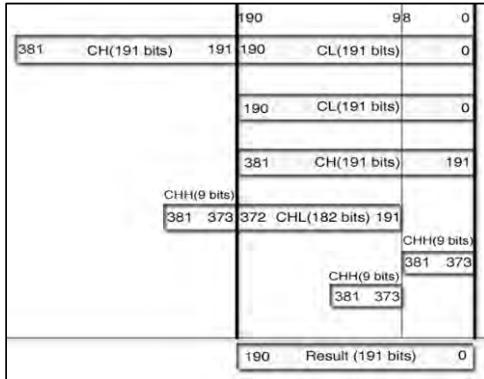


Fig.7. Reduction Step in GF(2¹⁹¹)

IV. ARCHITECTURAL DESIGN, IMPLEMENTATION, AND RESULTS

Depend on the architecture design illustrated in figure 7. A parallel architecture was used for computing hybrid Binary karatsuba multiplier truncated at 8 bit for $GF(2^{191})$ in 45.889 ns and 6,265 slices. This work uses hybrid Binary karatsuba multiplier (HBKM) and hybrid classic karatsuba multiplier (HCKM) (both truncated at 4 bit and use any efficient classic multiplier) for 191 bits in different devices to illustrate the high cost of zero computation in classic karatsuba algorithm. Also, to illustrates that the number of slices constant in all devices. But delay time change according to the device chosen and its speed this is because of different FPGA technology in each device as shown in table 2.

TABLE 2: CLASSIC/HYBRID KARATSUBA MULTIPLIERS FOR $GF(2^{191})$ DESIGN ON DIFFERENT XILINX DEVICES

Device	Algorithm	CLB slices	Time delay
xcv3200efg1156-8	HCKM (256 bits)	9,672	52.711 ns
xcv3200efg1156-8	HBKM(truncated at 4 bits)	6,632	48.950 ns
xcv3200efg1156-6	HCKM (256 bits)	9,672	63.967 ns
xcv3200efg1156-6	HBKM(truncated at 4 bits)	6,632	59.203 ns
xc2vp40ff1148 -7	HCKM (256 bits)	9,672	34.184 ns
xc2vp40ff1148 -7	HBKM(truncated at 4 bits)	6,632	32.632 ns
xcv2600efg1156-8	HCKM (256 bits)	9,672	50.708 ns
xcv2600efg1156-8	HBKM(truncated at 4 bits)	6,632	50.194 ns
xcv2600efg1156-6	HCKM (256 bits)	9,672	60.763 ns
xcv2600efg1156-6	HBKM(truncated at 4 bits)	6,632	59.203 ns

Also, we design the hybrid karatsuba multiplier with different n-bit truncated level (4, 8, and 16 bit) on a Xilinx VirtexE XCV2600 FPGA device. The results show different values of area and timing delay with different truncated level. The design shows that for an implementation of m bit hybrid karatsuba multiplier 8 bit truncated level needs less number of FPGA Slices and less time delay on the XCV2600efg1156-8 device. Figures 8 and 9 shows the number of occupied FPGA Slices and the time delay according to the size of the two multiplicand operands using Binary karatsuba algorithm truncated at different levels designed on a Xilinx VirtexE XCV2600 FPGA device.

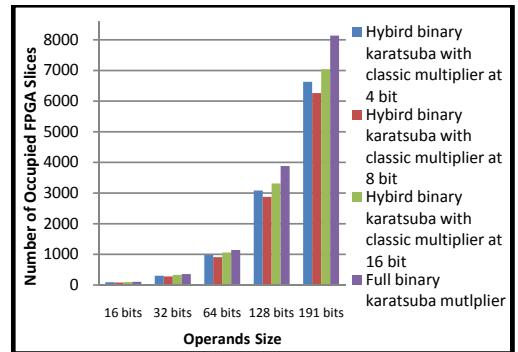


Fig.8. Number of occupied FPGA Slices according to the size of the two multiplicand operands

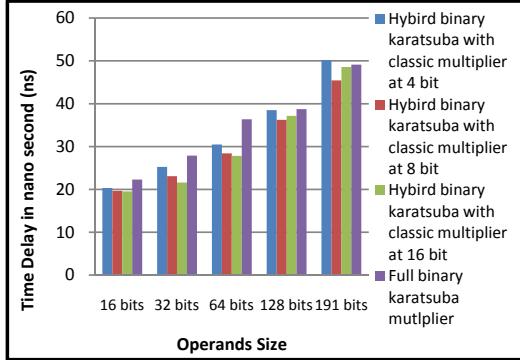


Fig.9. Time delay according to the size of the two multiplicand operands

Also, making a comparison between different hardware implementation is not directly. This is because of different FPGA technology used for each implementation and the degree of finite field used. But, [14] shows an efficient measure to be the key of the comparison between different keys computed as:

$$S = \frac{\text{number of bits}}{\text{number of slicing} \times \text{timing}}$$

In table 3, this study is compared with several hardware implementations reported in previous works.

TABLE 3: COMPARISON BETWEEN DIFFERENT HARDWARE GF(2^M) MULTIPLIERS

Reference and algorithm	FPGA Platform	Field	Number of slices	Timing	S
Ref[1] Montgomery multiplier	Virtex	160	1427 Slices	1.66 μ s	0.0675
Ref[17], Karatsuba–Ofman multiplier.	Virtex 2	163	5840 Slices	14.73 ns	1.895
Ref[3], Binary multiplier	VirtexE XCV2600	163	351 Slices	2.2 μ s	0.2110
Ref [13], Karatsuba–Ofman multiplier.	VirtexE XCV3200E	191	8721 Slices	43.1 ns	0.5081
This work, Karatsuba–Ofman multiplier.	VirtexE XCV2600	191	6265 Slices	45.889 ns	0.6645

V. CONCLUSIONS AND FUTURE WORK

In this work, an architecture of implement polynomial multiplier for Binary Field $GF(2^{191})$ is presented using Xilinx xcv2600efg1156-8 FPGA device results 6,265 occupied slices with time delay 45.889 ns. Also, this design use ISE 9.1 foundation tool for design the hybrid Binary karatsuba multiplier (HBKM) and hybrid classic karatsuba multiplier (HCKM) for 191 bits on different devices. Results show that truncated Binary karatsuba multiplier at low level and use any efficient classic algorithm is more efficient rather than full Binary Karatsuba multiplier. Also, the results show that 8 bit truncated level is the best level for minimize number of slices and time delay to use classic Multiplier. But,

delay time changes according to the device chosen and its speed. In the future work we will implement full ECC scalar multiplication for $GF(2^{191})$. Expected results will be minimums the number of slices and time delay needed according to efficient implementation for underlying field arithmetic.

REFERENCES

- [1] Batina L., Mentens N., Ors S.B., and Preneel B. Serial Multiplier Architectures over $GF(2^n)$ for Elliptic Curve Cryptosystems. In Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference MELECON 2004, volume 2, pages 779-782. IEEE Computer Society, May 2004.
- [2] Cheung Ray C.C., Wayne Luk and Cheung Peter Y.K., "Reconfigurable Elliptic Curve Cryptosystems on a Chip", Proceedings of the Design, Automation and Test in Europe Conference and Exhibition (DATE'05), IEEE, 2005.
- [3] El hadj Youssef Wajih, Guitouni Zied, Machhout Mohsen and Tourki Rached,"Design and Implementation of Elliptic Curve Point Multiplication Processor over $GF(2^m)$ ", IJCSES International Journal of Computer Sciences and Engineering Systems, Vol.2, No.2, 2008.
- [4] Ernst M., Jung M., and et al. F. M., "A Reconfigurable System on Chip Implementation for Elliptic Curve Cryptography over $GF(2n)$," Cryptographic Hardware and Embedded Systems CHES 2002, 4th International Workshop, Redwood Shores, CA, USA,2002.
- [5] Hankerson Darrel, Menezes Alfred and Vanstone Scott, "Guide to Elliptic Curve Cryptography", Springer, ISBN 038795273,2004.
- [6] IEEE P1363. "Standard specifications for public-key cryptography". Draft Version 7, September 1998.
- [7] Lenstra A. and Verheul E., "Selecting Cryptographic Key Sizes," Proc. Workshop on Practice and Theory in Public Key Cryptography, Springer-Verlag, ISBN 3540669671, pp. 446–465, 2000.
- [8] Lopez J. and Dahab R., "An Overview of Elliptic Curve Cryptography", Tech. Report, IC-00-10, May 2000.
- [9] Lopez J. and Dahab R., "Fast multiplication on elliptic curves over $GF(2m)$ without precomputation", Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems (CHES '99), Springer-Verlag LNCS 1717, 1999, pp. 316–327, Cancun, Mexico, May 2003.
- [10] McEliece R.J, "Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers, 1987.
- [11] Orlando G. and Paar C., "A Scalable $GF(p)$ Elliptic Curve Processor Architecture for Programmable Hardware," Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings, vol. 2162, pp. 348–363,May 2001.
- [12] Paar C., Fleischmann P., and Soria-Rodriguez P., "Fast Arithmetic for Public- Key Algorithms in Galois Fields with Composite Exponents". IEEE Trans.Computers, 48(10): 1025-1034, 1999.
- [13] Rodriguez-Henriquez F., Saqib N.A. and Diaz-Perez A., "A fast parallel Implementation of Elliptic Curve point multiplication over $GF(2m)$ ", Computer Science Section, Electrical Engineering Department, Centro de Investigacion y de Estudios Avanzados del IPN.,Microprocessors and Microsystems, Vol. 28, Issues 5-6, 2 August 2004, pp. 329- 339.
- [14] Rodriguez-Henriquez F., Saqib N.A., Diaz-Perez A. and Koc Cetin Kaya, "Cryptographic Algorithms on Reconfigurable Hardware",Springer, ISBN 0387338837,2006.
- [15] Rodriguez-Henriquez F. and Kog. Q. K. "On Fully Parallel Karatsuba Multipliers for $GF(2^m)$ ". In International Conference on Computer Science and Technology (CST), pages 405-410, 2003.
- [16] Saqib N.A., Rodríguez-Henruez F., and Díaz-Pérez A., "A Reconfigurable Processor for High Speed Point Multiplication in Elliptic Curves," Int'l J. Embedded Systems, vol. 1, nos. 3/4, 2005.
- [17] Sherigar M. B., Mahadevan A. S., Kumar K. S., and David S. A Pipelined Parallel Processor to Implement MD4 Message Digest Algorithm on Xilinx FPGA. In VLSID '98: Proceedings of the Eleventh International Conference on VLSI Design: VLSI for Signal Processing, page 394, Washington, DC, USA,1998. IEEE Computer Society.

Nonlinear Congestion Control Scheme for Time Delayed Differentiated-Services Networks

R. Vahidnia
Faculty of Engineering
Tarbiat Modares University
Tehran, Iran 14115-111
r.vahidnia@modares.ac.ir

M. Najafi
Kent State University
3300 Lake Road West,
Ashtabula, OH 44004
mnajafi@kent.edu

H. Firouzi
Faculty of Engineering
Tarbiat Modares University
Tehran, Iran 14115-111
h_firouzi@modares.ac.ir

M.T.H. Beheshti
Kent State University
3325 W 13th St.
Ashtabula, OH 44004
mhamid_gst@kent.edu

Abstract— Using non-linear control theory we developed and analyzed a generic Integrated Dynamic Congestion Controller “IDCC” scheme for controlling differentiated-services network traffic, having the information on the status of queue in the network. The controller scheme is based on a nonlinear model of the network which is generated using fluid flow model, considering time delay. The time delay is introduced in the control signal of premium service. In addition, a Lyapunov approach is employed to guarantee the stability of the closed loop system for premium traffic control strategy.

I. INTRODUCTION

Computer networks have experienced an explosive growth over the past few years and with that growth have come severe congestion problems. For example, it is now common to see internet gateways drop 10 percent of the incoming packets because of local buffer overflows.

A network is considered congested when too many packets try to access the same router's buffer, resulting in an amount of packets being dropped. In this state, the load exceeds the network capacity. During congestion, actions need to be taken by both the transmission protocols and the network routers in order to avoid a congestion collapse and furthermore to ensure network stability, throughput efficiency and fair resource allocation to network users. Indeed, during a collapse, only a fraction of the existing bandwidth is utilized by traffic useful for the receiver.

Quality of services is one of the most attractive sectors in the research of computer networks in the recent years. As a result, the Integrated Services architecture “Int-Serv” [1] was proposed. Nonetheless, it failed to be adopted for widespread use because of its scalability problems. Therefore, the Internet Engineering Task Force offered a new approach which did not need significant changes to the Internet infrastructure and provided differentiation of services “Diff-Serv” [2]. Two proposals have been made to the direction of QoS provisioning, the Resource Management in Diff-Serv “RMD” [3] and the Integrated

Dynamic Congestion Control “IDCC” [4]. Both protocols are based on Diff-Serv principles regarding traffic differentiation, but each one approaches the problem in a different way. RMD provides resource reservation and IDCC ensures congestion control.

IDCC is a dynamic congestion control scheme, based on differentiated service principles. It separates the traffic into three aggregate classes: the premium, the ordinary and the best effort. The premium traffic requires strict guarantees on delay and loss, the ordinary traffic can tolerate delay but cannot tolerate loss, and best effort offers no guarantees either on delay or on loss. Premium traffic will be used for real time applications. Its rate can only be regulated at the connection phase. When the connection is established, the network has to offer services in accordance with the given guarantees. Ordinary traffic, on the other hand, will be used for elastic applications. It allows the network to regulate its flow. When premium traffic needs more resources or severe congestion is detected, IDCC reduces the ordinary traffic by reducing the rate that the sources sent data. When there are available resources, it increases the ordinary traffic by increasing the rate. Finally, best effort traffic uses resources, which are instantaneously unused.

Several researches have been done on the delay processes. Sliding mode control is one of the powerful control methods for nonlinear systems because of its admirable control performance and robustness. In some researches, a neural network based sliding mode controller is proposed for a class of state-delayed systems with mismatched parameter uncertainties, unknown nonlinearities and external disturbances. The major advantage is the relaxation of the requirement that the unknown nonlinearities are to be bounded. For a class of point-delayed systems, sliding mode control is used in other papers where a linear transformation is applied to convert the delayed system to delay free system.

The control problem of the time-delay systems via predictor-based controllers has been dealt by many authors (Fiagbedzi & Pearson, 1986; Furukawa & Shimemura,

1983). Predictor-based controllers include a predictor to compensate for the time delay, and so are well known as a remedy to overcome the effect of the time delay. Under a predictor-based controller, therefore, a time-delay system can be transformed into a delay-free system in which the delay is eliminated from the closed-loop system.

In designing a sliding mode control, the current system state variables are needed. But in the delay system, we cannot get the system state variables in time. In this case, if we still control delay system based on current state variables, the system will be unstable and we cannot get the desired control performance. So in the letter, a new controller, including the sliding mode is presented for the delayed differentiated service network.

Lyapunov methods for the stability analysis of time-delay systems has been an ever growing subject of interest starting with the pioneering works of Krasovskii [5] and Repin [6]. In [7] modified Lyapunov–Krasovskii functional was introduced for which the time derivative includes terms which not only depend on the present but also on the past states of the delay system. This modification allows using the functional for robustness analysis of time delay systems.

In [8] the authors proposed a nonlinear congestion control scheme. The design objective is to regulate the buffer queue length to a constant reference value. Using feedback linearization and robust adaptive control ideas, the authors achieved bounded regulation in the face of unknown time varying interfering traffics.

In [9] the authors have proposed a robust control technique for congestion control problem of time-delayed scalable differentiated services networks. They also have introduced a new robust feedback linearization congestion control strategy for a fluid flow model in [10]. In [11] OPNET simulations have been used in order to demonstrate the performance of proposed adaptive nonlinear controller for diff-service network.

The physical constraints are important issues in many control systems. Numerous results have been established on the stabilization of linear systems with control input saturation constraint, while less work is known for general nonlinear systems. One contribution of our paper is that we give quantitative bound for choosing controller parameters such that the physical constraints of limited capacity and buffer size are satisfied. Based on this concept, we propose a dynamic congestion control framework for time delay networks. The rest of this paper is organized as follows: in section 2 we introduce a dynamic model for the network and based on this model the control strategy for premium traffic will be illustrated in section 3. Consequently, simulation results and conclusion have been explained in section 4 and 5.

II. DYNAMIC MODEL OF THE NETWORK

In this section we are about to find a model which captures the essential dynamic behavior, but has low-order complexity, as for example relative to detailed probabilistic models such as the Chapman–Kolmogorov equations for determining time-dependent state probability distribution for a Markovian queue [12]. Using the approximate fluid flow modeling approach proposed by Agnew [15], various dynamic models have been used by a number of researchers [14]–[16] to model a wide range of queuing and contention systems. Note that several variants of the fluid flow model have been extensively used for network performance evaluation and control, see, for example, an early reference that stimulated a lot of interest thereafter [17], and a recent reference of the present interest [18].

Using the flow conservation principle, for a single queue and assuming no losses, the rate of change of the average number of cells queued at the link buffer can be related to the rate of cell arrivals and departures by a differential equation of the form:

$$\dot{x}(t) = -f_{out}(t) + f_{in}(t) \quad (1)$$

Note that $x(t)$ is the state of the queue, given by the ensemble average of the number of cells in the system (i.e., queue + server) at time t . $f_{out}(t)$ is the ensemble average of cell flow out of the queue at time t ; $f_{in}(t)$ is the ensemble average of cell flow into the queue at time t .

The fluid flow equation is quite general and can model a wide range of queuing and contention systems as shown in the literature [14]–[16].

Assuming that the queue storage capacity is unlimited and the customers arrive at the queue with rate $\lambda(t)$, then $f_{in}(t)$ is just the offered load rate $\lambda(t)$ since no packets are dropped. The flow out of the system, $f_{out}(t)$, can be related to the ensemble average utilization of the link $\rho(t)$ by $f_{out}(t) = C(t)\rho(t)$, where $C(t)$ is defined as the capacity of queue server. We assume that $\rho(t)$ can be approximated by a function $G(x(t))$ which represents the ensemble average utilization of the queue at time t as a function of the state variable. Thus, the dynamics of the single queue can be represented by a nonlinear differential equation of the form

$$\dot{x}(t) = -G(x(t))C(t) + \lambda(t), \quad x(0) = x_0. \quad (2)$$

This is valid for $0 \leq x(t) \leq x_{\text{buffersize}}$ and $0 \leq C(t) \leq C_{\text{server}}$, where $x_{\text{buffersize}}$ is the maximum possible queue size and C_{server} is the maximum possible server rate. Many other

approaches can be used to determine $G(x(t))$. A simple commonly used approach to determine it is to match the steady-state equilibrium point of (2) with that of an equivalent queuing theory model, where the meaning of equivalent depends on the queuing discipline assumed.

Some other approaches such as system identification techniques and neural networks can also be used to identify the parameters of the fluid flow equation. We illustrate the derivation of the state equation for an M/M/1 queue following [12]. We assume that the link has a First-In-First-Out “FIFO” service discipline and a common (shared) buffer. The following standard assumptions are made: the packets arrive according to a Poisson process; packet transmission time is proportional to the packet length; and that the packets are exponentially distributed with mean length 1. Then, from the M/M/1 queuing formulas, for a constant arrival rate to the queue the average number in the system at steady state is $\lambda/(C - \lambda)$. Requiring that $x(t) = \lambda/(C - \lambda)$ when, $\dot{x}(t) = 0$, the state model becomes:

$$\dot{x}(t) = -\frac{x(t)}{1+x(t)}C(t) + \lambda(t), \quad x(0) = x_0. \quad (3)$$

The validity of this model has been studied by a number of researchers, including [15] and [19]. Here we assume that the applied control is delayed due to time delays in queue length measurement. Thus, the state equation of premium switch is considered as follows.

$$\dot{x}_p(t) = -C_p(t - \tau_p) \frac{x_p(t)}{1+x_p(t)} + \lambda_p(t). \quad (4)$$

Premium service requires strict guarantees of delivery within given delay and loss bounds. It does not allow regulation of its rate. Any regulation of this type of traffic has to be achieved at the connection phase. Once admitted into the network the network has to offer service in accordance with the given guarantees. This is the task of the premium traffic controller. On the other hand, ordinary traffic allows the network to regulate its flow into the network. It cannot tolerate loss of packets. It can however tolerate queuing delays. This is the task of the ordinary traffic controller. Best effort service on the other hand offers no guarantees on either loss or delay. It makes use of any instantaneous leftover capacity.

III. PREMIUM SERVICE CONGESTION CONTROL

The control goal for premium class is to tightly control the length of the premium traffic queue to be always close to a reference value, chosen by the network operator, so as

to indirectly guarantee acceptable bounds for the maximum delay and loss. The capacity for the premium traffic is dynamically allocated up to the physical server limit or a determined maximum. In this way, the premium traffic is always given resources up to the allocated maximum to ensure the provision of premium traffic service with known bounds. Due to the dynamic nature of the allocated capacity, whenever this service has excess capacity beyond that required to maintain its QoS at the prescribed levels it offers it to the ordinary traffic service. This algorithm uses the error between the queue length of the premium traffic queue and the reference queue length as the feedback information and calculates the capacity to be allocated to premium traffic once every control interval ms, based on the control algorithm discussed in this section. Therefore, the control objective is to choose $C_p(t)$ to be allocated to the premium traffic under the constraint that the incoming traffic rate $\lambda_p(t)$ is unknown but bounded by $\lambda_{p\max}$ and the link capacity for premium service is less than or equal to the capacity of server i.e. $C_p(t) \leq C_{server}$ so that the average buffer size $x_p(t)$ is as close to the desired value $x_p^{ref}(t)$ as possible.

Theorem. Choosing a linear sliding surface like

$$e(t) = x_p^{ref}(t) - x_p(t)$$

and assuming $\left| C_p(t - \tau_p) \frac{x_p(t)}{1+x_p(t)} \right| < M_p$, the control

signal $C_p(t)$ can be find as

$$C_p(t) = C_{peq}(t) - k \operatorname{sgn}[e(t)], \quad (5)$$

$$C_{peq}(t) = \frac{-\lambda_p + \dot{x}_p^{ref}(t)}{\left(-\frac{x(t)}{1+x(t)} \right)} \quad (6)$$

In order that the error dynamic

$$\begin{aligned} \dot{e}_p = & -C_p(t - \tau_p) \frac{e_p(t) + x_p^{ref}(t)}{e_p(t) + x_p^{ref}(t) + 1} \\ & + \lambda_p(t) - \dot{x}_p^{ref}(t) \end{aligned} \quad (7)$$

obtained by substituting (5) in (4) would be asymptotically stable. Where $0 < M_p \tau_p < k$.

Proof: Considering $V = \frac{1}{2}e^2(t)$ as a candidate Lyapunov function, which derivative will be studied in relation with convergence of $x(t)$ to the manifold $e(t)$. It is obvious that the error dynamic can be written as

$$\dot{e}(t) = \Delta_t^{t-\tau_p}(C_{peq}) - k \operatorname{sgn}[e(t - \tau_p)] \quad (8)$$

where $\Delta_t^{t-\tau_p}(C_{peq}) = C_{peq}(t - \tau_p) - C_{peq}(t)$. Therefore, the derivative of Lyapunov function is

$$\dot{V} = [e(t - \tau_p) + \int_{t-\tau_p}^t \dot{e}(\xi) d\xi] \times [\Delta_t^{t-\tau_p}(C_{peq}) - k \operatorname{sgn}(e(t - \tau_p))]. \quad (9)$$

Hence

$$\begin{aligned} \dot{V} &= -k |e(t - \tau_p)| + \Delta_t^{t-\tau_p}(C_{peq})e(t - \tau_p) \\ &\quad + k^2 \int_{t-\tau_p}^t [\operatorname{sgn}[e(t - \tau_p)].\operatorname{sgn}[e(\xi - \tau_p)] d\xi] \\ &\quad + \int_{t-\tau_p}^t [\Delta_t^{t-\tau_p}(C_{peq})\Delta_\xi^{\xi-\tau_p}(C_{peq})] d\xi. \end{aligned} \quad (10)$$

It is clear that

$$\int_{t-\tau_p}^t [\operatorname{sgn}[e(t - \tau_p)].\operatorname{sgn}[e(\xi - \tau_p)] d\xi] \leq \tau_p \quad (11)$$

Assuming that $|\Delta_t^{t-\tau_p}(C_{peq})| < M_p \tau_p$, then

$$\dot{V}(t) < (M_p \tau_p - k) \sqrt{V(t - \tau_p)} + \tau_p (k^2 + M_p^2). \quad (12)$$

From (12) it is straightforward to see that $M_p \tau_p < k$ is a necessary condition, and will be considered through the rest of this section. Defining $\tilde{V} = v_\infty^2$ the equilibrium point of (12) is

$$v_\infty^2 = \frac{\tau_p^2(k^2 + M_p^2)^2}{(k - M_p \tau_p)^2}. \quad (13)$$

Under condition $M_p \tau_p < k$, notation $V = y + v_\infty^2$ leads to

$$\dot{y}(t) < -\frac{\alpha}{2v_\infty^2} y(t - \tau_p) + \frac{\alpha y^2(t - \tau_p)}{2v_\infty^2 [v_\infty^2 + \sqrt{v_\infty^2 + y(t)}]^2} \quad (14)$$

where $\alpha = k - M_p \tau_p$. It can be shown that the previous inequality is negative and ensures the neighborhood

$$R_\infty = \left\{ e \in R : e^2 < 2v_\infty^2 = 2 \frac{\tau_p^2(k^2 + M_p^2)^2}{(k - M_p \tau_p)^2} \right\} \quad (15)$$

of the manifold $e(t)$ to be locally attractive. Solutions will reach R_∞ only for initial values sufficiently closed to it. At the price of stronger conditions, one can obtain an estimate D_0 of the initial conditions for which solutions tend to R_∞ . Knowing that

$$v_\infty^2 < \left[v_\infty + \sqrt{v_\infty^2 + y(t)} \right]^2$$

and integrating from $t - \tau_p$ to t inequality (14) can be written as

$$\begin{aligned} \int_{t-\tau_p}^t \dot{y}(\xi) d\xi &< \\ \int_{t-\tau_p}^t \left[-\frac{\alpha}{2v_\infty^2} y(\xi - \tau_p) + \frac{\alpha}{2v_\infty^3} y^2(\xi - \tau_p) \right] d\xi. \end{aligned} \quad (16)$$

Following the Lyapunov-Razumikhin's theory [20], we assume that $|y(t + \theta)| < \vartheta |y(t)|$, $\forall \theta < 0$ for some $\vartheta > 1$.

Therefore

$$\begin{aligned} |y(t)| &< -\frac{\alpha}{4v_\infty^2} (2v_\infty - \alpha \tau_p \vartheta) |y(t)| \\ &\quad + \frac{\alpha}{4v_\infty^4} \vartheta^2 (2v_\infty + \alpha \tau_p) y^2(t). \end{aligned} \quad (17)$$

This leads to the asymptotic stability condition $2v_\infty - \alpha \tau_p > 0$ and ensures convergence for any initial condition in the domain

$$D_0 = \left\{ e \in R : |e^2 - 2v_\infty^2| < v_\infty^2 \frac{2v_\infty - \alpha \tau_p}{2v_\infty + \alpha \tau_p} \right\}. \quad (18)$$

□

IV. SIMULATION RESULTS

Simulation results prove the effectiveness of the proposed control strategy in presence of time delay in the control signal. Besides, we have represented the simulation results for the proposed controller and evaluate the performance of the system in the presence of 30ms delay.

The control objective for the premium service is to choose $C_p(t)$ to be allocated to the premium traffic under the constraint that the incoming traffic rate $\lambda_p(t)$ is 430 packets per second. The maximum available service capacity is considered 1000 packets per second i.e. $0 \leq C_{server} \leq 1000$. The reference queue length is $x_p^{ref}(t) = 250 \pm 30 \sin(t)$. As it is depicted in Fig. 1 $x_p(t)$ tracks the reference and the error tends to decrease. It is

obvious that the queue length of the premium service reaches the reference value in a short time. Hence, it can be concluded that the controller has a suitable performance even in the case of high frequency changes in the reference signal.

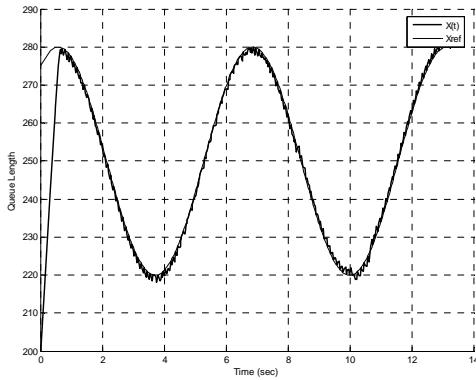


Fig. 1 Tracking the reference value by premium service queue length where delay=30ms.

V. CONCLUSION

In this report using a new Lyapunov approach an attractively domain for the sliding mode control of premium service network in the presence of time delay was obtained. In this case the time delay was considered in the link capacity control signal. Simulation Results illustrated the feasibility of the proposed design scheme.

VI. REFERENCES

- [1] R. Braden, D. Clark and S. Shenker, "Integrated services in the internet architecture: an Overview", IETF RFC-1633, Jun. 1994.
- [2] D. Black, S. Blake, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An architecture for differentiated services", RFC 2475, December 1998.
- [3] L., Jacobsson, M., Karagiannis, G., Oosthoek, S., Partain, D., Rexhepi, V., Szabo, R., Wallentin, P., "Resource management in diffserv framework", Internet Draft, Work in Progress, 2001.
- [4] P. Ioannou, L. Rossides, "Congestion control for differentiated-services using non-linear control theory", in Proceedings of the Sixth IEEE Symposium on Computers & Communications, ISCC 2001, Hammamet, Tunisia, 3-5, pp. 726-733, July 2001.
- [5] N.N. Krasovskii: On the application of the second method of Lyapunov for equations with time delays, Prikl. Mat. Mekh. 20, pp. 315-327, 1956.
- [6] M.I. Repin "Quadratic Lyapunov functionals for systems with delay", J. Appl. Math. Mech. 29, pp. 669-672 (Translation of Prikl. Mat. Mekh. 29, pp. 564-566), 1966.
- [7] V.L. Kharitonov, A.P. Zhabko: Lyapunov-Krasovskii "Approach to the robust stability analysis of time-delay systems," Automatica 39, pp. 15-20, 2003.
- [8] T. Alpcan and T. Baser, "Global stability analysis of end-to-end congestion control schemes for general topology networks with delay" In proceedings of the 42nd IEEE Conference on Decision and Control, Maui, Hawaii, 2003, 1092~1097.
- [9] K. Bouyoucef and K. Khorasani, "A sliding mode-based congestion control for time delayed differentiated-services networks", Proceeding of the 15th Mediterranean conference on control & automation, july 2007 Athens.
- [10] K. Bouyoucef and K. Khorasani, "Robust feedback linearization-based congestion control using a fluid flow model," in Proceedings of IEEE 2006 American Control Conference, Minneapolis, USA, 14-16 June 2006, pp. 4883-4887.
- [11] A. Pitsillides, P. Ioannou, M. Lestas, and L. Rossides, "Adaptive nonlinear congestion controller for a differentiated-services framework," IEEE Transactions on Networking, vol. 13, No.1, pp. 94-107, February 2005.
- [12] D. Tipper and M. K. Sundareshan, "Numerical methods for modelling computer networks under nonstationary conditions," IEEE J. Select. Areas Commun., vol. 8, no. 6, pp. 1682-1695, Dec. 1990.
- [13] C. Agnew, "Dynamic modeling and control of congestion-prone systems," Oper. Res., vol. 24, no. 3, pp. 400-419, 1976.
- [14] J. Filipiak, "Modeling and control of dynamic flows in communication networks". New York: Springer-Verlag, 1988.
- [15] S. Sharma and D. Tipper, "Approximate models for the study of nonstationary queues and their application to communication networks," in Proc. IEEE Int. Conf. Communications (ICC'93), pp. 352-358, May 1993.
- [16] X. Gu, K. Sohraby, and D. R. Vaman, "Control and performance in packet circuit and ATM networks.", Norwell, MA: Kluwer, 1995.
- [17] D. Anick, D. Mitra, and M. Sondhi, "Stochastic theory of data handling system and multiple sources," Bell Syst. Tech. J., vol. 61, pp. 1871-1894.
- [18] Y. Wardi and B. Melamed, "Continuous flow models: Modeling simulation and continuity properties," in Proc. 38th Conf. Decision and Control, vol. 1, pp. 34-39, Dec. 1999.
- [19] J. Filipiak, "Modeling and control of dynamic flows in communication networks". New York: Springer-Verlag, 1988.
- [20] J.-P. Richard, "Some trends and tools for the study of time-delay systems", Plenary lecture, 2nd IEEE-IMACS Conf. CESA'98, Computational Engineering in Systems Applications, Tunisia, 1-4, Proc. Vol. P, pp. 27-43, April 1998.

Effect of Packet Size and Channel Capacity on the performance of EADARP Routing Protocol for Multicast Wireless ad hoc Networks

(1) (2) (3)

Dina Darwish Imane Aly Saroit Abdel wehab Hassan

- (1) Lecturer ,International Academy for Engineering and Media Science - Egypt
(2) Professor, Faculty of Computers and Information , Cairo University – Egypt
(3) Professor, Faculty of Engineering , Cairo University – Egypt

ABSTRACT

An ad hoc network is a dynamically reconfigurable network without any infrastructure or centralized administration and which is formed of a group of wireless mobile hosts, each of which have a limited wireless transmission range. EADARP is an Energy Adaptable Distance Aware Routing Protocol (EADARP) for wireless mobile ad hoc networks is developed to improve basic performance metrics for multicast protocols. This paper investigates the effect of changing packet size and channel capacities on the performance of EADARP . Simulation program was developed using Glomosim to study such effect The results showed that a bigger packet size consumes more energy, and that a bigger packet size leads to less TTL expired, also smaller channel capacity leads to more power consumption.

1. INTRODUCTION

Wireless communications has two types; fixed or mobile. The fixed wireless communication is often called cellular networks, in which communication is achieved through a fixed number of base stations whose locations are known. The capacity of the channel given to a single session in a wireless cellular system can be either a point-to-point or a multipoint communication. Sharing the wireless cellular communication system capacity among multiple users is accomplished through various access methods, such as time division multiple access (TDMA), frequency division multiple access (FDMA) and code division multiple access (CDMA) [1- 4].

Mobile wireless communication; also called mobile ad hoc networks; does not have a fixed infrastructure or centralized administration. Each host in the mobile ad hoc network communicates with the other hosts via packet radios to form a temporary network its infrastructure varies according to the hosts' mobility.

The way of routing information in ad hoc networks is divided into two parts: *route discovery* and *route maintenance*. In route discovery, a host that wants to send information to another host must discover initially a suitable route for transmitting packets to the destination host. In route maintenance, the route should continue to send packets to the destination if the conditions remained unchanged. Otherwise, if the status of the links or hosts used in this route changed, some changes may be done to the route or there is a need to discover a new route [4-6].

The applications of wireless ad hoc networks determine if a communication session should be unicast (one-to-one), multicast (one-to-many), broadcast (one-to-all) or group communication (many-to-many). The rise in the number of mobile users has led to a wide variety of applications to become available. Some of these new applications depend on multicast communication to perform their operation. Multicasting has been implemented to the wireless ad hoc networks to make benefit from the dynamically reconfigurable nature of these wireless ad hoc networks [7-9].

A multicast protocol implemented in an ad hoc network should have the ability to connect all group members and then to maintain this connectivity after topological changes in the network [10-16]. Multicast ad hoc networks is the focus in this paper. Since multicast mobile ad hoc networks face the same constraints as unicast ad hoc networks, the efficient utilization of routing packets and energy efficiency must be taken into consideration when routing packets and recovering route breaks in multicast ad hoc networks. Some papers have considered minimum energy multicast routing in wireless multihop ad hoc networks, and for this purpose, a concept such as virtual relay [17-20] have been proposed. Also, several algorithms for energy efficient multicasting in static wireless ad hoc networks has been

presented [21,22]. Energy efficient adaptation of multicast protocols in power controlled wireless ad hoc networks is the basic idea presented in [21- 26].

An Energy Adaptable Distance Aware Routing Protocol (EADARP) for wireless mobile ad hoc networks is developed in [27] to improve basic performance metrics for multicast protocols The EADARP protocol is similar to ODMRP, a mesh-based protocol that employs the same concept of forwarding group, but here, the forwarding group is a set of nodes responsible for forwarding multicast data on the paths selected based on the most efficient path in terms of distance and energy between any member pairs with two enhancements added: first, the network bandwidth is increased according to the need, second, the nodes' level of energy is adjusted if there is a must.

The EADARP shows better performance such as number of TTL expired, number of unreachable nodes when compared to other multicast protocols . In this paper the effect of changing packet size and channel capacity on the performance of EADARP are thoroughly investigated and the results are presented and discussed .

2. EADARP DESCRIPTION

The EADARP protocol [27] is similar to ODMRP, a mesh-based protocol that employs the same concept of forwarding group, but here, the forwarding group is a set of nodes responsible for forwarding multicast data on the paths selected based on the most efficient path in terms of distance and energy between any member pairs with two enhancements added: first, the network bandwidth is increased according to the need, second, the nodes' level of energy is adjusted if there is a must. In EADARP route selection, a multicast receiver selects the most stable route having the largest remaining energy, in other words, selecting the route with the highest lifetime. Finding the route having the highest lifetime is done by measuring each route's nodes lifetimes, and choosing the node with the least lifetime in each route, and then selecting the route having the node with the highest lifetime among the least energy remaining nodes. Then eliminating the nodes having energy below the level required (energy threshold level) in the selected route, for the purpose of avoiding route breakage if these nodes fail. But the eliminated nodes do not include neither the source node nor the destination node, to preserve the original route. After that, some nodes are eliminated between the source node and the destination node to make the selected route shorter, in other terms, reducing the path length leads to decreasing the power consumption during the transmission. Then, EADARP performs adjustments of nodes batteries power levels when required, and also it increases the network bandwidth when there is a congestion in traffic and decreases it when there is no traffic.

To select a route, a multicast receiver must wait for an appropriate amount of time after receiving the first JOIN QUERY so that all possible routes and their lifetimes will be known. The receiver then chooses the most stable route and broadcasts a JOIN REPLY.

3. SIMULATION ENVIRONMENT

We are going to describe the simulation environment in which we simulated the multicast protocols, and produced the results which are compared after that to conclude the characteristics of each protocol.

3.1. Description of the Simulation Model

Several important parts of the simulation environment are going to be described below, including the model itself, channel and radio model we

used here, Medium Access Control protocol, multicast protocols used here, parameter values used in the simulation, the traffic pattern and the mobility model.

For evaluating the effect of changing packet size and channel capacity on the performance of EADARP, a simulation program was developed within the GloMoSim library [28]. The GloMoSim library is a scalable simulation environment for wireless network systems using the parallel discrete-event simulation capability provided by PARSEC [29].

The simulation is based on modeling a network of 30 mobile hosts placed uniformly within a 1000 m \times 1000 m area. Radio propagation range for each node was 250 m during all experiments. The used channel capacity is 8 Mbps when comparing the protocols with each others and when evaluating the performance of EADARP using different packet sizes. Each simulation is executed for 100 sec of simulation time. The network traffic loads used were between 100 packets/sec and 1500 packets/sec.

The IEEE 802.11 MAC with Distributed Coordination Function (DCF) [30] was used as the MAC protocol. DCF is the mode which allows nodes to share the wireless channel in an ad hoc configuration. The specific access scheme is Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) with acknowledgments.

3.2. Performance Metrics

The following performance metrics are proposed to evaluate the performance of EADRARP protocol:

3.2.1. Efficiency

Efficiency is the ratio of the number of data packets delivered to the destinations versus the number of data packets supposed to be received. This number presents the effectiveness of a protocol. Efficiency is also called the packet delivery ratio.

Efficiency = Total number of delivered packets/Total number of sent packets (calculated at each node) for all nodes and then the sum of ratios is divided by the number of active nodes.

3.2.2. Total number of control packets

It is the total number of control packets delivered during packets transmission in the network. Control packets include: beacons, route updates, join requests, acknowledgments, ----- etc.

Total number of control packets = beacons + CTRL + acknowledgments + join requests + join tables + route updates packets for all nodes.

3.2.3. Total power consumed

It is the sum of the power consumed at each node measured in mw/hr (milliwatts per hour) during packets transmission in the network.

Total power consumed = The sum of power consumed for all nodes = Pow_{node1} +-----+ Pow_{node30}

3.2.4. Total number of collisions

It is the total number of collisions that occurred during packets transmission in the network.

Total number of collisions = The sum of collisions for all nodes = Coll_{node1} +-----+ Coll_{node30}

3.2.5. Total number of unreachable nodes

It is the total number of unreachable nodes during packets transmission in the network.

Total number of unreachable nodes = The sum of unreachable nodes for all nodes = Unreach_{node1} +-----+ Unreach_{node30}

3.2.6. Total number of TTL (Time-To-Live) expired

It is the total number of TTL (Time-To-Live) expired during packets transmission in the network.

Total number of TTL expired = The sum of TTL expired for all nodes = TTL_{exp,node1} +-----+ TTL_{exp,node30}

4. EFFECT OF PACKET SIZE ON THE PERFORMANCE OF EADARP

In this section we evaluate the effect of increasing the packets size on the performance of EADARP under different network traffic loads beginning from 100 packets/second to 1500 packets/second. Packet sizes were taken respectively as: 64 bytes, 512 bytes, 1460 bytes and 2048 bytes. The results are discussed below.

4.1 Efficiency

Figure 1 illustrates the efficiency of EADARP using a variable packet sizes under different network traffic loads. EADARP shows a similar behavior using different number of packets sizes, whatever the packet size is, EADARP begins with a lower efficiency and the efficiency increases at a traffic load of 300 packets/second and decreases at a traffic load of 500 packets/second till 1500 packets/second. EADARP with 64 bytes packets and 2048 bytes packets provides better performance, and then followed by 512 bytes packets, and finally EADARP with 1460 bytes packets providing worst performance.

This was expected due to the fact that at a traffic load of 300 packets/second, the EADARP protocol exhibits the best efficiency before reaching the saturation point. Also, that increasing packet sizes could provide better efficiency to some extent as 2048 bytes packets shows better efficiency.

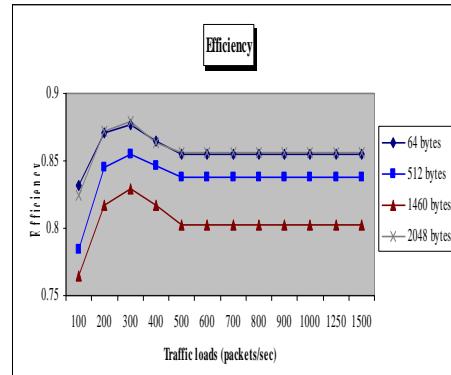


Figure 1: The efficiency of EADARP vs Traffic Load

4.2 Total number of control packets

Figure 2 illustrates the total number of control packets issued by EADARP under a variable network traffic loads using different packet sizes. EADARP with 2048 bytes packets shows better performance than with other packets sizes. The differences in the total number of issued control packets between 64 bytes, 512 bytes and 1460 bytes packet sizes is very small. The performance of EADARP using the preceding packet sizes is similar in terms that they begin with a smaller number of control packet at a traffic load of 100 packets/second and end with a higher number of control packets at a traffic load of 1500 packets/second, also, the total number of control packets is the same between a traffic load of 500 packets/second to a traffic load of 1500 packets/second. This means that the biggest packet size issues less number of control packets.

This was expected due to the fact that increasing the packet sizes has no great effect on the total number of control packets.

4.3 Total power consumed

Figure 3 illustrates the total power consumed in EADARP during packets' transmission using different packet sizes. The performance of EADARP in terms of power consumed using different packet sizes is the same, because EADARP begins with a lower value for power consumed when the traffic load is lower and this value increase as the traffic load increases and reaches 1500 packets/second, another notice is that the

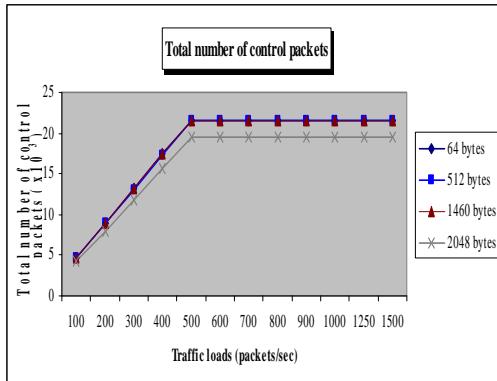


Figure 2: The total number of control packets vs Traffic Load

power consumed is fixed between a traffic load of 500 packets/second till a traffic load of 1500 packets/second and the differences between the values of the power consumed when changing the packet sizes is small. But in general, EADARP with a 2048 bytes packets consumed more energy, followed by 1460 bytes packets, then by 512 bytes packets, and finally by 64 bytes packets. So, EADARP with 2048 bytes packets is the worst performer, and EADARP with a 64 bytes packets is the best performer. This means that a bigger packet size makes our EADARP consumes more power. This was expected due to the fact that longer packet sizes need more energy to be transmitted, then resulting in higher power consumed.

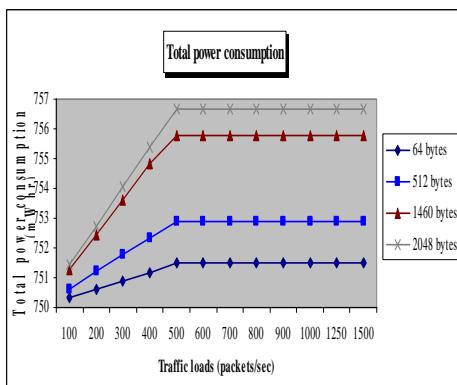


Figure 3: The total power consumed vs Traffic Load

4.4 Total number of collisions

Figure 4 illustrates the total number of collisions issued by EADARP under different traffic loads using different packet sizes. EADARP behavior is similar under different traffic loads using different packet sizes, because it begins with a lower number of collisions when the traffic load is low and the number of collisions increases as the traffic load reaches 1500 packets/second, also, the number of collisions becomes fixed between a traffic load of 500 packets/second and a traffic load of 1500 packets/second. The values of the number of collisions under different packet sizes are very close, but EADARP with 2048 bytes packets has the least number of collisions in comparison with the other three packet sizes.

This was expected due to the fact that increasing packet sizes has no important effect on the total number of collisions, since collisions occur due to increased network traffic not due to packets sizes.

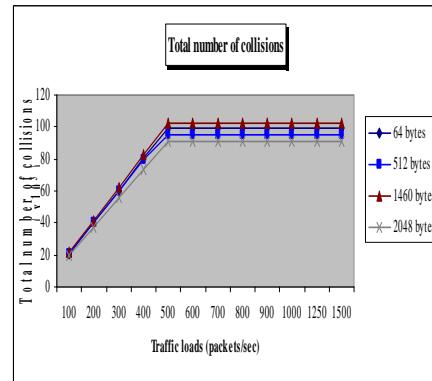


Figure 4: Total number of collisions vs Traffic Load

4.5 Total number of unreachable nodes

Figure 5 illustrates the number of unreachable nodes in EADARP under different network traffic loads using different packet sizes. EADARP under different network traffic loads changing from 100 packets/second to 1500 packets/second using different packets sizes gives the same number of unreachable nodes which is zero. This means that changing the packet size does not affect the number of unreachable nodes, and that none of the nodes were missed during packets' transmission in EADARP.

This was expected due to the fact that increasing packet sizes does not the protocol operation, then not affecting the number of nodes that can't be reached by other nodes. And this represents a good point in the EADARP protocol.

4.6 Total number of TTL expired

Figure 6 illustrates the total number of TTL expired in EADARP during packets' transmission under different traffic loads using different packet sizes. EADARP with a 64 bytes packets has the highest number of TTL expired during packets' transmission, followed by 512 bytes packets, then by 1460 bytes packets, and finally by 2048 bytes packets. EADARP under different traffic loads using different packet sizes shows the same performance, because it begins with a smaller number of TTL expired when the traffic load is 100 packets/second and ends with a higher number of TTL expired when the traffic load is 1500 packets/second, also the number of TTL expired becomes fixed from a traffic load of 500 packets/second till the end of the simulation when the traffic load reaches 1500 packets/second. Another notice, is that the number of TTL expired in EADARP using different packets sizes between traffic loads of 100 packets/second to 500 packets/second is very close and between traffic loads of 500 packets/second and 1500 packets/second the difference between the number of TTL expired for each packet size increases a little.

Also, we noticed that a bigger packet size means a smaller number of TTL expired.

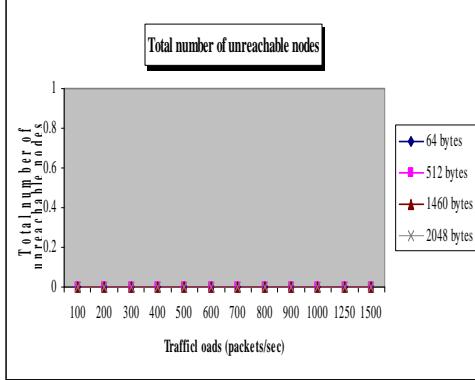


Figure 5: The number of unreachable nodes vs Traffic Load

This was expected due to the fact that when the packet size increases, it will cause nodes wanting to join a multicast group easier, resulting in a shorter waiting time for a node to join a group and then to a smaller number of TTL (Time-To-Live) expired. But at a traffic load of 500 packets/second, the EADARP protocol reaches its saturation point and can not accept more traffic loads, since every packet transmitted to one node is retransmitted as it is without changes.

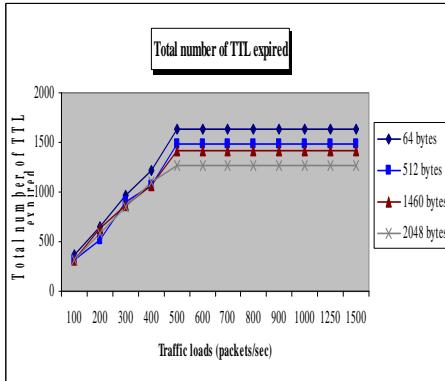


Figure 6: Total number of TTL expired vs Traffic Load

5. EFFECT OF CHANNEL CAPACITY ON THE PERFORMANCE OF EADARP

In this section we evaluate the effect of increasing the channel capacities on the performance of EADARP under different network traffic loads beginning ranging from 100 packets/second to 1500 packets/second. Channel capacities were taken respectively as: 3 Mbytes, 5 Mbytes, 7 Mbytes and 9 Mbytes, and the results of the simulation are discussed and evaluated.

5.1 Efficiency

Figure 7 illustrates the efficiency of EADARP under different network traffic loads using a variable channel capacities. EADARP with a 3 Mbytes channel capacity shows the worst performance with the lowest efficiency,

followed by 5 Mbytes channel capacity, then by 9 Mbytes channel capacity, and finally by 7 Mbytes channel capacity which is the best performer. We notice that the values of efficiency in the 5 Mbytes, 9 Mbytes, and 7 Mbytes are very close, and that the efficiency of EADARP at 3 Mbytes is a little far from them. EADARP under different network traffic loads using different channel capacities shows similar performance, in terms that it begins with a lower efficiency at a traffic load of 100 packets/second, and the value of the efficiency increases when the traffic load reaches 300 packets/second, then decreases at a traffic load of 500 packets/second, and it becomes fixed at a traffic load of 500 packets/second until 1500 packets/second.

The channel capacity of 3 Mbytes to have the lowest efficiency was expected during the simulation. This was expected due to the fact that increasing the channel capacity could make packets' transmissions easier, thus reducing the packets' loss during the simulation and causing the efficiency to improve. The efficiency becomes fixed from the traffic load of 500 packets/second because the EADARP protocol reaches its saturation point and can not accept more traffic loads.

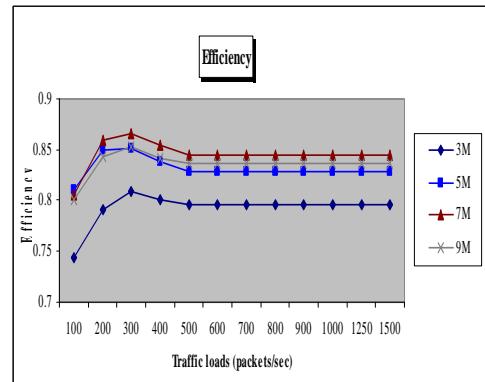


Figure 7: The efficiency of EADARP vs Traffic Load

5.2 Total number of control packets

Figure 8 illustrates the total number of control packets transmitted by EADARP under different network traffic loads using a variable channel capacities. EADARP has approximately the same total number of control packets under different network traffic loads using different channel capacities, and it shows the same behavior under a variable channel capacity, since it begins with a smaller total number of control packets at the beginning of the simulation at a traffic load of 100 packets/second, the total number of control packets increases as the network traffic load reaches 500 packets/second and this number becomes fixed between network traffic loads ranging from 500 packets/second to 1500 packets/second. We can interpret from the above figure that increasing channel capacities has no effect on the total number of control packets transmitted.

This was expected due to the fact that changing the channel capacity does not affect the protocol operation, since the total number of control packets transmitted during the simulation depend upon the protocol steps not on the environment in which the nodes reside.

5.3 Total power consumed

Figure 9 illustrates the total power consumed during packets' transmission in EADARP under different traffic loads using a variable channel capacities. EADARP performance under different traffic loads using a variable channel capacities is the same, because it begins with a smaller value for the total power consumed when the traffic load is 100 packets/second, then this value increases when the traffic load reaches 500 packets/second, and then it becomes fixed between traffic loads ranging from 500 packets/second to 1500 packets/second. EADARP with a channel capacity of 3 Mbytes

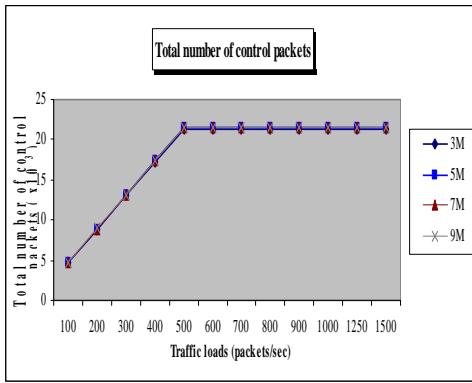


Figure 8: The total number of control packets vs Traffic Load

consumes more power, followed by 5 Mbytes, then by 7 Mbytes, and finally by 9 Mbytes, this means that EADARP with smaller channel capacities leads to more power consumption, but in general, the differences in EADARP power consumption under different traffic loads using variable channel capacities are not very big.

This was expected due to the fact that increasing the channel capacity makes packets' transmission easier in the network, thus a little less effort is done during the transmission due to reduced collisions, retransmissions and TTL expired, thus causing a reduction in the total power consumed during the simulation.

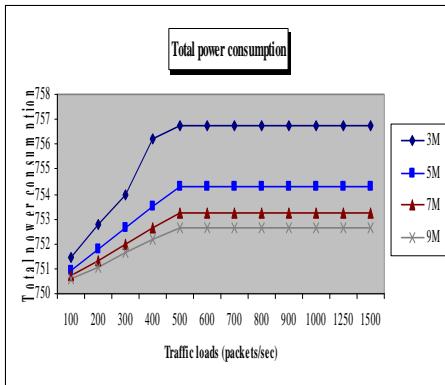


Figure 9 The total power consumed vs Traffic Load

5.4 Total number of collisions

Figure 10 illustrates the total number of collisions in EADARP under different network traffic loads using different channel capacities. EADARP has approximately the same total number of collisions under different network traffic loads ranging from 100 packets/second to 1500 packets/second using variable channel capacities. It performs in the same manner when using different channel capacities, because it begins with a lower number of collisions when the traffic load is 100 packets/second and ends with a higher number of collisions when the traffic load reaches 500 packets/second and becomes fixed between traffic loads ranging from 500 packets/sec to 1500 packets/sec. There is a reduction in the total number of collisions when increasing the channel capacity respectively from 3 Mbytes to 9 Mbytes, but, in general the change in the total number of collisions is not so great.

This was expected due to the fact that increasing the channel capacity result in packets' transmission more easily inside the network, thus resulting in a lower possibility of packets to collide, and in a smaller number of collisions.

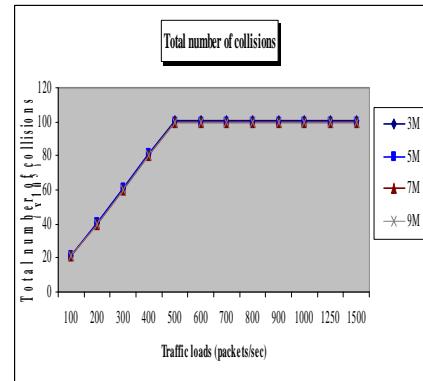


Figure 10: The total number of collisions vs Traffic Load

5.5 Total number of unreachable nodes

Figure 11 illustrates the total number of unreachable nodes during packets' transmission in EADARP under different network traffic loads using different channel capacities. EADARP has zero unreachable nodes under different network traffic loads ranging from 100 packets/second to 1500 packets/second using varying channel capacities: 3 Mbytes, 5 Mbytes, 7 Mbytes and 9 Mbytes. EADARP performance shows that varying channel capacities has no effect on the total number of unreachable nodes.

This was expected due to the fact that increasing the channel capacity does not have an effect on the total number of unreachable nodes, since the channel capacity does not change neither the protocol operation nor the effective traffic load being transmitted.

5.6 Total number of TTL expired

Figure 12 illustrates the total number of TTL expired during packets' transmission in EADARP under different network traffic loads using different channel capacities. The total number of TTL expired is very close using different channel

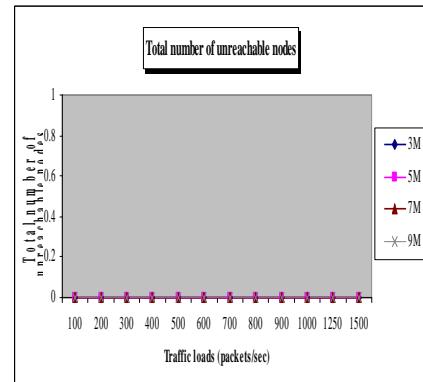


Figure 11: The total number of unreachable nodes vs Traffic

capacities in the first three cases, but the channel capacity of 9 Mbytes has the lowest number of TTL expired. EADARP shows similar performance under different network traffic loads using different channel capacities, because it begins with a lower number of TTL expired at a traffic load of 100 packets/second and this number increases as the traffic load reaches 500 packets/second and becomes fixed from network traffic loads ranging between 500 packets/second to 1500 packets/second.

This was expected due to the fact that increasing the channel capacity has not a great effect on the total number of TTL expired, since channel capacity does not change the effective traffic load. But in general, bigger channel capacity makes packets' transmission easier, then resulting in a smaller number of TTL expired, as in the case of the channel capacity of 9 Mbytes.

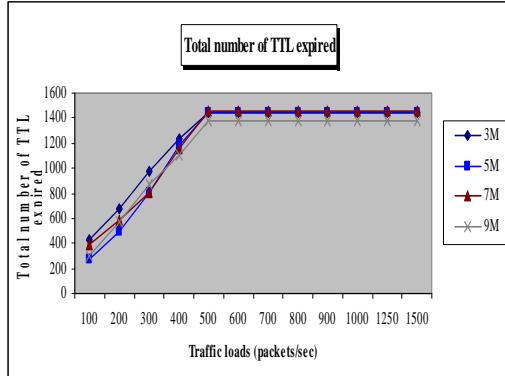


Figure 12: The total number of TTL expired vs Traffic Load

6. CONCLUSION

EADARP is an Energy Adaptable Distance Aware Routing Protocol (EADARP) for wireless mobile ad hoc networks is developed to improve basic performance metrics for multicast protocols . This paper investigates the effect of changing packet size and channel capacities on the performance of EADARP . Simulation program was developed using Glomosim to study such effect The results showed that a bigger packet size consumes more energy, and that a bigger packet size leads to less TTL expired, also smaller channel capacity leads to more power

REFERENCES

- D. Darwish , I. Sarwat, and A. Hassan , “ An Energy Efficient Dynamic Routing Protocol for ad-hoc wireless networks ” , AUEJ journal ,vol. 11 , No. 4 , September 2008 , pp. 543-570
- C. Diot, W. Dabbous and J. Crowcroft , “Multipoint communication: A survey of protocols, functions and mechanisms ” , IEEE Journal on Selected Areas in Communications vol.15, No. 3 , April 1997 , pp. 277–290.
- C.-C. Chiang, M. Gerla and L. Zhang , “Forwarding Group Multicast Protocol (FGMP) for multihop, mobile wireless networks, Cluster Computing vol. 1 ,No.2 , 1998,pp. 187-196.
- J. Xie, R. Talpade, T. McAuley and M. Liu , “ AMRoute: Ad hoc multicast routing protocol ” , ACM Mobile Networks and Applications (MONET) Journal vol.7 ,No.6 ,2002, pp. 429-439.
- L. Xiao, A. Patil, Y. Liu, L.M. Ni and A.H. Esfahanian, “ Prioritized overlay multicast in mobile ad hoc environments ” , IEEE Computer vol. 37 , No. 2 , 2004.
- Z. zhang , “Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges ” , IEEE communications, 1st quarter vol. 8, no. 1 , 2006
- H.Hass , J.Halpern and L.Li , “ Gossip-Based Ad-hoc routing ” IEEE/ACM Transactions on Networking , vol.14 , no.3 , June 2006 , pp: 479-491 .
- B.Biskupski ,J.Dowling and J.Sacha , “ Properties and mechanisms of self organizing MANET and P2P Systems ” , ACM Transactions on Autonomous and Adaptive systems , vol. 2 ,no. 1 , March 2007 , pp:1-34
- L.Lin , N.Shroff and R.Srikant , “ Asymptotically optimal energy aware routing for multihop wireless networks with renewable energy sources ” , IEEE/ACM Transactions on networking , vol. 15 , no. 5 , October 2007 , pp: 1021 – 1034
- C.-C. Chiang, M. Gerla and L. Zhang , “ Forwarding Group Multicast Protocol (FGMP) for multihop, mobile wireless networks ” , Cluster Computing vol.1, No.2, 1998 , pp. 187–196.
- M.S. Corson and S.G. Batsell, “ A Reservation-Based Multicast (RBM) routing protocol for mobile networks: Initial route construction phase ” , Wireless Networks vol.1 ,No.4 , December 1995 , pp. 427–450.
- P.Santi , “ Topology Control in wireless Ad-hoc and sensors networks ” ACM Computing surveys , vol.37 , no.2, June 2005 , pp: 164-194
- M. Grossglauser and M. Vetterli, “Locating Nodes with EASE: Mobility Diffusion of Last Encounters in Ad Hoc Networks,” INFOCOM, 2003
- M. Gerla, C.-C. Chiang and L. Zhang , “ Tree multicast strategies in mobile, multihop wireless networks ” , Mobile Networks and Applications vol. 4 , No.3 ,October 1999 , pp. 193–207.
- T. Ozaki, J.B. Kim and T. Suda , “ Bandwidth-efficient multicast routing protocol for ad-hoc networks ” , in: *Proceedings of IEEE ICCN'99*, Boston, MA ,October 1999, pp. 10–17.
- A.Michail and A.Ephremides , “ Energy Efficient routing for connection oriented traffic in wireless ad-hoc networks ” , Mobile Networks and Applications , vol. 8 , 2003 , pp: 517-533
- E.Sun Jung and N.Vaidya , “ A power control MAC protocol for Ad-hoc networks ” , Wireless networks , vol.11 , 2005 , pp: 55 – 66
- G. Jorjeta , H. Jetcheva and B. Johnson: “Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks”, In *Proc. of the 2nd ACM International Symposium on Mobile and Ad-hoc Networking & Computing (MobiHOC)*, Long Beach, CA, October 2001, pages 33 - 44
- Chao Gui and P. Mohapatra , “ Overlay multicast for MANETs using dynamic virtual mesh ” , Springer Science and Business Media, LLC 2007, May 2006
- S. guo and O. yang , “ A Constraint Formulation for Minimum-Energy Multicas Routing in Wireless Multihop Ad-hoc Networks ” , Springer Science and Business Media Inc., wireless networks vol.12, No.3 , 2006 , pp. 23-32.
- C Tang , S . Cauligi, And R.Vendra, “ Energy Efficient Adaptation of Multicast Protocols in Power Controlled Wireless Ad Hoc Networks ” , Mobile Networks and Applications vol..9 , 2004, pp. 311-317.
- Elizabeth M. Belding-Royer and Charles E. Perkins, “ Transmission Range Effects on AODV Multicast Communication ” , published in 2002 Mobile Networks and Applications vol. 7 , 2002 , pp. 455-470.
- Z. Li, B. Li , and L. Lan “ On Achieving Maximum Multicast Throughput in Undirected Networks ” , IEEE transactions on information theory, vol. 52, No. 6, June 2006, pp. 24- 37.
- C. Perkins ; E. Belding-Royer and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561, IETF Network Working Group July 2003
- D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, vol. 35, No. 3, 1996
- J. Garcia and E.L. Madruga, “The core-assisted mesh protocol”, IEEE Journal on Selected Areas in Communications vol.17,No.8 , August 1999, pp. 1380–1394.
- Dina Darwish ,Imame Saroit and Abdelwehab Hassan , “ Energy Adaptable Distance Aware Routing Protocol for Multicast Wireless ad hoc Networks ” , to appear in International journal of Information and Intelligent Computing .
- .Glomosim User Manual, <http://pcl.cs.ucla.edu/projects/glomosim>.
- R. Meyer and R. Bagrodia, “PARSEC User Manual Release 1.1,” January 1999, <http://pcl.cs.ucla.edu/>.
- T. Rappaport, “ Wireless Communications: Principles and Practice” Prentice Hall, 1995.

Improving BGP Convergence Time via MRAI Timer

Abdelshakour Abuzneid and Brandon J. Stark, *Member, IEEE*

Abstract- The Border Gateway Protocol (BGP) is the path vector protocol that routes inter-domain traffic, connecting Autonomous Systems (AS's) together to form the decentralized backbone of the Internet. In the event of a network failure, BGP can take minutes to converge under default settings. With the route withdrawal rate limit (WRATE) change in the new BGP specification, the effect of the Minimum Route Advertisement Interval (MRAI) timer on convergence time needs to be re-evaluated. This paper shows that the reduction of the MRAI timer remains critical to the improvement of BGP convergence time. This paper also shows that while WRATE is not effective in improving convergence time, it reduces the number of transient loops and messages on the network at the optimal MRAI value.

Index Terms— BGP, routing convergence, optimal timer.

I. INTRODUCTION

The Border Gateway Protocol (BGP) [1] is the path vector protocol that is the inter-domain routing protocol of the Internet. The BGP connects smaller Autonomous Systems (AS's) together which provides the decentralized backbone to the Internet. These AS's are connected together with multiple point to point connections but rarely in a complete full-mesh topology. It then becomes critical that packets are routed correctly and quickly from AS to AS. However, there are many factors that can lead to a delay in convergence time. In the BGP routing protocol, each node contains a list of the entire best path to a particular destination node, as well as a handful of alternate paths. In the case of a topology change, due to a policy change or either a failed link or node, if the current best path becomes invalidated, the node will switch to the next best path. Occasionally, this new path is far from ideal and may be unstable due to an unintentional loop. Packets will be caught in this loop until the paths are discarded, a process that may add a substantial delay in BGP convergence time.

While the path vector routing protocol allows each node to check for a loop in the advertised path, transient loops formed

by inaccurate path information are harder to detect or prevent quickly. Though there have been many studies on improving BGP convergence time by improving the efficiency of routing protocols [2,5,6,8], there has been evidence that the duration of transient loops are proportional to BGP convergence time [4]. There have been a handful of algorithms proposed to reduce transient loops [4,7,10], though they are very rarely implemented in real-world settings.

One of the methods for improving BGP convergence time that has been studied is the reduction of the Minimum Route Advertisement Interval (MRAI) timer [2,4,5,6]. Its has been shown that reducing this timer from the default value of 30 seconds to a much lower value around 2-5 seconds has been effective for both a single node failure [2,4] as well as for larger failures [5]. The MRAI timer limits the BGP route advertisements each node sends out to each peer in order to prevent the network from being overloaded with messages as well as to prevent frequent oscillations of routes from a large influx of varying route update messages. In addition to route update messages, the recently published official BGP4 protocol specification RFC 4271 now suggests that route withdrawal messages are also to be limited by the MRAI timer [1]. This is a significant departure from the previous iteration of the BGP protocol where route withdrawal messages were able to be sent instantaneously.

With this new change in the functionality of the MRAI timer, the effectiveness of the MRAI timer adjustment must be examined. The primary recipient of this change is likely to be in the loop detection or prevention algorithms, where the route withdrawal messages were frequently used to alert nodes to topology changes [4,7,10]. This paper examines the effect that the reduction of the MRAI timer route has on convergence time and loop detection and removal in conjunction with the addition of the withdrawal rate limit (WRATE) in the BGP specification RFC 4271 [1].

The remainder of the paper is organized as follows. Section II reviews previous studies and conclusions on improving BGP convergence time and routing loops. Section III discusses in detail on the topic of routing loops, including the formation and duration of such loops. Section IV presents the simulation tools and design metrics. Section V examines the simulation results. Section VI contains the concluding remarks followed by references.

Manuscript received April 15, 2008.

F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (corresponding author to provide phone: 303-555-5555; fax: 303-555-5555; e-mail: author@ boulder.nist.gov).

B. Stark, is with the University of Bridgeport, Bridgeport, CT 06604 USA. (e-mail: bstark@bridgeport.edu).

II. PREVIOUS RESEARCH

The BGP convergence delay is a significant issue because BGP is the backbone of the Internet. In [8], Labovitz et al., point out that the average delay in Internet traffic due to failed nodes is around 3 minutes in addition to a high percentage of packet loss. In its previous iteration, the BGP protocol was shown to be unequipped to handle the increasing demands of the emerging QoS and VoIP standards. It became clear that more research was needed to improve the BGP protocol to meet the new demands. In following studies [2,5], it is noted that convergence time is decreased remarkably by adjusting the MRAI timer to around 5.0 seconds. However, these simulations were run on a full-mesh topology known as a clique (Figure 2). While it is pointed out as a worst case model [2] due to its numerous alternate paths, it is not an accurate model for the complexity that is the current Internet infrastructure. In addition, due to its full-mesh topology, few if any transient loops are formed. Nonetheless, it is shown that the MRAI timer has the most significant effect on convergence time [2]. Further studies have demonstrated that the optimal MRAI time is dependent on the size of the topology and the number of failed node and/or links [5]. It is important to note that all of these previous studies were conducted under the older BGP specifications. With the changes enacted by the latest BGP specification, it is evident that the MRAI timer is even more critical to the convergence time in BGP.

The relevance of routing loops to convergence time has been previously demonstrated by Pei et al. [4], depicting that the duration of transient loops are proportional to the BGP convergence time. Routing loops have been documented for many years [4], but little research was done on the underlying cause until only in the past couple of years. While the path vectoring routing in BGP was designed against persistent routing loops, little has been done to safeguard against transient loops. Transient loops are significantly harder to detect due to its formation from the dynamic routing changes [9]. The formation of a transient loop is dependent on the remaining topology as opposed to an error in protocol. A few proposed algorithms include Assertion Approach [4], Ghost Flushing [10], Anti-Loop Probing [7], and Sender Side Loop Detection [2,4].

III. ROUTING LOOPS

Figure 1(a), 1(b) and 1(c) demonstrate the formation of a transient loop using the BGP protocol. Given that all packets are to be routed from node 6 to node 0, the best path at node 6 is obviously the path (6 5 0), which is marked with an *. In addition, all other nodes also contain their best path towards node 0. In the case of node 4, this path is (4 5 0), however in its routing table, it does include alternate pathways including (4 3 2 1 0). In the case that the link from node 5 to 0 breaks, node 5 alerts its neighboring nodes 6 and 4 by withdrawing the current best path that includes node 5. Node 6 changes its

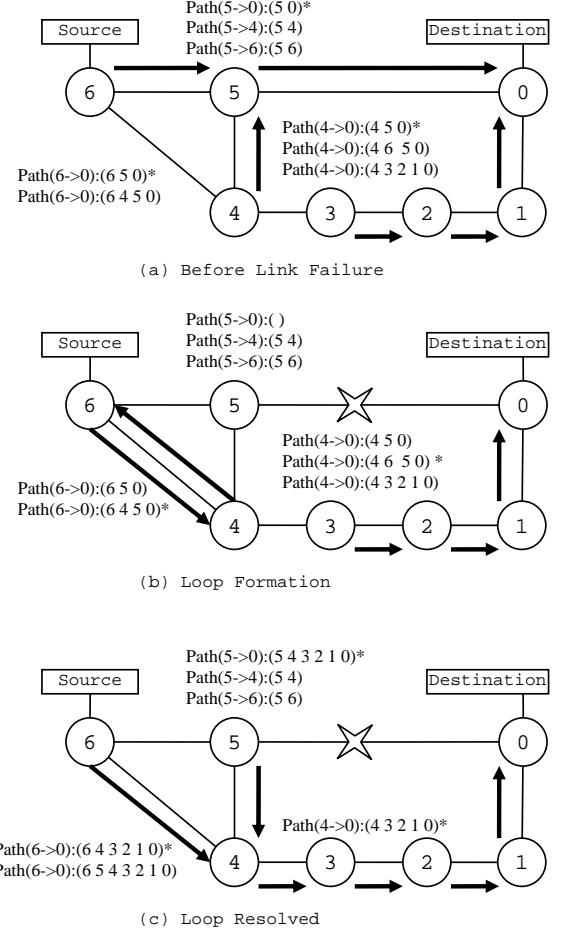


Fig. 1. Loop Formation and Resolution

best path to (6 4 5 0), while node 4 changes to path (4 6 5 0) [4].

While both nodes are aware that they cannot expect packets sent directly to node 5 to make it to node 0, they are unaware that they are sending each other packets whose path has been invalidated. In this simple case, the loop is quickly discovered when node 6 and node 4 send withdrawal messages to each other informing that the next best path is invalid. The best path for node 4 becomes (4 3 2 1 0), which is a stable path. Node 4 then advertises this new path to node 5 and 6 and the network finally converges. In practice, however, loops are much larger. This particular case converges before any MRAI timer expires, making it inadequate for simulation purposes. After node 5 sends withdrawal messages to node 6 and 4, it does not need to send any more out. Node 4 and 6 both send withdrawal messages, however only node 4 is required to send out any more messages. However, because the withdrawal message is directed to node 6, and the subsequent

advertisement message updates the path to node 0, they are not on the same MRAI timer. The MRAI timer is set to limit route advertisement and route withdrawal messages on a per destination basis [1,4].

In the previous simple example, the loop was resolved quickly with just the standard BGP protocol using withdrawal messages. However, this method has been shown to be less than ideal in the case of more complex topologies [2, 4, 5, 7, 10]. As a result, more advanced loop detection or prevention techniques have been studied.

The Assertion Approach [4] improves loop detection by allowing each node to check paths for known invalidated pathways. This technique has been shown to be effective in simulation [4]. Unfortunately, it has not been implemented in any commercial BGP routers as of yet. With the BGP specification change limiting the rate of withdrawal messages, it is likely that this technique may not be as effective.

Another algorithm likely to not be as effective due to the BGP specification change is known as Ghost Flushing [10]. This also relies on sending withdrawal messages as quickly as possible to remove invalidated path information. This technique has been demonstrated to be effective in simulation [4, 10], but has not been implemented outside of academia.

A more aggressive form of loop detection was proposed as Anti-loop Probing [7]. In this technique, upon the withdrawal of path, a specialized probe message travels down the next best path searching for a loop. If a loop is found, the path is invalidated with another withdrawal message. This technique may not be as affected by the new BGP specification change as the previous two techniques. However, like the other two, this technique has yet to see an implementation outside of the lab.

It becomes quite apparent that while these techniques may be effective, they are of little use if they are not implemented in real-world BGP routers. Currently, there are no high profile routers or routing software that implements any of the previous techniques. However, there has been a significant enough of a following for a technique known as Sender Side Loop Detection (SSLD) [2,4,8]. In SSLD, before a node advertises a path, it checks to see if the receiver is present in the path, indicating a loop. In the previous routing example, after the link [5 0] fails, node 4 and 6 receive withdrawal messages from node 5. Node 4 switches to its next best path [4 6 5 0] and will advertise it to node 5, as per the path vector algorithm. With SSLD, before node 4 advertises the path, it will notice that node 5 is in the path and instead of advertising the loop, it will instead send a withdrawal message to prevent the transient loop. Due to its simple algorithm and its presence in the common BGP simulation tool SSFNet [3], it is the most likely to be implemented in the future. As such, this is the technique that this paper will examine in conjunction with the new BGP specification.

IV. METHODOLOGY

SSFNet [3] is a comprehensive network simulation tool, capable of simulating large BGP networks. The BGP

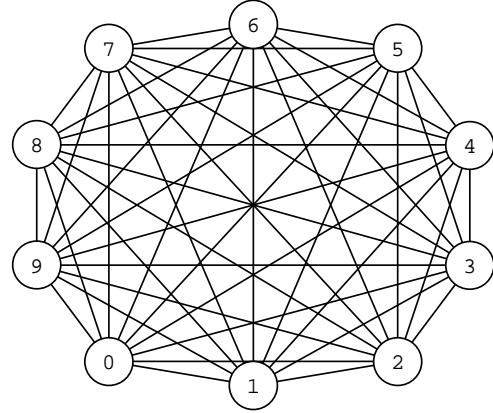


Fig. 2. Clique Topology, Size 10 (Topology 1)

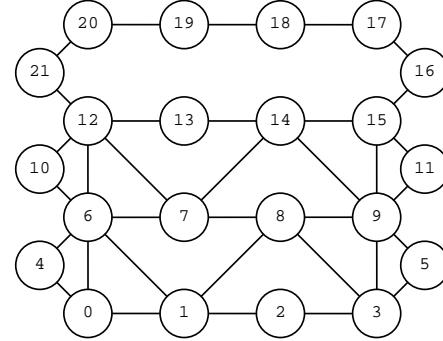


Fig. 3. Custom topology with long backup path (Topology 2)

implementation found in this simulation however is based on the older BGP-4 specification found in RFC 1771. While not all the new specification changes could be immediately implemented, the ability to implement WRATE is available as well as SSLD.

In SSFNet, a network is created manually then simulated for a specified running time. Each router may be auto-configured to typical default settings or manually configured giving the user precise control over each router. The network topology, however, must be manually designed and constructed by specifying exact ports on each router form a particular link. During a simulation run, the specific remarks about each router, including when they send or receive route advertisement or withdrawal messages may be selected to be outputted to a text file. SSFNet also provides the ability to use random number stream seeds, which allow reproducibility. This is particularly important in this simulation as they are used in the MRAI jitter and the average CPU delays.

Additional simulation specifications include setting the link delay to 2 ms and the CPU processing delay to a uniform

distribution between .1 and 1.0 second. While some routers may implement MRAI timer on a per-node basis, this simulation implemented the MRAI timer on a per-destination basis, as suggested in the BGP-4 specification [1].

The simulations are broken down into two parts. The first will demonstrate whether the convergence time improves with the implementation of WRATE and SSLD. In order to do this, two networks will be used. The first topology is a clique (Topology 1, Fig. 2) with size 10. This is to verify our results with previous research [2,4,8]. The second topology is a custom designed topology (Topology 2, Fig. 3), designed to intentionally create loops of varying sizes. In this topology, this paper simulates the event of a failure at node 21. The convergence time is recorded as the time it takes for all nodes to have stable paths after a node failure.

The second part explores the effectiveness of SSLD and WRATE with the optimal MRAI adjustment. Using Topology 2 (Fig. 3), the number of loops created at each route change at each node is counted. This involves counting the number of times a node advertises a particular path that is unstable at the next hop and resulting in a loop.

V. RESULTS

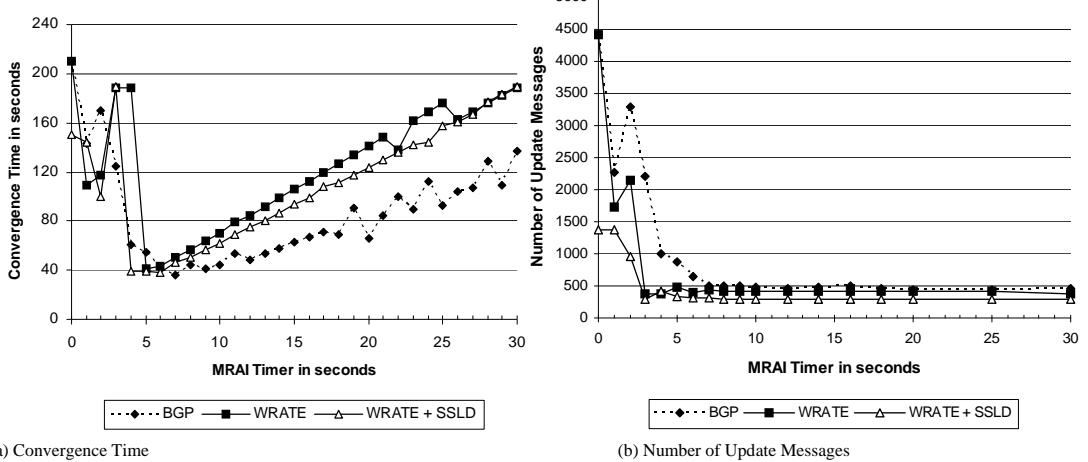
The effect of the MRAI timer on convergence time, as noted in previous research [2,4,5,8], is significant in reducing convergence time in both topologies. The results from Topology 1 can be seen in Figure 4, while the results from Topology 2 can be seen in Figure 5. Convergence time is longer in Topology 1 as expected [2,4,8] due to the significant number of alternate routes. However, both simulation topologies show that the optimal MRAI time for these topology sizes is approximately 5 seconds and increasing as the MRAI time increases. While the convergence time at

MRAI = 5 seconds is roughly the same for the old BGP specifications, BGP with WRATE and BGP with both WRATE and SSLD, it appears that the inclusion of WRATE has a negative impact on convergence time elsewhere. This is consistent with findings from [2,4], where it is shown that WRATE is ineffective when using the default value for MRAI. These results indicate that the MRAI timer change is more critical to improving convergence time than the newer BGP-4 specification with WRATE or the use of SSLD.

However, using WRATE or SSLD is not without its benefits. The number of messages sent by the nodes with WRATE and WRATE + SSLD was uniformly lower than the older BGP-4 specification, as were the number of loops. While the time for the all the new paths to be stable may not have decreased, packets sent while the paths were unstable would likely have reached their destination quicker. The addition of WRATE prevents rapidly changing alternate pathways which often led to the creation of new loops. SSLD decreased the number of loops even further when combined with WRATE.

Figure 5 depicts the results from the simulation of Topology 2. At MRAI = 5 seconds, the convergence time for all three BGP implementations is roughly 40 seconds, well below the convergence time when MRAI = 30. However, this topology is not a good evaluation of convergence time due to its limited number of alternate paths. Many of the loops found in this topology were centered on nodes 6,7,10 and 12 as they forwarded packets to each other before the long backup path route was advertised. In the cases where MRAI > 5 seconds, the addition of WRATE prevented unstable paths to these nodes from being withdrawn in a timely manner, explaining why the convergence time with WRATE was longer than without.

The results from the simulation with Topology 1 (Fig. 4) provide more insight into the effectiveness of WRATE.



(a) Convergence Time

(b) Number of Update Messages

Fig. 4. Convergence Time and Number of Update Messages in Topology 1 (Clique, Size = 10).

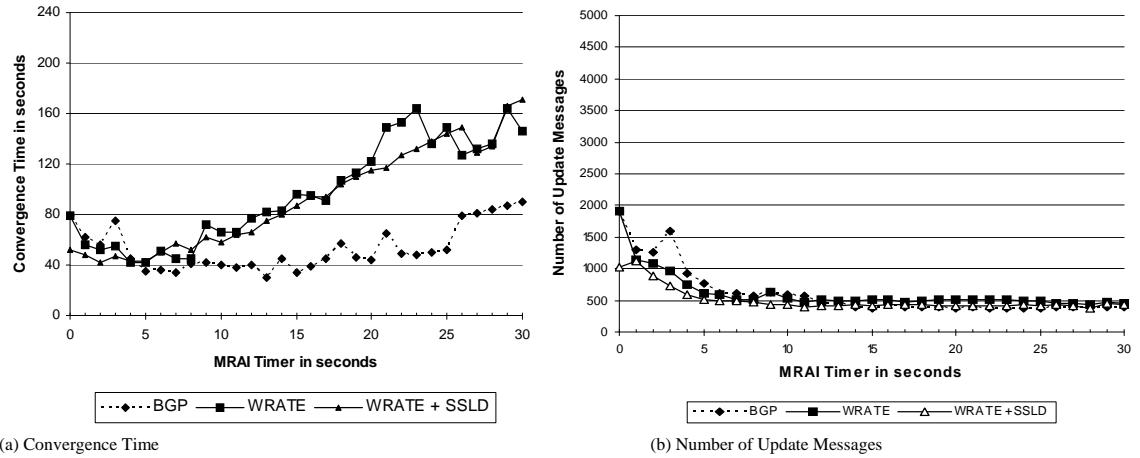


Fig. 5. Convergence Time and Number of Update Messages in Topology 2.

While the WRATE implementation again performs poorly when $MRAI > 5$ seconds, the results are closer, indicating that WRATE is more effective with larger amounts of alternate paths. Intuitively, this appears accurate. WRATE suppresses the nodes from changing alternate paths too quickly which disrupts packet routing. The addition of SSLD appears to have little effect on convergence time on both topologies.

However, the biggest difference between these implementations in this part of the simulation is the number of messages sent. In both topologies, the implementations with WRATE had a consistently lower number of route advertisement update messages sent. For $MRAI = 5$, this difference is even more pronounced, lowering it by almost half. Although reducing the number of messages on the network had little effect on convergence time in these simulations, it would likely have a more significant effect in real-world applications.

The results from the second part of the simulation (Fig. 6) depicts the number of loops detected when $MRAI = 5$

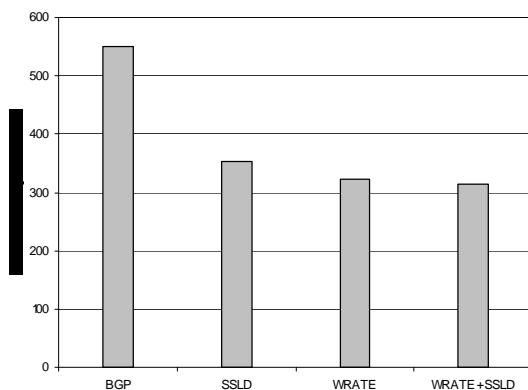


Fig. 6: Number of Loops, $MRAI = 5$

seconds. In the older implementation of BGP without WRATE or SSLD, there were a significant number of forwarding loops found. Loops were counted manually by examining the path a node directs a packet and determining whether or not the aggregate path directed from the nodes would form a loop. The implementation of BGP with SSLD indicates that SSLD is effective at preventing loops from forming by preventing packets from being sent to where they might form a loop. WRATE was also effective in preventing the formation of loops, although as a result of preventing frequent path changes as opposed to actively searching for and suppressing loops. The combination of the two implementation shows an improvement in loop prevention, however not a significant one.

VI. CONCLUSION

The results of these simulations depict that while the convergence time decreases with the reduction of the MRAI timer, the addition of WRATE or the use of SSLD has little effect on convergence time. However, the inclusion of WRATE and SSLD does reduce the number of BGP messages sent on the network as well as the number of transient loops. While these changes may not be noticeable on convergence time, they do show an improvement in the efficiency of BGP. A reduced number of messages sent by routers running BGP may ease network congestion both by saving valuable bandwidth and by reducing the processing delay at the router. While the network may still be unstable, this increases the likelihood that a packet sent will reach its destination in a timely manner.

It would be worthwhile to do further research into this topic. A simulation could be set up to explore the time it takes for a packet to reach its destination immediately following a node failure. While convergence time maybe

unaffected by WRATE or SSLD when the MRAI timer is optimized, packet arrival time may be. Other improvements to this research also include determining better topologies for the purposes of artificially creating loops for study. Research has indicated that transient loops are random events and are hard to study [4,7,8,9] however they are affected by the network topology [4,9]. Currently the idea of the creation of a long backup chain is the only topology to invoke a loop, however this is only one possibility of loop creation. It is likely that there are more situations that lend to the creation of transient loops.

This paper suggests that while the addition of WRATE increases the efficiency of BGP, that reducing the MRAI timer to an optimal value is the most effective way to reduce convergence time. It also suggests that the effectiveness of WRATE is at its greatest at this optimal MRAI value. In addition, SSLD had little affect on convergence time or number of loops and thus may not be necessary in light of the addition of WRATE in the new BGP-4 specification.

REFERENCES

- [1] Y. Rekhter and T. Li, "Border Gateway Protocol 4," RFC 4271, Jan. 2006
- [2] T.G. Griffin and B.J. Premore, "An Experimental Analysis of BGP Convergence Time," in Proc. ICNP 2001.
- [3] "SSFNet: Scalable Simulation Framework". [Online] Available: <http://www.ssfnet.org>
- [4] D. Pei, X. Zhao, D. Massey, and L. Zhang, "A Study of BGP Path Vector Route Looping Behavior," in Proceedings of ICDCS 2004.
- [5] A. Sahoo, K. Kant, and P. Mohapatra, "Improving BGP Convergence Delay for Large-Scale Failures," in Proceedings of ICDSN 2006.
- [6] R. Viswanathan, K. Sabnani, R. Holt and A. Netravali, "Expected Convergence Properties of BGP," in Proc. ICNP 2005.
- [7] L. Li, and C. Chen, "Anti-Loop Probing: Achieving Fast BGP Convergence," in Proceedings of AINA 2006.
- [8] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed Internet Routing Convergence," SIGCOMM 2000.
- [9] A. Sridharan, S. Moon and C. Diot, "On the Correlation between Route Dynamics and Routing Loops," in Proceedings of IMC 2003.
- [10] A. Bremer-Barr, Y. Afek and S. Schwarz, "Improved BGP Convergence via Ghost Flushing," in Proceedings of IEEE INFOCOM 2003.

Brandon J. Stark is a graduate student studying computer engineering at the University of Bridgeport, Bridgeport CT, USA. He received his bachelors of science in computer engineering at the University of California at Irvine, Irvine, CA, USA.

Error Reduction using TCP with Selective Acknowledgement and HTTP with Page Response Time over Wireless Link

Adelshakour Abuzneid, Kotadiya Krunalkumar

{abuzneid, kkotadiy }@bridd deport.edu

Computer Science and Engineering Department

University of Bridgeport

Bridgeport, CT 06604

Abstract: This paper evaluates error reduction in wireless communication networks. We have reviewed selective acknowledgement schemes to provide reliable end-to-end communication on wireless-link. TCP (Transport control protocol) has poor performance over wireless-link. Due to high error rate, page response time (sec), and retransmission count over wireless-link. We present a scheme to improve performance using TCP/IP compression, fast retransmission and fast recovery new Reno techniques which directly decreases selective-acknowledgement, page response-time, and retransmission count.

I – INTRODUCTION

In recent few years we witness tremendous evolution in communication technologies both in hardware and software. This rapid progress has made it possible the birth of mobile computing. The popularity of laptop computers, cellular phones, and other mobile devices are growing day by day. Wireless communication will be an integral part of future networks. The increasing role of mobile computing in our life has produced vast deal of research in this area. However, it is very important to note that wireless network, which is widely used nowadays, have fundamentally different characteristics than wired networks. The low bandwidth, high error rates, burst and time-varying, caused by the noisy transmission environment, are only basic features of wireless links [1]. TCP is widely used transport layer protocol and it is connection-oriented protocol.

This paper represents the performance of TCP with selective-acknowledgement over HTTP. We are concerned with page response time (sec) and retransmission count over wireless link. In section

II, we present a simple overview of various commonly used techniques for error control over wireless link. Such as analyzing TCP with selective-acknowledgement enabled, fast-retransmission disabled and fast-recovery disabled over wireless link. We use OPNET IT GURU (as simulation software / tool). Primary results are presented in section III. Section IV presents our implementation in which we enable selective-acknowledgement, TCP/IP compression, fast-retransmit, and fast-recovery (New-Reno) showing how doing such can help improving the performance over wireless link.

II - RELATED WORK

A. Selective Acknowledgment (SACK)

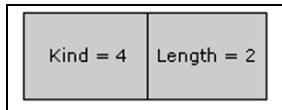
Selective Acknowledgment (SACK) is a strategy which corrects multiple dropped segments. With (SACK) the data receiver can inform the sender about all segments that have arrived successfully, this implies the sender needs to retransmit only the segments that have actually been lost.

The (SACK) extension uses two TCP alternatives. The first is an enabling option, "SACK-permitted", which may be sent in a SYN (Synchronization) segment to indicate that the SACK option can be used once the connection is established. The second is the SACK option itself, which may be sent over an established connection once permission has been given by SACK-permitted. The SACK option is to be included in a segment sent from a TCP that is receiving data to the TCP that is sending that data; we will refer to these TCP's as the data receiver and the data sender, respectively. We will consider a particular simplex data flow; any data flowing in the reverse direction over the same connection can be treated independently.

SACK-Permitted Option:

This two-byte option may be sent in a SYN by a TCP segment that has been extended to receive (and presumably process) the SACK option once the connection has opened. It must not be sent on non-SYN segments.

TCP Sack-Permitted Option:



Sack Option Format:

The SACK option is to be used to convey extended acknowledgment information from the receiver to the sender over an established TCP connection.

The SACK option is to be sent by a data receiver to inform the data sender of non-contiguous blocks of data that have been received and queued. The data receiver awaits the receipt of the data (perhaps by means of retransmissions) to fill the gaps in sequence space between received blocks. When missing segments are received, the data receiver acknowledges the data normally by advancing the left window edge in acknowledgement Number Field of the TCP header. The SACK option does not change the meaning of the Acknowledgement Number field.

TCP SACK Option:

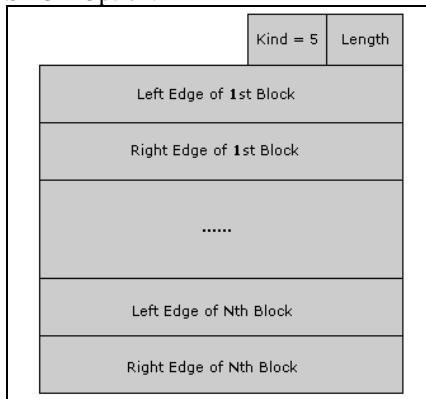


Fig- 1 Structure of Selective Acknowledgement

Each contiguous block of data queued at the data receiver is defined in the SACK option by two 32-bit unsigned integers in network byte order:

As shown in Figure-1, “Left Edge of Block” specifies the first sequence number of this block.

“Right Edge of Block” specifies the sequence number immediately follows the last sequence number of this block. *Each block represents received bytes of data that are contiguous and isolated; that is, the bytes just below the block, (Left Edge of Block - 1), and just above the block, (Right Edge of Block), have not been received.* A SACK option that specifies n blocks will have a length of $8*n+2$ bytes, so the 40 bytes available for TCP options can specify a maximum of 4 blocks. It is expected that SACK will often be used in conjunction with the timestamp option used for RTT (Round trip time), which takes an additional 10 bytes (plus two bytes of padding); thus the maximum of 3 SACK blocks will be allowed in this case.

This option contains a list of some of the blocks of contiguous sequence space occupied by the data that has been received and queued within the window. TCP with the Selective Acknowledgment option (TCP SACK) was originally designed to improve TCP recovery from busy congestion losses; it may also benefit the performance of the TCP over wireless links [1].

B. Fast Retransmit

Fast Retransmit is an enhancement to TCP which reduces the time a sender waits before retransmitting a lost segment. The TCP sender uses timer to recognize lost segments. If an acknowledgement is not received for a particular segment with a specified time (a function of the estimated Round-trip delay time), the sender will assume that the segment is lost in the network, and will retransmit the segment.

The fast retransmit enhancement works as follows: If the TCP sender receives three duplicate acknowledgements with the same acknowledgement number (that is, a total of four acknowledgements with the same acknowledgement number), the sender can reasonably be confident that the segment with the next higher sequence number is dropped, and will not arrive out of the order. The sender will then retransmit the packet that was presumably dropped before waiting for its timeout.

As an example, Slow Start and Congestion Avoidance:

Let $cwnd$ (congestion window) and $ssthresh$ (slow-start threshold) refer to the current congestion window size and the current slow start threshold,

respectively. It implies that $cwnd < ssthresh$, the receipt of a non-duplicate ACK results in $cwnd$ increasing by one segment. Thus, in the absence of segment loss, $cwnd$ doubles every round-trip time (RTT) until it reaches the slow start threshold value $ssthresh$. This algorithm is called the *slow start* algorithm [9]. This window evolution in which the congestion window size increases by about one segment every RTT is referred to as the *congestion avoidance* algorithm [9].

Fast Retransmit, Fast Recovery

During slow start or congestion avoidance, receipt of four back-to-back identical ACKs (referred to as “triple duplicate ACKs”) causes the sender to perform *fast retransmit* [10]. In fast retransmit, the sender does the following. First, the segment implicitly requested by the triple duplicate ACK is retransmitted. Second, $ssthresh$ is set to $cwnd=2$. Third, $cwnd$ is set to $ssthresh$ (new) plus 3 segments. Following these steps, the sender enters *fast recovery* [10, 11].

Once it is entered in to a fast recovery mode the sender continue to increase the congestion window by one segment for each subsequent duplicate ACK received. The intuition behind the fast recovery algorithm is that the duplicate ACKs indicate the reception of some segments by the receiver, and thus can be used to trigger the new segment transmissions. The sender transmits the new segments if it is permitted by sender’s congestion window.

TCP New Reno (unlike Reno) distinguishes between a “partial” ACK and a “full” ACK. A full ACK acknowledges all segments that were outstanding at the start of fast recovery, while a partial ACK acknowledges some but not all of this outstanding data. Unlike Reno, the New Reno retransmits the segment which is next in the sequence based on the partial ACK, which consequently result in the reduction of the congestion window by one less than the number of segments acknowledged by the partial ACK. This window reduction, referred to as *partial window deflation*, allows the sender to transmit new segments in subsequent RTTs of fast recovery. On receiving a full ACK, the sender sets $cwnd$ to $ssthresh$, which terminates the fast recovery, and resumes congestions avoidance.

C. TCP/IP Header Compression

TCP/IP Header Compression: is the data compression protocol described specifically to improve the TCP/IP performance over slow serial links developed by the Van Jacobson this compression reduces the normal 40 byte TCP/IP packet headers down to 3-4 bytes for the average case. It does this by saving the state of TCP connections at both ends of the link, and only sending the differences in the header fields that change. This makes the big difference for interactive performance on low speed links, although it has noting to do with anything about the processing delay inherent to most dialup modems [8].

III. METHODOLOGY



Fig-2 Simulation Topology

We have initially discussed the SACK over wireless network, in which we have used Hypertext Transfer Protocol (HTTP) built on top of the TCP and served our purposes. We have transferred 1 MB file at a time over a could which represent a WAN (IP-capable) that supports up to 32 serial links. In the cloud, we set the packet-discard-ratio to 1% which means that 1 in 100 packets will be discarded as they pass through the WAN. We set Packet latency to 0.25 seconds which means that the round-trip delay will be at least of 0.5 seconds. PPP_DS1 link is used to connect the HTTP client to the cloud and then to the server. The PPP protocol is commonly used for long-distance links with the DS1 speed of 1.5Mbps. The maximum segment size set to 512 bytes which will ensure that each TCP packet sent is 512 bytes long and it's buffer size is 8764 [4]. We analyze the results of SACK (using the parameters above), the page-response-time (download time) and retransmission count over wireless link.

Figure-3 shows retransferred packets. Figure-4 shows the page response time in which 1 Mb file takes 147 second time to reach at destination. Figure-5 shows the retransmission count. As

presented before, the cloud represents a WAN consisting of IP-capable that supports up to 32 serial links with the packet-discarded-ratio set to 1.0%. This implies packet latency of 0.25 seconds.

IV- SIMULATION IMPLEMENTATION

As presented earlier the transmission of 1 MB file at a time with 1% packet-discard-ratio resulted in decreased SACK by 48% and page-response-time by 65% and retransmission count .Figure-6 shows that we have to retransfer the shown packets. Figure-7 shows the page response time in which 1 Mb file takes 97 seconds to reach at destination. Figure-8 indicates the retransmission count. Figure-9 illustrates the comparison of Selective Acknowledgement and Figure-10 shows the comparison of Retransmission Count.

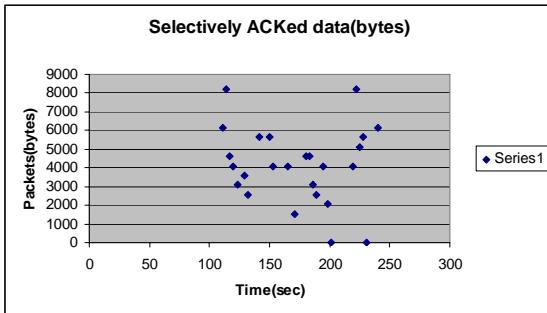


Figure 3 TCP with selective Acknowledgement

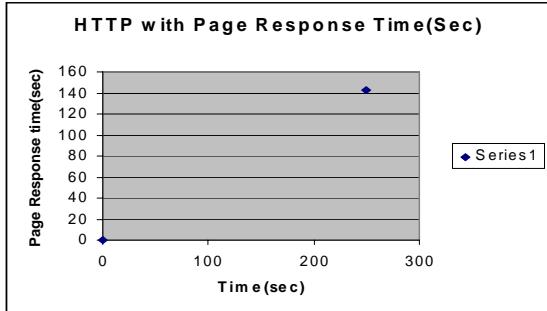


Figure 4 HTTP with Page Response Time (Downloading Time)

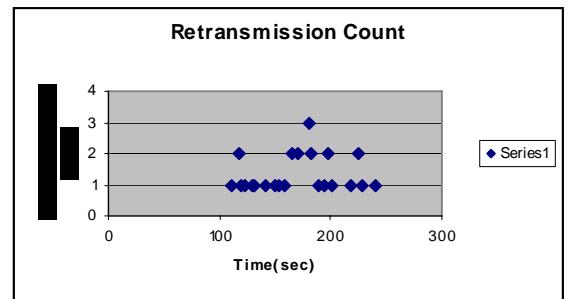


Figure 5 Retransmission Count

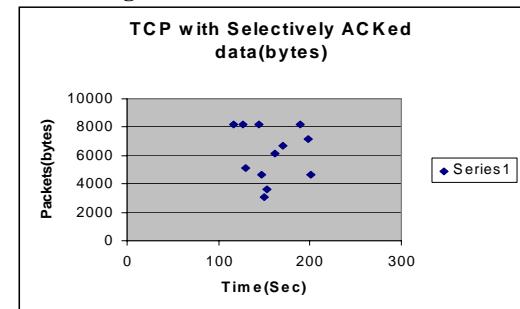


Figure 6 TCP with Selective Acknowledgement

Table 1: selective Ack data (bytes) as shown in Fig-3

Time(sec)	Selective Acknowledgement number
111	6144
114	8192
117	4608
120	4096
123	3072
129	3584
132	2560
141	5632
150	5632
153	4096
159	4096
165	4096
171	1536
180	4608
183	4608
186	3072
189	2560
195	4096
198	2048
201	0
219	4096
222	8192
225	5120
228	5632
231	0
240	6144

Table-2 Retransmission Count as shown in Figure-5

Time(sec)	Retransmission Count
111	1
117	2
120	1
123	1
129	1
132	1
141	1
150	1
153	1
159	1
165	2
171	2
180	3
183	2
189	1
195	1
198	2
201	1
219	1
225	2
228	1
240	1

Table-3 selective Ack data (bytes) as shown in Figure-6

Time (sec)	Selective Acknowledgement packet number
117	8192
126	8192
129	5120
144	8192
147	4608
150	3072
153	3584
162	6144
171	6656
189	8192
198	7168
201	4608

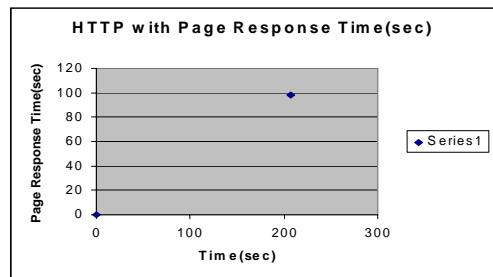


Figure-7 HTTP with Page Response Time (Downloading Time)

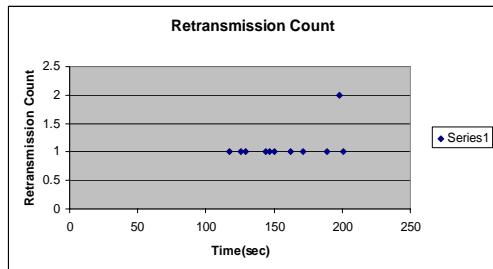


Fig-8 Retransmission Count

Table-4 Retransmission Count as shown in Figure-8

Time(sec)	Retransmission Count
117	1
126	1
129	1
144	1
147	1
150	1
162	1
171	1
189	1
198	2
201	1

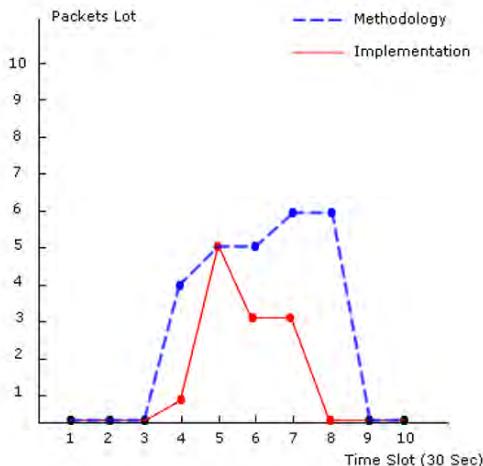


Figure-9 Comparison of Selective ACK

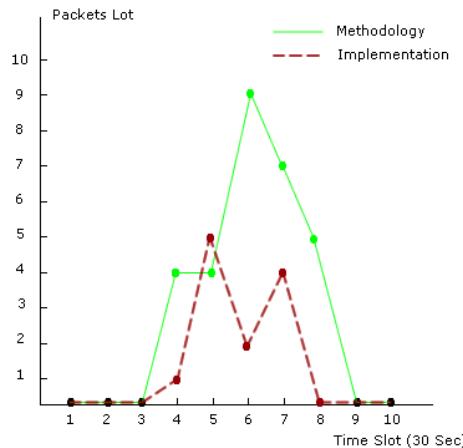


Figure-10 Comparison of Retransmission Count

V- CONCLUSION

In this paper, we have analyzed the issue of error control in wireless communication networks. We reviewed SACK scheme to provide reliable end-to-end communication on wireless-link. TCP has poor performance over wireless-link. We have done experimental study of TCP with SACK, HTTP with page-response-time and retransmission count over wireless link. By using TCP/IP compression technique, the fast-retransmit and fast-recovery-new-Reno, could be possible thus we can reduce SACK by 48% and the page response time by 65% and by the retransmission count over wireless link.

REFERENCES

- [1] TCP error handling, with Explicit Notification Schemes “Andrei Khurri, university of Helsinki, Publish Paper Oct 14 2004.
- [2] Fast transmit and fast recovery new Reno algorithm-S.Floyd ACIRI T.Henderson, U.C.Berkeley, april-1998.
- [3] RFC 2018 – TCP Selective Acknowledgement Option - M.Mthis,J ,Mahdavi ,PSC ,S.Floyd LBNL,A.Romanow,Sun Microsystems october-1996
- [4] Opnet it leb manual-
- [5] Novel IP header Compression Technique for wireless Technologies with fixed link layer packet types,Tatina K.madsen,Frank H.P.fitzek,shekar nethi,Thomas Arildsen and gain paolo perrucci,Department of communication Technology, Aalborg university,Niel Jermes
- [6] Charles Perkins, David B.Johnson: Mobility Support in IPv6.internet Engineering Task Force, Internet Draft (Work in Progress), and January 26, 1996.
Draft-ietf-mobileip-ipv6-00.txt
- [7] Low-loss TCP/IP Header Compression for Wireless Networks-Michael Degermark, Mathias Engan, Bjorn Nordgren, and Stephen pink
- [8] Van Jacobson: Compressing TCP/IP Headers for low-speed serial links. Request for comment 1144,feb-1990.
- [9] V. Jacobson, Congestion Avoidance and Control. In Proc. Of ACM SIGCOMM, pages 314–329, Stanford, USA, August 1988.
- [10] V. Jacobson, Berkeley TCP evolution from 4.3-Tahoe to 4.3 Reno. In Proc. of the 18th Internet Engineering Task Force, Vancouver, Canada, August 1990.
- [11] S. Floyd, T. Henderson, and A. Gurtov. The New Reno Modification to TCP’s Fast Recovery Algorithm. RFC 3782, April 2004.

Enhanced Reconfigurability for MIMO Systems using Parametric Arrays

Nicolae Crișan, Ligia Chira Cremene
Technical University of Cluj-Napoca, 15 Daicoviciu street, Romania
Faculty of Electronics, Telecommunications and Information Technology
Nicolae.Crisan@com.utcluj.ro, Ligia.Cremene@com.utcluj.ro

Abstract – In the context of new high-data-rate wireless communications, multiple antenna systems are now taken into account early in the design phase. A new combining technique, OSC-SSBC (Orthogonal Space Combining – Space-Space Block Coding), was proposed by the authors as an alternative to STBC (Space-Time Block Coding) in MIMO systems, which is still based on high redundancy algorithms. The new receiver technique enables multiple antenna systems to significantly increase capacity (close to double), using a special adaptive antenna array. Based on the block diagram and mathematics of a 2Tx-2Rx OSC-SSBC configuration, we propose here an implementation solution that we call a virtualized parametric antenna.

Keywords - pixel-patch antenna, virtualized parametric antenna, OSC – Orthogonal Space Combining, MIMO – Multiple-Input-Multiple-Output.

I. INTRODUCTION

This paper proposes an antenna solution that will enable the operation of the OSC-SSBC (**Orthogonal Space Combining – Space-Space Block Coding**), technique proposed by the authors in [1]. MIMO seems to work best indoors, where there are slow changing NLOS (Non Line-of-Sight) conditions, and multipath is used to a benefit. MIMO needs highly uncorrelated paths, so it cannot operate with significant LOS. In outdoor environments LOS is common and performance is achieved using receive diversity rather than MIMO, especially for cell edge coverage. Another reason to study and attempt to enhance receive diversity performance is the fact that, as stated in [2], for UE cost reasons, it was decided to only mandate 2x2 SU-MIMO for the downlink. Although 4x4 MIMO is defined in the standards, this is probably only going to be practical for PC-based devices.

By implementing the OSC (Orthogonal Space Combining) method at the receiver, a multiple-antenna wireless communication system can almost double its capacity, even in LOS conditions [1]. Part of the physical solution would be an adaptive smart antenna array. We call the proposed implementation solution a virtualized parametric antenna; its multi-reconfigurable capabilities were prefigured by the authors in [7] and [9]. Section II discusses the OSC-SSBC performance and conditions. Section III mathematically explains the adaptive beamforming achieved by using the OSC technique. Section IV discusses the role of the antenna array

in finding an ortho-goal matrix in the infinity of matrices displayed by the spatial channel at a certain moment. Section V presents the implementation solution that we have imagined to meet the multi-reconfiguration requirements, especially the one of capturing the ortho-goal channel matrix. We called this a virtualized parametric antenna. Our provisional conclusions are expressed in the final section.

II. THE OSC-SSBC TECHNIQUE PERFORMANCE

The idea is to transmit two symbols at the same time, on two antennas, in an OSC-SSBC 2Tx – 2Rx configuration which resembles the Alamouti 2x2 MIMO-STBC. At the receiver, the two symbols will be orthogonal if we use a smart antenna array that finds the right spacing (d) and angle (Ω) in the electromagnetic field, with respect to the channel matrix. It is known that adaptive beamforming and beam-steering can enhance the performance of a space diversity scheme by significantly increasing the channel capacity. Reference [3] discusses the benefits of adaptive antenna spacing and angle diversity, based on accurate simulations, but without an explanatory mathematical model. Passive antenna diversity alone is not enough to ensure significant capacity improvements in MIMO systems, and we have shown in [1] that spacing and angle reconfiguration of the antenna array is enough to significantly increase the system data rate; the impact of adaptive antenna reconfiguration on LOS wireless communications is mathematically evaluated and demonstrated in this section.

OSC-SSBC 2Tx – 2Rx is a space-to-space orthogonal combiner that works similarly to the Alamouti STBC but behaves differently. Redundancy is reduced here by transmitting a symbol only once, thus enabling almost a doubling of the data rate. The role of the redundant symbols is here assumed by the antenna spatial reconfiguration capabilities, which is explained in section IV.

As long as the channel is flat-fading, and can be considered constant over two symbols, the STBC scheme can be applied, and the channel is described by the 2x2 matrix, H_1 :

$$H_1 = \begin{bmatrix} h_{11} & h_{12} \\ h_{21} & h_{22} \end{bmatrix} \quad (1)$$

The MIMO channel capacity is [5]:

$$C_{MIMO} = \log_2 \left(\det \left[I_{M_r} + \frac{\rho}{M_t} H_1 H_1^H \right] \right) [\text{bps} / \text{Hz}] \quad (2)$$

where M_r and M_t are the number of the receiver and transmit antenna, respectively. I_{M_r} is the unit matrix of order M_r and

H_1^H is the Hermitian of matrix H_1 .

In the OSC-SSBC scheme the interfering terms appear, but in order to avoid their affecting the received signal, they are equalled to zero. This condition is fulfilled for a matrix of the following form:

$$H_2 = \begin{bmatrix} h_{11} & h_{11} e^{j\frac{\pi}{2}} \\ h_{22} e^{-j\frac{\pi}{2}} & h_{22} \end{bmatrix} \quad (3)$$

We call the H_2 matrix the matrix of the orthogonal channel due to the fact that H_2 matrix is an ortho-goal matrix [5] ($(H_2 H_2^H = nI_n)$ considering all modules $|h_{ij}| = 1$, where n is the number of transmit or receiver antennas, $n = 2$ in our case, and I_n is the identity matrix). It is proven in [5] that the capacity of the MIMO channel is maximized for an ortho-goal matrix that is, as we assumed,

$$C_{mimo} = 2 \log_2 (1 + \rho_{osc-ssbc}) \quad (4)$$

(double if $\rho_{osc-ssbc} = \rho$ where ρ is the SNR, for a SISO system).

It is remarkable that, when the ortho-goal matrix is found, there are two orthogonal space sub-channels and the resulted channel matrix is the convolution of the two sub-channel matrices [1].

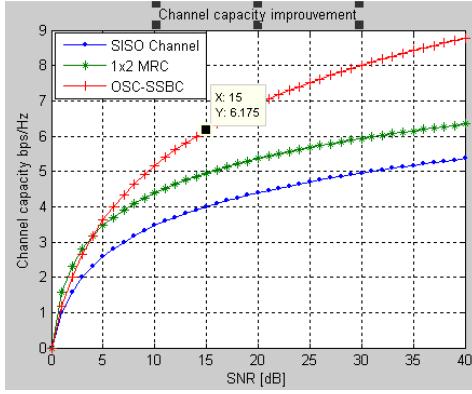


Figure 1. Capacity comparison

A comparison in terms of capacity vs. SNR is depicted in Fig. 1, for three configurations: 2x2 OSC-SSBC (worst

case $\rho_{OSC-SSBC} = \rho/2$), 1x2 MRC and a simple SISO channel. As we anticipated, the capacity increases significantly (close to double) especially for higher SNR values, reaching a 50% improvement for a 10 dB SNR. In a real case scenario, with a pseudo ortho-goal matrix, the capacity is not that high. Even so, a 15 to 20% increase of the channel capacity can be remarkable.

III. ADAPTIVE BEAMFORMING USING OSC

The proposed method smartly combines steering and beamforming, based on the antenna array. For the sake of simplicity we assume only two antennas, in a LOS, 2Tx - 2Rx MIMO configuration. In this case only two signals (two equal-phase fronts) arrive at the receiver array, having the same frequency: y_A , arriving perpendicularly onto the receiver antenna array from TxA, and y_B , arriving at an angle α (fig. 2) from TxB. The block diagram resembles that of a classical MRC (Maximum Ratio Combing) receiver with some differences.

The smart antenna array has the ability to dynamically change the antenna spacing d , with a given step Δ (where $n \in N^*$, fig.2). Signals y_A and y_B arrive at the receiver at the same time.

At decision time, both signals are crossing through the antennas, and the resulted signal will be a sum [6]:

$$y_S = y_1 + y_2 = |y_A|c_1 e^{j\omega_c t} + |y_A|c_2 e^{j\omega_c t} + |y_B|c_1 e^{j(\omega_c t + \theta + \varphi)} + |y_B|c_2 e^{j(\omega_c t + \theta)} \quad (5)$$

where ω_c is the angular carrier frequency, θ is the phase due to the path delay, and φ is the phase the AC distance adds to signal y_B (A and B are Rx A and Rx B in fig. 2), CB is the equal-phase wave front of y_B , that reaches the array.

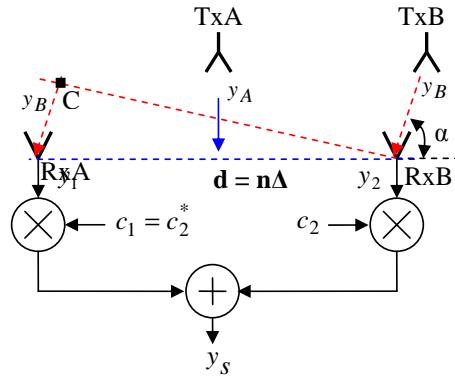


Figure 2. Proposed Orthogonal Space Combiner – based on the ability to control antenna spacing (d) and angle (α -Figure 4)

An equal-phase wave front is a plane where the waves have the same phase, in the far-field of the transmitter, and the direction of the propagating wave is always perpendicular to the equal-phase front ($\angle BCA = 90^\circ$). The input signals, y_1 , y_2 , and the weights, c_1 and c_2 , are all complex numbers. We consider that the useful signal, y_S , can be expressed in a simplified form as: $y_S = |y_A|e^{j\omega_c t}$, by keeping the weights unchanged, but dynamically spacing the antennas (the OSC concept).

The initial idea, in the case of the OSC combiner, is to find the right antenna spacing, d , for which: $\varphi = \beta|AC| = \frac{\pi}{2}$ which is valid when:

$$d = \frac{\lambda_c}{4 \cos \alpha} \quad (6)$$

in order to separate one wave from the other (λ_c is the carrier wavelength). In this case we try to select the y_A wave and equation (5) becomes:

$$\begin{aligned} y_S = y_1 + y_2 &= |y_A|c_1 e^{j\omega_c t} + |y_A|c_2 e^{j\omega_c t} + \\ &+ |y_B|c_1 e^{j(\omega_c t+\theta+\frac{\pi}{2})} + |y_B|c_2 e^{j(\omega_c t+\theta)} = \\ &= |y_A|e^{j\omega_c t}(c_1 + c_2) + |y_B|e^{j(\omega_c t+\theta)} \left(c_1 e^{-j\frac{\pi}{2}} + c_2 \right) \end{aligned} \quad (7)$$

The interferer (undesired) signal is:

$$|y_B|e^{j(\omega_c t+\theta)} \left(c_1 e^{-j\frac{\pi}{2}} + c_2 \right) \quad (8)$$

and it will be equal to zero when: $\text{Real}\{c_1\} = \text{Real}\{c_2\} = a$, $c_1 = c_2^* = a + jb$ where $a, b \in R$. Then, one possible solution is:

$$c_1 = \frac{1}{2} + j\frac{1}{2} = \frac{\sqrt{2}}{2}e^{j\frac{\pi}{4}}, \quad (9)$$

$$c_2 = \frac{1}{2} - j\frac{1}{2} = \frac{\sqrt{2}}{2}e^{-j\frac{\pi}{4}}, \quad (10)$$

$$\begin{aligned} y_S &= |y_A|e^{j\omega_c t}(c_1^* + c_2) + |y_B|c_2 e^{j(\omega_c t+\theta)}(jc_2^* + c_2), \\ y_S &= |y_A|e^{j\omega_c t} \end{aligned} \quad (11)$$

As one can notice, the signal y_B becomes orthogonal to the desired signal y_A , and the resulted signal, y_S , is not influenced by y_B when $d = \frac{\lambda_c}{4 \cos \alpha}$. This result leads to the idea that the antenna array can discriminate two signals arriving at the same time, but under different angles. When the coefficients c_1 and c_2 are under control, we deal with a beamsteering procedure and we can change the directions of the

antenna lobes. When distance d is changed the antenna spacing is affected and we deal with a beamforming effect, this time the shape of the lobes is affected [6].

IV. THE ANTENNA ARRAY AND THE ORTHO-GOAL MATRIX

The distance between transmitter and receiver, their speed, their transmit powers, the obstacles, all have an impact on the channel matrix. These are factors difficult to control. Yet, there is another system that has a great influence on the H_2 matrix, a system that is under the control of the receiver: it is the receiver antenna array. The position of the antenna array in the field and the spacing between array elements are the main parameters that can influence the H_2 matrix. There is an antenna condition that brings the H_2 matrix to the form presented in equation (3). Multiple waves always travel following the equal-phase front. For the 2x2 MIMO configuration there is an equal-phase front corresponding to each transmitter. In the far field of the Tx antenna, the equal-phase front is a plane and propagates at the speed of light in free space. According to the LOS assumption and considering the H_1 matrix, there is only one equal-phase front for each transmit antenna. Based on the 2Tx-2Rx OSC-SSBC proposed configuration, let us consider the two equal-phase fronts, one coming from Tx antenna 1 and the other one from Tx antenna 2; both arrive at the Rx antennas under the same angle α (Fig. 3-Case 1).

Arrows NA and MB indicate the direction of each front, BN and AM, respectively. The AM front carries symbol S_2 and the BN front, symbol S_1 .

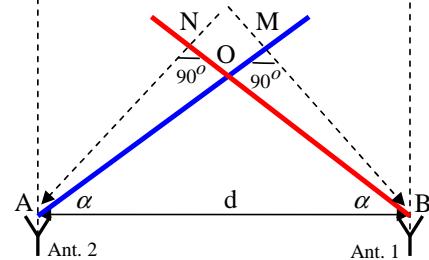


Figure 3. Case 1 - Equal-phase fronts AM and BN arrive at the same angle α

The angle $\alpha \in (0, \pi)$ and there is a diversity factor because a symbol is not received at the same time by the antennas. In this case, Rx antennas are decorrelated. When $\alpha = k\pi$, $k \in N$, the Rx antennas are correlated and there is no diversity because there is no path differences ($AN=BM=0$). As we demonstrated in section III, the antenna beamforming can mitigate the effect of one front against the other by means of OSC concept, but applying a different diversity scheme. In case 1 (Fig. 3) the matrix channel is in the desired form (ortho-goal form) when

we assume that the wave magnitude is constant across a wavelength (d , BN, AN, BM, AM are smaller than λ_c) which is true when $d < \lambda_c$. It is proved in III that the antenna spacing must be: $d = \frac{\lambda_c}{4 \sin \alpha}$ (eq. (6) $\sin \alpha$ for figure 4), OSC concept, and matrix H_2 is found in the ortho-goal form:

$$H_2 = \begin{bmatrix} h_{11} & h_{11}e^{j\varphi} \\ h_{22}e^{j\varphi} & h_{22} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{11}e^{\frac{j\pi}{2}} \\ h_{22}e^{\frac{j\pi}{2}} & h_{22} \end{bmatrix}$$

where $\varphi = \frac{2\pi}{\lambda_c} d \sin(\alpha)$. When $d = \frac{\lambda_c}{4 \sin \alpha}$, then $\varphi = \frac{\pi}{2}$, and the receiving system can discriminate symbols S_1 and S_2 , if the receiver applies a combining scheme. Symbols S_1 and S_2 are now orthogonal, and only the antenna spacing is the key for equation (6). The optimal antenna spacing $d = \frac{\lambda_c}{4 \sin \alpha}$, geometrically obtained here, matches Amir's results [10-pg. 4 eq. (31)] that were obtained using a different method.

V. IMPLEMENTATION SOLUTION – THE PARAMETRIC ANTENNA APPROACH

Classical smart antennas are based on antenna arrays, of different configurations, and controlled by means of a specialized signal processor. Smart antennas have been proved to significantly improve system performance in terms of capacity and reliability, for various communication systems.

The adoption of smart antenna techniques in future wireless systems is expected to have a significant impact on the efficient use of the spectrum, the minimization of the cost of establishing new wireless networks, the optimization of service quality, and realization of transparent operation across multi-technology wireless networks.

In our case, we turned to smart antenna techniques because we noticed that the antenna structure can help in compensating the spatial channel effects. Namely, it can help to choose/detect an ortho-goal matrix, from an infinity of channel matrices. In this paper we chose to present only the basic reconfiguration capabilities of the radiating structure that we can call a virtualized antenna which is, in essence, a parametric array. For instance, we can modify the antenna resonance frequency with a corresponding step.

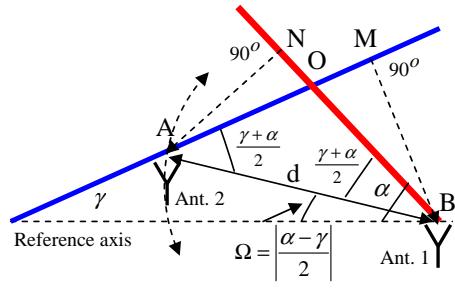


Figure 4. Case 2 – equal-phase fronts AM and BN arrive at different angles

This enables the frequency scan of a certain band, which is very useful for cognitive, agile, radios that aim to achieve a more efficient use of the radio spectrum. Polarization reconfiguration and input-impedance adaptive-matching are the other capabilities of such a parametric array (fig. 5) [7], [9].

Figure 5 presents the reconfigurable pixel-patch antenna for which the first reconfiguration equations were reported by the authors in [9]. This was the idealized approach that allowed the primary mathematical modeling.

The structure is that of an array of length L and width W , made up of small cells (metallic pixel-patches in this case) activated by MEMS switches [4] or PIN diodes (fig. 5 and fig. 6). In the idealized approach, a square metallic pixel-patch is of size $dl \times dl$. Due to the dispersion effect at its ends, the array appears longer with $2\Delta l$. The array can be lengthen, shorten or shifted by MEMS actuation or by PIN diodes command.

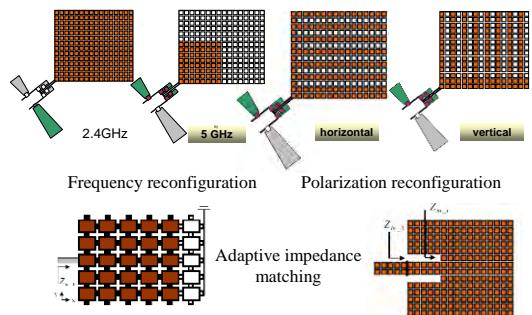


Figure 5. Reconfigurable pixel-patch antenna

TABLE I
OSC-SSBC 2X2 CONFIGURATION – ANTENNA ARRAY PARAMETERS

Case	a	b	c	d	e	f
Rotation direction	A – CW	B – CCW	A – CCW	B – CW	-	-
Ω	$\frac{\alpha - \gamma}{2}$	$\frac{\gamma - \alpha}{2}$	$\frac{\alpha - \gamma}{2}$	$\frac{\gamma - \alpha}{2}$	0	0
d	$\frac{\lambda_c}{4 \sin \frac{\gamma + \alpha}{2}}$	$\frac{\lambda_c}{4 \sin \frac{\gamma + \alpha}{2}}$	$\frac{\lambda_c}{4 \sin \left(\pi - \frac{\gamma + \alpha}{2} \right)}$	$\frac{\lambda_c}{4 \sin \left(\pi - \frac{\gamma + \alpha}{2} \right)}$	$d = 0$ no diversity	$\frac{\lambda_c}{4}$ Minimum distance

Its length becomes $l - idl = \frac{\lambda_{i0}}{2\sqrt{\epsilon_{eff}}} , \text{ where: } i = \overline{0, N-1}$

and λ_{i0} is the antenna wavelength in free space. Index i is zero when all pixel-patches are active (brown color in fig. 5), and $i = N-1$ when only one column, along the y axis, is activated (the rest are inactive – white filled in figure 5).

We found that the antenna is tuned on the frequency

$$f_{i0} = f_0 \frac{l}{l - idl} \quad (12)$$

(f_0 being the resonance frequency in ON condition, when all pixel-patches are active, and $i = 0$); this can be controlled by MEMS actuation, varying the value of i .

The resonance frequency is then:

$$f_{i0} = \frac{N}{N-i} f_0 \quad (13)$$

with respect to the ON/OFF MEMS condition. According to the simulations [7], equation (13) is valid only when the distance between the pixel-patches is no smaller than a quarter of a wavelength ($\lambda_{pix-patc} / 4$); the pixel-patch is tuned to this very high frequency (the smaller the pixel-patch, the higher the frequency).

Another antenna reconfiguration approach that we have considered is based on the input impedance control (fig. 5). It is well known that matching between antenna and transmission line is important, in order to control the amplifier's efficiency and noise figure. In this case, the MEMS or the PIN diodes enable the variation of W (array width) which influences the antenna input impedance. We found the following expression for the input impedance:

$$Z_{in_i} = Z_{in_0} \left(\frac{N-i}{N} \right)^2 \quad (14)$$

where Z_{in_0} is the left side impedance, and Z_{in_i} is the inset impedance (fig. 5).

It is also important to notice that the $\frac{N}{N-i}$ factor behaves like an antenna factor in all these reconfiguration approaches. In case the inset impedance reconfiguration method is replaced by the $\lambda/4$ -line method, this factor acts in a similar manner.

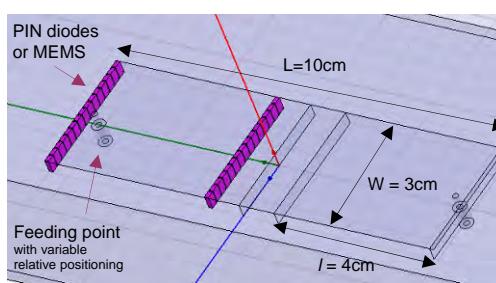


Figure 6 Two-patch array design for the 2.5 GHz band

In our approach, we start from the half-patch antenna ($\lambda/4$) model – for which the minimum field value is no longer in the middle, as in the case of a standard $\lambda/2$ - patch antenna, but on the sides - the sides are short-circuits. This is very important because it allows us to reduce the element spacing below $\lambda/4$. As one can see in figure 8 the influence of a radiating area on the adjacent “inactive” area is very small (0.004 – 1.135 V/m). When using a perfect conducting plane between the patches we can even reduce the spacing to $\lambda/12$, but this is subject of another paper.

For instance, by geometrically shifting the patch structures with a given step (e.g. 5-mm shift equals 5 steps) we can “capture” the ortho-goal matrix without affecting the resonance frequency and bandwidth (fig. 7). The slight change in the RL (return loss) value is not an impairment for the correct operation of the antenna.

The 3D radiation pattern of the two-patch reconfigurable structure (one patch active) is shown in figure 9. One can see the maximum directivity (8.4529 dB) of the two lobes.

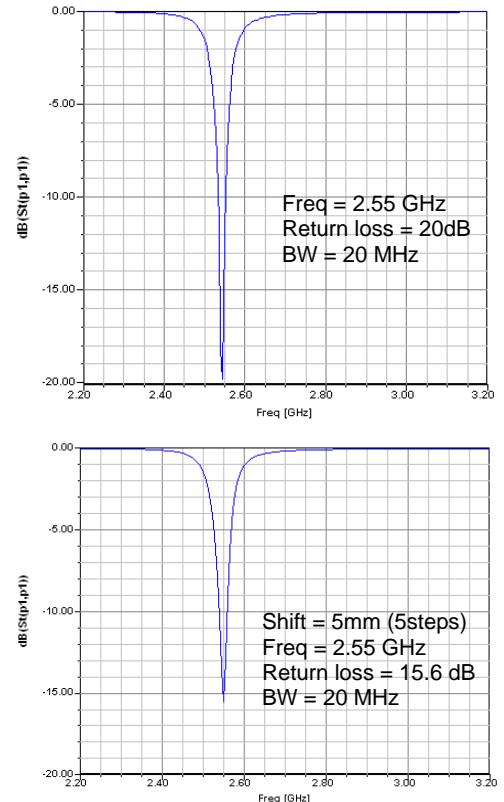


Figure 7. Radiating structure features: a) initial positioning, b) 5-mm shift

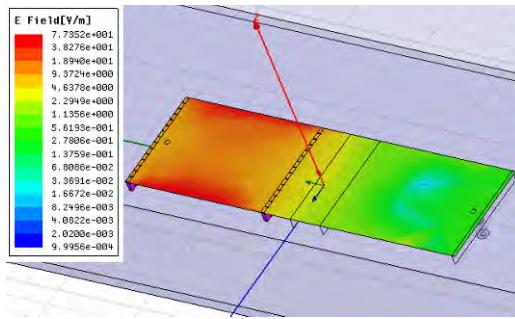


Figure 8. E-field intensity in the two-patch parametric radiating structure

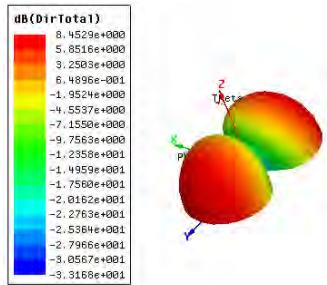


Figure 9. Radiation pattern and directivity of the fed area

CONCLUSIONS

This paper proposes an antenna solution that will enable the operation of the OSC-SSBC (**O**rthogonal **S**pace **C**ombining – **S**pace-**S**pace **B**lock **C**oding), technique proposed by the authors in [1]. By implementing the OSC method at the receiver, a multiple-antenna wireless communication system can almost double its capacity, even in LOS conditions where the paths are initially correlated.

We have mathematically explained the adaptive beamforming achieved by using the OSC technique and we have also discussed the role of the parametric antenna array in finding an ortho-goal matrix in the infinity of matrices displayed by the spatial channel at a certain moment. The parametric array was simulated for the 2.5 GHz frequency band and met the multi-reconfiguration requirements, especially the one of capturing the ortho-goal channel matrix, without affecting the resonance frequency. We called this a virtualized parametric antenna because of its high degree of flexibility – present and potential. The next steps will be towards a software-controlled polymorphic antenna based on parameterized arrays. This part of the future cognitive antenna system envisaged by the authors in [8].

REFERENCES

- [1] Nicolae Crisan, Ligia Chira Cremene, "A Novel Combining Technique for Adaptive Antenna Arrays", *Acta Technica Napocensis - Electronics and Telecommunications*, 2/2008, ISSN: 1221-6542, p.27-34
- [2] Sandy Fraser, "Examining the Design and Test Challenges of the 3GPP LTE", Agilent Technologies Inc., WiMAX Supplement, nov. 2007.
- [3] J. D. Boerman, J. T. Bernhard, "Performance Study of Pattern Reconfigurable Antennas in MIMO Communication Systems", *IEEE Transactions on Antennas and Propagation*, Vol. 56, No. 1, January 2008.
- [4] Bedri A. Cetiner, H. Jafarkhani, J.Y. Qian, Hui Jae Yoo, A. Grau, and F. De Flaviis, Univ. of California, "Multifunctional Reconfigurable MEMS Integrated Antennas for Adaptive MIMO Systems", *IEEE Communications Magazine*, pp.62-69, 2004
- [5] Ed. By G. Tsoulos, *MIMO System Technology for Wireless Communications*, CRC Press Boca Raton London New York, ISBN – 13: 978-0-8493-4190-6, 2006
- [6] J. Litva, T. K. Yeung Lo, "Beamforming in Wireless Communications", Artech House Publisher, ISBN 0-89006-712-0, 1996.
- [7] Ligia Chira Cremene, Nicolae Crisan, "The Adaptive Potential of Reconfigurable MEMS in MIMO Antenna Technology", CISSE 2007 IEEE Conference, University of Bridgeport, USA Dec 3 -12, 2007.
- [8] Ligia Chira Cremene, Nicolae Crisan, Tudor Palade, "Cognitive Antenna Systems", International Conference on Evolvable Systems – ICES 2008, Prague, Czech Republic, Sept 21-24, 2008
- [9] Nicolae Crisan, Ligia Chira Cremene, "The Impact of Novel RF MEMS and SDCs on Smart Antenna Technologies", The Fourth International Conference on Wireless and Mobile Communications - ICWMC 2008, Athens, Greece.
- [10] Amir Masoudi Nasri Nasrabadi, H. R. Bahrami, S. H. Jamali, A. Afzali Kusha, "Effect of Antenna Separation on Capacity and Performance of MIMO Systems", 2003

Modified LEACH – Energy Efficient Wireless Networks Communication

Abuhelaleh, Mohammed

Elleithy, Khaled
School of Engineering, University of Bridgeport
Bridgeport, CT 06604
[{mabuhela, elleithy, tmismar} @bridgeport.edu](mailto:{mabuhela, elleithy, tmismar}@bridgeport.edu)

Mismar, Thabet

Abstract-Many algorithms and techniques were proposed to increase the efficiency of Sensor Networks. Due to high restrictions of this kind of networks, where the resources are limited, many factors may affect its work. These factors are: System throughput, system delay, and energy. Clustering protocols have been proposed to decrease system throughput and system delay, and increase energy saving. In this paper, we propose a new technique that can be applied to sensor networks to produce high performance and stable Sensor Networks.

Index Terms- LEACH (Low Energy Adaptive Clustering Hierarchy), Sensor Networks, Network Performance, Routing.

I. INTRODUCTION

There are many advantages of using sensor networks. They provide dynamic and wireless communication between nodes in a network, which provides more flexible communication. At the same time, sensor networks have some special characteristics compared to traditional networks, which makes it harder to deal with. The most important property that affects this type of networks is the limitation of the resources available, especially the energy.

Wireless Sensor Networks (WSNs) [2] are a special kind of Ad hoc networks that became one of the most interesting areas for researchers. Routing techniques are the most important issue for networks where resources are limited. Cluster-based organization has been proposed to provide an efficient way to save energy during communication [3]. In this kind of organization, nodes are organized into clusters. Cluster heads (CHs) pass messages between groups of nodes (group for each CH) and the base station (BS), (Figure1). This organization provides some energy saving which is the main advantage for proposing this organization. Depending on this organization, LEACH (Low Energy Adaptive Clustering Hierarchy) [3] enhanced security, where the CHs are rotating from node to node in the network making it harder for intruders to know the routing elements and attack them. [4]

In this paper, we discuss some existing work of LEACH and we focus on two important criteria; the performance and energy consumption. In section two, we discuss the original work of LEACH, and then in the third section we discuss one of the most interesting modifications proposed for LEACH to increase network performance (TCCA). In the fourth section, we discuss our proposal and we explain the main modifications that we applied on LEACH to improve network performance. In section 5, we discuss our experiment that we applied to

show the improvements that may gain from applying our protocol comparing to the existing protocols.

II. LEACH

Low Energy Adaptive Clustering Hierarchy has been presented by [1] to balance the draining of energy during communication between nodes in sensor networks. The BS assumed to be directly reachable by all nodes by transmitting with high enough power. Nodes send their sensor reports to their CHs, which then combine the reports in one aggregated report and send it to the BS. To avoid the energy draining of limited sets of CHs, LEACH rotates CHs randomly among all sensors in the network in order to distribute the energy consumption among all sensors. It works in rounds; in each round, LEACH elects CHs using a distributed algorithm and then dynamically clusters the remaining sensors around the CHs. Sensor-BS communication then uses this clustering result for the rest of the round. (See Fig.1)

A. LEACH Protocol

Routing in LEACH works in rounds and each round is divided into two phases, the Setup phase and the Steady State; each sensor knows when each round starts using a synchronized clock [1, 2].

Initially, each sensor decides if it will be a CH or not based on the desired percentage of the CHs for the network, and the number of times the sensor has been a CH (to control the energy consumption), this decision is made by the sensor (s) choosing a random number between Zero and One. Then it calculates the threshold for (s) T(s), then it compares the random number with resulting T(s); if the number is less than

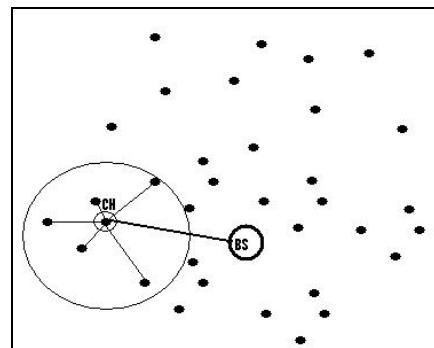


Figure1. Cluster organization for sensor networks

$T(s)$, (s) becomes a CH for the current round. $T(s)$ for x round with desired percentage of cluster heads P is calculated by (1):

$$T(s) = \begin{cases} P \frac{P}{1 - P * (x \bmod \frac{1}{P})} & \dots \dots if n \in G \\ 0 & \dots \dots otherwise \end{cases} \dots \dots (1)$$

G is a set of nodes that have not been CHs in the last $1/p$ round.

Setup phase includes three steps. Step1 is the advertisement step, where each sensor decides its probability to become a CH, based on the desired percentage of CHs and its remaining energy, for the current round; Sensor who decides to become a CH broadcasts an advertising message to other nodes that it is ready to become a CH. Carrier sense multiple access protocol is used to avoid the collision. Clustering joining step is the second step, where the remaining sensors pick a cluster to join according to the highest signal received; then they send request messages to the desired CHs. Step three starts after the CHs receive all requests from other sensors, where CHs broadcast confirmation messages to their cluster members; these messages include the time slot schedule to be used during the steady state phase.

The Steady State phase (the actual communication) then starts. It consists of two steps; in the first step each nodes starts by send its sensor report to its CH based on the time provided by the time slot schedule. When CH receives all the reports, it aggregates them in one report and it sends this report to the BS (step 2). Next we show the details of each step by providing the content of each one; for this purpose we combine the two phases in one phase with five steps.

In step one, CH broadcasts to the rest of sensors, its ID and the Advertising message, then, in step two, each sensor sends its ID, CH ID, and the Join Request message to its desired CH. When CH received all requests, it broadcasts its ID, and the time slot schedule for sensors that includes each member with its time slot (step three). Each sensor then sends its ID, CH ID, and the sensing report to its CH (step four). Finally, each CH sends its ID, BS ID, and the aggregate report of its members to the BS.

The transmission of information between sensors, and between sensors and BSs, are performed using CSMA MAC protocol. On the other hand, they communicate using CDMA codes to reduce the interference that may occur from communication of nearby nodes.

B. Energy saving in LEACH

LEACH is a self-organization adaptive protocol, and it uses randomization to evenly distribute the energy load among the sensors in the network; this and the random way that CHs rotate around the various sensors reduce the possible draining of the battery for each sensor.

A local data compression to compress the amount of data being sent from clusters to BS is used to reduce the energy consumption and to enhance the system lifetime.

The time schedule that is being performed by CHs to their members, gives break time for sensors that have not reached their time yet, to be in sleeping mode which helps them save their energy for their scheduled time.

Finally, the nature of the way that LEACH changes CHs each round, and the way that each CH can be elected, provides high energy saving for whole network.

C. Security in LEACH

LEACH is more powerful against attacks than most other routing protocols [2, 4]. CHs in LEACH that directly communicate with BS can be anywhere in the network and they are changing from round to round, which makes it harder for intruders to identify the critical nodes in the network.

On the other hand, LEACH is vulnerable to a number of security attacks [2, 4], including spoofing, jamming, and replay attacks. Since LEACH is a cluster based protocol, it relies mainly on the CHs for routing and data aggregation, which makes the attacks involving CHs, the most harmful attacks.

Some kinds of attacks, such as sinkhole and selective forwarding, may occur if an intruder manages to become a CH, which results in disrupting the work of the network.

III. TCCA

Time-Controlled Clustering Algorithm (TCCA) allows multi-hop clusters using message time-to-live (TTL) and timestamp to control the way the clusters form. Residual energy is also considered before a sensor volunteers to become a CH, and a numerical model is provided to quantify its efficiency on energy usage.

A. TCCA Protocol

Similar to LEACH, TCCA's operation is divided into rounds with two phases concluded in each round (Setup phase and the Steady State phase). CHs are elected and the clusters are formed in Setup phase; then the complete cycle of data collection, aggregation and transfer to the BS occurs in the Steady State phase.

To determine the eligibility of sensor to be CH, TCCA adds some modifications to the LEACH technique. A sensor residual energy is considered and a random number between 0 and 1 (T_{min}) is generated by each sensor to determine its eligibility to become CH. If this number is less than the variable threshold, the sensor becomes a CH for the current round. The threshold for sensor ' s ' in round r , with desired CH percentage p , residential energy RE and maximum energy MaxE is calculated by (2):

$$T(s) = \begin{cases} \max(P \frac{p}{1 - p(r \bmod \frac{1}{P})} \times \frac{RE}{MaxE}, T_{min}) & , \forall s \in G \\ 0 & \forall s \notin G \end{cases} \dots \dots (2)$$

G is a set of nodes that have not been CHs in the last $1/p$ round

When CH is elected, it advertises to other sensors to become its members; this advertisement message contains CH ID, initial TTL, timestamp and its residual energy. Sensors

receive the message will forward it to their neighbors based on TTL value which may be based on the current energy level of CH; at the same time they join this CH with the rest of sensors who received the message. Once a sensor decides to join the cluster, it informs the corresponding CH by sending a join request message that carries sensor ID, CH ID, the original timestamp from advertising message and the remaining TTL value. The CH uses the timestamp to approximate the relative distance of its neighbors and to learn the best setup phase time for future rounds [3].

The time schedule that is to be advertised by the CH is based on the total number of its members and their relative distance, to avoid collision.

Timestamp and TTL are used in TCCA to give the CH the ability to produce multi-hops clusters in efficient way that has the same performance of the one-hop clusters.

B. Energy saving in TCCA

TCCA applies a new condition for electing CHs by considering the remaining energy of the sensors. At the same time, it guarantees that every sensor will become a CH at least one time per 1/P rounds, where P is the desired percentage of CHs. These modifications provide the network with high energy balance by distributing the energy among all sensors.

TCCA provides optimum cluster size (K) for K-hops in order to produce high performance similar to the performance in the one-hop network. Also it reduces the complexity of transmission schedule generation to O (1).

TCCA uses timestamp and Time to live (TTL) tags to control the cluster formation; this leads to gain more energy balance.

C. Security in TCCA

TCCA follows the main steps provided by LEACH with some modifications that do not affect the level of security that is provided by LEACH; this means that TCCA does not have enough protection against Spoofing, Jamming, Replay and some other kind of attacks.

IV. MODIFIED-LEACH

The operation of Modified-LEACH (Mod-LEACH) works in two rounds: a Full transmission round and a half transmission one.

Each sensor checks its ability to become a CH depending on the desired percentage of CHs, current round, and the remaining energy; we used the same formula used by TCCA to calculate the threshold.

The sensors that are able to become CH (ready sensors) for the current round start listening for any query that might be sent by other sensors; the other sensors start broadcasting their reports to their neighbors, the packets contain some other tags to determine the status of the packets; any ready sensor that receives the report saves it temporarily and sends a confirmation/request to the related sensor confirming that it is ready to send its report and providing its ability status to become a CH for next round. Sensors who receive the confirmation, reply back to the CH with another confirmation and save the CH id to use it for the next round (if the status of

the CH shows that it is able to be a CH for two rounds; CHs will collect all the reports that have been confirmed in one compressed report and forwards it to the B.S. (This is considered as a full transmission round).

For the next round, the sensors with no CHs will repeat the same scenario, and the sensors with CHs will send the report only to their CHs; when the old CHs receive the reports, it will aggregate them in one report and forward it to the B.S. (this considered as a half transmission report).

Next we will explain in details the complete protocol.

A. Mod-LEACH Protocol

The operation of the Mod-LEACH occurs in rounds, and rounds are classified into two kinds, the full transmission round and the half transmission round. The main idea here is to skip the setup phase that is proposed by all other discussed protocols.

At the beginning of each round, CHs elect themselves. In order to determine the eligibility of sensor to be a CH, each sensor (S) generates a random number between 0 and 1; then this number is compared to a sensor variable threshold value T(S); if the value of the threshold is greater than the random number, the sensor becomes a CH for the current round (R). The Threshold value can be calculated using the same formula that is used by TCCA; first it calculates the threshold for two rounds as follows:

$$T(S)_a = \begin{cases} \max(P \frac{P}{1 - P(R \bmod \frac{1}{P})} \times \frac{\text{RemEng}}{\text{MaxEng} * 2}, \dots, T \text{ min}) & \text{if } S \in G \\ 0 & \text{otherwise} \end{cases} \dots (3)$$

If formula (3) is approved, then it is ready to become a CH for two rounds. If formula (3) is not approved, the sensor will calculate the formula (4) to see if it is able to become a CH for only one round.

$$T(S) = \begin{cases} \max(P \frac{P}{1 - P(R \bmod \frac{1}{P})} \times \frac{\text{RemEng}}{\text{MaxEng}}, \dots, T \text{ min}) & \text{if } S \in G \\ 0 & \text{otherwise} \end{cases} \dots (4)$$

Where P is the desired percentage of CHs, Tmin is a minimum threshold (to avoid the possibility of remaining energy shortage), and G is the set of sensors that have not became CHs in 1/P round, MaxEng is the maximum energy that the sensor could have, RemEng is the sensor remaining energy.

Each elected CH starts listing to the network; other sensors start broadcasting their reports to their neighbors (using Carrier sense multiple access protocol for transmission to avoid collisions); this message consists of Sensor ID, report, Requesting type tag (RT: 0 for request, 1 for approves), Time to live (TTL: set to 1, broadcast to only direct neighbors), packet request status tag (PR: 0 for the first packet, 1 for the second packet). When ready sensors (CHs) receive the messages, it saves each report with the node id temporarily in its memory, and then it sends requests with confirmation to those sensors indicating that it is ready to become their CH for

the current round, when formula3 applies, it also indicates that it is also ready to be their CH for the next round; the message contains: CH id, pairs of Sensor id with its time (to prevent collisions and provide less delay), TTL (set to 1), RT (set to 1), PR (set to 0) and the ability tag (AT: 0 for one round ability, and 1 for two rounds ability). Sensors receive the message from CHS; if they receive more than one request then they will choose the one with the ability to become CH for two rounds, AT=1 (here it will save the CH id to use it in the next round); if they receive many requests with the same values, then they pick the CH randomly; Sensors then reply to CHs with confirmation; the message contains: Sensor id, CH id, and an Acknowledgment tag (ACK: set to 1). When a CH receives the confirmations it combines all the reports that it has in one compressed report and forwards it to the B.S.; the message contains: CH id, BS id and the aggregation report.

In the next round, sensors check first if they are group members of a CH with an ability to handle two rounds, if they are, then they use it for the current round (half transmission round is applied); the sensor sends its report to its CH; the message contains: Sensor id, CH id, PR (set to 1), TTL (set to 1), PR (set to 1). CH receives the reports, aggregate them in one report, and then send them to the B.S., the message contains: Ch id, B.S id, and the aggregation report; then the CH will send acknowledgments to its members and remove them from its memory; the acknowledgment message contains: Ch id, Sensor id, and ACK (set to 1); sensors who receive the acknowledgment then remove CH info from their memories.

In the case that the sensor does not have a CH from the previous round, it will repeat the first scenario for full round transmission.

B. Energy saving in Mod-LEACH

Mod-LEACH applies the same condition that has been applied by TCCA for electing CHs by considering the remaining energy of the sensors. At the same time, it guarantees that every sensor will become a CH at least one time per $1/P$ rounds, where P is the desired percentage of CHs. These modifications provide the network with high energy balance by distributing the energy among all sensors.

Mod-LEACH provides enhanced energy saving by dealing with double round technique, where it saves almost half of the energy used in one regular round; for the full transmission round, it will consume more energy than LEACH and TCCA, but it covers that gap in the next round, and even saves more total energy than other protocols may save.

Mod-LEACH uses Time to live (TTL) tags to control the cluster formation, where the broadcasting occurs only on the direct neighbors; this leads to a more energy balanced network.

C. Security in Mod-LEACH

Mod-LEACH provides the same level of security that has been provided by LEACH and TCCA, where it didn't affect the main idea of these protocols which is the dynamic rotation of CHs around the network.

V. EXPERIMENTATION AND ANALYSIS

In this section, we discuss the numerical experimentation; here we describe the chosen parameters groups for each protocol, following the same scenario. The experiment is applied on LEACH, TCCA, and Mod-LEACH protocols; we applied them on three different network sizes (100, 1000, and 10000 sensors); for each size, 1000 rounds were processed with the following initial values of main parameters:

- The desired percentage of CHs (P) is set to 0.05.
- Each sensor starts with 0.5 j energy.
- The amplifier energy is assumed to be 100 pj.
- The electronic energy is assumed to be 50 nj.
- Each sensor data range is set to 30m.
- The message size of a sensor data is set to 50 bits.
- Each node has 2000-bit data packet to send to the BS.

Next, we analyze the results that appeared from applying our experiment on each of the protocols discussed before, using the same initial values and following the same scenario. We start with comparing the results based on energy saving results from each protocol, and then we discuss them based on data overload produced by each protocol, then we compare the results based on the number of the dead sensors at the end of the experiment for each protocol..

A. Energy saving

LEACH provides many techniques to save energy during network communication; where it is a self-organization, adaptive protocol and it uses randomization to evenly distribute the energy load among the sensors in the network, in addition to the random way that CHs rotate around the various sensors which is reducing the possible draining of the battery for each sensor. Also, performing a local data compression to compress the amount of data being sent from clusters to BS reduces the energy consumption and enhances the system lifetime. These factors, in addition to the way that CHs change every cycle provide LEACH with High energy saving. Mod-LEACH applies the same factors to Sensor networks which provide it with similar energy saving to the LEACH at this point.

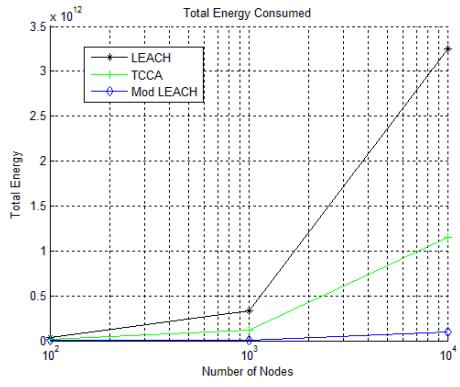


Fig.2. Total energy consumption in LEACH, TCCA, and Mod-LEACH after 1000 rounds for different network sizes (100, 1000, 10000).

TCCA adds additional factors to save energy; it uses Time to live (TTL) tag to control the cluster formation, which leads to gain more energy balance. It also uses the new condition provided by TCCA to elect CHs each round, which results in more energy control. [3] Shows that TCCA works almost three times better than LEACH in energy saving. Mod-LEACH applied TCCA factors, which means that it works three times better than LEACH in energy saving. Now by applying the new idea that we discussed before, we can notice that Mod-LEACH provides the network with almost four times more energy saving than what is provided by LEACH, and almost double of that in TCCA.

Our experiment shows that the variation of energy consumption is very small when network size is small (i.e. 100 sensors), but it varies more if we increase the network size. Fig.2 shows that, for network size of 10,000 sensors, total energy consumption is minimum in Mod-LEACH with almost 0.1×10^{12} nj, then TCCA comes with energy consumption of almost 1.2×10^{12} nj at second place, and last comes LEACH with 3.3×10^{12} nj. The variation comes from the nature of how Mod-LEACH works; using TTL, in addition to continuous checking of residual energy of each sensor, gives Mod-LEACH and TCCA protocols more energy balance for large network size; working and double round technique provides Mod-LEACH with more energy saving.

B. Data Overload

TCCA works with multi-hops clusters; this reduces the number of clusters, which reduces the total transactions required in network communications; this leads to highly reduce data overload compared with LEACH. Mod-LEACH has two different round types; in the full transmission round it will produce more data overload than that produced by TCCA and LEACH, but by applying the half transmission technique on the next round, we balance the increase in the data in the previous round and we provide less total data overload than that provided in double rounds with LEACH and TCCA.

Our experiment shows that, for a large network size (i.e. 10000 sensors); the total data overload is minimized using Mod-LEACH. Fig.3 shows that with Mod-LEACH data overload reaches almost 0.1×10^{12} bits, where in TCCA it reaches 2.2×10^{12} bits and in LEACH it reaches 9.3×10^{12} ; this

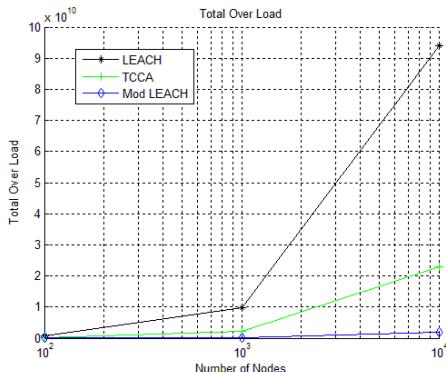


Fig.3. Total data overload in LEACH, TCCA, and Mod-LEACH after 1000 rounds for different network sizes (100, 1000, 10000).

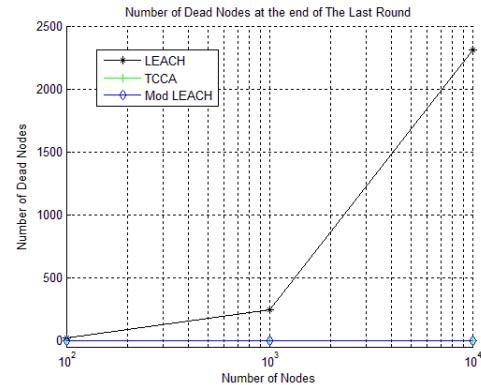


Fig.4. Dead nodes occur in LEACH, TCCA, and Mod-LEACH after 1000 rounds, for different network sizes (100, 1000, 10000).

shows that LEACH produces more data overload, almost nine times more than the data overload produced by Mod-LEACH. Moreover, TCCA produces more data overload, almost twice as much data overload produced by Mod-LEACH.

C. Performance

Here, we analyze the performance based on the expected Dead Nodes that may result in each solution after the same number of rounds.

According to the energy saving analysis, we can figure out that the number of Dead Nodes that may appear in LEACH will be much higher than the number of dead nodes in Mod-LEACH, where the number of Dead Nodes depends on the energy consumption by the network.

Fig.4 shows that Mod-LEACH and TCCA remain completely alive (i.e. no dead sensors) after 1000 rounds. On the other hand, in the case of 10000 sensors network size LEACH results in almost 2300 dead sensors.

VI. CONCLUSIONS

Modified-LEACH provides large sensor networks with high energy saving, and high level of performance, more than nine times better than LEACH and twice better than TCCA. At the same time it produces a much higher level of network stability than offered by LEACH. These results show that our proposal provides an efficient solution for high performance sensor networks communication.

REFERENCES

- [1] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In IEEE Hawaii Int. Conf. on System Sciences, pages 4–7, January 2000.
- [2] Leonardo B. Oliveira, Hao C. Wong, M. Bern, Ricardo Dahab, A. A. F. Loureiro. SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks. Fifth IEEE International Symposium on Network Computing and Applications (NCA'06)
- [3] S. Selvakennedy, and S. Sinnappan. A Configurable Time-Controlled Clustering Algorithm for Wireless Networks. 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05).
- [4] Chris Karlof, Naveen Sastry, and David Wagner. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks. 2004 Conference on Embedded Networked Sensor Systems Proceedings of the 2nd international conference on Embedded networked sensor systems.
- [5] Senyun Zhu, Shouhuai Xu, Sanjeev Setia, and Sushil Jajodia. Establishing Pairwise Keys for Secure Communication in Ad Hoc Networks: A Probabilistic Approach. Proceedings of the 11th IEEE International Conference on Network Protocols (ICNP'03)

Intrusion Detection and Classification of Attacks in High-Level Network Protocols Using Recurrent Neural Networks

Vicente Alarcon-Aquino, Carlos A. Oropeza-Clavel, Jorge Rodriguez-Asomoza, Oleg Starostenko, Roberto Rosas-Romero

Department of Computing, Electronics, and Mechatronics

Communication and Signal Processing Research Group

Universidad de las Américas Puebla

72820 Cholula, Puebla MEXICO

E-mail: vicente.alarcon@udlap.mx, spieledateien@yahoo.com

Abstract - This paper presents an application-based model for classifying and identifying attacks in a communications network and therefore guarantees its safety from HTTP protocol-based malicious commands. The proposed model is based on a recurrent neural network architecture and it is therefore suitable to work online and for analyzing non-linear patterns in real time to self-adjust to changes in its input environment. Three different neural network-based systems have been modelled and simulated for comparison purposes in terms of overall performance: a Feed-forward Neural Network, an Elman Network, and a Recurrent Neural Network. Simulation results show that the latter possesses a greater capacity than either of the others for the correct identification and classification of HTTP attacks, and it also reaches a result at a great speed, its somewhat taxing computing requirements notwithstanding.

I. INTRODUCTION

Network security poses an ever-growing, evolving task of increasing complexity due to the sheer size of the distribution and array of computer network interconnections, whatsoever the environment may be [6]. This is why several approaches (see e.g. [15], [16], [17]) have already been developed as alternatives to solve the problem of network intrusion detection, focusing for the most part in detecting attacks and enable pertinent corrective or preventive measures to take [15]. The problem of network intrusion detection may be solved from the statistical perspective as discussed in [16] or as discussed in [15] a security issue as the one we are facing may find a correct solution depending on whether we use a host-based model or a network-based model. For a host-based model, intrusion detection systems (IDS) find their decisions on information obtained from a single or multiple host systems, while for a network-based model, IDS find their decisions by monitoring the traffic in the network to which the hosts are connected [15].

It is the very dynamic and ever-changing nature of computer network attacks that makes an approach based on neural networks an efficient course of action. Since neural networks excel in pattern recognition, classification and parallel computation tasks due to the fact that they are

essentially an array of massively interconnected parallel processing elements [1]-[5], [12], recent research (see e.g. [18]) has turned to them as applied to globally-efficient systems.

In the following sections, three different bases for the computer IDS are modeled and analyzed in order to show that RNN systems are indeed able to outperform them: a feed-forward neural network system, an Elman system and a RNN system. Comparison of performance percentages shows that RNN are the best alternative for IDS applications. The remainder of this paper is organized as follows. Section II presents a description of intrusion detection techniques. Section III describes the HTTP protocol. In Section IV, a brief overview of neural networks is presented. In Section V we propose the IDS to detect and classify attacks in high-level network protocols by using neural networks. Performance evaluation of the intruder detection system is presented in Section VI. In Section VII, conclusions are reported.

II. INTRUSION DETECTION TECHNIQUES

Intruder detection systems as a whole will base their performance on two main attack detection paradigms, regardless of their network or host-based architecture [10], [17]. These are the misuse detection model and the anomaly detection model. In the former, the IDS will compare any new sequence of input parameters, which in the context of this application correspond to HTTP protocol commands, to a known database of signatures that signify attacks that have already been identified and classified previously [17]. When faced with attacks as intruders revise and improve their disruptive commands over time, the misuse detection model is left as an alternative of medium effectiveness [10]—even new variations of previously known attacks will elude the network security barrier and will easily affect any number of end systems within the network itself. The anomaly detection model, on the other hand, detects intrusions by searching abnormal network traffic (see e.g., [16], [19]). That is, this model tries to determine if a

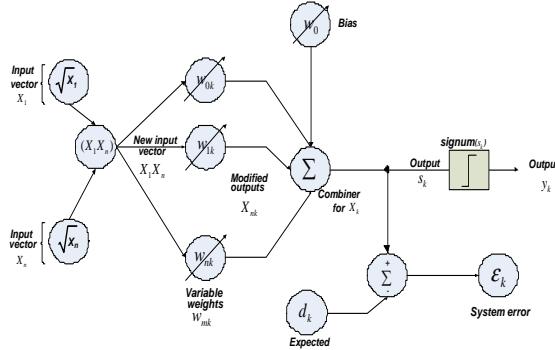


Fig. 1.Neuron-based Adaptive Linear Element [2].

deviation from the established normal usage patterns can be flagged as intrusion. The anomaly detection approach, which is based on finding patterns on Internet data, determines whether the data have an intrusive nature or normal behaviour [19]. With this type of characterization we may be able to decide if unknown data is an attack without having to know previous information about it [16].

III. DESCRIPTION OF HTTP PROTOCOL

The HTTP (Hyper-Text Transfer Protocol) has become the most widely used protocol in the field of computer communications [9]. Any IDS that attempts to identify and classify HTTP-based attacks successfully must then be given a starting database that is representative of the main types of attacks and the main types of normal commands that can be present in a network. The database will assist the system to have a starting point from which to begin deriving its own normal and intrusive data pattern comparison sequences [6], [8], [11]. In this work, five main categories of possible data flow have been considered [6], [8]: Normal, Path modification, code injection, Cross-Site Scripting (XSS) and Structured Query Language (SQL) attacks, with the following characteristics:

- **Normal:** This classification includes the normal behaviour of a system command meaning that no attack is involved.
- **Path modification:** Modification of the address of a file or directory to make access to it impossible by its owner.
- **Code injection:** Malicious code embedded in e-mail attachments or an Internet site that is executable.
- **XSS:** Access to private IDs, passwords and usernames from different browser windows active at the same time.
- **SQL:** Database altering, deleting or copying.

IV. FEED-FORWARD, ELMAN AND RECURRENT NEURAL NETWORKS

The main element in a neural network is the neuron, which is defined as a node that will produce an output \$s_k\$ for every input \$x_k\$ which is modified by a dynamic factor called the weight of that particular neuron, \$w_k\$ (see Fig. 1). In an IDS, neurons are expected to work in a value range of 0-1, due to the inclusion of an output threshold function such as a sigmoid modifier that experiences its greatest slope precisely between these values [3]. The training input vector to a network consists of \$n\$ elements in the vector \$X_n\$, each of which is directed in its turn to one of the neurons in the first layer, or input layer. After being affected by the weights in each neuron, the vector then passes through all the other layers of the network and the output layer. The weights change through time based on how similar the output of the network is to an expected output \$d_k\$ and change based on the error \$E_k\$ until it reaches a state where output matches expected performance [4], [5].

A. Feed-forward neural networks

A complete network structure in the simplest level of complexity consists of layers of neurons interconnected in such a way that the output of a neuron in any given position is biased by the inputs it receives, modified by its own weight \$w_k\$, and which come from many or all of the neurons in the preceding layer. Due to the fact that network connections limit the flow of information within its architecture to a forward direction, without any sort of feedback paths, this kind of network is known as a feed-forward network [3]. Such a network is capable of classifying and identifying patterns of a non-linear network, but its performance across time is limited due to its inability to keep previous states at the beginning of the training. The training is performed following an algorithm for weight update known as Back-propagation [11].

B. Elman recurrent neural networks

An option in terms of neural network architecture is the Elman network. The main difference between this kind of network and a feed-forward model is the fact that there exist simple feedback paths from a layer to its preceding counterpart, thus enabling the network to store information across time and improve its performance. The Elman network is called a simple recurrent network (SNR) because it is similar to a fully connected network, but the number and complexity of interconnections is lower than in a RNN [3], [13].

C. Recurrent neural networks

An improvement of SNR, fully connected RNN models have feedback connections between all neurons in a layer to the preceding layers, and even feedback connections from a neuron to itself. This increased complexity allows the neuron to store the state of its outputs from the moment the training sequence began up the present. The benefits of this are manifold, as such a network will require less training input vectors to reach a,

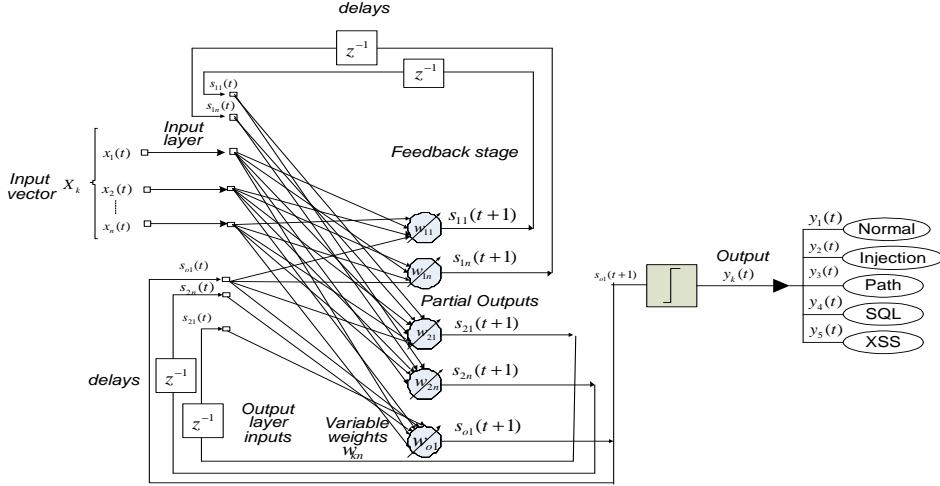


Fig. 2. RNN architecture

state where it will be suitable for testing patterns it has not been exposed to before, and the fact that it holds a memory of past events will make it easier for the network to classify certain patterns as normal or abnormal with a smaller probability of error. Nevertheless, RNN systems should be trained with a particular kind of algorithm: the Real-Time Recurrent Learning Algorithm (RTRL) [5], [12], [14].

In Fig. 2, it is possible to see the architecture of a RNN. The inputs from the first layer are propagated to the layer after it, called the first hidden layer, but also to all other processing elements in all other layers. This means that the outputs of any given neuron in a layer are connected to every other neuron and thus what happens in one affects the changes in the others, specifically modifying the weight parameter. After each output, as well, there is a brief stage of delays whose purpose is to give the network memory of past events in order to use all available information to identify, generalize and predict when faced with new input sequences. The output is passed through a threshold function of sigmoid nature when the process is over and thus the final output y_k is obtained.

C.I Real-Time Recurrent Learning Algorithm

As its name implies, this training algorithm makes the neural network able to learn and subsequently perform in an online, real-time mode. As opposed to the back-propagation algorithm, RTRL requires significantly greater processing resources: standard back-propagation techniques call for computational resources equal to $O(n^2)$, where n is the number of neurons in the entire system, while RTRL calls for $O(n^4)$ [12]—a comparatively big difference that has significant impact on larger neural networks, sometimes overriding their inherent benefits. For medium and small networks,

nevertheless, this additional processing cost is within acceptable ranges of performance goals [11]. The RTRL algorithm essentially gives a network the capability to use all the information on past outputs since the moment it began training plus the current input to predict the next output sequence.

$$y(t) = \Phi(x(t), x(t-1), \dots, x(1), x(0)) \quad (1)$$

where Φ is a non-linear function. Each of the processing nodes in charge of modifying input sequences from previous layers is required to produce an output of the form:

$$s_k(t) = \sum_{p \in I} w_{kp} x_p(t) + \sum_{q \in U} w_{kq} y_q(t), \quad k \in U \quad (2)$$

where s_k is the output calculated by multiplying each weight w_{kp} with input sequences $x(t)$ and other outputs $y(k)$. I and U refer to groups of elements within the network. The final output of the RNN after the threshold function is given by

$$y_k(t+1) = f_k(s_k(t)) \quad (3)$$

The overall error network at time t is defined in terms of $e_k(t)$ by

$$E(t) = \sum_{k \in U} e_k^2(t) = \frac{1}{2} \sum_{k \in T(t)} \{d_k(t) - y_k(t)\}^2 \quad (4)$$

The weight change per iteration is computed using the error value as follows:

$$\begin{aligned}\Delta w_{ij}(t) &= -\alpha \frac{\partial E(t)}{\partial w_{ij}} = \alpha \sum_{k \in U} e_k(t) \frac{\partial y_k(t)}{\partial w_{ij}} \\ &= \alpha \sum_{k \in U} e_k(t) p_{ij}^k(t), \quad i \in U, j \in U \cup I \\ p_{ij}^k(t+1) &= f'_k(s_k(t)) \left\{ z_j(t) \delta_{ki} + \sum_{q \in U} w_{qj} p_{qj}^q(t) \right\}, \\ i, k \in U, j \in U \cup I\end{aligned}\quad (5)$$

where α is a constant known as the learning parameter and δ_{ki} denotes the Kronecker delta. The symbol p_{ij} represents the node sensitivity as a whole when a weight changes value and these five equations represent the general concepts of RTRL.

RTRL as a whole offers the capacity for the network to compute its current output based on all previous inputs. The activation function for each node is the result of evaluating the current input, modified by the neuron weight, plus that of the previous steps throughout time for that neuron, limited by a threshold function [1], [3], [5]. The error signal which is fed back into the weight vectors for each layer depends on the minimum square error of expected output versus actual result, and the sensitivity of each individual weight to changes brought about by deviations from expected outcomes is heavily dependent on all previous states of the network. In effect, it is possible for a RNN training with RTRL to calculate the next output value in relation to current time steps, thus propagating information forward in time, not merely backward like a back-propagation network [12], [13].

V. ATTACK DETECTION WITH NEURAL NETWORKS

All HTTP requirements that the intruder detection system will come across belong to any of the five categories under consideration. The system will classify as well as detect all incoming input vectors correctly. For training and testing purposes, the dataset has 488 requirements representing abnormal commands and 285 representing normal commands [6]. The IDS was implemented through the use of MATLAB® script divided into two main sections: data pre-processing and neural network training and testing.

A Data Pre-processing

An example of a typical HTTP requirement is given by `//name.exe?param1=..|..|file..`. Most of this string consists of filenames, parameters, and alphanumeric strings, which normally change from system to system. The most significant part of this string is the file extensions, and special characters. As a result, every alphanumeric string is replaced with the special character '@' [6]. Thus, the example requirement shown before takes the following shape `//@.exe?@=..|..|@.` Using this format, the data are converted to ASCII and then to binary in a fixed string size of 64 as inputs for the IDS. To achieve this a sliding window approach is used. Its main

function is to convert a variable length vector in several fixed length vectors. The length is determined by a constant defined by the problem's nature. The sliding window approach can be described as follows. Consider a decimal vector with six elements. Now suppose that a neural network requires a fixed input length M equal to three. The sliding window approach delivers $(N-M+1)$ vectors of fixed length M, where N is the length of the original vector. As a result, we have static length vectors which are able to work as input vectors for a neural network. In order to have a better network performance, these vectors are then converted to their binary form [6]. After the binary conversion, a binary matrix is obtained, which has to be converted to a single vector of length $M \times 8$, where M is the fixed length defined by the sliding window.

B Neural Network Architecture

The first network to be tested is a multi-layer feed-forward network (FFN) with two hidden layers with 15 neurons each, plus 5 output neurons for the 5 possible categories of attacks. This network is trained with a resilient back-propagation algorithm and all neurons are sigmoid. It has been trained with 70% of the dataset and reached the estimated error goal of 0.015 upon completion of the training sequence (see Fig. 3). The number of neurons per hidden layer was chosen based on [12] and was calculated subtracting the number of neurons in the output layer from the number of inputs to the system, divided by 2 for the Elman and RNN networks and by 4 for the FFNN.

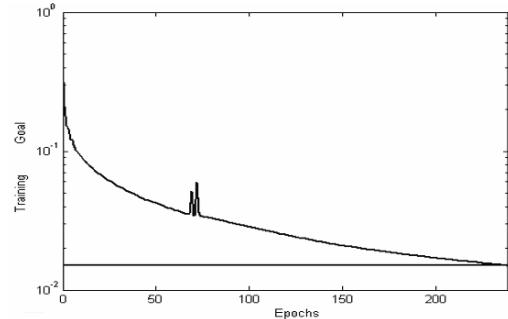


Fig. 3. Feed-forward network training

The second network was an Elman network. Following the principle for input and output layers, this network was designed to bear 30 neurons in its first hidden layer and 30 neurons in its second layer. The network reached the expected minimum error value of 0.015 just as its predecessor but it did so in much less time as measured by the number of epochs (see Fig. 4). The third and last neural network subject to evaluation was the fully connected recurrent neural network. It bore the same number of neurons in its input and output layers, but the number of hidden layers was cut in half due to several criteria. In the first place, more than one hidden layers do give neural networks better time non-linear phenomena processing qualities, but an IDS is not a highly nonlinear phenomenon as it is based merely on pattern classification, even if its inherent

permutations are nonlinear in and of themselves [11]. Secondly, training a RNN with the RTRL algorithm allows for much faster convergence upon the desired error minima, albeit at the cost of a significant increase in processing time. Following the calculation parameters in [12], the number of neurons per layer, 30, was assigned to the hidden layer but the number thereof was reduced to one to reduce processing time of the network as a whole. In small networks such as this, the total number of neurons is not a major determining factor in performance and speed [13], but better results than those of either of the previous neurons were achieved by the RNN even despite its having only one hidden layer. As expected, the network reached the desired error percentage at a staggering 50% of the time it took the Elman network to do likewise (see Fig. 5).

Fig. 4. Elman network training

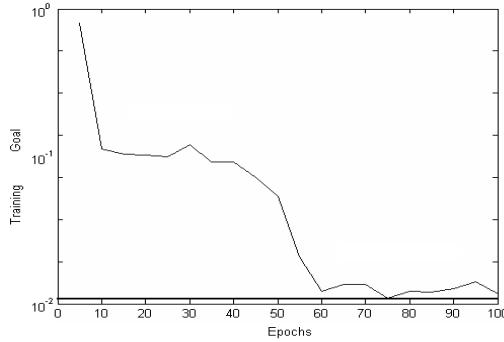


Fig. 5. RNN training

VI. PERFORMANCE EVALUATION

All three networks under analysis went through test periods in which 30% of the original dataset was used to assess their identification, classification and global error performance parameters. At the output layer, a competence function was called upon. Identification and classification were used to evaluate network performance besides speed of convergence, cost, and number of neurons.

Classification corresponds to the event where an input sequence has been accurately labeled as an attack (of any sort) or as a normal command sequence. This percentage takes into account only which of those inputs the network provides are correctly labeled in those two main categories, and does not take into consideration whether the particular command at an instant in time was correctly labeled according to its origin out of the four possible kinds of attack. Identification, on the other hand, concerns itself with the correct placing of any input pattern in its correct slot from out of the five. It should be evident that the expected percentages for identification are lower than those of classification, and in practice it was indeed so. In practice, too, it may have occurred that while classification was correctly assigned, identification itself failed (see Fig. 6), and it is why identification is in fact harder to attain by an IDS.

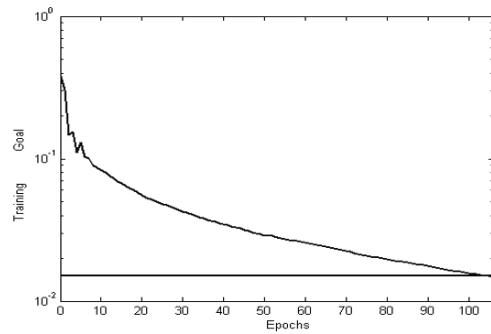


Table I summarizes all neural network performance parameters after testing, and provides two final measures of network effectiveness as well: false positives and false negatives. True to their names, a false positive will occur when the network mistakenly classifies an HTTP command as an intrusion when it is not, and a false negative conversely involves the classification of an attack as normal network behavior. In overall terms, the RNN has outperformed all other networks in all parameters, reaching a classification percentage of over 94% and thus clearly stating its superiority when compared to other architectures for this particular application.

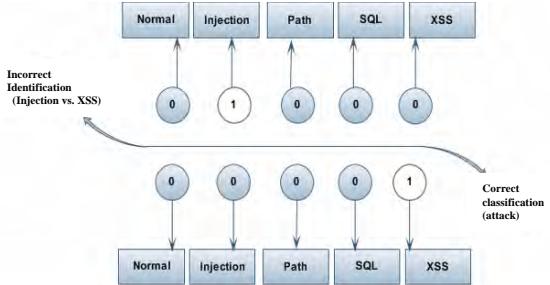


Fig. 6. Identification and Classification

TABLE I. RECOGNITION PERFORMANCE FOR EACH NEURAL NETWORK

NETWORK TYPE	FEEDFORWARD	ELMAN	RNN
ERROR	0.2572	0.1994	0.1735
Convergence speed (epochs)	239	125	75
Classification	0.8788	0.8745	0.9425
Identification	0.8355	0.8485	0.8508
O(n)	n^2	n^2	n^4
False negatives	0.95%	0.92%	0.87%
False positives	4.94%	4.90%	4.73%

VII. CONCLUSIONS

A suitable, working model for computer networking intrusion detection has been proposed throughout this paper. Following careful evaluation of performance parameters in

training and testing, it has been shown that recurrent neural networks trained by the RTRL algorithm offer the best results in all matters. The only drawback of RNN-based IDS is the slightly taxing computational cost, which is nevertheless overridden by the speed and accuracy that such a system can achieve. A global correct classification percentage of over 94% was reached with the fully connected RNN that was developed, thus ensuring sufficient accuracy for its use in an online, real-time computer system. Future work will focus on improving the results obtained through modifications of the RTRL algorithm into many of its adapted, application-specific versions in study and its subsequent implementation into a neural network system to enhance its capabilities. A hardware implementation on an FPGA, which may work with a firewall for detecting intruders and protecting the system, is also considered. Furthermore, multi-resolution recurrent neural networks are considered for improving the detection and classification performance (see e.g., [7]).

REFERENCES

- [1] R. P. Lippmann, An Introduction to Computing with Neural Nets, in *Neural Networks: Theoretical Foundations and Analysis*, Edited by Clifford Lau, IEEE Press, 1992.
- [2] C. Lau, *Artificial Neural Networks: Paradigms, Applications, and Hardware Implementations*. IEEE Press, New Jersey, 1992. pp. 64- 90
- [3] B. Widrow, *30 Years of Adaptive Neural Networks:Perceptron, Madaline, and Backpropagation*. Proc. IEEE, Vol. 78. 1990.
- [4] J. A. Anderson, *An Introduction to Neural Networks*. MIT Press, Cambridge, Massachusetts. 1997. pp. 12 - 52
- [5] S. Haykin, *Neural Networks*, Prentice Hall, 1998. pp. 274 - 298
- [6] V. Alarcon-Aquino, J.A. Mejía Sánchez, R. Rosas-Romero, J.F. Ramírez-Cruz., *Detecting and Classifying Attacks in Computer Networks Using Feed-forward and Elman Neural Networks*. Proceedings of the 1st European Conference on Computer Network Defense, EC2ND 2005, Wales, Uk. Springer Verlag 2005.
- [7] V. Alarcon-Aquino, J. A. Barria, *Multi-resolution FIR Neural-Network-Based Learning Algorithm Applied to Network Traffic Prediction*, IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Review, Vol. 36, Issue No. 2, March 2006. pp. 208-220
- [8] E. Torres, *Sistema Inmunológico para la Detección de Intrusos a Nivel de Protocolo HTTP*. Pontificia Universidad Javeriana, Bogotá, Colombia 2003.
- [9] Digital Security of the Future S21SEC URL <http://www.s21sec.com>.
- [10]P. Inella, *The Evolution of Intrusion Detection Systems*, Tetrad Digital Integrity, LLC. EE.UU., 2001. pp. 1 - 15
- [11]M. Embrechts, *MetaNeural[™] – Hands-on*. Rensselaer Polytechnic Institute, Troy NY. 1993. pp. 1 - 5, 8 - 13
- [12]J. Willams, D. Zipser, *Gradient-Based Learning Algorithm for Recurrent Connectionist Networks*. La Jolla, CA Press. California, 1990. pp 1-5
- [13]M. Mak, K. Ku, Y. Lu, *On the improvement of the Real-Time Recurrent Learning Algorithm for Recurrent Neural Networks*, Department of Electronic Engineering, Hong Kong Polytechnic University, Hong Kong, 1998. pp. 1 - 4
- [14]M. Mak, *Application of A Fast Real Time Recurrent Learning Algorithm to Text-to-Phoneme Conversion*, Department. of Electronic Engineering, Hong Kong Polytechnic University, Hong Kong, 1995. pp. 1- 5
- [15]A. Bivens, C. Palagiri, R. Smith, B. Szymanski, and M. Embrechts, Network-Based Intrusion Detection Using Neural Networks, *Intelligent Engineering Systems through Artificial Neural Networks*, Proc. Of ANNIE-2002, vol. 12, ASME Press, New York, 2002 pp. 579-584.
- [16]C. Manikopoulos, C. and S. Papavassiliou, Network Intrusion and Fault Detection: A Statistical Anomaly Approach, *IEEE Communications Magazine*, October 2002, pp. 76-82.
- [17]J. P. Planquart, Application of Neural Networks to Intrusion Detection, *SANS Institute*, July 2001.
- [18]W. Lisheng, X. Zongben, *Sufficient and Necessary Conditions for Global Exponential Stability of Discrete-time Recurrent Neural Networks*, IEEE Transactions on Circuits and Systems I, Vol. 5, Issue 6, June 2006.
- [19]V. Alarcon-Aquino, J. A. Barria, *Anomaly Detection in Communication Networks Using Wavelets*, IEE-Proceedings-Communications, Vol.148, No.6; Dec. 2001; p.355-362

Automatic Construction and Optimization of Layered Network Attack Graph

Yonggang Wang, Nike Gui, Jianbin Hu, Zhong Chen

Network and Information Security Lab, Peking University, Beijing 100871, China

wangyg@infosec.pku.edu.cn; guink@infosec.pku.edu.cn

hjbin@infosec.pku.edu.cn; chen@infosec.pku.edu.cn

Abstract-For solving scalability problem of Network Attack Graph(NAG), this paper presents a new method for network modeling based on layered NAG. Layered NAG includes “attack subgraph” and “attack supergraph”. The attack subgraph describes specific attack scenarios from the source host to the destination host and efficiently produces the attack planning after eliminating redundant paths and nodes. The attack supergraph describes the attacker’s privilege transition to allow the network administrator to evaluate the vulnerabilities of the network.

I. Introduction

Network Attack Graph(NAG) has been widely used in network attack modeling. In traditional NAG, nodes represent attack states and directed edges represent rules that cause the transition between states. However, in large-scale networks, it usually takes a long time to construct the NAG and the ultimate graph is always very large. This paper presents the construction and optimization of layered NAG in which NAG is divided into “attack supergraph” and “attack subgraph” to make NAG concision and to reduce complexity.

II. Network attack model

The network attack model we built mainly consists of attack states, attackers and attack rules. They are defined as follows:

(1) To describe the attack process accurately, the attack state in our model is represented by a sextuplet $(Prvl, Svcs, Conn, Trust, \text{boolKnld}, \text{objKnld})$. $Prvl$, defined as $Prvl(H) \rightarrow \{\text{None}, \text{Access}, \text{User}, \text{Superuser}, \text{Root}\}$, represents the level of privilege the attacker can achieve in host H and satisfies a partial order: $\text{None} < \text{Access} < \text{User} < \text{Superuser} < \text{Root}$. $Svcs$, $Conn$ and $Trust$ respectively represent the information about service, connection and trust that the attacker has

obtained. BoolKnld and objKnld represent other information that may be necessary to describe the attack process. While boolKnld represents Boolean knowledge, ObjKnld represents knowledge of objects and consists of three parts: the object name, the attribute name and the attribute value.

(2) The attacker is represented by a quadruplet $(\text{Goal}, \text{CurHost}, \text{Knld}, \text{Cap})$. Goal represents the attack target. CurHost represents the current host of the attacker. Knld represents the knowledge that the attacker has obtained about the target network which mainly consists of information about host, user id, password and file. Cap describes the attacker’s capabilities and includes four parts: IP address of the source host, IP address of the destination host, the top privilege of the destination host that the attacker can obtain in the source host, and ID of the attack subgraph.

(3) The attack rules describe the transition between attack states. Each attack rule $r \in R$ corresponds to one or more attack tools in the library and is represented by a quintuplet $(ID, \text{Name}, \text{Para}, \text{Precond}, \text{Postcond})$. In this tuple, ID and $Name$ represent identity and name of the attack rule. Para represents the set of parameters of the rule and it starts with abstract or default value. As attack tools being executed, parameters become specific before the corresponding attack tool is used. Precond and Postcond respectively represent the precondition of matching the rule and the post-condition of using the rule.

III. Construction and optimization of layered NAG

A. Construction and optimization of attack subgraph

The attack subgraph is represented by a sextuplet $(S, \Sigma, \delta, S_0, S_f, D)$. In this tuple, S is the set of attack states. Σ is the library of attack rules. $S_0 \subseteq S$ is the

set of initial states. $S_f \subseteq S$ is the set of target states. $\delta: S \times \Sigma \rightarrow S$ represents rules of state transition (i.e. a transition between states is an atomic attack). D is the weight of state transition. Each atomic attack is given the corresponding weight. In order to simplify the structure of the attack subgraph, we assume that the attacker will not execute attacks that can weaken his capabilities (i.e. an attacker's capabilities can only be strengthened during the attack process). According to the definitions above, we have devised the positive, breadth-first-search generation algorithm for attack subgraph, as shown in Figure 1.

```

1 ConstructAttackSubgraph (I, R)
2 Input: I (initial attack state)
3 Input: R(the set of attack rule)
4 Output: output_queue (the set of attack states)
5 output_queue $\leftarrow$  $\Phi$ ;
6 state_queue $\leftarrow$ state_queue+I ;
7 while(state_queue is not empty)
8     cur_state $\leftarrow$ the first state in state_queue;
9     while(the attack target has been given and reached)
10        set cur_state as target state;
11        delete the first state in state_queue;
12        cur_state $\leftarrow$ the first state in state_queue;
13        for(each rule r in R that match cur_state)
14            child_state $\leftarrow$ cur_state;
15            child_state $\leftarrow$ child_state+the postcondition of r;
16            if(cur_state!=child_state)
17                if(child_state==a state having been constructed)
18                    set child_state as substate of cur_state;
19                else
20                    set new state ID of child_state;
21                    set child_state as substate of cur_state;
22                    state_queue $\leftarrow$ state_queue+child_state;
23            output_queue $\leftarrow$ output_queue+cur_state;
24        delete the first state in state_queue;
25 return output_queue;

```

Figure 1. The algorithm of automatic construction of attack subgraph

Having constructed the attack subgraph, we start from the target state and adopt the backward-search algorithm to obtain all the attack paths from the initial state to the target state. However, there's still redundancy. We eliminate redundant paths by the following recursive algorithm in Figure 2.

B. Construction and optimization of attack supergraph

The attack supergraph is represented by a quintuplet (H, C, H_0, H_f, δ) . In this tuple, H is the set of hosts in the network and C is the set of attack subgraphs.

$H_0 \subseteq H$ is the host where the attacker resides.

$H_f \subseteq H$ is the attack target host. $\delta: H \times C \rightarrow H$ is the function of state transition and represents the attacker's privilege transition between hosts.

```

1 FindMinimalAttackPathSet(R)
2 Input: R (all the sets of attack paths)
3 Output: MAPS (the minimal attack path set)
4 MAPS $\leftarrow$  $\Phi$ ;
5 paths $\leftarrow$ R;
6 while(true)
7     minlen $\leftarrow$ the step number of the shortest attack path in paths;
8     minpath $\leftarrow$ the attack path matched with minlen;
9     MAPS $\leftarrow$ MAPS+minpath;
10    tmppaths $\leftarrow$ paths—the attack path which covers minpath;
11    if (tmppaths is empty)
12        return MAPS;
13    else
14        paths $\leftarrow$ tmppaths; //recursion

```

Figure 2. The algorithm of searching for the minimal attack path set

When the attack subgraph from the source host to other hosts in the network has been constructed, the attack capability from the source host to the target host will have been stored in the attribute Cap of the attacker. Therefore, traverse all the hosts in the network according to the attribute Cap and then the attack supergraph will be constructed. Thus we can obtain all the attack paths by adopting depth-first-search algorithm.

Given the attack supergraph and the attack subgraph $C' \subseteq C$, if the attacker cannot reach the target state after removing C' from C , then C' is called the critical set of attacks. If there's no other critical set C'' that satisfies $|C''| < |C'|$, then C' is called the minimal critical set of attacks. It is the set of attack scenarios that the attacker has to execute because of the target state. The greedy algorithm of searching for the minimal critical set of attacks is shown in Figure 3.

```

1 FindMinimalCriticalAttackSet(P,C)
2 Input: P (the set of attack paths)
3 Input: C (the set of attack subgraph ID)
4 Output: MCSA (the minimal critical set of attacks)
5 MCSA $\leftarrow$  $\Phi$ ;
6 paths $\leftarrow$ P;
7 while(paths is not empty)
8     for(c $\in$ unvc, the set of unvisited attack subgraph ID)
9         if(the number of attack paths that cover c is the biggest)
10            tmppaths $\leftarrow$ the set of attack paths that cover c;
11            MCSA $\leftarrow$ MCSA+c;
12            Unvc $\leftarrow$ C—MCSA;
13            paths $\leftarrow$ paths—tmppaths;
14 return MCSA;

```

Figure 3. The algorithm of searching for the minimal critical set of attacks

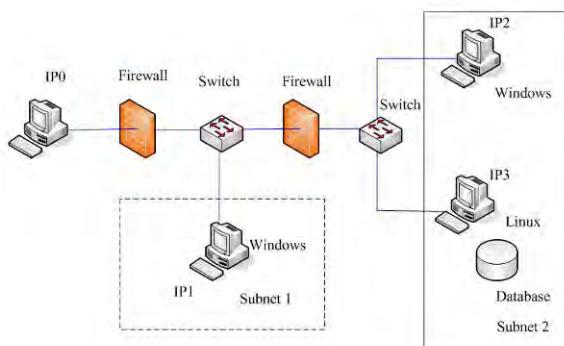
IV. Experiment analysis

In our experiment, the network topology structure is shown in Figure 4. The firewall divides the network into two subnetworks. The outer hosts can only visit Subnetwork 1 and cannot visit Subnetwork 2 directly. However, the hosts in Subnetwork 1 can visit Subnetwork 2. Assuming that IP0 is the address of the

Table 2. List of matched attack rules

Rule ID	Name of Rule	Parameter	Precondition		Postcondition	
			Local precondition			
			Source host	Destination host		
			Vulnerability、privilege、service、information、object		Relation of connection	
R1	Windows SMB crack	(un, pd)	microsoft-ds(445/tcp)=open		c(hs, ht, 445) username=un &password=pd	
R2	IPC connection	(un, pd, ut=Superuser)	netbios-ssn(139/tcp)=open microsoft-ds(445/tcp)=open&username=un&password=pd&user_type=ut		c(hs, ht, 445) c(hs, ht, 139) Prvl=ut	
R3	Raising local Serv-U privilege		Prvl>=User&ftp=open&ftp_type=serv_u&ftp_version<6.0		Prvl=Root&ftp=killed	
R4	Bypassing remote RealVNC identification	(pt=5800)	vnc-http=open&vnc_type=RealVNC&vnc_version<4.1.1		c(hs, ht, pt) Prvl=Superuser	
R5	Remote heap overflow of SRVSVC		os_name=windows2000&os_version<=sp4µsoft-ds(445/tcp)=open		Prvl=Rootµsoft-ds=killed	

attacker's initial host and the attacker's target is to destroy the database in IP3, the attacker needs to obtain the Root privilege of IP2 as a result.

**Figure 4. Network structure of our example**

A. Analysis of attack subgraph

Here we analyze one attack subgraph($IP0 \rightarrow IP1$) for example. The information of IP1 obtained by scanning tools in IP0 is shown in Table 1. The attack rules matching these information are described in Table 2.

Table 1. Scanning information of IP1

OS	Microsoft Windows 2000 sp4		
	s_name	s_type	s_version
	ftp(21/tcp)	FTP_Serv-U	5.0
	vnc-http(5800/tcp)	RealVNC	4.0
Services			epmap (135/tcp)
	netbios-ssn(139/tcp)		
	microsoft-ds(445/tcp)		
	general/icmp		
		

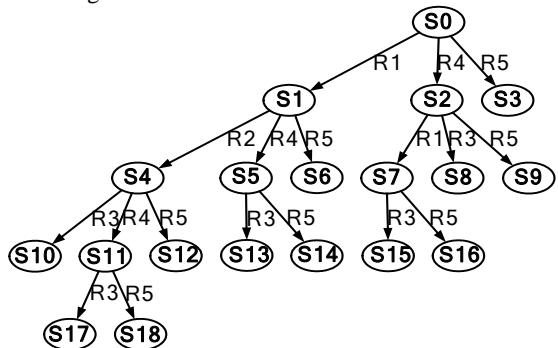
The subgraphs ($IP0 \rightarrow IP1$) constructed according to the algorithm in Figure 1 are shown in Figure 5 and 6. Nodes, labeled with increasing numbers, represent attack states. Edges, labeled with rule ID, represent attack rules. Figure 6 shows the attack subgraph that has eliminated the redundancy in Figure 5. However, there's still redundancy. So we optimize these attack paths by adopting the algorithm of searching for the minimal set of attack paths. Finally, we get 3 minimal attack paths and sort them by the step number:

Ap1: S0 → (R5) → S3

Ap2: S0 → (R4) → S2 → (R3) → S8

Ap3: S0 → (R1) → S1 → (R2) → S4 → (R3) → S10

These attack paths have higher priorities when the attacker wants to make an attack. Likewise, we can construct the attack subgraphs aiming at IP2 and IP3 according to their vulnerabilities.

**Figure 5. Attack subgraph from IP0 to IP1**

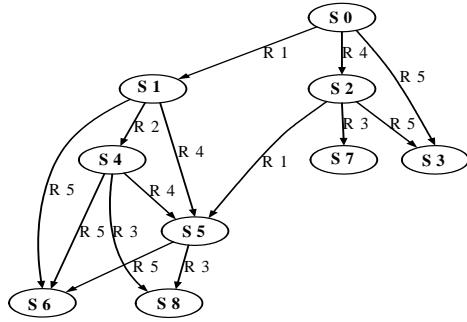


Figure 6. Attack subgraph from IP0 to IP1 after eliminating the redundancy

B. Analysis of attack supergraph

When the attack subgraphs aiming at all the hosts in the network have been constructed, the attack supergraph of the whole network will be constructed according to the attribute Cap of the attacker, as shown in Figure 7. Nodes, labeled with IP address, represent hosts in the network. Edges represent privilege transition of the attacker and are labeled with 4 properties: the source host, the destination host, the highest privilege that can be obtained, ID of the attack subgraph.

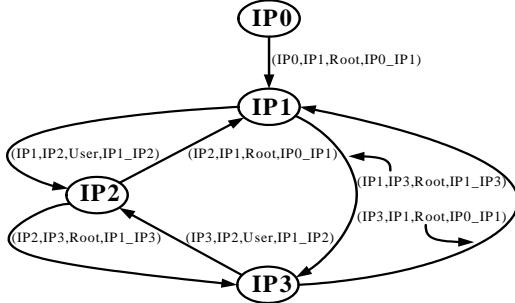


Figure 7. Attack supergraph constructed by our system

V. Conclusion

This paper presents a novel approach to automatic construction and optimization of the network attack graph. A hierarchy has been adapted for the network structure that can be divided into “attack supergraph” and “attack subgraph” so as to make the network attack graph concision and to reduce complexity. After eliminating the redundant paths and nodes, the attack subgraph has a remarkable smaller scale and can make attack plans efficiently. The attack supergraph describes the attacker’s privilege transition process from the perspective of the whole network and enables a system administrator to evaluate the vulnerabilities of the network automatically.

References

- [1] P. Ammann, J. Pamula, and R. Ritchey, “A Host– Based Approach to Network Attack Chaining Analysis”, Proceedings of the 21st Annual Computer Security Applications Conference 2005.
- [2] R. Ritchey, B. O’Berry, and S. Noel, “Representing TCP/IP Connectivity for Topological Analysis of Network Security”, Proceedings of the 18th Annual Computer Security Applications Conference, 2002, pp. 25-31.
- [3] O. Sheyner, “Scenario graphs and attack graphs”, PhD Thesis, School of Computer Science Carnegie Mellon University, 2004.
- [4] L. Swiler, C. Phillips, D. Ellis, and S. Chakerian, “Computer-attack graph generation tool”, Proceedings of DARPA Information Survivability Conference & Exposition II, June 2001, pp. 307-321.
- [5] P. Ammann, D. Wijesekera, and S. Kaushik, “Scalable graph-based vulnerability analysis”, Proceedings of the 9th ACM Conference on Computer and Communications Security, 2002, pp. 217-224.

Parallel Data Transmission: A Proposed Multi-layered Reference Model

¹Thomas Chowdhury , ²Rashed Mustafa

¹Department of Computer Science and Engineering
Chittagong University of Engineering & Technology, Chittagong, Bangladesh
² Department of Computer Science and Telecommunication Engineering
Noakhali Science & Technology University, Noakhali, Bangladesh,

Abstract--Data transmission process between host to host in the computer network follows a basic system namely OSI reference model. In this model data processing starts at the application layer, breaks the data into segments at the transport layer and processing ends at the physical layer. Afterwards it transfers segmented data between different layers, bit wise conversion taking place at the physical layer through the medium. In this paper a new parallel data transmission process has been proposed. In this research all segmented data broken in the transport layer at the same time, transfer through the medium. There is an interrelationship between layers in the proposed model. Moreover this system has both way data transmission capability. Layers can inherit information from upper or lower section. This leads the system to more dynamic that is evolutionary. To support this type of data transmission process, a new reference model proposed in this research. And thus the system model works faster and more error free than the existing data transmission system.

Keywords--OSI Reference model, Frame, Packet, Data Segment, Sequence Number, Checksum, Flag, Address Information.

I. INTRODUCTION

Existing OSI reference model has seven layers. Reference [1] denotes that application layer interfaces with applications that desire to communicate and is in contact with the application layer of the remote machine it is communicating with. Presentation layer converts into general format so remote machine understand it. Session layer makes a session with remote machine. Reference [2] denotes that transport layer breaks data into segments and also controls error, flow etc. Network layer converts segment into packet adding logical addresses. Data link layer converts packet into frame adding physical addresses. Reference [3] depicts that physical layer converts frame into bit to transfer through the medium. Our proposed reference model has six layers and it shows how data transfers from host to host. Our proposed parallel data transmission follows this proposed reference model.

II. PROPOSED MODEL AND PROPOSED PARALLEL DATA TRANSMISSION

A. Proposed Reference Model.

The proposed reference model has six layers. They are described below.

• Application layer.

Application layer is the top layer of the proposed reference model. Application layer actually interfaces the application that desires to communicate. The application layer is in contact with the application layer of the remote machine it is communicating with. A PC setup as a network workstation has a software “Network Redirector”. Its function is to check the file either it is for local computer or for the remote machine. If the file is for remote computer, application layer converts the format of the data to general format so that remote machine can understand easily.

• Session layer.

The session layer manages the communications between the workstation and the network. It provides service to the upper application layer and lower transport layer. It has five fields.

- Source port: it defines the port number for the application in the local machine.
- Destination port: it defines the port number for the application in the destination remote machine.
- Serial / Parallel transmission: it is one bit which defines either it is serial transmission or parallel transmission. ‘0’ for serial and ‘1’ for parallel.
- Control: it is the control information for session management.
- File: it is the data portions which come from application layer.

It also manages log on procedures and password recognition.

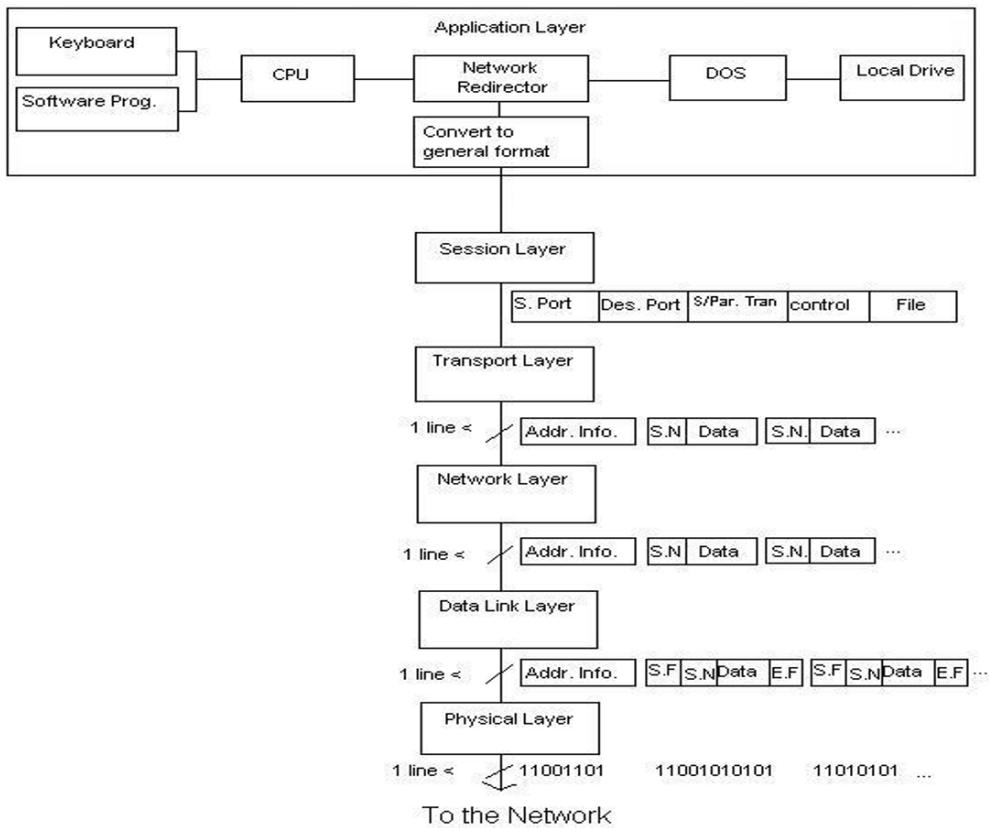


Fig 01. Functional Drawing of the Proposed Model

- *Transport layer.*

In order for the data to be sent across the network, the file must be broken up into usable small data segments (typically 512 - 18K bytes). The Transport layer breaks up the file into segments for transport to the network, and combines incoming segments into a contiguous file. The Transport layer does this logically, not physically. It checks to see the serial / parallel transmission bit. If it is zero ('0') then it indicates it is serial transmission so it transfers data one by one segment adding sequence number, acknowledgement number, checksum field to every segment. If it is one ('1') then it is parallel transmission. This bit also helps the remote machine to understand either the starting data transmission is serial or parallel transmission. In the case of parallel transmission there are more than one line to transmit data. One for address line. It will hold all the address information such as Source Port, Destination Port, control etc. The other lines are for data segments. The address information also has sequence number, acknowledgment number, checksum etc. Each data segment has the sequence number. This sequence number is not same as address sequence number. If it is

the first data segment, the sequence number for the first data segment is

First Data Segment Sequence Number = Address Sequence Number + 1

So for Nth Data Segment the sequence number is

Nth Data segment Sequence Number = Address Sequence Number + N

The next address sequence number comes after transmitting N segments simultaneously.

Next Address Sequence number = Previous Address Sequence Number + N+1

The sequence number in the each data segment helps the remote machine to reassemble the data segment correctly.

- *Network Layer.*

The Network layer is concerned with the path through the network. It is responsible for routing, switching, and controlling the flow of information between hosts. The network layer adds the source and destination IP address to each segment if it is serial transmission or adds IP addresses of the source and the destination to the address information if it is parallel transmission.

The router operates at this layer -- sending data throughout the extended network and making the Internet possible.

- *Data Link Layer.*

The Data Link layer is a firmware layer of the network interface card. The data link layer adds MAC addresses to each segment if it is serial transmission and adds MAC addresses to the address line if it is parallel transmission. It also adds start flag and end flag to each data segment. MAC address is 6 bytes long. The first 3 bytes identify the vendor such as 3Com or Intel, the last 3 bytes are unique for each card produced by the vendor. Switches work at the Data link layer.

- *Physical Layer.*

The Physical layer concerns itself with the transmission of bits. It also manages the network card's hardware interface to the network. The hardware interface involves the type of cabling (coax, twisted pair, etc.), frequency of operation (1 Mbps, 10Mbps, etc.), voltage levels, cable terminations, topography (star, bus, ring, etc.), etc.

B. Proposed Parallel Data Transmission.

Parallel data transmission means data transmit in parallel. i.e. data broken into segments transmit simultaneously in the data segment lines. All data segments, broken at the same time, have common address information, which also transmits simultaneously with the data segments. So each data segment has no individual address information but only sequence number and start flag and end flag and common address information in the address line. Every time when data are broken into segments according to the data segment line number one address information is created for those data segments. This address information transmitted in address line

Parallel data transmission starts when the serial/parallel transmission bit is '1'. If there are 4 lines then every time three data segments transmit simultaneously in three data lines and one address information transmit in the address line. If First sequence number in the address information is 'x', then first data segment's sequence number is 'x + 1', second data segment's sequence number is 'x + 2', third data segment's sequence number is 'x + 3'. Second address information in the address line is same as the first address

information if the destination and application is same but sequence number is different from the first one. The sequence number in the second address information is 'x+4'. Every time a new address information is created for the transmission of the three data segments. This address information is different from the previous one in sequence number. This process continues until the data transmission process end. If the remote machine does not know how many data segments come in parallel, it can calculate it from first address information and second address information of the transmission process.

Sequence Number in Second address information –

$$\text{Sequence Number in first address information} - 1 = x + 4 - x - 1 = 3 \text{ data segments transmit in parallel.}$$

At the time of reassembling, it can also detect all segments by subtracting sequence number in the address information from data segment sequence number.

$$\text{First data segment detection} = \text{data segment sequence number} - \text{address sequence number} = x + 1 - x = 1$$

$$\text{Second data segment detection} = \text{data segment sequence number} - \text{address sequence number} = x + 2 - x = 2$$

$$\text{Third data segment detection} = \text{data segment sequence number} - \text{address sequence number} = x + 3 - x = 3$$

From these values the remote machine can easily detect the segments. In case of single data segment transmission error, the remote machine, taking the address from address information, sends the sequence number of that data segment as an acknowledgment to the sender to retransmit that segment. The sender follows the serial transmission process to send that segment i.e. adding all address information to that data segment and send it. For more than one data segment error the remote machine sends the sequence number taking from the address information as an acknowledgment to send all data segments following that address information.

III. BENEFITS OF OUR PROPOSED SYSTEM

The main benefits of our proposed system is that our system is faster and better error free than the existing system. We assume there are 3 lines for data segment transmission and 1 line for address information transmission. Each data segment has 18k byte data. (Maximum size of data for each segment). Each data segment at the time of transmitting consists of the following.

Data segment for transmit = Start Flag + Sequence Number + Main data segment + End Flag.

Table 1.1 Comparison of data transmission time between existing system and proposed system

Size of the file selected for transmission	10 Mbps Line for Data Transmission		100 Mbps Line for Data Transmission	
	data transfer time in second according to existing model	data transfer time in second according to proposed model	data transfer time in second according to existing model	data transfer time in second according to proposed model
1 MB	0.80148	0.26675	0.08014	0.02667
5 MB	4.00743	1.33373	0.40074	0.13337
10 MB	8.01487	2.66746	0.80149	0.26675
15 MB	12.0223	4.00119	1.20223	0.40012
20 MB	16.02973	5.33492	1.60297	0.53349
100 MB	80.14865	26.67462	8.01487	2.66746
500 MB	400.74327	133.37311	40.07433	13.33731
1 GB	820.72222	273.14815	82.07222	27.31482

A. It will be Faster.

Our proposed system will be faster than the existing system. It can be described easily by the following calculated value given in the table 1.1.

B. It will be more error free.

Our proposed system will be more error free than the existing system. It can be described easily by the following calculation given in the table 1.2. We assume minimum error rate is 1 bit error occurs in case of 100000 bits transmission.

Table 1.2 Comparison of error rate between existing system and proposed system

Size of the file selected for transmission	Error rate in case of data transmission in the existing model	Error rate in case of data transmission in the proposed model
1 MB	84.04	83.96
5 MB	420.21	419.80
10 MB	840.42	839.61
15 MB	1260.63	1259.41
20 MB	1680.84	1679.21
100 MB	8404.20	8396.08
500 MB	42020.98	41980.4
1 GB	86058.96	85975.85

As the file size increases, error rate in the existing model increases more than our proposed model error rate. So our proposed model is better than the existing model.

IV. CONCLUSION

We can say that our proposed model is faster and better error free than the existing model. It can be used in the places where faster and error free communication is necessary. We shall improve our proposed system so that it will be faster, better error free, secured and also design new protocols to support the proposed system better in future.

REFERENCES.

- [1]. A. S. Tanenbaum, "Computer Networks", pp 37-46,184-187.
- [2]. D. E. Comer, "Computer Networks and Internets", pp 94-96, 229-230, 236-237.
- [3]. P. C. Gupta, "Data Communications", pp 152-156, 165-169, 418-434.
- [4].P. Keleher, S. Dwarkadas, A. L. Cox, and W. Zwaenepoel. Treadmarks: Distributed Vern Paxson. Automated packet trace analysis of TCP implementations. In SIGCOMM, pp-167-179, 1997.
- [5].E. Kohler, M. F. Kaashoek, and D. R. Montgomery. A readable TCP in the J. Postel. Transmission control protocol. RFC 793, USC/Information Sciences Institute, September 1981.

Besides Tracking – Simulation of RFID Marketing and Beyond

Zeeshan-ul-Hassan Usmani¹, Fawzi Abdulkhalil Alghamdi², Amina Tariq³ and Talal Naveed Puri⁴

¹*Dept. of Computer Science, Florida Institute of Technology, Melbourne, FL, USA*

²*Dept. of Electrical and Computer Engineering, Florida Institute of Technology, Melbourne, FL, USA*

³*National University of Computer and Emerging Sciences, Islamabad, Pakistan*

⁴*General Electronics Transportation, Melbourne, FL, USA*

zusmani@fit.edu, falghamd@fit.edu, amina.tariq@nu.edu.pk, talal.puri@ge.com

Abstract: This paper asks a new question: how we can use **RFID** technology in marketing products in supermarkets and how we can measure its performance or **ROI** (Return-on-Investment). We try to answer the question by proposing a simulation model whereby customers become aware of other customers' real-time shopping behavior and may hence be influenced by their purchases and the levels of purchases. The proposed model is orthogonal to sales model and can have the similar effects: increase in the overall shopping volume. Managers often struggle with the prediction of **ROI** on purchasing such a technology, this simulation sets to provide them the answers of questions like the percentage of increase in sales given real-time purchase information to other customers. The simulation is also flexible to incorporate any given model of customers' behavior tailored to particular supermarket, settings, events or promotions. The results, although preliminary, are promising to use **RFID** technology for marketing products in supermarkets and provide several dimensions to look for influencing customers via feedback, real-time marketing, target advertisement and on-demand promotions. Several other parameters have been discussed including the herd behavior, fake customers, privacy, and optimality of sales-price margin and the **ROI** of investing in **RFID** technology for marketing purposes.

I. INTRODUCTION

Humans generally follow the opinion of the majority — referred as mob-mentality in social sciences. An animal observing others performing a task is inclined to "join in" and perform the same task. The same is true in sales: the spread of information about a particular deal (i.e. products going on sale) from person to person may be an interesting sales tool. If many people refer to the price of a product as being a "good deal," people are inclined to believe and be led to buy the product in question. Still, it is thought that improvement in sales is possible if customers are provided with more information about sales — such as what other customers are buying. Such an approach needs to encompass a new understanding of customers' shopping behavior and its effect on their purchase levels.

From the point of view of supermarket sales, it is not hard to show that the analysis of customers' activities (movement, shopping behavior, etc.), while inside the supermarket, falls in the category of a complex system. One needs to look at only a

few examples: (i) customers act independently of each other while in the supermarket — the path they take nor the products they buy is directed by the supermarket; (ii) the level of sales of products is an emergent value dependent upon customers' buying power that day, the level of discount for the product, the location of the product in the supermarket, and many others; (iii) external factors such as weather and natural disasters can drive behavior in sales that is hard to predict.

Shopping in the supermarkets may not seem like a psychological battle but with the help of current technologies we can do the unthinkable. Today's technology can easily enable this information to be fed to all customers in real-time. Examples of such technology via the use of **RFID** and intelligent carts are already in place in many experimental supermarkets, such as TESCO retail stores in UK and Metro experimental future-marts [13]. The simulation shows that a model considering the information of what in-store customers are buying is likely to increase the volume of sales.

Researchers and managers have been working to improve the share and demands of all stakeholders for last eight decades with almost opposite needs. Retailers want to keep the customers in the store for as long as possible while customers want to leave the store as soon as they can, most likely after they get their planned shopping done [1]. A good body of research has been carried out to find the ways to keep customers longer within stores like Internet booths, Coffee shops, Reading zones, Saloons, Drugstores, etc. Customers are also interesting in getting the best value for their money while retailers want the maximum sales and profits. There is always a tension between these two worlds to favor customers or retailer while designing and setting supermarkets [6]. They are in a constant crash but they both need each other — competition and collaboration in the same world. More profit and sales is the number one priority for every manufacturer to thrive, succeed and continue to be in the business. And there are generally two ways to do this [12], [11]:

Out-store tactics: This deals with supply-chain management, personnel management, inventory management, advertising campaigns, marketing, product positioning, pricing and all other stuff related from manufacturing of the product to its placement in the supermarket shelves. Out-store tactics generally deals with operational costs and procedures.

Table 1. Trends in Supermarket Optimization

What	Out-Store	In-Store	Real-Time	Impulse	Shelf
Shopping Paths		✓			✓
Neural Networks for Future Sales		✓			
Shelf-Management and Space Elasticity		✓			✓
Genetic Algorithm for Marketing	✓				
KBS for Product Positioning		✓			✓
Demand and Supply Chain Management	✓				
Optimization in Sales and Marketing	✓				✓
KBS for Market Analysis	✓				
Data Mining		✓			
Expenditure Decisions		✓		✓	
Shelf Allocation		✓			✓
Store Environment and Available Time		✓		✓	
Optimization of Retail Space		✓			✓
Shelf-Space and Unit Sales		✓			✓
Factors of Impulse Purchases		✓		✓	
Customers' Learning from Experience		✓			
Modeling Stimulus-Organism-Response		✓			
Effect of Background Music		✓	✓		
Store Ergonomics		✓			✓
Mental Mapping of Supermarkets		✓			✓
Impulse Buying Factors		✓		✓	

In-store tactics: This is when customers reach the supermarket. How sales and profits can be increased. This includes (but not limited to) bargains, everyday low prices, special and limited offers, buy-one-get-one type of schemes, free samples, shelf-reorganization, cross-categorization and use of previous data to forecast the sales and requirements for the future.

Table 1 summarizes many works related to in-store and out-stores tactics. The bulk of the research has been focused on the use of neural networks [12], genetic algorithms [7], KDD (Knowledge Discovery in Databases) and data mining [2], [5] to search the patterns and information in the past data to predict the future sales and requirements [12]. For example, a neural network is trained to predict the future values of a time series that consists of the weekly demand on items in a supermarket. Genetic algorithms are used to find out the most competitive marketing strategy for product positioning by creating the population of all available strategies and taking out the best after evolution, based on some goodness criteria [7].

As can be seen in Table 1, there is only one work where real-time issues have been considered as a mechanism to increase in sales [9], [10]. None of the works discussed the possibility of real-time increase in sales and profits based on real-time customers' feedback but it can be done via proposed Herd model. Milliman realized the need to influence the customers in real-time [9]. He used background music to produce certain attitudes among customers to stimulate customers purchasing.

The majority of the work described in this section either work before customer gets in the market (out-store tactics) or after customer leaves the market (in-store tactics). Our aim is to work on existing customers, those who are already in the supermarket, busy in their shopping. How we can stretch their buying limits and what we can offer to them in real-time by imposing the herd behavior? Ideally, the implementation of the

proposed model can provide costumers with a better shopping experience and retailers with a higher sales level, thus easing the tension that we described earlier between the customers' and the stores' goals. The proposed model can also gives the general idea about return-on-investment (ROI) on using such a technology for supermarkets.

Based on this initial analysis of the literature next section explains the three models of supermarket optimization derived from multiple perspectives. Section 3 explains the implementation details of the super market simulation. The analysis of the results of the simulation is presented in Section 4. The paper concludes by highlighting some of the limitations of the research along with proposed extensions for this research work.

II. MODELS

There are three models and a set of special animates (cheaters) explained in this section. The first model is the base model of customer profiles. The second model of Sales is derived from the literature review of supermarket optimization. The third model of Herd generator is the key contribution to portray and measure the effectiveness of generating herd behavior. The models are being tested and compared in the simulated environment of supermarket. There are few animates – that programmed to cheat the system – to measure the vulnerability of such a technology.

A. Customers' Profiles

It is quite intuitive to think that customers have profiles that represent their product preference. Customers may be very interested in CDs but not very interested in books. What the profile of such a customer represents is the likelihood that (all

things being equal) a customer will pick up a product *A*. It should be clear that what this profile indicates is that a customer is more inclined to buy products in *c(A)*, meaning the class of product *A*, than in *c(B)*, with $c(A) \neq c(B)$, it will have a higher probability of purchasing *A* than *B*. By “all things being equal” it is meant that the product *A* and *B* have the same characteristics that influence purchase such as price, discount level, etc. Hence, the profile represents a purchase probability of customer per product category. This probability let us call *ip*, is influenced by other factors described in sales and herd model – discount level, and collective sale level.

B. Sales Model

Everyone likes a bargain and our model does not disregard this. It has been argued that the influence of sales spikes in sales volume against the depth of promotion [3]. Equation 1 attempts to capture this behavior. In the equation, μ is a constant that controls the location of the spike in sales. Essentially the growth in sales is not linearly proportional to the sale level. For instance, the influence of a 10% off sale in a product is not always 10%.

$$f_{onsale}(x) = 1 - e^{x \log(1-a)} - \mu \quad (1)$$

In the implementation used here, we have used $\mu = 0.1$. The value of a controls the slant of the curve. The value $a = 0.03$ has been used in this paper. Note that x is the discount level being offered to the product.

C. Herd Model

The proposed Herd model attempts to capture the collective average choice’ that costumers are taking. Customers equipped with RFID-enabled shopping carts can get information about other customers purchase patterns and are constantly informing the store of their own shopping behavior. This can be easily achieved because the carts “know” what products are inside the cart at any point. Unlike bar codes, RFID tags do not need line-of-sight to scan the products and can be scanned simultaneously [8]. The combination of what all the customers are doing can be used to indicate to some customers about how good a particular deal in the store actually is — if many people are buying, it is probably a good deal. Recommendations should be able to vary significantly with time. Note that the recommendations are considering customers in store and the emergent behavior of one group may not necessary be the behavior of another group on a different day. We do not need to worry about why people buy, what are their ages, race, sex or financial status to increase the shopping. All this information although important is embedded in their behavior and will be captured by Herd model because it considers what each customer is doing.

The Herd model is based on the level of purchase of products by other costumers in the store at the same time. The behavior of this influence is based on a step-function

(represented by a sigmoid function). The function conveys the idea that customers do not care about others’ purchases until it reaches a threshold when the influence greatly improves and then stabilizes. The Equation 2 represents this step-like behavior where x represents the percentage of people currently buying the product in supermarket. Constants a and b control the slant of the function and the mid point of the step function. In our simulations we have used $a = 0.1$ and $b = -50$.

$$f_{HERD}(x) = \frac{1}{1 + \frac{1}{e^{a(x+b)}}} \quad (2)$$

D. Cheaters

The discussion on Herd model is not complete without mentioning the privacy concerns that comes with it. After implementation of the Herd model, the next concern arises is of the technology misuse? How we measure the penetration of false or controlled information within the Herd model? How vulnerable the proposed system is when it comes to feedback, trust and recommendations?

To address these and several others related issues we have introduced the controlled animates. We call them *Cheaters* – a cheater is an animat that can be controlled by the supermarket for their own benefit but it treated as an ordinary animate by other animates. Think of a customer who is buying just to increase the number of units sold and therefore increasing the chances of products’ recommendation by Herd model. It should be noted that cheaters are ordinary animates and not leaders, no body is following them. We have tried to intervene in this complex system of supermarkets through Soft-Control by inducing the several cheaters within the system for the benefit of the supermarkets. Soft-Control is a natural way to intervene in the complex systems [4]. The cheaters can cheat and exploit the portion of influence they have being a customer (animat) on overall supermarket’s Herd behavior. The cheaters have their own list of items to purchase, we call it list C – that contains the products supermarket wanted to sell more. All cheaters have the same list to increase the influence of their recommendation on Herd model. The simulation details presented in the next section also tested the influence of cheaters on the performance of the Herd model as an optimum tool of sales.

III. THE SIMULATION

For validating the recommendation of using Herd model as a marketing tool a simulation was implemented and tested using test dataset. The implementation of supermarket simulation used a database where profiles of animates (customers) and products are present. The product profiles basically represented the product description, that included name, code, color, size, weight, price, promotion, brand, expiry date (if any) etc. The database consisted of 120 products in total.

There were few assumptions that were taken for this simulation: animates have enough money to buy, animates can see only one product at a time and cannot buy the same product twice, there is no shortage of products in the shelves and all animates are equipped with RFID-equipped shopping carts. The rationale for having these assumptions was to retain the focus of the research onto the applicability of Herd's Model in a supermarket scenario.

$$P_{new} = P_{profile} + (1 - P_{profile}) \times F(x) \quad (3)$$

To make the decision to buy an item or not, program uses Equation 3 where a factor $f(x)$ is applied to the main probability of buying (from the animates profile), the factor $f(x)$ represents the sales model (in Equation 1), or the Herd model (in Equation 2), or both applied in series. The probability p_{new} is then used by the animat to get the product or not. The probability p_{new} is then used by the animat to get the product or not.

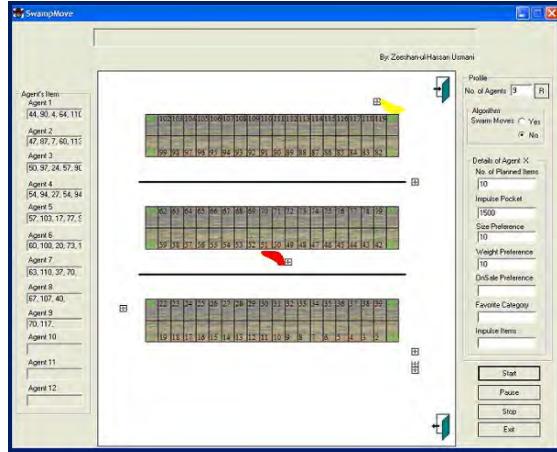


Figure 1. Visual Depiction of the Supermarket Simulation

IV. RESULTS

This section concentrates on demonstrating that Herd model is indeed a model that enables improvement of overall sales volume in supermarkets. Based on what can be seen here in simulations, it is argued that Herd model is an interesting sales and marketing tool. As observed by results presented later, the effects of Herd model is comparable to the effects of sales prices and price promotions in the supermarket but more significantly the Herd model offers similar results without losing money on sales deals or price reduction. It is also argued that Herd model is able to generate better unit sales by

incorporating *average common choice* as a feedback to other customers.

The following results are average of 2,000 sample runs with different number of animates in each set of simulation (ranging from 200 to 500 — experiments used minimum 200 animates to have enough animates to calculate the average common choice and maximum 500 animates due to the limited supply of unique customer profiles). Products and animates details were loaded from their respective profiles, and no random value (i.e. value for likelihood, favorite category, product price etc) has been selected during the simulation.

Figure 2 clearly demonstrates the performance of Herd model over Customer profiles and Sales model, Herd model is able to get more than double sales over Customer profiles and 29% extra over Sales model.

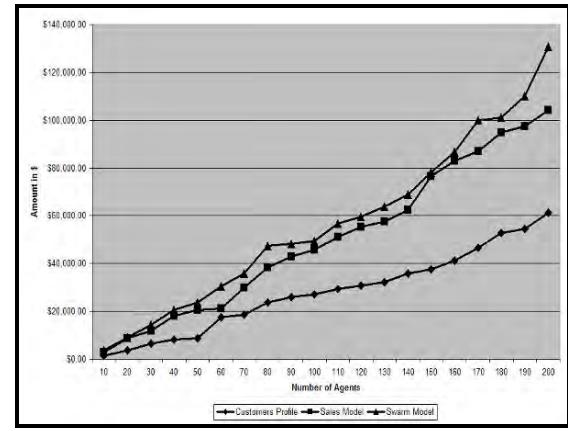


Figure 2. Total Sales with Customer Profiles, Sales and Herd Models

Few cheaters have been introduced with Herd model to measure their influence and power to silently orient the customers towards the item from their buying list C. Interestingly, the number of cheaters required to influence the ordinary customers found to be almost same as ordinary customers present in the supermarket. Since, proposed Herd model works on sigmoid function, ordinary customers need a certain threshold to be inclined towards some product.

To introduce same number of controlled customers (Cheaters) as the ordinary customers to influence their shopping behavior is not an economical approach for supermarkets. The few cheaters in due time can create a cloud of feedback (where more customers joined in as time passes), but the total time they will need to influence is way more than the average time a typical customer spend in the supermarket. Figure 3 presents the same linear growth of influence proportional to the number of cheaters being used. This finding in fact is the good news for customers, so that they can confidently buy and listen to Herd model recommendations without the fear of being seduced by fake or controlled customers.

The supermarket simulation was used to run a few other interesting experiments with Herd and Sales Model to find out the optimum percentage of average promotion-depth in the supermarket. The chart depicted in Figures 4 demonstrates a loss in profit after the depth in promotion (percentage off from the regular price) reaches 50%, since the average profit margin is 50% in the supermarket (this value is coming from the items profiles – product actual price minus (-) retail price to calculate the profit).

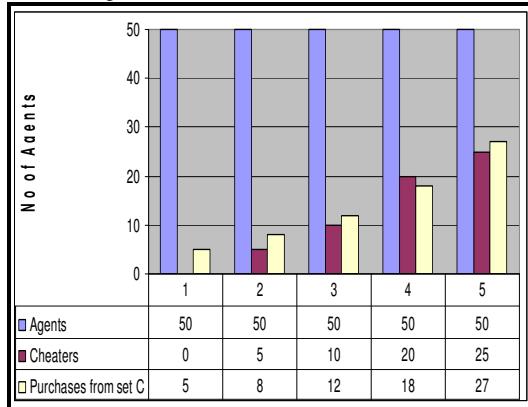


Figure 3. Influence of Cheaters

The 20% average sales-off price has achieved the highest profit and 50% average sales-off price has achieved the highest sales-volume in both models in the simulation. As observed in this simulation, if the supermarket wants the highest profit, the average depth of promotion can go up to 20%. If the highest sales-volume is the priority, the average depth of promotion can go up to 50%. These results clearly indicate how supermarkets can forecast their performance based on their prioritized parameters by using Herd model as a marketing tool.

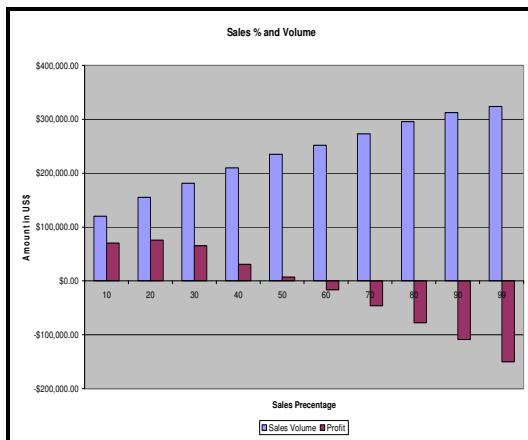


Figure 4. Optimum Percentage of Depth-of-Promotion in Sales Model

V. CONCLUSION AND FUTURE WORK

This paper proposed the implementation of Herd model to generate and analyze the herd behavior in shopping at supermarkets, and a simulation to measure its performance. The simulation demonstrated Herd model as an effective marketing tool for supermarkets to increase their sales volume based on emergent properties of customers in the store. As of today, Herd model with the simulation can answer many questions such as what would be the benefit of using RFID tags and scanners in the supermarkets. For instance questions like what is the collective customers' choice in given amount of time with a set of customers? What is the effect of depth of promotion on sales volume? How and on what level systems based on proposed model can be compromised for marketing purposes with fake customers.

There are several improvements that can be made in the future. First, the simulation does not act on all customers at the same level. As the customers who first enter in the supermarket have least benefits, all new settings and patterns are for late customers who can already get the benefits of the emergent properties of other customers captured by Herd model. This problem can be solved by using parallel layout or multiple entrances and exits. A controversial parameter is on-Sale, if we place the products on sale in real-time by incorporating customers interest in a particular product in real-time, customers can have different prices of the same product bought from the same store in the same day. We would also like to work on offering bargains of two or more things together. Herd model can also be extended to offer clues on how shelf-organization should take place. It may be possible to use the emergent properties of the customers to change shelf organization in a more agile manner. Further more extensive research on the impact of cheaters on the use of Herd model can be done to identify any exceptional instances where cheaters can negatively influence the Herd model performance.

Our initial results in this paper indicate that environmental information can be used to influence customers and make them buy more in real-time. However should be validated in a real supermarket setting.

REFERENCES

- [1] Randolph E Bucklin, David R Bell and Catarina Sismeiro, Consumer Shopping Behaviors and In-store Expenditure Decisions, In Consumer Shopping Behaviors, 2001.
- [2] Dorothy G. Dologite, Developing a Knowledge-based System for Product Position Advertising Strategy Formulation, IEEE, 0-18186-3730-7, 1993.
- [3] G Garrick, Spend Better Advertising Dollars, Not More, Advertising Research Foundation, Electronic Media Workshop, 1986.
- [4] Jing Han, Ming Li and Lei Guo, Soft Control on Collective Behavior of a Group of Autonomous Agents by a Shill Agent, Journal of Systems Science and Complexity, 2006, Vol 19, pp. 54-62.

- [5] Jacob Jacoby, Stimulus-organism-response reconsidered: An Evolutionary Step in Modeling (consumer) behavior, *Journal of Consumer Psychology*, Vol 12(1), 2002. pp 51-57.
- [6] Jeffrey S. Larson, An Exploratory Look at Supermarket shopping Paths, 2004.
- [7] Robert E. Marks and G. M. Shiraz, Using genetic algorithms to breed competitive marketing strategies, 1998.
- [8] K. Micheal and L. McCathie, The Pros and Cons of RFID in Supply Chain Management, *IEEE Proceedings of the International Conference on Mobile Business*, 2005, pp. 623-629.
- [9] Ronald E. Milliman, Using Background Music to Affect the Behavior of Supermarket Shoppers, *Journal of Marketing*, Vol 1, 1982, pp 86-91.
- [10] Michael Morrison, The Power of Music and Its Influence on International Retail Brands and Shopper Behavior: A Multi Case Study Approach. Monash University, 1999.
- [11] Philippe Naert and Alain Bultez, SHARP: Shelf allocation for retailers' profit. *Marketing Science*, Vol 7, 1988.
- [12] Hawkins Stern, The significance of impulse buying today, *Nature and Significance of Consumer Impulse Buying*, Vol I, 1962, pp 59-62.
- [13] Supermarket Research, Supermarket strategic alert special report, 2004.

Light Path Provisioning using Connection Holding Time and Flexible Window

Fatima Yousaf, Savera Tanvir, SMH Zaidi

School of Electrical Engineering and Computer Sciences

National University of Science and Technology

Chaklala Scheme III, Rawalpindi, Pakistan

{Fatima.yousaf, Savera.tanvir, drzaidi}@niit.edu.pk

Abstract-Connection provisioning with survivability has become very critical in optical networks in order to meet the increasing bandwidth requirements of applications. Shared path protection is a promising technique to provide survivability in network, but this technique also suffers from some redundancy in network. In this paper we have surveyed algorithms that support provisioning of connections with shared path protection and mixed shared path protection. Different connection provisioning strategies have been compared with respect to complexity and blocking probability. This paper focuses on exploiting the knowledge of holding time of connections to make an advance reservation of connection request in a given larger window, which will reduce blocking for future connections. For this purpose paper we proposed an enhancement in HT-AGSDP algorithm [1], that already exploit the knowledge of connection holding time in making choice of primary and backup path connection.

Keywords: Hold time, Wavelength Division Multiplexing (WDM), Shared Path Protection (SPP), Survivability, Resource overbuild, Blocking probability.

I. INTRODUCTION

Wavelength Division Multiplexing (WDM) networks has gained increasing importance due to their scalability. A lot of research has been done on maximizing the utilization of WDM resources, so that maximum connections can be established leading to low blocking in network. A WDM network carries a large number of connections at a time and a failure in network can cause huge loss of data. So focus of research is also to provide survivability in network along with the objective of minimum blocking probability. Survivability can be achieved in two ways, restoration and protection. Restoration is efficient in resource utilization and slow in recovery time as in restoration when a failure occurs the backup path is allocated to connection. Opposed to it, protection provides fast recovery time at the cost of less utilization of resources. Protection requires establishment of primary and backup paths at the time of connection request. The protection can be link or path based. The path protection can be dedicated or shared. Dedicated protection can be (1+1) or (1:1). In dedicated (1+1) source send data on both primary and backup links simultaneously. In dedicated (1:1) the data is send on

primary path only and backup path is used to transmit the unprotected data. So the resources are underutilized in (1+1) protection as compared to (1:1) protection, but the recovery speed of (1+1) is better than (1:1). Shared path protection allows the backup path wavelengths to be shared among the connection provided the corresponding primary paths are node and link disjoint. This will maximize the utilization of network resources, but the recovery speed will decrease.

A lot of research has been conducted in provisioning of primary and backup path for a connection in network. In today's environment, the start time, end time and the holding time of a connection can be known in advance through the service level agreement (SLA), which is an agreement between the network operator and its customers. This paper proposed enhancement in HT-AGSDP [1] algorithm that adds flexibility in HT_AGSMP. The set up time of demand is not known in advance, only holding time, start time and end time of larger window is known. Given these parameters our proposed algorithm will use concept of advance reservation with flexible scheduling window that will select a time slot in a larger window that will maximize the resource utilization in network and will result in low blocking probability for future demands.

HT-AGSDP is chosen because it was the first algorithm that jointly considered availability guaranteed and holding time aware approach. It's a connection holding time aware algorithm, among the multiple candidate backup paths it chooses the one that ensure higher degree of sharing, and tends to decrease dedicated path protection. The holding time algorithm chooses 15% dedicated paths rather 20% in AGSDP and it has around 2.5% gain in Resource overbuild (RO) as compare to AGSDP [1].

Section II discusses the related work in area of path protection, section III discusses the problem statement and section IV discusses the base line algorithm followed by proposed algorithm and its complexity. We conclude paper with a summary and future work in the section V.

II. RELATED WORK

Many algorithms have been proposed that have used SPP for selection of primary and backup paths. CAFES computes two link disjoint paths based on a two step approach. In first step a

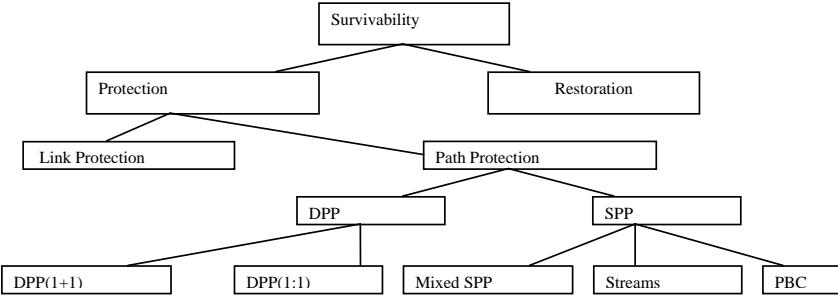


Figure 1: Classification of survivability schemes

set of K minimal cost primary paths is calculated base on Yen's algorithm.

In the second step the cost of links are updated. Base on the link cost assignment minimum cost backup path is calculated for each primary path in a set of k paths. Given the cost of set of k working and backup paths that combination of primary and backup path is chosen which has minimum cost [4]. AGSDP provides availability guaranteed connections. It decides based on Service Level Agreement (SLA) requirements that either of the unprotected path, shared path protection or dedicated path protection provisioning is needed to satisfy the availability requirement of an in coming connection. Two step, edge disjoint, path pair algorithm is used in AGSDP which tries to find the primary and backup paths one after the other using a shortest path algorithm, according to assigned link cost for a given source destination pair [2].

To improve sharing in network MIX shared path protection (MSPP) has been introduced. MSPP allows the Primary (p_1) and backup path (b_0) to share the capacity if p_0 is completely covered by p_1 . A link is traversed by both p_1 and b_0 . Primary Wavelength link w_0 is not mix wavelength link (if it has been changed to a mixed wavelength link, it will be marked by a flag).

MSSP further enhanced the sharing by allowing a mixed wavelength link to be shared by another new coming backup path if the two corresponding primary paths of backup paths are link disjoint. This allowed the redundancy to be reduced from the network [7].

The issue of SRLG disjoints Path protection in WDM Mesh networks is addressed by an algorithm called Mixed Shared Multi path protection (MSMPP). The MSMPP tried to find Shared resource Link Group (SRLG) disjoint path [8]. Simulations have proved that by making the two stages of primary path selection and backup path selection correlated, the network performance can be improved. During the first phase of algorithm all those links are removed from network that do not provide the connection requested bandwidth w , then it assign a cost of $w + \beta_e(w)$ to each link before the AP is selected, where $\beta_e(w) \leq w$ represents the Potential- Backup-Cost (PBC) i.e. backup bandwidth to be used in corresponding backup path which is to be chosen in next phase. This is how PBC-Based method correlate the two phases [10].

A limitation of SPP is its slow recovery time. The calculation of recovery time for SPP can be performed as follows [12]:

Following notations are use to calculate recovery time.

F : time to detect a link failure by the node adjacent to the link.

D : Message processing time at a node.

P : propagation delay on each fiber.

C : Time to configure and test a cross connects.

h_s : the number of hops from node adjacent to the failed link to the source node of the connection. .

h_b : the number of hops in a backup route from source node to destination node.

Restoration time for SPP is calculates as

$$F + P \times h_s + (h_s + 1) \times D + h_b \times C + 2 \times h_b \times P + 2 \times (h_b + 1) \times D. \quad (1)$$

To improve the recovery speed of SPP the Pre-Cross configuration has been implemented. Stream algorithm provides a way where the recovery time is comparable to DPP and Capacity utilization is comparable to SPP. The backup wavelength is shared only if backup paths do not diverge. All the PXCs on backup path that act as intermediate PXCs are preconfigured. In case of failure, switching takes place only at end nodes as in DPP. So its recovery speed is identical to DPP 1:1 [11].

The calculation of recovery time for streams can be performed as follow:

$$F + P \times h_s + (h_s + 1) \times D + 2 \times C + 2 \times h_b \times P + 2 \times (h_b + 1) \times D. \quad (2)$$

Another limitation of SPP is that to better use protection capacity the connections with shorter paths are assigned longer paths that result in high PI-expansion (ratio between allocated backup path and the shortest backup path for a connection request) values as compare to streams even when the average path length is low [11]. All the sharing techniques that have been described so far either focus on maximizing the sharing of resources or improving the recovery speed but none of these take into consideration holding time of connections. In Holding time unaware approaches the link cost assignment for back up path basically identifies three link states with respect to incoming backup path: not sharable (infinite cost), sharable but not usable (full cost), sharable (negligible cost).

Actually the state of a given link changes during the incoming connection holding time. For example a connection

which is considered as sharable at the arrival instant of a new connection may, during the lifetime of the incoming connection, assume a different state due to allocation or deallocation of connection arrivals and departures. Resource Overbuild (RO) in shared-path protection can be decreased by exploiting the holding-time information of connections which have already been provisioned in the network.

Provisioning by Holding Time Opportunity (PHOTO) Algorithm consider the holding time of connections. The main idea of PHOTO was to check the holding time of all existing connections when a new connection request arrives, and for the backup path use the link corresponding to backup path of the connection with the longest holding time as it will stay longer in the network and hence will be sharable for a longer time [6].

The concept of advance reservation with flexible scheduling window allows selecting a setup and teardown time of a connection request in a given sliding window [13], [14]. The flexible window scheduling allocates resources in such a way that minimizes the congestion in network. As the SLA give information about the setup time, hold time and tear down time of a connection, so the concept of similar sliding window has been proposed in this paper that help to choose time slot that will allow maximum sharing of resources using the integrated cost function of HT-AGSDP and link load cost. The link load cost is a function of number of connections that are already reserve for a link in a specific time slot, which will result in load balancing. The two step algorithm approach suffers from the disjoint trap or a Resource shared caused trap. Many papers have proposed survival of traps using K-shortest paths [7], our proposed algorithm also uses k-shortest path strategy in order to avoid traps in network.

Another important concern is to have either partial or complete information about the routing and wavelength assignment of existing light paths to decide on backup up sharing. Two Shared Backup Path Protection (SBPP) methods, sharing with Partial information (SPI) and Sharing with Complete information (SCI) have been analyzed in [8], [10]. The difference between these methods involves the aspects of routing information sharing and route searching algorithms. SPI and SCI have same order of control overhead, state storage memory and computational complexity.

SPI shows higher blocking probability than SCI. SCI can quite significantly outperform than SPI, so it is of significance importance to allow network to share complete routing information. Per- Flow SCI has shown a marginally inferior performance as to aggregate SCI. In this paper we focus on complete information based algorithm.

In a network traffic can be static, incremental or dynamic. In case of static traffic all the connection requests are known in advance. In incremental traffic light paths established for connection remain in network indefinitely, while in case of dynamic traffic a light path is established

for each connection as it arrives, and the light path is released after some finite amount of time. In case of static traffic aim is to minimize network usage, while in case of incremental and dynamic traffic aim is to minimize blocking probability. Our paper only considers the case of dynamic traffic, where connection holds for a specified time. In order to minimize blocking probability Advance reservation is an attractive choice.

Our proposed algorithm uses Slide Window First (SWF) scheduling strategy, in which one path is checked at a time for all of the sliding window slots. If path can not be reserved during scheduling window a next shortest paths is checked for all sliding window slots [14].

III. PROBLEM STATEMENT

The dynamic path protection problem in WDM networks can be formally stated using following inputs, constraints and objectives.

A. Inputs:

1. A weighted directed graph $G=(V,E,C, \lambda)$, where V is the set of nodes, E is the set of unidirectional fibers, C is the cost function for each link, $C: E \rightarrow R^+$ denotes set of positive real numbers , and λ is number of wavelengths on each link $\lambda: E \rightarrow Z^+$ denotes set of positive integers . λ_e denotes number of free wavelengths on link e , $e \in E$.
2. The set of existing light paths in the network at any time is denoted by $L=\{l_w^i, l_b^i, t_a^i, t_h^i\}$ } where the quadruple specifies the working path, the backup path, arrival time and holding time for i_{th} light path.
3. A connection request(s, d, t_h , α , γ), where s is the source node, d is the destination node t_h is the hold time along with ‘ α ’ Start time ‘S’ and ‘ γ ’ end time ‘E’ of larger window.
4. The ‘ s_t ’ setup time of a demand must meet the condition that $S < s_t < E$.
The s_t can be represented as set of time slots $s_t = \{a_1, a_2, \dots, a_n\}$, where $a_1 \geq \alpha$ and $a_n \leq \gamma - t_h$.
 $a_{i+1} = a_i + t_h$ for $i = 1, 2, \dots, n$

B. Constraints:

Following are the constraints that any shared path looks for.

- C.1 Working and back up paths are link disjoint and node disjoint.
- C.2 Any two working paths do not utilize the same wavelength on any common link they traverse.
- C.3 A working path does not share any wavelength with any backup path on common link they traverse.
- C.4 Any two backup paths can share a wavelength on a common link only if their working paths are link disjoint.
- C.5 Working and backup path should be established in same time slot.

C. Objective:

Given these constraints, objective is to dynamically select

TABLE I
COMPARISON OF SOME RESEARCH WORK THAT HAS BEEN DONE IN AREA OF SURVIVABILITY.

Research Work	D/N	P/L	WC	L/N	Contributions
Mixed SPP	D	P	N	L	Reduce blocking probability as compare to SPP.
Streams	D, N	P	Y	L,N	Develop to implement in all optical networks. Reduce Recovery Time as compare to SPP.
MultiPath Mixed SPP	D	P	N	L	Reduce blocking probability as compare to SPP.
PBC	D	P	N	L	Reduce the complexity as compare to ILP for shared path protection.
AGSDP	D	P	N	L	Provide Service differentiated Services with availability guaranteed.
HT-AGSDP	D	P	N	L	Consider connection Holding time in provisioning of backup paths.

D/N: Dynamic/Non-Dynamic. P/L: Path/Link protection.
WC: Wavelength Continuity Constraint. L/N: Link /Node Failure

working path and a back up path from a set of given paths. Given start time, end time and holding time of requesting connection, select a time slot that ensures maximum remaining resources on the links on selected path. It will help to reduce blocking probability in network for future requests.

IV-PROPOSED ALGORITHM

A. Base Line Algorithm (HT-AGSDP):

HT-AGSDP provides availability guaranteed connections. It's the first algorithms that jointly considered availability guaranteed and holding time aware approach. By using a holding time aware approach, future sharing of candidate back up paths can be estimated and this additional information, if opportunistically exploited, can lead to more efficient resource utilization.

Each release of a share backup path within the holding time duration of a connection will change the sharing of some candidate backup links, which will modify availability and thus the cost of our candidate links in the algorithm.

The Steps of HT-AGSDP can be described as follow.

1. Compute the most reliable path (MRP), the path with maximum availability from s to d among all the path candidates [12]. Choose it as the primary path for the connection t. if $A_p \geq SLA$, Set $A_t = A_p$ and go to step 6. If no such path is found, the connection is blocked and returns NULL.

2. Compute the backup path b from s to d according to newly defined link cost function C(e).

$$C(e) = 1/t_b(\Delta t_1) \cdot C(e, \Delta t_1) + \Delta t_2 \cdot C(e, (\Delta t_2) + (\Delta t_3)) \cdot C(e, (\Delta t_3)), \quad [1]$$

if no such path is found connection is blocked and return NULL. Each $C(e, \Delta t_i)$ is calculated as follows.

$$C(e) = \begin{cases} \infty & (i), \\ \varepsilon \times \alpha(e) \times (-\log(A(e))) & (ii), \\ 1 + \varepsilon \times \beta(e) \times (-\log(A(e))) & (iii). \end{cases}$$

Where

$$\varepsilon = \text{Small number e.g } 10^{-5} \quad [1]$$

$$\alpha(e) = (N(e)+1)/(B(e)+1) \text{ for link } e$$

$$\beta(e) = (N(e)+1)/(B(e)+1) \text{ for link } e$$

$N(e)$ = Number of connections, $B(e)$ = Number of Wavelengths on link e

Case (i) (infinite cost) corresponds to insufficient resources in the link for routing the backup path. Case (ii) (negligible cost) correspond to the sharable back up pool where there is no need to allocate extra spare capacity for the incoming connection. Case (iii) (Full Cost) gives the cost of the link where a new wavelength needs to be added in the backup pool.

The time-interval-weighted sum and partial cost calculation of HT-AGSDP allows defining different sharing degrees. Partially sharable links are the ones that are sharable at the moment of an incoming connection request but will be unsharable due to future connection departures within the holding time duration. Initially partially sharable (case ii with negligible cost) may then become un-sharable due to some departures, and so the cost assignment should switch to case (iii) with full cost. Therefore, the cost of partially sharable links will increase inversely proportional duration of time interval in which the backup pool is sharable. On the other handful sharable links will stay at case (ii) with negligible cost. [1]

3. Compute A_t as follow.

$$A'_t = A_p + (1 - A_p) \times A_b \times \prod_{e \in b} \frac{B(e)}{N(e)+1} \times \prod_{e \in b_u} \frac{B(e)+1}{N(e)+1} \quad [1]$$

if $A_t < SLA$ reserve one more backup wavelength on each link $e \in b$. If reservation fails due to link bandwidth limit, go to step 4, else go to step 5.

4. Reserve one dedicated backup wavelength on each link $e \in b$. If reservation fails due to link bandwidth limit, the connection is blocked and return NULL, Compute A_t as follow.

$$A_t = A_p + (1 - A_p) A_b \quad [1]$$

if $A_t < SLA$, the connection is blocked , and return NULL, else go to step 6.

5. Re-compute the availabilities for all connections in BSCG (e) for each link $e \in b$. If there is any connection

- $i \in \text{BSCG}(e)$ whose recomputed availability does not meet its SLA , reserve one more backup wavelength on each link $e(i) \in b(i)$. If the reservation fails due to link bandwidth, go to step 4, else recompute A_t , if $A_t < \text{SLA}$, go to step 4.
6. The connection is accepted and a path p , or a path pair p and b is set up. Update link resource information according to different provisioning and protection schemes.

B. Proposed Algorithm:

Part I

```

 $i = 1$ 
 $MTC, Tc = \infty$ 
 $s, d, t_b, \alpha, \gamma$ 
while( $i \leq k$ )
  start time =  $\alpha$ 
  end time =  $s + t_b$ 
  find shortest path with Dijkstra's algorithm with slot load link cost
  if a path is found then
    while (end time  $< \gamma$ )
      if wavelength available on all links during a slot
        if  $A_p > \text{SLA}$ 
           $Tc = \text{Slot load cost}(p)$ 
        else
          find backup path with Dijkstra's algorithm with integrated cost of  $C(e)$  and slot load link cost
          if a path is found then
            if  $A_{\text{shared}}(p,b) > \text{SLA} \&& \text{if No Violation}$ 
               $Tc = \text{Slot load cost}(p) + \sum \text{link cost } (C(e)) (b)$ 

```

Part II

```

else
  if free wavelength on backup path
    Reserve  $w$  on backup path  $B(e)++$ 
    if  $A_{\text{shared}}(p,b) > \text{SLA}$ 
       $Tc = \text{Slot load cost}(p) + \sum \text{link cost } (C(e)) (b)$ 
    else
      if  $A_{\text{dedicated}}(p,b) > \text{SLA}$ 
         $Tc = \text{Slot load cost}(p) + \sum \text{link cost } (C(e)) (b)$ 
      end if
    end if
  end if
end if

```

```

if  $Mtc > Tc$ 
   $Mtc = Tc$ 
  Primary path =  $p$ 
  Backup path =  $b$ 
  Setup time = start time
end if
start time = start time +  $t_b$ 
end time = start time +  $t_b$ 
end if
end while

Part III
else
  remove the busiest link during the window from topology
end if
 $i++$ 
end while
if  $Mtc < \infty$ 
  reserve wavelengths and update link costs.
  return
else
  block connection
end if
Where:
Mtc: Minimum Total Cost
Tc: Total Cost
 $\alpha$ =Start time of larger window
 $\gamma$ =End Time of larger window
Ap= Primary Path Availability

```

Three parts of algorithm are performing different task. Part I find the shortest path, and check that wavelengths are available or not. If wavelengths are available then it checked that Ap meets SLA or not. If not then in Part II, a new wavelength is reserved. Part III controls when the algorithm will stop executing.

C. Computational Complexity

(i). Complexity of AGSDP and HT-AGSDP:

The computational complexity of AGSDP is $O(|E|^2)$. The over all complexity of HT-AGSDP is $O((R \times H) + X |E|^2)$, where E stands for edges, R stands for number of connections offered in a time unit and H is the holding time of the connection.

(ii). Complexity of proposed Algorithm:

The over all complexity of proposed algorithm is $O(K \times N \times ((R \times H) + X |E|^2))$, where N is the number of time slots in the sliding window for which the algorithm repeats and K is the number of paths that algorithm might traverse.

D. Advantages of Proposed Algorithm

The proposed algorithm adds flexibility in HT-AGSDP. It uses two step algorithm to find the link disjoint primary and

backup path. The algorithm avoids traps using K-Path strategy as suggested by [4]. It will reduce blocking probability in network as the algorithm for each of k paths uses SWF which will check for all slots in the larger window in order to search the slot that offers the path with minimum cost and that also meet SLA availability requirements either through unprotected, protected or dedicated path provisioning. So, minimum resources will be utilized in network for a connection request, which in turn will leave maximum resources in network for future connection request.

A connection will be blocked if and only if any of the k paths in any of the slots of the larger window does not meet SLA requirements either through the unprotected, protected or dedicated path provisioning.

In order to improve the computational complexity the part III of algorithm can be changed as follow.

```

if Mtc<∞
    reserve wavelengths and update link costs.
    return
else
    remove the busiest link during the window
    from topology
end if
i++
end while
else
block connection
end if
```

Change in this part of algorithm reduce the computational complexity of algorithm as the algorithm will now first take a path and will check all the slots of larger window to find a slot that offer minimum cost and also meet SLA, then if a slot is found ,the path is returned and next paths are not checked.

V. CONCLUSION

In this paper an algorithm has been proposed that is going to add flexibility in HT-AGSDP and will reduce blocking probability as if a path pair is not found that meets SLA in first time slot then it may be found in next time slots. In addition it will choose that pair of primary and backup costs that will minimize the total cost of primary and backup paths, resulting in maximization of resource utilization that will reduce blocking probability for future connection requests. The algorithm will also help reduce the problem of traps without using the K-Shortest paths. Main objective of algorithm is to add flexibility to optimize backup sharing. It will show savings in backup resource usage that can be achieved at moderate load levels.

REFERENCES

- [1] Cicek Cavdar, Lei Song, Massimo Tornatore, and Biswanath Mukherjee, “Holding-Time-Aware and Availability Guaranteed Connection Provisioning in Optical WDM Mesh Networks”.

[2] Lei Song, Student Member, IEEE, Jing Zhang, Member, IEEE, and Biswanath Mukherjee “Dynamic Provisioning with Availability Guarantee for Differentiated Services in WDM Mesh Networks.” proc. of IEEE OFC’ 2005.

[3] Lei Song, Student Member, IEEE, Jing Zhang, Member, IEEE, and Biswanath Mukherjee “Dynamic Provisioning with Availability Guarantee for Differentiated Services in Survivable Mesh Networks.” IEEE Journal On Selected Areas In Communications, Vol. 25, No. 4, April 2007.

[4] C. Ou, J. Zhang, L. H. Sahasrabuddhe, and B. Mukherjee, “New and improved approaches for shared-path protection in WDM mesh networks,” IEEE/OSA Journal of Lightwave Technology, vol. 22, no.5, May 2004, pp. 1223-1232.

[5] J. Zhang, K. Zhu, H. Zang, and B. Mukherjee “A New Provisioning Framework to Provide Availability-Guaranteed Service in WDM Mesh Networks,” Proc. of IEEE ICC’03, May 2003, pp. 1484-1488.

[6] Massimo Tornatore, Canhui Ou, Jing Zhang, Achille Pattavina and Biswanath Mukherjee. “PHOTO: an Efficient Shared-Path-Protection Strategy Based on Connection-Holding-Time Awareness”, Journal of Lightwave Technology. VOL.23. NO.10. October 2005.

[7] Lei Guo, Jin Cao, Hongfang Yu and Lemin Li “Path based Routing Provisioning with Mixed Shared Protection in WDM Mesh Networks” Journal of lightwave technology. VOL 24, No.3, March 2006.

[8] Gangxiang Shen , Wayne D. Grover. “ Survey and Performance Comparison of Dynamic provisioning Methods for Optical Shared Backup Path Protection” IEEE 2005, pp 387- 396.

[9] Zong-Li Tang, Xing- Ming Li “ A Mixed Shared and Multi Paths Protection Scheme with SRLG Constraints” . pp-60- 65, Eight ACIS international Conference on Software Eng, AI, Networking and parallel / Distributed Computing. IEEE 2007.

[10] Dahai Xu, Chunming Qiao, and Yizhi Xiong “Ultra fast Potential- Backup-Cost (PBC)- based Shared path Protection Schemes”, Jounal of Light Wave Technology , Vol. 25 . No 8, August 2007.

[11] Sun-il Kim, Xiaolan J.Zhang and Steven S.Lumetta. “Rapid and efficient Protection for All-Optical WDM Mesh Networks” IEEE journal selected areas in communications. VOL 25 No. 9. December 2007.

[12] Wensheng He and Arun K. Soman “Comparison of Protection Mechanisms : Capacity Efficiency and Recovery Time”, 2007, pp 2218- 2223.

[13] A.Jackel “Lightpath Scheduling and Allocation under a flexible Scheduling Traffic Model”, IEEE 2006.

[14] Savera tanvir, Lina Battestilli, Harry Perros, Gigi Karmous-Edwards “Dynamic Scheduling of Network Resources with advance reservation in Optical Grids”, august 19, 2007.

Distributed Hybrid Research Network Operations Framework

Dongkyun Kim, Kwangjong Cho, and Huhn-Kuk Lim

Cyber Network Infrastructure (CNI) Division
Korea Institute of Science and Technology Information (KISTI)
P.O. Box 122, Yuseong, Daejeon, Korea
mirr@kisti.re.kr, kjcho@kisti.re.kr, hklim@kisti.re.kr

Abstract – Distributed Virtual Network Operations Center (dvNOC) presents virtualized network management framework on hybrid research networks for both network operators and end-users (e.g. researchers) to monitor and manage their own virtual networks. Another purpose of dvNOC is to meet the network demands of advanced applications on hybrid research networks, e.g. very high bandwidth, no datagram loss, almost zero jitter with strict traffic isolation. Based on hierarchical architecture consisting of dNOC (distributed NOC) and vNOC (virtual NOC), users can acquire three functionalities, multi-domain network awareness, efficient NOC-to-NOC cooperation, and user-oriented virtual network management, which are essential elements to achieve automated and virtual network management based on users, over multi-national and inter-domain hybrid research networks.

Keywords – Distributed Virtual NOC, Network Management, Hybrid Research Network, Advanced Applications

I. INTRODUCTION

Hybrid research network has been deployed on almost all the advanced national research and educational networks (NRENs) worldwide, e.g. Internet2 and ESNet in USA, CANARIE Network (CA*net4) in Canada, GEANT2, SURFnet, Nordunet in Europe, KREONet2 in Asia [1-7], etc. Hybrid research network is required by variety of researchers with advanced applications demanding very high bandwidth (1Gbps ~ 100Gbps), no datagram loss, and almost zero jitter with strict traffic isolation [8]. The high performance network needs to be in place for the applications such as nuclear fusion energy science, high energy physics, astronomical data analysis, high definition video transmission, and so on. In order to provide required network performance, hybrid network is designed for layered network architecture that allows datagrams (or packets) to bypass layer 3 network, guaranteeing quality of services demanded by advanced applications. That is, hybrid research network infrastructure consists of two different types of environments, IP network and circuit-based network, to provision dedicated congestion-free network (lightpath) mostly based on layer 2 or layer 1 (e.g. gigabit Ethernet, STS channel, optical wavelength), as well as to provide limitless network reachability on layer 3.

In the mean while, network operation and management is a primary role of network operations center (NOC) that provides critical services for telecommunication networks, enterprise networks, campus networks, etc. Generally, NOC monitors and operates thousands of routers, switches, optical cross-connectors, etc., while it carries out its most important job to keep network very reliable. Regarding hybrid research networks, additional network services to above traditional facilities are necessary to have special type of requirements for advanced applications resolved. In particular, since

advanced application experiments should frequently be performed based on dedicated lightpath provisioned between end users in the multi-domain global networks (e.g. between a research lab in USA and a university in the Netherlands), new research network services need to include not only hybrid networking technologies, but also global NOC-to-NOC collaboration.

In this paper, we suggest a framework for distributed and virtual network operations based on hybrid research networks and efficient cooperation between multi-domain hybrid networks, which aims to provide future network environment for high-end applications users in the long run. Two types of NOC schemes are proposed to meet the advanced application requirements, distributed NOC (dNOC) and virtual NOC (vNOC). Both schemes are integrated as dvNOC (distributed virtual NOC) with its basic framework as shown in Fig. 1, and Fig. 2 respectively. The main goals of dvNOC are as follows.

- Multi-domain network awareness: dvNOC pursues automated network resource exchange between NOCs so that each NOC can have complete network resource information (e.g. network topology) of other associated NOCs with dvNOC functionality. Such a multi-domain resource sharing makes it easier to monitor and manage inter-domain network and eventually to share network resources with end-users who want dedicated virtual networks worldwide for their research and experiment purposes.
- Efficient NOC to NOC cooperation: one NOC usually talks to other NOCs when it comes to multi-domain network failure recovery in particular. Traditional way of such communication is achieved via e-mail or phone call, but dvNOC will help each NOC handle network problem more efficiently based on visualized multi-domain network monitoring and virtual problem handling space. Multi-domain network awareness is a primary part for this NOC to NOC cooperation.
- User-oriented virtual network (UoVN) management: along with NOC to NOC cooperation designated to network operators or engineers, there is still an issue of end-user oriented network management. Once users create their own virtual network that is a set of lightpaths on hybrid research networks, it is necessary for them to monitor and manage their virtual network to ensure network quality and performance needed for their advanced applications..

There are several related projects. PerfSONAR [9] is research network monitoring platform designed for multi-domain global networks. Basically it adopts service oriented

architecture (SOA) and provides its functionalities for NOCs and PERTs (Performance Response Teams). That is, PerfSONAR provides various network performance analysis tools including end-to-end lightpath monitoring between multiple hybrid research NOCs. However, PerfSONAR doesn't support layered topology visualization and monitoring on multi-domain networks. In addition, network resource sharing and trouble recovery efficiency need to be taken into consideration as well.

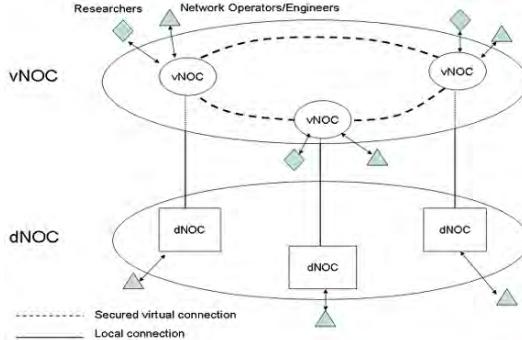


Figure 1. Overall Architecture of dvNOC

Coalition Network Management System (CNMS) [10] is a multi-national NOC environment focused on network policies for each network. CNMS is designed to hand over its network controls to another network domain's NOC from its NOC when a network failure happens on inter-domain network. In other words, a network domain A has a problem, but NOC A doesn't have a good condition to handle the problem (e.g. night time, or short of network engineers), NOC B can take over network control permission from NOC A and investigate the problem. This network control exchange is based on strict policy rule definition between NOCs. CNMS is, though, not flexible in terms that it doesn't have reasonable architecture considering expansion of NOC-to-NOC cooperation. When a NOC newly added, it is necessary to apply a complicated policy rules and create a new relationship to every other associated NOCs.

UCLPv2 [11] is designed to create APNs (Articulated Private Networks), developed by CANARIE [12]. APN is a virtual network consisting of network resources and computational resources requested by end-users across different network domains using web services. Each user who acquired an APN can allocate resources without limitations inside the APN for own researches and experiments. Meanwhile, the resources reservations for an APN need to be allowed by relevant NOCs mainly because of security reasons and resource management on each network domain. That is, one NOC should talk to another NOC either manually or automatically to have an APN generated and operated without any interruption e.g. due to firewall regulations. dvNOC adopts the concept of virtual network and web services introduced by UCLPv2 to come up with cooperative virtual NOC framework, considering NOC-to-NOC communications before actual user-oriented virtual networks are in place for global researches.

NDL (Network Description Language) [13] introduces a way to express network resources of NRENs and GOLEs (GLIF Open Lightpath Exchanges) [14] by describing nodes,

cross-connects, node-to-node connections, etc. TL1 toolkit [15] released through GLIF uses this language to visualize international and inter-domain networks particularly in terms of lightpath provisioning. dvNOC uses NDL as well to write network resource information and exchange it with NOCs. Furthermore, dvNOC expands NDL to query availability of lightpath, other network resources such as nodes and interfaces, and additional information such as contacts, applications, network provisioning period, etc.

GLIF produced failure recovery procedure [16], explaining structural approaches to recover problems possibly happening over lightpath provisioning and operations between international hybrid research NOCs and GOLEs. dvNOC follows up this procedure basically, while it adopts virtual controls suggested by CNMS and virtual network developed by UCLPv2. dvNOC allows each NOC to take controls of specific network resources on inter-domain environment with a time or permission limit based on pre-defined network policies between hybrid research NOCs beforehand.

The remainder of this paper is organized as follows. Section II describes the basic framework of dvNOC, and section III explains the dvNOC architecture and core systems. User oriented virtual network (UoVN) is introduced in section IV. Finally we conclude this paper in section V.

II. BASIC FRAMEWORK OF DVNOC

dvNOC framework consists of two core elements, distributed NOC (dNOC) and virtual NOC (vNOC). By introducing hierarchical model that logically divides dNOC and vNOC, we categorized network functions based on traditional NOCs with a few additional requirements, and new virtual overlay architecture for collaborative network operations between hybrid research NOCs and eventually end-users. Fig. 1 shows the overall architecture of dvNOC where depicts how dNOC and vNOC interoperates with each other.

Basically, a dNOC provides network information base as well as general NOC services maintaining each hybrid research network domain. Traditional network operations include management of equipment change, network trouble, device installations, wiring, etc. Network information base is added to this general NOC's functionality. Network information base of dNOC is a repository of network resources that is a collection of data acquired from various types of network gears using management protocols such as SNMP, TL1, and CLI (Command Line Interface). Having network resource information stored in network information base, dNOC can exchange the data with its corresponding vNOC.

A pair of dNOC and vNOC is working as dvNOC on one hybrid research network domain. Supposing there are several other network domains adopting dvNOC architecture, we call them members of dvNOC association. One member can communicate with other members based on virtual overlay networks made by vNOCs. Based on a dNOC element, its corresponding vNOC talks to other vNOCs (on different hybrid research network) to share network resource information, and eventually to provide virtual collaborative network operation services between all members of dvNOC association.

In our scheme, every resource repository at each dNOC is designed to acquire complete set of information base of all the hybrid research NOCs in the end, so that, for instance, each dNOC can keep global network topology of members of dvNOC association. Furthermore, dvNOC can provide rich data set and services based on resource information of hybrid research NOCs.

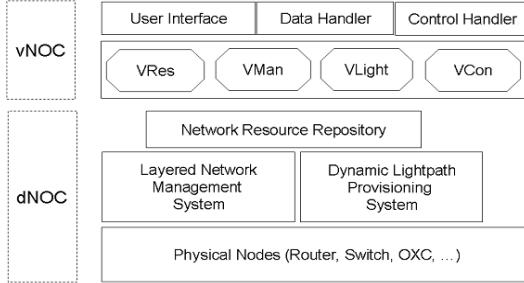


Figure 2. Basic Framework of dvNOC

As shown in Fig. 2, dNOC includes two more functional elements, layered network management system, and dynamic lightpath provisioning system. Layered network management system performs network monitoring, measurement, and management based on different network layers, e.g. layer 0 thru layer 3. Layered network management is necessary for hybrid optical and packet network infrastructure, since dNOC needs to manage both routed path and lightpath. While Layered network management system is focused on visualizing and analyzing hybrid network resource states, dynamic lightpath provisioning system carries on allocating and controlling network resources. It requires inputs about lightpath from network engineers or end-users on demand or scheduling basis. Those inputs include requested time frame, connecting end-points (A and Z), user information, protocols, etc. Dynamic lightpath provisioning system uses the inputs to control network devices in a domain, provisioning end-to-end lightpath, and computing optical paths, based on the control protocols such as GMPLS and TL1. Layered network management system and dynamic lightpath provisioning system stores network states into resource repository regarding network monitoring, measurement, management, and lightpath, so that a dNOC can operate a stateful network domain. Eventually the network information stored in resource repository is used for a vNOC to share network information with other vNOC domains. Therefore resource repository is a very important part of dvNOC when it comes to open and shared architecture for NOC-to-NOC cooperation. It keeps network resource information from physical nodes and circuits to lightpath monitoring states, user contact information, etc. Detailed schema of resource repository is described in chapter III.

In Fig. 2, there are four functional elements and three interfaces in vNOC. Among the functional elements, vRES plays a role of sharing network resource information stored in the local network resource repository. Resource queries can be made both by network operators/engineers and end users. For example, network operators want to find performance measurement data such as packet loss and delay during a certain time frame, while end users need to see if there are available network resources (e.g. bandwidth) between two end institutes. Note that properties of performance

measurement data are only shared by vRES, rather than data archives. vMAN provides a way to share monitoring, measurement, and management information with other vNOC domains, as vLIGHT provisions multi-domain end-to-end lightpaths. vCON is designed to exchange trouble ticket information and give a specific time window to control network resources for end-users or network operators based on very strict policy.

III. dNOC ARCHITECTURE AND CORE SYSTEMS

A. Distributed NOC Architecture and Functions

The principle of dNOC is to build distributed network information base using a defined set of system which includes network resource repository, layered network monitoring & management system, and dynamic lightpath provisioning system. Based on these systems, each dNOC keeps its local information base, and gathers other dNOC's resource information by interfacing with vNOC facility. For instance, resource repository at dNOC starts to collect and maintain its own NOC's network resource information such as network devices, interfaces, ports, connections, etc. Then, it tries to gather other NOC's resource information as well which is retrieved from its correspondent vNOC. The vNOC communicates with other vNOC entities to receive and transmit resource information required by one another. Eventually every resource repository at each dNOC has a complete picture of information base of all the NOCs in a distributed manner. In addition to the network resource information, dNOC's resource repository is designed to store user information, so vNOC can share and maintain end-to-end connections between users. Table 1 shows an example of data schema for network resource repository.

Layered network management system (LNMS) is required to monitor the status and performance of hybrid networks at near real time on layer 1 thru layer 3, and eventually manage the whole layered network infrastructure such as OXCs, SONET/SDH muxes, ethernet switches, and routers. Fig. 3 indicates layered network management framework that provides a way to manage routed path and lightpath by reading or recording over network resource repository, being used by end-users as well as network operators/engineers.

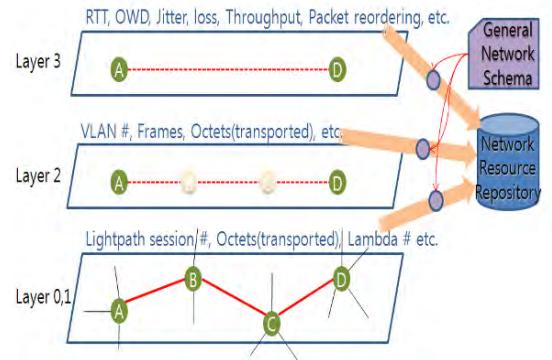


Figure 3. Layered Network Management Framework

Table 1. Network Resource Repository Schema Example

	Filed Name	Format	Description
User Information Base	Org-ID	Text(10)	Organization ID
	Org-name	Text(20)	Organization name
	Apps	Text(20)	Applications
	Contacts	Memo	Contact information
	IPv4-addr-block	Text(30)	IPv4 address block
	IPv6-addr-block	Text(50)	IPv6 address block
	ConnectedTo-ID	Text(10)	Upper network ID
	ConnectedTo	Text(40)	Upper net:gear:port
	Acc-bw	Float(20)	Access bandwidth
	Acc-gear-ID	Text(10)	Access gear ID
	Acc-gear-name	Text(20)	Access gear name
	Acc-port	Text(15)	Access gear port
	Acc-port-type	Text(15)	Access port type
	Net-ID	Text(10)	Owner network ID
Network Information Base	Net-name	Text(20)	Owner network name
	Contacts	Memo	Chief engineer info.
	Gear-ID	Text(10)	Gear ID
	Gear-name	Text(20)	Gear name
	ConnectedTo-ID	Text(10)	Connected net ID
	ConnectedTo	Text(40)	Cntd net:gear: port
	Port	Text(15)	Gear port
	Port-type	Text(10)	Type of port
	Port-bw	Float(20)	Bandwidth
	Xconnected-port	Text(20)	Cross-connected port
	Port-IPv4	Text(30)	Port IPv4 address
	Port-IPv6	Text(50)	Port IPv6 address

Dynamic lightpath provisioning system is an integral part of dNOC, because congestion-free path needs to be provisioned for the demands of advanced applications on demand or on scheduling-basis. Currently there are several dynamic lightpath provisioning systems being developed or deployed [17]. Therefore dNOC can simply choose one of them, but it is strongly advised that every associated vNOC uses a standard interface for lightpath provisioning so that the lightpath can be efficiently built on inter-domain and multi-national characteristics of global hybrid research networks, ensuring lightpath compatibility. Dynamic lightpath provisioning systems refers to the information that resides on network resource repository to have the proper lightpath across global network. Standard interface of multi-domain lightpath provisioning is proposed in the section B.

B. Virtual NOC Architecture and Functions

vNOC is designed to distribute and share network resource information between dvNOC domains, based on network operators and end-users. vNOC framework needs secured web service architecture to share the network resource information in a highly protected manner. Using web services, locally collected network information at each dNOC is converted into XML format to be shared between vNOCs. Eventually, every network resource data can be equally distributed between dvNOCs. Building information sharing infrastructure using web service is a basic and primary work for vNOC framework, so that virtual spaces can be generated with specific network instances. One issue for the data distribution is fast convergence between dvNOCs, which is not described in this paper.

vNOC framework proposes four functional entities, vRES (Virtual Network Resources), vMAN (Virtual Network

Management), vLIGHT (Virtual Lightpath Provisioning), and vCON (Virtual Network Trouble Controls). It also requires three interfaces such as graphical user interface, data handling and control handling interfaces. GUI of vNOC provides a first-contact for users or operators to choose specific services and interact with functionalities listed below. Data and control messages are exchanged based on secured web services between vNOCs.

vRES is related to network resource exchange, resource query, and integrated topology generation with visualization interfaces to LNMS in dNOC. Converted XML messages from NRR (Network Resource Repository) Data Schema are exchanged between vRESs through secured web service interfaces, and in turn, they are stored into each NRR to be queried by both end-users and network operators. In other words, each vRES on its dvNOC domain communicates with other domains' vRESs to acquire complete available network resources over virtual connections by exchanging locally gathered data. Data exchange modules use XML resource specifications. Note that XML resource specification needs to include available resources at specific time window because end-users and network operators generally want to use lightpath(s) with designated time period. Following XML specification example suggests what kind of information is exchanged to find available network resources over dvNOC system.

```
<?xml version="1.0" encoding="UTF-8"?>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
    xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
    xmlns:ndl="http://www.science.uva.nl/research/sne/ndl#"
    xmlns:grdl="http://www.gloriad.org/grdl#">

    <grdl:lightpath>
        <grdl:id>lp:01-dae:sea-10G</grdl:id>
        <grdl:section start="Daejeon:KR" end="Chicago:US"/>
        <grdl:bandwidth ndl:capacity="1.244E+09"/>
        <grdl:protocol uni="10GigabitEthernet" nni="SONET"/>
        <grdl:timeframe start="03-22-2007:10:00:00" end="03-30-2007:10:00:00"/>

        <grdl:userA>
            <grdl:name>KISTI</grdl:name>
            <grdl:contact name="Gu" e-mail="gu@kisti.re.kr" phone="82-42-869-0589"/>
            <grdl:connection ndl:name="www.kisti.re.kr#Force10-E300:ten2/1"
                ndl:connectedTo="www.krlight.net#Force10-E600:ten10/5"
                ndl:capacity="1.250E+09" />
            <grdl:application>OptIPuter</grdl:application>
        </grdl:userA>
        <grdl:netA>
            <grdl:name>KRLight:GLORIAD-KR</grdl:name>
            <grdl:contact name="Dongkyun Kim" e-mail="mirr@kreonet2.net"
                phone="82-42-869-0516" />
            <grdl:connection ndl:name="www.krlight.net#Force10-E600:ten10/5"
                ndl:connectedTo="www.kisti.re.kr#Force10-E300:ten2/1"
                ndl:capacity="1.250E+09" />
            <grdl:connection ndl:name="www.krlight.net#Force10-E600:ten1/2"
                ndl:connectedTo="www.krlight.net#ONS15600:3/1"
                XconnectedTo="www.krlight.net#ONS15600:4/1"
                ndl:capacity="1.244E+09" />
            <grdl:connection ndl:name="www.krlight.net#ONS15600:4/1"
                ndl:connectedTo="www.canarie.ca#ONS15454:15/1"
                ndl:capacity="1.244E+09" />
        </grdl:netA>
    <!--grdl:netB abbreviated-->
    </grdl: lightpath>
```

Above example includes reserved resource information for a lightpath provisioned between two network domains which are a part of the multi-national end-to-end lightpath. That is, a part of lightpath information is assembled with other parts of lightpaths, and each dvNOC domain has the full information of end-to-end lightpath after all. The example references NDL (Network Description Language) [13] that is being deployed on GLIF network playground [14] over the world.

In addition, vRES is designed to generate layered topologies with network management interfaces so that network users can easily check and detect what is currently undergoing on entire multi-domain networks with granular layered network information. vMAN is closely related to vRES in the management context. vMAN collects management data from NRR, and bind the data to vRES to represent visualization of layered networks with management and monitoring information such as link up and down, status of traffic and performance, etc. The topology visualization is also combined with vLIGHT and vCON in terms of shared end-to-end lightpath information and trouble tickets respectively. Fig. 5 shows how these systems are associated with each other.

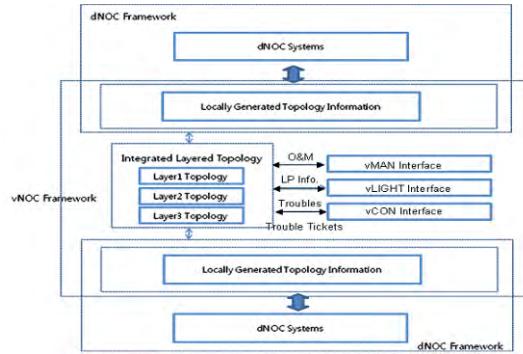


Figure 4. Layered Network Topology and Interactions

vLIGHT is a virtual lightpath provisioning system of local lightpath provisioning systems (as is “a system of systems”). There are about a dozen number of dynamic provisioning systems such as DCN, DRAC, HPDM, G-Lambda, LambdaStation, UCLP, etc.[17]. Therefore, vLIGHT needs to provide a virtual space not only to share lightpath resource information but to exchange control messages of multi-domain lightpath provisioning with simplified and standardized method defined among the local lightpath provisioning systems.

Fig. 5 indicates how vLIGHT manipulates data generated from its local dvNOC facilities. In this figure, vLIGHT consists of five functional elements. User interface receives queries for available resources during specific time frame as well as lightpath provisioning requests. Fig. 5 shows how the queries are processed with network resource repository and other vLIGHT elements, while lightpath requests go to resource handler which interacts with dvNOC’s local lightpath provisioning system using web service interfaces or native configuration commands such as TL1. Resource handler also interacts with XML translator & parser to store new requests into resource repository. Eventually resource handler sends the request to other dvNOC’s vLIGHT, through data/control handler and secured web interface of vNOC.

Regarding vCON, generally there are NOCs that control their own nodes for international connections as well as their NRENs in each country. In terms of international connections, each NOC maintains and controls its international node connected to other member’s networks that are operated by their traditional NOC(s). Every NOC easily detects and figure out any problems that happen on its

node(s), but when the problem happens at other NOCs’ nodes connected to its own, there is no way but waiting after several e-mails or phone calls until the problem is gone away (or sent back). This kind of work flow is usually performed when it comes to traditional NOC to NOC (international) cooperation so far.

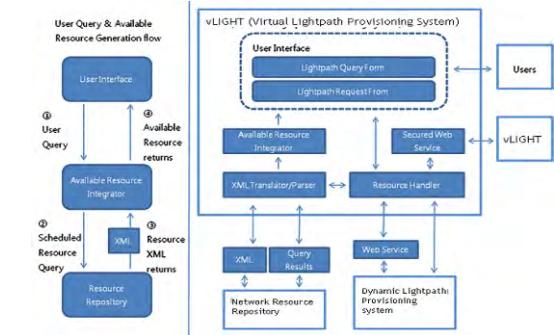


Figure 5. vLIGHT Data Flow Diagram

vCON is designed to issue and assign trouble ticket(s) for network troubles, and to control international networks in a distributed way among dvNOC domains, excluding several exceptional hardware related breakdowns such as network OS failure, interface card crash, fiber cut, etc. In order to do the distributed operations, first, it is required that vCON acquire network resource information. It mainly relies on vRES and vMAN for the information. vRES provides layered topology information to allow each dvNOC domain to figure out which layer of network incurs the trouble at a certain location of hybrid research networks. In the mean while, vMAN gives a way for network engineers to analyze the status of network, traffic, performance, etc. They can recognize how much traffic is utilized, and who generates the traffic on a specific link on international paths. Also, each dvNOC’s pre-deployed monitoring tools such as ping, traceroute, MRTG, etc. give clues for any other network troubles such as BGP routing anomaly.

Based on the monitoring results from all above systems, network engineers detect a problem. Once the detection done, the first detector reports the problem to vCON to issues a trouble ticket that is, in turn, delivered to all other dvNOC domains. The first detector can locate the problem at its own dvNOC, or can do that at any other dvNOCs. Then, vCON checks out (pre-registered) available human resources and working hours to assign the ticket to a proper engineer. When a ticket is assigned, trouble control broker invokes AAA functionality and provides access to the problematic node(s) according to pre-defined level of access permission of the engineer in charge. One important thing to provide the access for a node(s) is that control path should be arranged under vCON’s control, because access control needs to be done through secured connection, and data path is possibly down due to the problem.

Eventually, vCON assigns a control window to a specific network engineer (or an end-user) on one of dvNOC domains. That is, the engineer or end-user controls all the available network resources using CLI, SNMP, and TL1 with defined access policy during a certain time frame generated by vCON. When the problem is removed within the time frame, the

generated ticket will be closed by the assigned user. Otherwise, the trouble ticket holds and will be assigned to another user with the vCON work flows described above.

IV. USER ORIENTED VIRTUAL NETWORK MANAGEMENT

dvNOC scheme is originally designed for network engineers and operators as well as researchers and developers who want to manage their own virtual networks. When an end-user wants to use the view of its own virtual network, the user can acquire the same virtual space as network operators can. Only does one difference lie between two of them, which means end-users can have limited network resource information and access permission on virtual NOC space for their own virtual networks, while network operators have almost limitless network access controls. However network operators or engineers still have the constrained access or use of virtual networks by the permitted level when it comes to other dvNOC domain's network resources. More importantly, very strict policy is required to give resource controls to end users. One of virtual network example is shown in Fig. 6, which is a user-oriented virtual network for medical applications between Norway and Korea, which is a dedicated congestion-free network guaranteeing very high performance, e.g. no data1gram loss, zero jitter, optimized delay, etc. However, this type of virtual network still requires specified operations and management based on users. Fig. 7 shows a performance analysis result for network bandwidth on 1Gbps IP network path from a node in Daejeon, Korea to another node in Seattle, USA, showing sudden bandwidth drops during UDP data transmission. Therefore, it is advised to have virtual networks configured and managed particularly by end-users, guaranteeing a certain level of quality and performance for high-end applications.

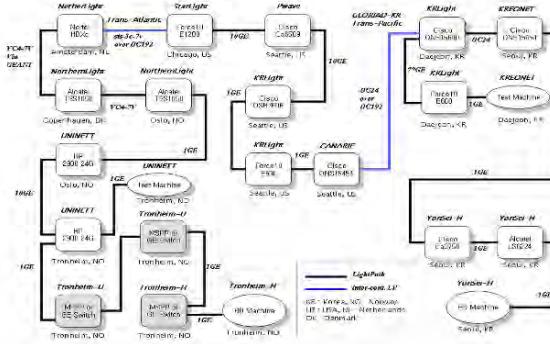


Figure 6. Norway-Korea Virtual Network on Hybrid Research Networks

V. CONCLUSIONS AND FUTURE WORKS

Given the increasing complexity of the underlying infrastructure and the increasing demand for both advanced and basic network services, dvNOC is designed to adopt decentralized model of multi-domain hybrid research network management. A collaborative and distributed virtual model that is characterized by cooperation among hybrid research networks that insist on maintaining their autonomy and control, can also contribute for researchers and other end-users to manage and operate their own virtual networks

within dvNOC's sphere. Future works of dvNOC will include more detailed resource specifications derived, but optimized from current research works, design of adaptation manager to interact with the developed NOC tools (e.g. PerfSONAR), development of strict policy control algorithm among hybrid research networks, fast convergence of network resource information, and so on.

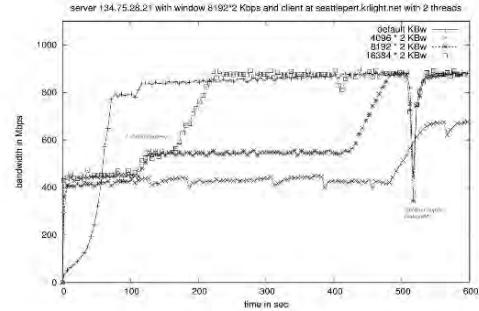


Figure 7. Network Performance Analysis Result between Korea and USA

References

- [1] The Internet2 Network, URL : <http://www.internet2.edu/network/>
- [2] Tom Lehman et al., "Hybrid Network Control Plane Interoperation Between Internet2 and ESnet," ESCC/Internet2 Joint Techs Summer Meeting, July 2007.
- [3] Andrew K. Bjerring, "Towards an Intelligent-Infrastructure for R&E in Canada," Ontario R&E Summit, June 2004.
- [4] Hybrid Network in GEANT2, URL : <http://www.geant2.net/server/show/nav.2140>
- [5] World-wide distribution of Large Hadron Collider data through SURFnet and NetherLight, URL : <http://www.surfnet.nl/en/nieuws/Pages/World-widistributionofLargeHadronColliderdatathroughSURFnetandNetherLight.aspx>
- [6] Lars Fisher, "Lambda Networking," 2nd Chinese-Nordic Network Workshop, April 2007
- [7] Dongkyun Kim, "Hybrid Network Initiative in Korea : KREONet2," 7th Global Lambda Grid Workshop, September 2007.
- [8] Harvey Newman, "LHC: A New Window on the Universe Frontiers of HEP & Cyberinfrastructure," 8th Global Lambda Grid Workshop, October 2008.
- [9] PerfSONAR, URL : <http://www.perfsonar.net/>
- [10] Scott Shyne et al., "Distributed Multi-National Network Operation Centres," IEEE MILCOM 2004, November 2004.
- [11] Grasa, E et al., "UCLPv2 : A Network Virtualization Framework built on Web Services [Web Services in Telecommunications, part II]," IEEE Communications Magazine, March 2008.
- [12] CANARIE, URL : <http://www.canarie.ca>
- [13] Jeroen van der Ham et al., "A Distributed Topology Information System for Optical Networks Based on the Semantic Web," Optical Switching and Networking 5 (2-3), June 2008.
- [14] GLIF Open Lightpath Exchange Resources, URL : <http://www.glif.is/resources/>
- [15] TL1 Toolkit, URL : <https://noc.sara.nl/nrg/TL1-Toolkit>
- [16] Rene Hatem et al., "The ordering and fault resolution process for multi-domain Lightpaths across hybrid networks," GLIF Technical WG, July 2006.
- [17] Erik-Jan Bos et al., "Optical Networking : GLIF," CCIRN Annual Meeting, May 2008.

Performance of the Duo-Binary Turbo Codes in WiMAX Systems

Teodor B. Iliev, Georgi V. Hristov, Plamen Z. Zahariev, Mihail P. Iliev

Department of Communication Systems and Technologies, University of Ruse, Ruse 7017, Bulgaria

E-mail: {tiliev, gchristov, pzahariev, miliev}@ccnrgroup.com

Abstract – In this paper the broadband wireless access system, provided by the IEEE 802.16 wireless MAN air interface with its amendment to mobile users (IEEE 802.16e), is being analyzed. We provide performance results for the most important forward error correcting (FEC) schemes intended for IEEE 802.16e – convolutional turbo codes (CTC) and Low Density Parity Check (LDPC) codes.

Keywords – WiMax, Forward error correction, Turbo codes, Convolutional codes

I. INTRODUCTION

The IEEE 802.16 telecommunications standard [1] envisions broadband wireless access technology as a means of providing wireless “last mile” broadband access in a metropolitan area network (MAN). The performance and services should be comparable or better than those provided by traditional DSL, cable or T1/E1 leased lines. Especially in areas beyond the reach of DSL and cable, IEEE 802.16 could offer a cost-effective broadband access solution. The term WiMax (worldwide interoperability for microwave access) has become synonymous with IEEE 802.16, promoting and certifying compatibility and interoperability of broadband wireless products. In its original release 802.16 focused on line-of-sight (LOS) applications in the licensed 10 to 66 GHz frequency range based on single carrier (SC) transmission (WirelessMAN-SC). In the first amendment of the standard were covered non-line-of-sight (NLOS) applications in licensed and unlicensed bands in the 2 to 11 GHz frequency range (WirelessMAN-SCa). To meet the requirements of a low cost solution in a multipath environment, orthogonal frequency division multiplexing (OFDM) was chosen as physical layer transmission technique (WirelessMAN-OFDM). To deliver optimum broadband wireless access performance, the concept of scalable OFDMA was adopted. The architecture is based on a scalable subchannel bandwidth using a variable sized FFT according to the channel bandwidth. Within task group E (IEEE 802.16e, [1]) there is an ongoing evolution of IEEE 802.16 addressing mobile applications thus enabling broadband access directly to portable devices like smart phones, PDAs, notebooks and laptop computers.

Our investigations are focused on the uplink of the WirelessMAN-OFDMA physical layer of IEEE 802.16 together with its amendments for mobile applications addressed in IEEE 802.16e. For the purpose of forward error correction (FEC) within the IEEE 802.16 WirelessMAN-OFDMA standard, there is a mandatory convolutional code

(CC) and an optional block turbo code (BTC) and convolutional turbo code (CTC). In the amendment for mobility (IEEE 802.16e) a Low-Density Parity-Check code (LDPC) was added.

The 8-state family has already been adopted in the digital video broadcasting (DVB) standards for return channel via satellite (DVB-RCS) [2] and the terrestrial distribution system (DVB-RCT) [3], and also in the 802.16a standard for local and metropolitan area networks [1]. Combined with the powerful technique of circular trellises, those duo-binary turbo codes offer good performance and versatility for encoding blocks with various sizes and rates, while keeping reasonable decoding complexity. The replacement of the 8-state component encoder by a 16-state encoder will provide better performance at low error rates, at the price of a doubled decoding complexity. The minimum Hamming distances are increased by 30%–50%, with regard to 8-state TCs, and allow frame-error rate (FER) curves to decrease below 10^{-7} without any noticeable change in the slope (the so-called flattening effect).

II. SYSTEM OVERVIEW

In IEEE 802.16e-2005, the channel coding stage consists of the following steps: (1) data randomization, (2) channel coding, (3) rate matching, (4) HARQ, if used, (5) and interleaving. Data randomization is performed in the uplink and the downlink, using the output of a maximum length shift-register sequence that is initialized at the beginning of every FEC block. This shift register sequence is modulo 2, added with the data sequence to create the randomized data. The purpose of the randomization stage is to provide layer 1 encryption and to prevent a rogue receiver from decoding the data. When HARQ is used, the initial speed of the shift-register sequence for each HARQ transmission is kept constant in order to enable joint decoding of the same FEC block over multiple transmissions.

Channel coding is performed on each FEC block, which consists of an integer number of subchannels. A subchannel is the basic unit of resource allocation in the PHY layer and comprises several data and pilot subcarriers. The exact number of data and pilot subcarriers in a subchannel depends on the subcarrier permutation scheme. The maximum number of subchannels in an FEC block depends on the channel coding scheme and the modulation constellation.

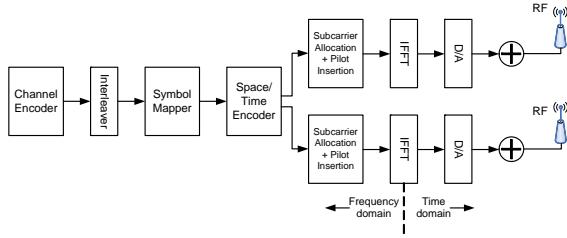


Fig.1 Functional stages of WiMAX PHY

If the number of subchannels required for the FEC block is larger than this maximum limit, the block is first segmented into multiple FEC subblocks.

These subblocks are encoded and rate matched separately and then concatenated sequentially, as shown in Figure 1, to form a single coded data block. Code block segmentation is performed for larger FEC blocks in order to prevent excessive complexity and memory requirement of the decoding algorithm at the receiver. The channel is assumed to be a time-variant multipath channel for modeling mobile users in an NLOS scenario. The receiver noise is modeled by an additive white Gaussian noise (AWGN) process added to the received signal.

Assuming perfect synchronization, the receiver extracts the useful symbol time and therefore removes the cyclic prefix. After the computation of the frequency domain signal via the FFT, the receiver extracts the user specific information (Data Extraction) and feeds it to the channel estimator and the 1-tap equalizer. With the assumption that the delay spread of the channel is smaller than the cyclic prefix and the time variance of the channel during one OFDM symbol is negligible, the received symbols in frequency domain R_i are given by:

$$R_i = H_i X_i + N_i, \quad i = 0, \dots, N_{\text{used}} - 1 \quad (1)$$

where X_i is the transmitted symbol, H_i is the complex valued sample of the channel transfer function and N_i is the complex valued noise sample in subcarrier i . The channel estimator computes \hat{H}_i , which are estimates of the real channel factor H_i . The topic of channel estimation for IEEE 802.16 is addressed in [4]. In the following we assume perfect knowledge of the channel transfer function and therefore also perfect channel estimation ($\hat{H}_i = H_i$). The 1-tap (zero forcing) equalizer computes:

$$\tilde{R}_i = \frac{R_i}{H_i} = X_i + \frac{N_i}{H_i} \quad (2)$$

These equalized symbols are fed into the soft output demodulator computing log-like ratios (LLRs) for bits. After deinterleaving the LLRs are fed into the FEC decoders using this soft input for decoding.

III. CONSTITUENT RCS CODES

A. Circular RCS Codes

Among the different techniques aiming at transforming a convolutional code into a block code, the best way is to use any state of the encoder as the initial state, and to encode the sequence so that the final state of the encoder is equal to the initial state. The code trellis can then be viewed as a circle, without any state discontinuity. This termination technique, called tailbiting [5], [6] or circular, presents three advantages in comparison with the classical trellis-termination technique using tail bits to drive the encoder to the all-zero state. First, no extra bits have to be added and transmitted; thus, there is no rate loss, and the spectral efficiency of the transmission is not reduced. Next, when classical trellis termination is applied for TCs, a few codewords with input Hamming weight of one may appear at the end of the block (in both coding dimensions), and can be the cause of a marked decrease in the minimum Hamming distance of the composite code. With tailbiting RSC codes, only codewords with minimum input weight of two have to be considered. In other words, tailbiting encoding avoids any side effects

B. Permutation

Among the numerous permutation models that have been suggested up to now, the apparently most promising ones, in terms of minimum Hamming distances, are based on regular permutation calling for circular shifting [7] or the co-prime [8] principle. After writing the data in a linear memory, with address i ($0 \leq i \leq N-1$), the information block is likened to a circle, with both extremities of the block ($i=0$ and $i=N-1$) being contiguous. The data is read out, such that the j^{th} data read was written at the position i , given by:

$$i = \Pi(j) = Pj + i_0, \quad (3)$$

where the skip value P is an integer, relatively prime with N , and i_0 is the starting index. This permutation does not require the block to be seen as rectangular; that is, N may be any integer.

In [9] and [10], two very similar modifications of (3) were proposed, which generalize the permutation principle adopted in the DVB-RCS or IEEE802.16a TCs. In the following, we will consider the almost regular permutation (ARP) model detailed in [10], which changes relation (3) into:

$$i = \Pi(j) = Pj + Q(j) + i_0 \bmod N. \quad (4)$$

Where $Q(j)$ is an integer, whose value is taken in a limited set $\{0, Q_1, Q_2, \dots, Q_{C-1}\}$, in a cyclic way. C , called the cycle of the permutation, must be a divisor of N and has a typical value of four or eight. For instance, if $C=4$, the permutation law is defined by:

$$\text{if } j = 0 \bmod 4, \quad i = \Pi(j) = Pj + 0 + i_0 \bmod N$$

$$\begin{aligned}
 & \text{if } j = 1 \bmod 4, i = \Pi(j) = Pj + Q_1 + i_0 \bmod N \\
 & \text{if } j = 2 \bmod 4, i = \Pi(j) = Pj + Q_2 + i_0 \bmod N \\
 & \text{if } j = 3 \bmod 4, i = \Pi(j) = Pj + Q_3 + i_0 \bmod N
 \end{aligned} \quad (5)$$

and N must be a multiple of four, which is not a very restricting condition, with respect to flexibility.

In order to ensure the bijection property of Π , the Q values are not just any values. A straightforward way to satisfy the bijection condition is to choose all Q 's as multiples of C .

IV. PERFORMANCE OF DUO-BINARY TURBO CODES

Several optional channel coding schemes such as block turbo codes, convolutional turbo codes, and low density parity check (LDPC) codes are defined in IEEE 802.16e-2005. Of these optional channel coding modes, the convolutional turbo codes (CTC) are worth describing because of their superior performance and high popularity in other broadband wireless systems, such as HSDPA and WCDMA. As shown in Figure 2, WiMAX uses duo-binary turbo codes with a constituent recursive encoder of constraint length 4. In duo-binary turbo codes two consecutive bits from the uncoded bit sequence are sent to the encoder simultaneously.

Duo-binary turbo codes are a special case of nonbinary turbo codes, which have many advantages over conventional binary turbo codes [1]:

✓ **Better convergence:** The better convergence of the bi-dimensional iterative process is explained by a lower density of the erroneous paths in each dimension, reducing the correlation effects between the component decoders.

✓ **Larger minimum distances:** The nonbinary nature of the code adds one more degree of freedom in the design of permutations (interleaver)-intrasymbol permutation, which results in a larger minimum distance between codewords.

✓ **Less sensitivity to puncturing patterns:** In order to achieve code rates higher than 1/3 less redundancy, bits need to be punctured for nonbinary turbo codes, thus resulting in better performance of punctured codes.

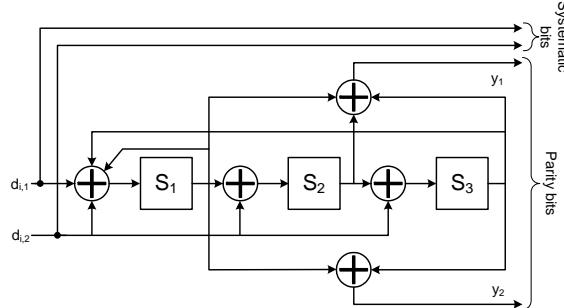


Fig.2 Duo-binary Turbo code

A. 8-state Duo-Binary Turbo Code

The parameters of the component codes are:

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \quad (6)$$

$$R_1 = [1 \ 1 \ 0], \quad R_2 = [1 \ 0 \ 0] \quad (7)$$

The diagram of the encoder is described in Fig. 3. Redundancy vector R_2 is only used for coding rates less than 1/2. For coding rates higher than 1/2, puncturing is performed on redundancy bits in a regular periodical way, following the patterns that are described in [5]. These patterns are identical for both constituent encoders.

The permutation function $i = \Pi(j)$ is performed in two steps. For $j=0, \dots, N-1$, we have the following:

Step 1: inversion of $d_{j,1}$ and $d_{j,2}$ in the data couple, if $j \bmod 2 = 0$;
Step 2: this permutation step is described by a particular form of (5).

$$i = (Pj + Q(j) + 1) \bmod N \text{ with}$$

$$Q(j) = 0 \text{ if } j \bmod 4 = 0$$

$$Q(j) = \frac{N}{2} + P_1 \text{ if } j \bmod 4 = 1$$

$$Q(j) = P_2 \text{ if } j \bmod 4 = 2$$

$$Q(j) = \frac{N}{2} + P_3 \text{ if } j \bmod 4 = 3 \quad (8)$$

Value $i_0=1$ is added to the incremental relation in order to comply with the odd–even rule [11]. The disorder is instilled in the permutation function, according to the ARP principle, in two ways.

✓ A shift by $N/2$ is added for odd values of j . This is done because the lowest subperiod of the code generator is one (see Fig. 3). The role of this additional increment is thus to spread to the full the possible errors associated with the shortest error patterns.

✓ P_1 , P_2 , and P_3 act as local additional pseudorandom fluctuations.

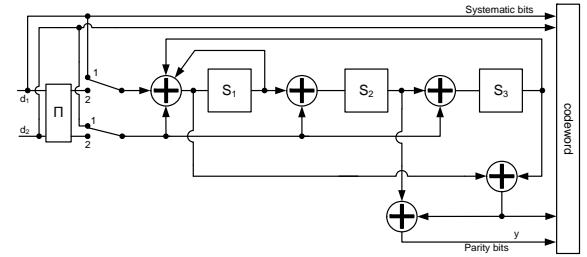


Fig.3 Structure of the 8-state encoder

B. 16-state Duo-Binary Turbo Code

The extension of the 8 state coding scheme to 16 states enables minimum distances to be increased by 50% on average. The parameters of the component code are:

$$G = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} \quad (9)$$

$$R = [1 \ 1 \ 1 \ 0] \quad (10)$$

The diagram of the encoder is described in Fig. 4. Puncturing is performed on redundancy in a periodic way, with identical patterns for both constituent encoders. It is usually regular, except when the puncturing period is a divisor of the LFSR period. For example, for coding rate 3/4, the puncturing period is chosen equal to six, with puncturing pattern [101000].

For this code, the permutation parameters have been carefully chosen, following the procedure described in [10], in order to guarantee a large minimum Hamming distance, even for high rates. The level-1 permutation is identical to the intrapermutation of the 8-state code. The level-2 intersymbol permutation is given by:

For $j=0, \dots, N-1$

$$\begin{aligned} i &= (Pj + Q(j) + 3) \bmod N \text{ with} \\ Q(j) &= 0 \text{ if } j \bmod 4 = 0 \\ Q(j) &= Q_1 \text{ if } j \bmod 4 = 1 \\ Q(j) &= 4Q_0 + Q_2 \text{ if } j \bmod 4 = 2 \\ Q(j) &= 4Q_0 + Q_3 \text{ if } j \bmod 4 = 3 \end{aligned} \quad (11)$$

The spirit in which this permutation was designed is the same as that already explained for the 8-state TC. The only difference is that the lowest subperiod of the 16-state generator is two, instead of one. That is why the additional shift (by $4Q_0$) is applied consecutively, twice every four values of j .

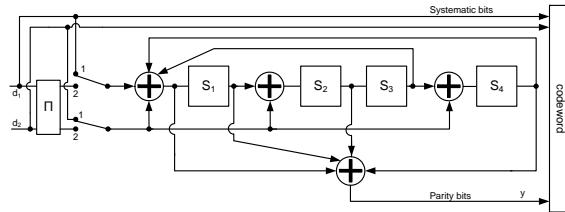


Fig.4 Structure of the proposed 16-state double-binary turbo encoder

V. BLOCK LDPC CODES OF WIMAX

The block irregular LDPC codes have competitive performance and provide flexibility and low encoding/decoding complexity [12]. The entire H matrix is composed of the same style of blocks with different cyclic shifts, which allows structured decoding and reduces decoder implementation complexity. Each base H matrix in block LDPC codes has 24 columns, simplifying the implementation. Having the same number of columns between code rates minimizes the number of different expansion factors that have to be supported. There are four rates supported: 1/2, 2/3, 3/4, and 5/6, and the base H matrixes for these code rates are defined by systematic fundamental LDPC code of M_b by N_b where M_b is the number of rows in the base matrix and N_b is the number of columns in the base matrix. The following base matrixes are specified: 12×24, 8×24, 6×24, and 4×24. The base model matrix is defined for the largest code length ($N=2304$) of each code rate. The set of shifts in the base model matrix are used to determine the shift sizes for all other code lengths of the same code rate. Each base model matrix has $N_b=24$ block columns and M_b block rows. The expansion factor z is equal to $N/24$ for code length N . The expansion factor varies from 24 to 96 in the increments of 4, yielding codes of different length. For instance, the code with length $N=2304$ has the expansion factor $z=96$. Thus, each LDPC code in the set of WiMAX LDPC codes is defined by a matrix H as:

$$H = \begin{bmatrix} P_{1,1} & P_{1,2} & \dots & P_{1,N_b} \\ P_{2,1} & P_{2,2} & \dots & P_{2,N_b} \\ \dots & \dots & \dots & \dots \\ P_{M_b,1} & P_{M_b,2} & \dots & P_{M_b,N_b} \end{bmatrix} = P^{H_b} \quad (12)$$

where P_{ij} , is one of a set of z -by- z cyclically right shifted identity matrixes or a z -by- z zero matrix [12]. Each 1 in the base matrix H_b is replaced by a permuted identity matrix while each 0 in H_b is replaced by a negative value to denote a z -by- z zero matrix. The codeword length can be calculated by $N=24z$ and ranges from $N=576$ to $N=2304$ bit with a granularity of 96 bit.

VI. SIMULATION AND RESULTS

We have simulated and compared LDPC codes and convolutional turbo codes intended for the WiMAX (IEEE 802.16e) forward error correcting schemes. For the CTC, iterative decoding was stopped after 10 iterations. Concerning the LDPC decoder, the maximum number of iterations of belief propagation decoding was limited to 100. The simulations were carried out for different code rates, lengths and modulation schemes in additive white Gaussian noise (AWGN) channel. Simulations were run to determine the performance of CTC and LDPC in AWGN channel with BPSK modulation. For each simulation, a curve showing the bit-error rate (BER) versus E_b/N_0 was computed.

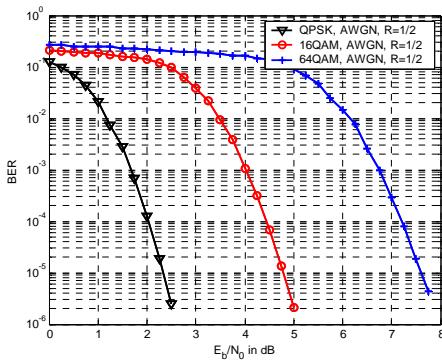


Fig.5. BER performance of CTC with different modulation schemes

In Fig. 5 we depicted the bit error rate (BER) versus E_b/N_0 for CTC with code length $N=576$ bits, code rate $R=1/2$ and different modulation schemes were computed. Fig. 6 shows the bit error performance of convolutional turbo code for various code rates, an input frame size of 288 bits and 64QAM used in 802.16e. Fig. 7 shows the comparison between LDPC codes and CTC codes with code rate of $R=1/2$, two modulation schemes (QPSK and 16QAM) and $N=576$ bits.

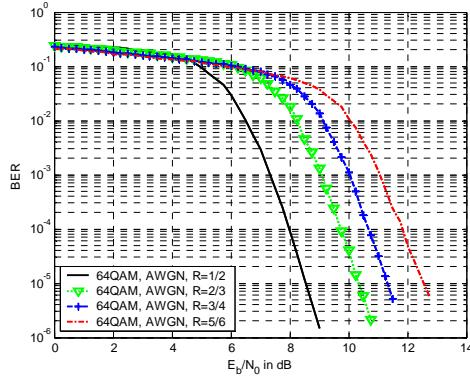


Fig.6. BER performance of CTC with different code rates

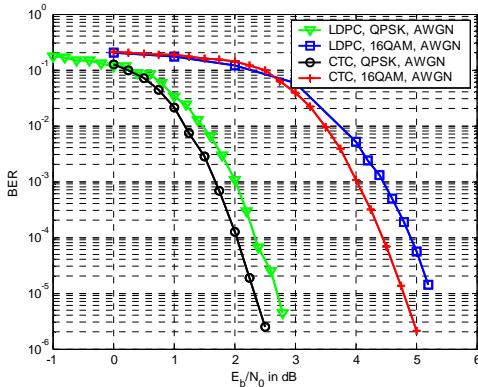


Fig.7. Comparison between LDPC and CTC with code rate $R=1/2$

The performance of the CTC and the LDPC code is quite similar, whereby there is a ‘tenth of a dB advantage’ for the CTC. To reach a BER of 10^{-4} the LDPC code needs round 0,4 dB more for QPSK and round 0,6 dB more for 16QAM compared to CTC.

VI. CONCLUSIONS

The contribution of this paper is a study of WiMAX forward error correcting codes. It presents a validation and a discussion of these types of codes. Secondly, this paper presents an implementation of convolutional turbo codes and LDPC codes developed in Matlab. The performance gain using advanced coding techniques like CTC and LDPC is quite small for rate 1/2 codes. One reason for this is that the standard only provides short to moderate code lengths ($N \leq 2304$), which is the most crucial parameter for this class of codes. The performance of CTC and LDPC is about the same and by changing some decoding parameters the small advantage of one of them can be interchanged. Nevertheless, LDPC decoding is less complex than CTC decoding.

ACKNOWLEDGMENT

This work is a part of the project BG051PO001/07/3.3-02/8—“MEQSIS”, funded by scheme “Support of the development of PhD students, postdoctoral, post-graduate and young scientists” from the program “Development of human resources” of the “European social fund”.

REFERENCES

- [1] IEEE P802.16e/D12, Draft IEEE Standard for LAN and MAN, Part 16: Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, 2005.
- [2] ETSI EN 301 790, DVB, “Interaction Channel for Satellite Distribution Systems”, vol. 1.2.2, 2000.
- [3] ETSI EN 301 958 DVB “Interaction Channel for Digital Terrestrial Television”, vol. 1.1.1, 2002.
- [4] J. Andrews, A. Ghosh, R. Muhamed, *Fundamentals of WiMAX: Understanding Broadband Wireless Networking*, Prentice Hall, 2007.
- [5] C. Weiss, C. Bettstetter, S. Riedel, and D. J. Costello, “Turbo decoding with tailbiting trellises,” in *Proceedings of International Symposium on Signals, Systems, and Electronics*, Pisa, Italy, 1998, pp. 343–348.
- [6] C. Douillard, C. Berrou, Turbo Codes With Rate- $m/(m+1)$ Constituent Convolutional Codes, *IEEE Transactions on Communications*, vol. 53, no. 10, 2005, pp. 1630 – 1638
- [7] S. Dolinar, D. Divsalar, “Weight distribution of turbo codes using random and nonrandom permutations,” JPL, TDA Report 42-122, 1995.
- [8] C. Heegard, S. Wicker, *Turbo Coding*. Kluwer Academic Publishers, 1999
- [9] S. Crozier, J. Lodge, P. Guinand, and A. Hunt, “Performance of turbo codes with relatively prime and golden interleaving strategies,” in *Proc. 6th Int. Mobile Satellite Conf.*, Ottawa, Canada, Jun. 1999, pp.268–275.
- [10] C. Berrou, Y. Saouter, C. Douillard, S. Kerouédan, and M. Jézéquel, “Designing good permutations for turbo codes: Toward a single model,” in *Proceedings of IEEE International Conference on Communication*, Paris, France, 2004, pp. 341–345.
- [11] A. Barbulescu, Iterative decoding of turbo codes and other concatenated codes, Ph.D. dissertation, University of South Australia, 1996
- [12] T. Iliev, G. Hristov, P. Zahariev and M. Iliev, “Application and evaluation of the LDPC codes for the next generation communication systems”, *Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics*, Springer, 2008, pp. 532 – 536

A unified event reporting solution for wireless sensor networks

Faisal Bashir Hussain^{1,2}, Yalcin Cebi¹

¹Department of Computer Engineering, Dokuz Eylul University (DEU),
35160, Izmir, Turkey

²National University of Sciences and Technology (NUST), Rawalpindi, Pakistan.

Abstract—Wireless sensor networks are deployed to observe a variety of events from the sensor field. Each event can have different constraints in terms of reporting rate, fairness, priorities and real-time information delivery. A number of event reporting, transport, congestion and rate control schemes have been proposed in the existing literature. However, these solutions have been proposed for different applications, spanning on different layers of protocol stack with contradicting basic assumptions. Therefore, due to the architectural and operational differences of these solutions, existing protocols are not appropriate to operate in a unified manner at the transport layer of sensor networks. This work presents a unified scalable, energy-aware and flexible event reporting solution for wireless sensor networks. The proposed event reporting solution provides different modes for event reporting like simple, fair, prioritized and real-time. Simulation study proves that the proposed event reporting solution provides maximum throughput, high packet delivery ratio, low energy consumption and achieves different event reporting mode requirements.

Keywords-sensor networks; event reporting; congestion control; fairness, real-time;

I. INTRODUCTION

Wireless Sensor Networks (WSNs) gather information from the environment. The electronics then process the information derived from the sensors and through some decision making capability direct critical information to the sink. The critical information of interest for an application is named as *event*. Sensor nodes are deployed to detect a number of application defined events. Each event has its own characteristics in terms of reporting rate, importance and reliability requirements.

We explain the nature of different events using WSN in the mining application. The network can perform following functions: 1) Monitoring environmental conditions inside a mine. For example, temperature, humidity, pressure and oxygen content in air etc. 2) Providing quick relief by triggering alarms, during disasters like fire, or leakage of poisonous gases. 3) Finding location of trapped miners within the mine in case of mine collapses. Different event reporting scenarios in mining application are list below:

- The sudden increase in the temperature of a certain region within a mine (possibly fire) must be quickly and reliably informed to the sink to trigger the fire alarms.

- Some events are inter-related e.g., fire and oxygen content in air. Therefore, multiple events can be triggered at the same time. In this case, one event can have higher priority than the other event.

- For events like leakage of poisonous gas, the sink requires precise per node information in order to identify unsafe regions in the mine. Hence, event reporting with fairness is also critical.

- The sensed data in terms of position of an object (human) is time-dependent and can have certain time bounds. Real-time event reporting of time-critical information with in certain bounds is another important issue.

Congestion control is another important issue related to event reporting in WSNs. Since the load on the network is increased by the sudden impulse of event information on event occurrence, congestion occurs. As a result, the destination does not get the correct picture of event region. Therefore, congestion avoidance and control is necessary for sensors-to-sink event reporting.

The research in the field of event reporting in WSNs, presents various individual solutions to fulfill different application dependent event requirements. The existing solutions have been proposed for different applications, spanning on different layers of protocol stack with contradicting basic assumptions. Therefore, due to the architectural and operational differences of these solutions, existing protocols are not appropriate to operate in a unified manner at a single layer of sensor networks.

This paper presents a unified scalable, energy-aware and flexible event reporting solution for wireless sensor networks. The solution is comprised of different event reporting modes such as: simple, fair, prioritized and real-time. The aim of the proposed solution is to fulfill different event requirements while providing high system throughput and minimum energy consumption.

The paper is organized as follows; next Section presents the related work on event reporting and reliable transport. Section

* The author is associated with NUST and currently doing research work at department of computer engineering, DEU, Izmir, Turkey.
This work is partially funded by scientific and technological research council of Turkey (TUBITAK) under grant number 2215-2006.

3 presents the basic network setup and system definitions for the proposed solution. Section 4, presents the operation of the proposed event reporting solution. In Section 5 we show the simulation results and the last section concludes this paper.

II. RELATED WORK

In this section, we summarize important event reporting, transport, congestion control protocols for wireless sensor networks.

Event to Sink Reliable Transport (ESRT) [3] provides an event transport mechanism, which is controlled by the sink. ESRT only provides general event region information and reliability is measured as the ratio of number of event packets delivered to destination to the required number of events packets defined by the application. Price-Oriented Reliable Transport (PORT) [5] defines sensor to sink data transport to be reliable when the transport mechanism can assure that the sink can obtain enough fidelity of the knowledge on the phenomenon of interest. PORT is also suitable for obtaining general event region information from the sensor field. COngestion Detection and Avoidance (CODA) [2] and SenTCP [4] provides different congestion control mechanisms based on channel sampling and packet inter-arrival time respectively. Nodes in these protocols adjust their reporting rate according to network conditions and they are only capable of providing general event based information.

Congestion Control and Fairness (CCF) [8] for many-to-one routing in sensor networks proposes an algorithm that ensure fairness by assuming that all the nodes are transmitting and routing data at the same time. Reporting rate is allocated to nodes depending on their sub-tree sizes. Every node maintains a separate queue for each of their previous hop nodes. In order to ensure fairness, nodes forward packets from these queues depending on their sub-tree sizes. Interference-aware Fair Rate Control (IFRC) [7] in WSNs, monitors average queue size to detect incipient congestion and uses Additive Increase Multiplicative Decrease (AIMD) scheme to adjust the reporting rate of nodes. IFRC provides high throughput from dense event regions and is also capable of proving considerably fair per node throughput.

Priority-based Congestion Control (PCCP) [6] in WSNs uses packet inter-arrival time and packet service time to detect congestion level at a node and employs weighted fairness to allow nodes to receive priority-dependent throughput. PCCP suggests that sensor nodes might have different priority due to their function or location. Therefore, nodes with higher priority-index gets more share of the bandwidth in order to ensure priority dependent throughput.

Delay-Aware Reliable Transport (DART) [9] in WSNs aims to provide time-bound and reliable event transport from the sensor field to the sink. DART uses time critical event packet scheduling policy to forward packets according to their deadlines. Sink-based rate control and congestion mitigation scheme is used in DART, in which the sink adjusts the reporting rate of the event region after periodic intervals.

As a summary, WSNs are application based networks [1]. Therefore, according to different application needs a number of protocols in the existing literature are proposed for simple, fair,

prioritized and real-time event reporting. However, due to different basic assumptions, protocol architectures and implementations, it is not feasible to construct a unified event reporting solution from these protocols. To the best of our knowledge this work presents a unique unified event reporting approach that encompasses simple, fair, prioritized and real-time event reporting.

III. NETWORK MODEL

The basic system related definitions, network setup and assumptions for the proposed event reporting solution are presented in this section.

The network comprises of non mobile wireless sensor nodes and a sink. The nodes in the network are categorized as event reporting (*E-REP*), routing (*E-R*), reporting and routing (*E-REP-R*), and idle nodes. If b, c, d are the nodes routing through node a , then b, c, d are the previous hop or child nodes of a and a is the next hop node of b, c, d , as shown in Figure 1. All nodes routing event information through node a are associated with the same information flow.

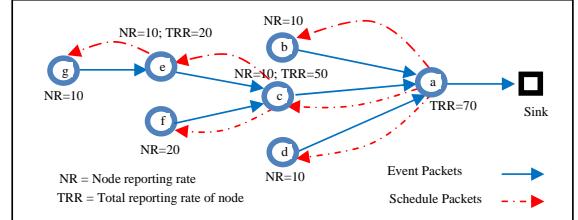


Figure 1 The flow of event and schedule packets with intial Node reporting Rate (NR) for each event reporting node and Total Reporting Rate (TRR).

In WSNs, upon the occurrence of event, sensor nodes send the event information to the sink according to a predefined reporting rate set by the application for each event. This reporting rate is defined as *initial reporting rate*. As the event is reported, the reporting rate of nodes needs to be adjusted in order to achieve maximum throughput. Since sensors-to-sink information flow is characterized by more than one unique flow, the proposed event reporting solution uses a flow based event reporting solution to provide maximum throughput. The flow associated with each first hop node is a separate flow. The first hop node in proposed system controls the reporting rate of the nodes in the flow. Flow based rate control divides the sensors-to-sink event flow into multiple small flows. Therefore, congestion in a single flow does not affect the whole sensors-to-sink information flow.

In the proposed solution, the sensors-to-sink information flow is comprised of different *Event Reporting Modes* (ERMs). The proposed event reporting solution is implemented at the transport layer and is shown in Figure 2. The basic goals of these modes are as follows:

1. Simple Event Reporting Mode (SERM): Sensor nodes report event to the sink in order to provide general event region information. SERM aims to achieve maximum

system throughput, irrespective of per node throughput at the destination. SETM is suitable for low priority events and also for obtaining a general sensing field status from the nodes.

2. Fair Event Reporting Mode (FERM): This mode is responsible for providing same per node throughput at the sink. Sensor nodes within a single flow adjust their reporting rates in order to fairly distribute the bandwidth among all the event reporting nodes.

3. Prioritized Event Reporting Mode (PERM): In sensor networks depending on application needs information regarding different events, node, or region can be reported with priority. In this work, event based priority for multiple events is considered, which aims to distribute the system bandwidth among different event reporting nodes depending on their initial reporting rates. As a result, nodes with high reporting rates deliver more packets to the sink than nodes with lower reporting rates; irrespective of node distance from the sink.

4. Time-bound Event Reporting Mode (TERM): This mode is responsible for delivering time-bound event packets to the destination within their respective deadlines.

Application	Application-specific event definition
Transport	Sensors-to-sink Event Reporting SERM FERM PERM TERM ↓ ↓ ↓ ↓ Congestion Control Scheme [11]
Network	Minimum hop routing
Data Link	IEEE 802.11
Physical	Radio - Industrial, scientific and medical (ISM) bands

Figure 2 Proposed event reporting solution for wireless sensor networks.

A. Congestion control scheme

All the ERMs interact with a congestion control scheme [11] which is based on buffer size and hop-by-hop packet delivery time. Packet delivery time is defined as *the time a packet takes to reach from the transport buffer of a previous hop node to the next hop node's transport buffer*.

The operation of the congestion control scheme is based on successive fixed size data (γ) and schedule (δ) intervals. During the data intervals, nodes route *available event information* and during schedule intervals, routing nodes send transmission schedule for their previous hop nodes. The schedule comprises of slot length (λ sec), total number of slots and allocated number of slots for a previous hop node. Slot length is defined as *a time duration during which a node forwards a single packet*. Nodes maintain a queue at the transport layer and forward a single packet from it during their allocated slots.

The basic components of congestion control scheme include slot length calculation and slot allocation procedures. All the ERMs use same slot length calculation procedures as defined in [11], while the slot allocation is done based on different ERMs and are explained in the next section.

IV. PROTOCOL OPERATION

The operation of proposed event reporting solution can be subdivided into slot length calculation, slot length allocation and the general operation of the proposed event reporting solution. All the ERMs use same slot length calculation procedure as defined in [11] while the slot allocation and the operation of the ERMs are explained below:

A. Slot length Allocation

A slot is a time interval during which a node can forward a single packet. Greater the number of slots assigned to a particular node greater will be its reporting rate. In case of simple, prioritized and real-time event reporting modes, slots are assigned equal to the total reporting rate of a node. In fair event reporting mode, slots are assigned by nodes, which are equal to their sub-tree size. The slot allocation procedure for different ERMs is explained below:

- SERM assigns slots to nodes with respect to total reporting rate (TRR) traversing through a node and the minimum reporting rate observed at the nodes.
- FERM assigns slots to nodes according to their *sub-tree size*. The sub-tree size depends on number of event nodes and not on their reporting rates. Even in case of multiple events with different reporting rates, nodes can forward packets with node based fairness so that all nodes have same representation at the destination.
- PERM assigns slots to nodes with respect to TRR and the minimum reporting rate among all the events observed by the network.
- Since TERM aims to provide general real-time event region information (without considering per node throughput at the sink), the slot allocation for TERM is similar to SERM.

Depending on the system given in Figure 1, the slot allocation by node a in SERM, PERM and TERM modes is shown in Table 1 and slot allocation by node a in FERM is shown in table 2.

Table 1 Transmission schedule generated by node a in SERM, PERM and TERM.

Node ID	Total Slots	Initial Slot	End Slot	Slot length (seconds)
B	7	1	1	0.1
C	7	2	6	0.1
D	7	7	7	0.1

Table 2 Transmission schedule generated by node a in FERM.

Node ID	Total Slots	Initial Slot	End Slot	Slot length (seconds)
b	6	1	1	0.1
c	6	2	5	0.1
d	6	6	6	0.1

Nodes b , c and d will divide their data interval into 0.1 second intervals; the initial slot length on event occurrence. These nodes will forward one event packet to node a during their allocated slots. Since, nodes c is an E-REP-R node therefore depending on event reporting mode node c will

generate a schedule for nodes *e* and *f*. The schedules given to nodes *e* and *f* by node *c* in SERM, FERM and PERM respectively are given in Tables 3, 4 and 5. Likewise, node *e* will generate schedules for child node *g*.

Table 3 Transmission schedule generated by node *c* in SERM and TERM

Node ID	Total Slots	Initial Slot	End Slot	Slot length (seconds)
e	4	1	2	0.1
f	4	3	4	0.1

Table 4 Transmission schedule generated by node *c* in FERM

Node ID	Total Slots	Initial Slot	End Slot	Slot length (seconds)
e	6	3	4	0.1
f	6	5	5	0.1

Table 5 Transmission schedule generated by node *c* in PERM.

Node ID	Total Slots	Initial Slot	End Slot	Slot length (seconds)
e	7	3	4	0.1
f	7	5	6	0.1

B. The operation of the ERMs

The sensors-to-sink event reporting is triggered by events. Sensor nodes after detecting an event send information to the sink via intermediate nodes. Initially event nodes transmit an *event packet* which contains event identification number, total reporting rate, sub-tree size of the node and the selected event reporting mode. If an event reporting node (*E-REP*) receives an event packet, then it changes its status to event reporting & routing (*E-REP-R*) node. Likewise, an intermediate idle node after receiving an event packet changes its status to routing node (*E-R*).

After receiving an event packet, nodes update their total reporting rates and transmit the new total reporting rate to their next hop node in the *event packet* until it reaches the first hop node. Also, the intermediate nodes maintain a previous hop table in order to determine the reporting rate and sub-tree size of previous hop nodes. The selection of an ERM in the proposed solution can be *node based* where nodes are preprogrammed to report a certain event in a specific mode, or *sink based* where the sink at event detection can indicate first hop nodes to report the event in some specific mode.

The first hop node from the sink in the proposed event reporting solution is responsible for sending the initial schedule to their previous hop nodes during the start of each schedule interval. The slot length for each data interval is updated by *E-REP-R* and *E-R* node during schedule interval depending on their local network conditions. The slot length received from a parent node or next hop node is termed as *basic slot length (BSL)* while the slot length calculated by the node itself is termed as *local slot length (LSL)*. Each previous hop node before forwarding their schedule to their child nodes compares its local slot length (LSL) with the next hop node's basic slot length (BSL). There are three possibilities local slot length less than, greater than or equal to basic slot length.

1. LSL < BSL: In this case the node receiving the schedule is locally less congested than its next hop node. Therefore it can allow its previous hop nodes to send packets at a

higher rate. This helps to increase the overall system throughput. However, will result into unordered delivery of packets to next hop node resulting into unfairness and affecting the prioritized delivery of packets. Therefore, in SERM & TERM the nodes will send LSL while in mode FERM & PERM, BSL is sent to their child nodes in the schedule.

2. LSL > BSL: In this case the node receiving the schedule is more congested than its next hop node. Therefore, in all modes the nodes will send LSL to their child nodes in the schedule. Although, it results in temporary unfairness in FERM but it mitigates local congestion.
3. LSL ≈ BSL: In this local and basic slot lengths are approximately equal therefore the nodes will send BSL to their child nodes.

During schedule intervals node only generate and send schedule packets. In real-time event reporting, schedule intervals insert an unnecessary delay in the delivery of delay-bound event packets. Therefore, overlapping schedule and data intervals are used in TERM. As a result, the flow of data packets continues during schedule interval. In TERM, the data and schedule packets contain additional “*time remaining*” and “*minimum hop delivery time*”, information respectively. The time remaining field contains the time after which the packet’s time bound expires. Since the information is not useful or valid to the destination as the time bound expires, the packet is dropped by the node.

The minimum amount of time required for the transmission of a packet from one hop to the other can be named as “*minimum hop delivery time (μ)*”, while “*minimum packet delivery time*” is the time required for the delivery of the event packet from the current node to the destination under ideal conditions. Nodes can be at multiple hop distance from the destination, therefore for packets with remaining time smaller than minimum packet delivery time are dropped by intermediate nodes in TERM. This helps to reduce energy consumption and lowers the load on the network. Let d_i be the hop distance of a node *i* from the destination and μ be the minimum hop delivery time then the minimum packet delivery time for a packet at node *i* will be $d_i \times \mu$.

V. SIMULATION RESULTS

The performance of the proposed event reporting solution is observed using network simulator NS-2 [10]. The simulation scenario is comprised of a wireless sensor network, with different numbers of sensor nodes deployed in a 100 x 100 m field. The basic simulation parameters are shown in Table 1. In the remaining of this section, we evaluate the performance of different ERMs in terms of throughput, energy consumption and packet delivery ratio.

A. Simple event reporting mode (SERM)

SERM is compared with an Additive Increase Multiplicative Decrease mechanism for Event Reporting (AIMD-ER). In the AMID scheme we use an increment factor

of 1.3 and decrement factor of 2. Moreover, for congestion mitigation a source-based technique ([2], [4]) is used which detects congestion using buffer size of nodes.

Table I Simulation parameters.

Transport Layer	Proposed event reporting solution
Network Layer	Minimum hop routing
MAC Layer	802.11
Data Packet	40 bytes
Schedule Packet	28 bytes
Transport Queue	50 Packets
Radio Range	20m
Data Interval Length	4 seconds
Schedule Interval Length	1 second

Separate simulations are conducted to obtain the throughput in terms of packets per second at the sink, observed for different number of event reporting nodes; during 150 second of event reporting (Figure 3). The simulation environment used to evaluate packet delivery ratio includes an event region which is centered at coordinates (40, 40) and has a radius of 20 meters.

The throughput of AIMD-ER, when the numbers of event reporting node are less (20 nodes) is considerably high (Figure 3). As the number of event reporting nodes increases, sending congestion signals over multiple hops towards source nodes becomes difficult due to congestion and throughput decreases. Also, AIMD based rate control schemes are not able to properly adjust the reporting rate of nodes as an increment/decrement factor is independent of the number of event reporting nodes. Since ERMs use a schedule based packet forwarding policy, the throughput is almost same for different number of event nodes. SERM efficiently handles congestion and packet drops due to inference. This is also evident from figure 4, in which the packet delivery ratio of

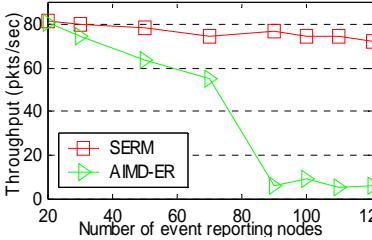


Figure 3. Average throughput observed at sink using different number of event reporting nodes.

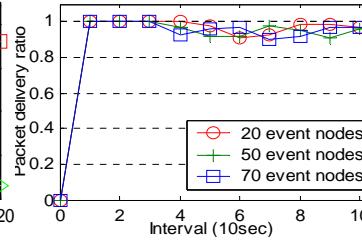


Figure 4. Packet delivery ratio of different number of event reporting nodes using SERM.

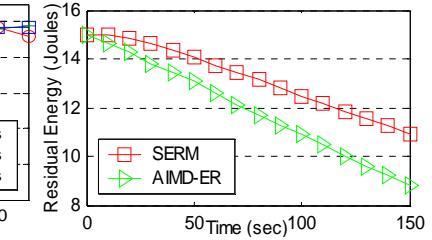


Figure 5. Residual energy of 150 nodes network with 50 event reporting nodes.

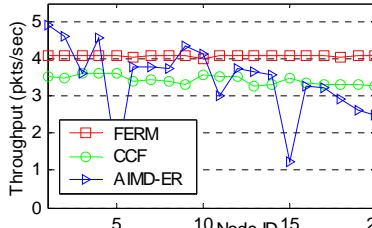


Figure 6. Per node throughput observed from 20 event reporting nodes.

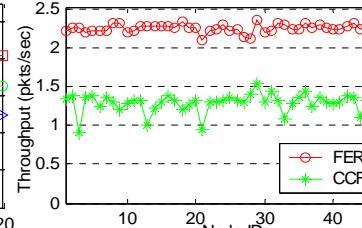


Figure 7. Per node throughput observed from 50 event nodes arranged on a same hop.

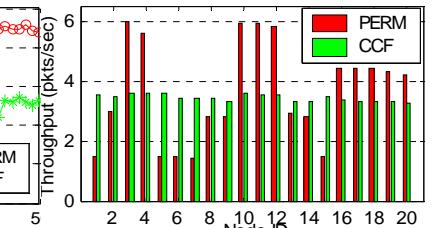


Figure 8. Per node throughput of 20 event nodes reporting four different events.

different number of event reporting nodes is shown. The packet delivery ratio of SERM is above 90% in all node arrangements.

The residual energy of 150 sensor nodes with 50 event reporting nodes is shown in Figure 5. Initial energy of all the nodes is set to 0.1 Joules for this simulation. SERM handles congestion efficiently and also it does not increase the reporting rate of nodes more than they can handle. Therefore, despite of the additional scheduled packet transmission, SERM decreases the energy consumption.

B. Fair event reporting mode (FERM)

FERM is compared with CCF [8]; commonly referenced fairness scheme for WSNs. The simulation scenario is comprised of 20 nodes arranged in 9 hops. In order to decrease multiple hop interference, the radio range used in the simulation scenario is 10meters. Figure 6 shows that CCF provides considerably fair output but FERM provides even better results with high per node throughput, because in FERM, each node is assigned a schedule in order to assure fair per node throughput. In order to further elaborate the performance of FERM, we compare the performance of both these schemes in Figure 7 using 50 event reporting nodes randomly arranged at a single hop distance from the destination (density of event nodes is 50). Since packet drops due to interference increases, the performance of CCF severely degrades. FERM with its scheduling scheme decreases interference while providing high and fair per node throughput.

C. Prioritized event reporting mode (PERM)

In this case, the simulation scenario consists of 20 events

nodes arranged in 9 hops. Four different events E1, E2, E3 and E4 are reported by nodes (1,5,6,7,15), (2,8,9,13,14), (16,17,18,19,20) and (3,4,10,11,12) respectively. The initial reporting rate of events E₂, E₃ and E₄ is twice, thrice and four times that of event E1 respectively. Figure 8 shows the per node throughput of PERM and CCF during 150 seconds of event reporting. Since CCF only considers node based fairness, it is unable to provide prioritized event reporting with respect to multiple event demands. However, PERM uses initial event reporting rate for rate allocation therefore nodes according to the event demand (priority) get a share of the bandwidth.

D. Time-bound event reporting mode (TERM)

We compare TERM with Time-bound AIMD-ER. The packets in Time-bound AIMD-ER are forwarded based on minimum remaining time first forwarding in order to meet event deadline. The deadline for each packet used in the simulations is 2 seconds.

Figure 9 shows the throughput of in-time packets received from 50 event reporting nodes, randomly arranged in an event region centered at (40,40) coordinated and with a radius of 20 meters. Initially the throughput of Time-bound AIMD-ER increases but as the reporting rate increases congestion occurs and mitigating congestion by sending congestion signal to source nodes becomes difficult. As a result, the delivery of packets within delay bound decreases for Time-bound AIMD-ER. TERM provides low throughput initially, due to small slot length (on event occurrence 0.1 sec). Also, the channel becomes suddenly busy on event impulse resulting in increase in slot length but later the throughput increases as the slot length decreases. Moreover, TERM maintains high throughput as reporting rate is adjusted according to network conditions.

Figure 10 shows the average packet delivery delay observed by 50 event nodes. An interesting fact shown in Figure 10 is that packets arrive late in case of TERM, as compared to Time-bound AIMD-ER. The reason for this delay is the combined effect of both high throughput and shortest remaining deadline forwarding policy used by TERM. This fact is further elaborated in Figure 11 in which, the ratio of throughput over average packet delivery delay is shown. The higher the throughput or shorter the average delivery delay, higher will be the output. The output of TERM is higher than Time-bound AIMD-ER, due to the greater throughput of TERM.

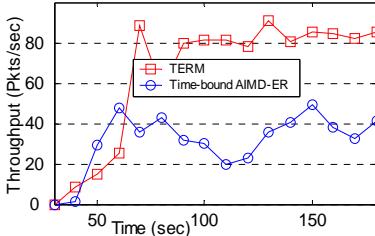


Figure 9. Throughput of in-time event packets received from 50 event nodes at the sink.

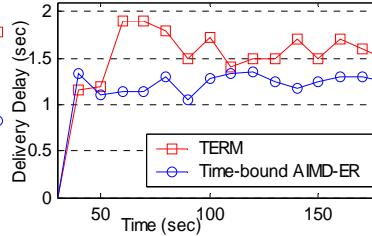


Figure 10. Average packet delivery delay of 50 event nodes observed during event reporting.

I. CONCLUSION

A unified event reporting solution has been presented in this paper. The solution encompassed simple, fair, prioritized and real-time event reporting modes at the transport layer. Nodes depending on event requirements can report an event in any of these modes. Simulation study showed that all event reporting modes provided high system throughput while decreasing energy consumption. Simple event reporting mode successfully delivered general event region information at high throughput, fair event reporting mode provided same per node throughput at the sink, prioritized event reporting mode divided system bandwidth among multiple events according to their reporting rates while real-time event reporting mode successfully delivered packets with in their deadlines.

REFERENCES

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. 38, pp. 393-422, 2002.
- [2] C.Y. Wan, S.B. Eisenman, and A.T. Campbell, "CODA: Congestion Detection and Avoidance in Sensor Networks," *First ACM Conference on Embedded Networked Sensor System*, pp. 266-279, 2003.
- [3] O.B. Akan, and I.F. Akyildiz, "Event-to-Sink Reliable Transport in Wireless Sensor Networks," *IEEE/ACM Transactions on Networking*, vol. 13, no. 5, pp. 1003-1016, 2005.
- [4] Y. Hu, Y. Xue, B. Li, Jianwen Xie, Haidong Yang "A Congestion Control Protocol for Wireless Sensor Networks," *Journal of Information and Computational Science*, vol. 2, no. 1, pp. 41-50, 2005.
- [5] Z. Yangfan, R. Micheal, L. Jiangchuan and W. Hui, "PORT: Price-Oriented Reliable Transport Protocol for Wireless Sensor Networks," *In Proceedings of 16th International Symposium on Software Reliability Engineering*, pp. 117-125, 2005.
- [6] C. Wang, B. Li, K. Sohraby, M. Daneshmand, and Y. Hu, "Upstream congestion control in wireless sensor networks through cross-layer optimization," *IEEE journal on Selected Areas in Communication*, vol. 25, pp. 786-795, 2007.
- [7] S. Rangwala, R. Gummadi, R. Govindan and K. Psounis, "Interference-aware fair rate control in wireless sensor networks," *ACM SIGCOMM, Computer Communication Review*, vol. 36, pp. 63-74, 2006.
- [8] C. T. Ee and R. Bajcsy, "Congestion Control and Fairness for Many-to-One Routing in Sensor Networks," *In Proc. 2nd International Conference on Embedded Networked Sensor Systems*, pp. 148-161, 2004
- [9] V.C. Gungor, and O.B. Akan, "Delay aware reliable transport in wireless sensor networks," *International Journal of Communication Systems*, vol. 20, pp. 1155-1177, 2007.
- [10] L. Breslau, D. Estrin, K. Fall, S. Floyd, J. Heidemann, A. Helmy, P. Huang, S. McCanne, K. Varadhan, Y. Xu, and H. Yu, "Advances in Network Simulation," *IEEE Computer*, Vol. 33, pp. 59-67, 2000.
- [11] F.B. Hussain, G. Seckin, and Y. Cebi, "Many-to-one congestion control scheme for densely populated WSNs," *Third IEEE/IFIP International Conference in Central Asia on Internet (ICI)*, pp. 1-6, 2007.

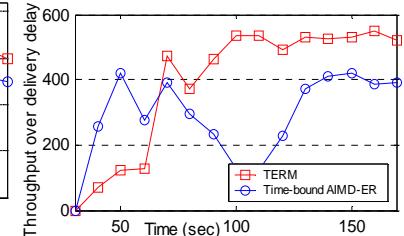


Figure 11. Ratio of throughput over average packet delivery delay observed from 50 event nodes.

A Low Computational Complexity Multiple Description Image Coding Algorithm Based on JPEG Standard

Ying-ying Shan, Xuan Wang

Department of Communication and Information System
Communication University of China, Beijing, 100024, China
shanyingying@126.com, wangxuan@cuc.edu.cn

Abstract-In this paper, a low complexity multiple description image coding scheme based on JPEG is proposed, which mitigates the image quality reduction due to packet loss during network transmission. The basic idea is to divide an image into multiple descriptions through multiple description scalar quantization (MDSQ) of DCT coefficients. Index assignment matrixes are produced according to the JPEG quantization table, which is implemented during the MDSQ process. Experimental results show that the proposed algorithm has a high transmission quality with lower computational complexity.

Keywords-Multiple Description Coding, MDSQ, JPEG

I. INTRODUCTION

JPEG is a commonly used still image compression algorithm for its excellent compression performance and low computational complexity. However, the retrieved quality of a JPEG image may reduce greatly due to packet loss during network transmission. Multiple description coding is one of the most effective methods to reduce the influence of transmission error. The principle of MDC is to represent the source signal by two or more independent descriptions of equal importance, and simultaneously transmitted through different channels. A basic quality is achieved at the decoder from each individual description. The quality is smoothly improved with the number of received descriptions increase [1]. In recent years, MDC has been deeply researched and many MDC algorithms have been proposed, to mention some, MD scalar quantization [2], MD lattice vector quantization [3], MD transform coding [4][5], MD down sampling coding [6], and MD motion compensated coding [7], etc.

Multiple description scalar quantization (MDSQ) is the first practical MDC scheme in which the separate descriptions are produced by scalar quantizers. The optimal design of MDSQ was pioneered by Vaishampayan in [2] which is further improved in [8] through using variable length code instead of fixed length code and designing the quantizer under constraint of a given entropy instead of a codebook size. Unfortunately, the design may lead to high encoding complexity which is not practical for image communication systems.

In this paper, a novel MDC scheme is proposed, in which MDSQ method is adapted into JPEG compression process. Experiment demonstrates the effectiveness and low computational complexity of the proposed method.

II. MULTIPLE DESCRIPTION SCALAR QUANTIZATION

Multiple description scalar quantization is a mature MDC with good comprehensive properties. The MDSQ system is shown in figure 1. The encoding is composed of two steps. The pre-encoder is a common scalar quantizer which partitions the real number line into several intervals as shown in figure 2. The process of index assignment $l(\cdot)$ produces a pair of indices (i, j) which is the coordinate of the input quantized scalar in the index assignment matrix [1]. Table 1 shows an index assignment matrix corresponding to figure 2, which maps one-dimensional value into a two-dimensional vector, $I : N \rightarrow N \times N$. Each element of (i, j) produced by index assignment process forms a description, and will be transmitted through independent channel. The receiver contains three decoders: a central decoder g_0 which can correctly decode the transmitted value in the case that both descriptions are received, and two side decoders, g_1 and g_2 which estimate the transmitted value from each description. In the case of only description is received, the receiver reduces into one side decoder. The index assignment l must be invertible in order that the central decoder can correctly decode the quantized value.

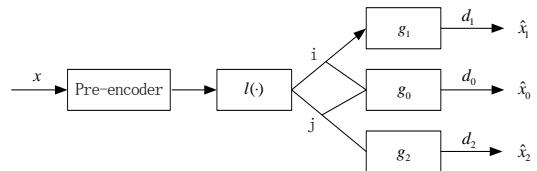


Fig. 1 Two-channel MDSQ scheme

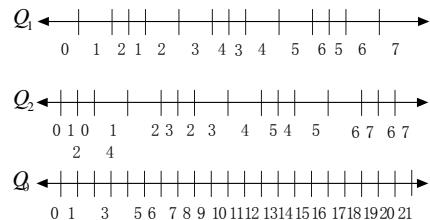


Fig.2 Three scalar quantizers: a central quantizer Q_1 , and two side quantizer Q_2 and Q_3

Table 1 Index matrix corresponding to Fig.2

	0	1	2	3	4	5	6	7
0	0	2						
1	1	3	4					
2	5	6	8					
3		7	9	10				
4			11	12	14			
5				13	15	16		
6					17	18	20	
7						19	21	

The performance of the whole system is very much dependent on the index assignment matrix. Suppose the value outputted from pre-encoder has a span of 0 to $x-1$, which means the elements of index assignment matrix have values from 0 to $x-1$. Numbers are filled into the matrix from upper-left to lower-right from small to large values, and forms $2k+1$ diagonals which include a main diagonal and $2k$ diagonals that lie closest to the main diagonal. The coding redundancy is controlled by choosing the value of k . As the value of k increases, coding redundancy decreases, and the quality of the reconstructed image becomes worse. Two different index assignment schemes, referred to as the nested index assignment and the linear index assignment, are proposed in [2]. Examples of modified nested and linear index assignments are given in table 2(a) and 2(b).

Table 2(a) Nested index assignment for $k=2$

	0	1	2	3	4	5	6	7
0	0	2	4					
1	1	5	7	9				
2	3	6	10	11	13			
3	8	12	15	16	18			
4		14	17	20	22	24		
5			19	21	25	27	29	
6				23	26	30	31	
7					28	32	33	

Table 2(b) Linear index assignment for $k=2$

	0	1	2	3	4	5	6	7
0	0	2	5					
1	1	4	6	8				
2	3	7	9	11	13			
3		10	12	14	16	19		
4			15		18	21	24	
5				17	20	23	26	27
6					22	25	28	30
7						29	31	32

The nested index assignment is composed of the east scan “E” and the south scan “S”. Each scan begins on a main diagonal element (i,i) . We define E and S as the sequence of index pairs (i,i) , $(i,i+1)$, $(i+1,i)$, $(i,i+2)$, $(i+2,i), \dots, (i,i+k)$, $(i+k,i)$ and (i,i) , $(i+1,i)$, $(i,i+1)$, $(i+2,i)$, $(i,i+2), \dots, (i+k,i)$, $(i,i+k)$. We use $(E_i)_{i=l}^m$ represent the sequence $E_l E_{l+1} \dots E_m$. For $k>0$, define the nested index assignment to be

$$((E_i)_{i=(2p)k+1}^{(2p+1)k} (S_i)_{i=(2p+1)k+1}^{(2p+2)k})_p \quad (1)$$

The linear index assignment is composed of the scan “U” and the scan “D”. We define U_j and D_j as the sequence of index pairs $(i+[k/2], i-[k/2])$, $(i+[k/2]-1, i-[k/2]+1)$, \dots , $(i-[k/2], i+[k/2])$ and $(i-[k/2], i+[k/2])$, $(i-[k/2]+1, i+[k/2]-1)$, \dots , $(i+[k/2], i-[k/2])$, where j is an even integer; and if j is an odd integer, define U_j and D_j by $(i+1+[k-1]/2)$, $i-[k-1]/2)$, $(i+[k-1]/2)$, $i-[k-1]/2+1)$, \dots , $(i-[k-1]/2)$, $i+1+[k-1]/2)$, $(i-[k-1]/2)+1$, $i+[k-1]/2)$, \dots , $(i+1+[k-1]/2)$, $i-[k-1]/2)$. For $k>0$, define the linear index assignment to be

$$((U_j)_{j=(2p)(2k)+1}^{(2p+1)(2k)} (D_j)_{j=(2p+1)(2k)+1}^{(2p+2)(2k)})_p \quad (2)$$

III. MDSQ CODING BASED ON JPEG

A. JPEG image compression standard

The JPEG baseline algorithm consists of color mode transformation and sampling, (8×8) DCT transformation, quantization and runlength Huffman coding. A key part of a JPEG system is the quantization of DCT coefficient, and the quantization table plays an important part during quantization. Table 3(a) and 3(b) shows, these are two quantization tables recommended in JPEG standard.

Table 3(a) Quantization table: luminance

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	14	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Table 3(b) Quantization table: chrominance

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

B. Proposed Method

In our scheme, data compression and error resilience can be achieved simultaneously through combining JPEG standard and MDSQ. As shown in figure 3, source image data are transformed through DCT, after that the DCT coefficients are quantized and split into two descriptions.

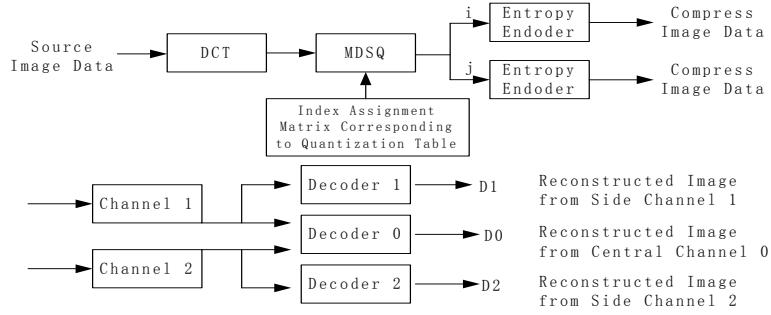


Fig. 3 MDSQ coding based on JPEG system

The performance of proposed system is decided by index assignment algorithm and the value of k . In our method, the value of k is corresponding to the quantization step of quantization table in JPEG standard. We use q to represent an element of quantization table. While q is an even integer, denote the value of k to be

$$k = (q-2)/2 \quad (3)$$

While q is an odd integer, denote the value of k to be

$$k = (q-1)/2 \quad (4)$$

From above, it can be seen that the smaller the quantization step, the smaller the value of k , in the same way, the bigger the quantization step, the bigger the value of k . Several experiments show that linear index assignment outperforms nested index assignment during index assignment matrix formation procedure.

The concrete steps of our algorithm are as follows:

(1) The input image is divided into 8×8 pixel blocks, and transformed by the DCT.

(2) Designing the index assignment matrix bases on the quantization table of JPEG. The concrete setting is shown in table 4 and table 5.

(3) Different DCT coefficient is quantized though MDSQ of different index assignment matrix into two descriptions.

(4) The two descriptions are then encoded using Huffman coding algorithm the same as JPEG standard and will be transmitted through two different channels.

Table 4 The value of k corresponding to quantization table 3(a)
(the number of diagonals are $2k+1$)

7	5	4	7	11	19	25	30
5	5	6	9	12	28	29	27
6	6	7	11	19	28	34	27
6	8	10	14	25	43	39	30
8	10	18	27	33	54	51	38
11	17	27	31	40	51	56	45
24	31	38	43	51	60	59	50
35	45	47	48	55	49	51	49

Table 5 Index assignment matrix when $k=4$

...	-5	-4	-3	-2	-1	0	1	2	3	4	5	...
-5	...		-27		-19							
-4		-26	-24	-20	-15	-10						
-3	-25		-21	-16	-11	-6						
-2		-22	-17	-12	-7	-3						
-1	-23	-18	-13	-8	-4	-1						
0		-14	-9	-5	-2	0	1	3	6	10		
1						2	4	7	11	15	19	
2						5	8	12	16	20		
3						9	13	17	21	24	27	
4						14	18	22		26		
5							23	25				...

At the decoding end, the received descriptions are decoded by Huffman decoder, after that the reconstructed image from central decoder and two side decoders are obtained. When both descriptions are received, the central decoder can correctly decode the coefficients through the index assignment matrix according to table 4, and when only one description is received, the side decoder can obtain the approximate value from row index and column index. Each individual description can

decode independently, and a base quality is achieved from each individual description. The quality is smoothly improved with the number of received description increase.

IV. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed method, a testing image "Lena" of 256*256 pixels and 8 bits per sample is used for simulation. Figure 4 shows the images reconstructed

from a single description and the combined bits of both descriptions. When both descriptions are received, a good quality is obtained. When only one description is available, an acceptable quality is achieved at the decoder, and the distortion can be controlled in a certain degree. The quality of reconstructed image becomes better with increasing bit rate.

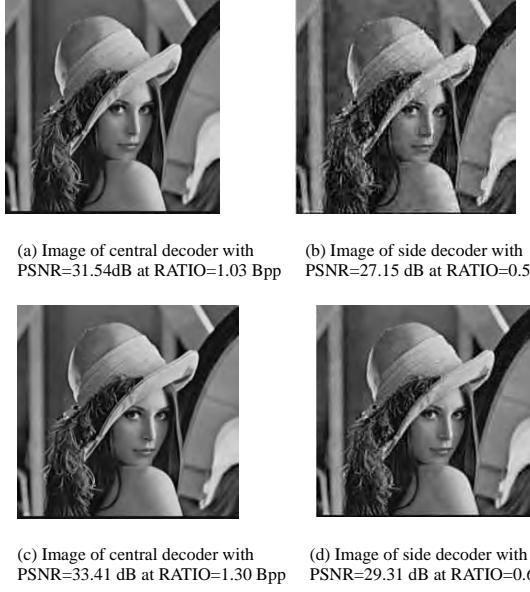
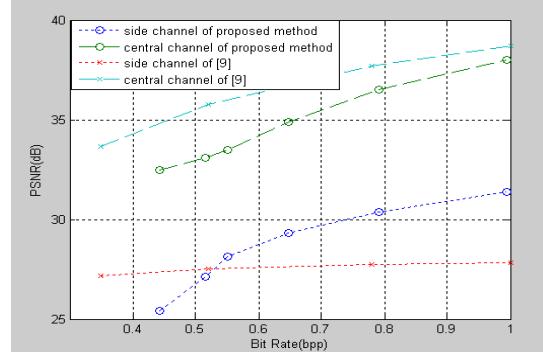


Fig. 4 Reconstructed image of central and side decoder

Figure 5 has provided a comparison between the proposed method and other MD image coding based on JPEG standard in the literature [9]. For side decoding, much better side PSNR performances have been obtained with the proposed method at high bit rate (above 0.5bpp), that is to say, a better efficiency is obtained with high redundancy. However, at lower rates, better side PSNR performances are obtained with the method in [9]. For central decoding, PSNR of the proposed method is slightly lower than the method in [9] (about 2 dB), and margin decreases gradually with increasing of bit rate.

Fig. 5 PSNR of proposed method versus the method in [9]



Simulation results show that the computational complexity of our method is similar to JPEG standard. In a comparison, which between JPEG image compression and our method, the running time of JPEG is 0.185 seconds, and our method is 0.443 seconds as only one description is available, and 1.002 seconds when both descriptions are received. The additional running time compared with traditional JPEG standard codec is consumed to produce several index assignment matrixes. While the index assignment matrixes have been produced before compression and decompression, there is no additional running time at the expense of additional memory. Because the number of elements of the JPEG quantization table is 64, the number of index assignment matrixes is less than 64, which means less than 2M bytes memory is needed to store the index assignment matrixes produced off line.

Experiment results show that the advantages of proposed method are the simpler algorithm relative to other methods of MDC and good coding efficiency. Although the quality of reconstructed image decoded from the side decoder is not good at low bit rate, the visual effect is acceptable. Meanwhile, this method is easy to realize due to combine the JPEG standard.

V. CONCLUSIONS

The MDC image coding algorithm based on JPEG incorporates multiple description scalar quantization with JPEG standard to realize the image compression, where several index assignment matrixes corresponding to each quantization steps. Experimental results show the scheme has characteristics of good coding efficiency, controllable compression ratio, and low computation complexity both in encoding and decoding procedures. Furthermore, the compatibility with traditional JPEG image compression standard will facilitate the implementation of this algorithm.

References

- [1] V. K. Goyal, "Multiple Description Coding: Compression Meets the Network", *IEEE Signal Process. Mag.*, vol. 18, no. 5, pp. 74-93, Sep. 2001
- [2] V. Vaishampayan, "Design of Multiple Description Scalar Quantizers", *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 821-834, May. 1993.
- [3] V. Vaishampayan, N.J.A. Sloane, S.D. Servetto, "Multiple Description Vector Quantization with Lattice Codebooks Design and Analysis", *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1718-1734, 2001.
- [4] V. K. Goyal, J. Kovacevic, R. Arean, M. Vetterli, "Multiple Description Transform Coding of Images", *IEEE Trans. Inf. Process.*, pp. 674-678, Oct. 1998.
- [5] Y. Wang, M.T. Orchard, V. Vaishampayan, et al, "Multiple Description Coding Using Pairwise Correlating Transforms" *IEEE Trans. Image Process.*, vol. 10, no. 3, pp. 351-366, Mar. 2001.
- [6] S. Shirani, M. Gallant, F. Kosseintini, "Multiple Description Image Coding Using Pre- and Post-processing", *IEEE International Conference on Information Technology*, pp. 35-39, Apr. 2001.
- [7] A.R. Reibman, H. Jafarkhani, Y. Wang, M.T. Orchard, R. Puri, "Multiple Description Video Coding Using Motion Compensated Temporal Prediction", *IEEE Trans. Circuits Syst. Video Technol.*, vol. 12, no. 3, pp. 193-204, 2002.
- [8] V. A. Vaishampayan, Jaroslaw Domaszewicz, "Design of Entropy-constrained Multiple Description Scalar Quantizers", *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 245-250, 1994
- [9] Ji Wen-ping, Shen Lan-sun, "Multiple Description Coding by Mojette Transform for Image", *Acta Electronica Sinica*, vol. 35, no. 3, pp. 526-529, Mar. 2007.

A General Method for Synthesis of Uniform Sequences with Perfect Periodic Autocorrelation

B. Y. Bedzhev, Member, IEEE

University of Shoumen “Bishop Constantin Preslavski”

115 Universitetska Str.

Shoumen, Bulgaria 9712, EU

M. P. Iliev

University of Ruse “Angel Kanchev”

8 Studentska Str.

Ruse, Bulgaria 7017, EU

Abstract-The families of radio signals possessing both autocorrelation functions (ACFs) with a small level of the side-lobes and small cross-correlation functions (CCFs) among all pairs of the members of a family have great importance for the present communications. Due to this reason in the paper a general method for synthesis of uniform sequences with perfect periodic ACF, resembling to a delta pulse, is proposed. It allows all known at present techniques such as Frank-Zadoff-Heimiller's, Chu's and Milewski's methods to be viewed by a common theoretical base.

Index Terms – Synthesis of signals, perfect periodic autocorrelation function, orthogonal sequences

I. INTRODUCTION

The families of radio signals possessing both autocorrelation functions (ACFs) with a small level of the side-lobes and small cross-correlation functions (CCFs) among all pairs of members of a family are often called sequences with optimal correlation properties (SOCP). They have great importance for the present communications due to the following reasons. First, SOCP allow the so-named self-interference (SI), caused by multipath spreading of electromagnetic waves, to be reduced by a separate processing of the direct and reflected signals. Second, it is possible the negative effect of simultaneous transmission of numerous users, named multi user interference (MAI), to be minimized. With regard to the positive features of the SOCP they have been intensively studied during the past sixty years. Despite of taken efforts many problems in the field of their synthesis are open still. Due to this reason in the paper a general method for synthesis of uniform sequences with perfect periodic ACF (PACF), resembling to a delta pulse, is proposed. It allows all known at present techniques such as Frank-Zadoff-Heimiller's, Chu's and Milewski's methods to be viewed by a common theoretical base.

Paper is organized as follows. First, the basics of the uniform sequences with perfect PACF are recalled. Second, our method for synthesis of these sequences is presented. At the end the possible areas of application of the proposed in the paper method are listed.

II. BASICS OF THE SYNTHESIS OF THE UNIFORM SEQUENCES WITH PERFEKT PACF

Let $N \geq 1, Q \geq 2$ be integers. Then the sequence:

$$\{u(k)\}_{k=0}^{N-1} = \{u(0), u(1), \dots, u(N-1)\}, \quad (1)$$

$$\forall u(k) \in \{\exp[(2\pi i l)/Q]; l = 0, 1, \dots, Q-1\}, \quad (2)$$

is called uniform sequence of length N . It is a mathematical model of the radio-signals, obtained only by Q -phase shift keying (Q -PSK) of the carrier frequency. The Q -PSK signals have the minimal possible peak – factor, which allows them to be easily generated by small, compact and cost – effective semiconductor elements. As a result the Q -PSK signals are widely applied in numerous communication systems today. Anyway, in order to resist to the SIs, the Q -PSK signals should possess a perfect PACF, which is similar to a delta-pulse. This condition can be described mathematically as follows:

$$P_u(r) = \sum_{k=0}^{N-1} u(k) u^* \langle k+r \rangle = \begin{cases} N, & r = 0, \\ 0, & r = 1, 2, \dots, N-1 \end{cases} \quad (3)$$

where r is the time-shift, $P_u(r)$ - the corresponding value of the PACF of the sequence $\{u(k)\}_{k=0}^{N-1}$, the symbol “ $*$ ” means “complex conjugation” and “ $\langle k+r \rangle$ “ denotes that the summa is taken modulo N .

Due to the importance for the present communications of the Q -PSK signals with a perfect PACF, the uniform sequences have been intensively studied by numerous authors during the past sixty years. As a result the following names for uniform sequences with a perfect PACF are used: polyphase codes with good (or optimum) correlation properties, e.g. [2], [8], perfect autocorrelation or root-of-unity sequences, e.g. [7], bent

functions, e.g. [3], sequences with thumb-tack ACF (especially in the field of radars and sonars).

Up to day two main methods for synthesis of uniform sequences with a perfect PACF (USPPACF) are known. The first of them is invented by Gauss and have been studied by Wiener and Chu [1] in more details. Due to this reason it will be called Chu's method in the rest part of the paper and can be described as follows. Let:

$$M = \begin{cases} N, & N \text{ odd}, \\ 2N, & N \text{ even}, \end{cases}$$

then the uniform sequence, consisting of N elements

$$u(k) = \exp(2\pi i k^2 / M), \quad k = 0, 1, \dots, N-1, \quad (4)$$

has a perfect PACF (according to (3)). When N is odd, Wiener has found a slightly more general form than (4):

$$u(k) = \exp[2\pi i(a k^2 + b k) / M], \quad k = 0, 1, \dots, N-1 \quad (5)$$

where a and N are relatively prime, i.e. $(a, N)=1$.

The second main method is independently proposed by Frank, Zadoff [5] and Heimiller [8]. It allows synthesizing USPPACF of length N^2 which elements are:

$$u(k) = \exp[2\pi i(\lfloor k/N \rfloor(k - \lfloor k/N \rfloor)/N)], \quad k = 0, 1, \dots, N^2 - 1. \quad (6)$$

Here $\lfloor x \rfloor$ is the greatest integer $n_x \leq x$.

Except above main methods at present two methods for synthesis of derivative USPPACF, invented by Ipatov [10] and Milewski [1] respectively, are known. In fact they construct long USPPACF on the base of given initial short USPPACF. Due to this reason, these methods are briefly viewed in the paper.

Up to day any connection among Chu's and Frank-Zadoff-Heimiller's methods is not found and it is not known if other methods for synthesis of USPPACF exist. These still open problems will be explored in the next section of the paper.

III. A GENERAL METHOD FOR SYNTHESIS OF UNIFORM SEQUENCES WITH PERFECT PERIODIC ACF

The main result of our paper is that the Frank-Zadoff-Heimiller's, Chu's and Milewski's methods can be viewed by a common theoretical base, which will be given by Theorem 3.3. Before that it is necessary the following definition to be introduced.

Definition 3.1: Two uniform sequences $\{u(k)\}_{k=0}^{N-1}$ and $\{v(k)\}_{k=0}^{N-1}$ will be called *orthogonal* if their periodic CCF (PCCF) $P_{uv}(r)$ is zero for every time-shift r , i.e.:

$$P_{uv}(r) = \sum_{k=0}^{N-1} u(k) v^*(k+r) = 0, \quad r = 0, 1, \dots, N-1 \quad (7)$$

Proposition 3.2: Let the length of the USPPACF $\{u(k)\}_{k=0}^{N-1}$, synthesized by the Chu's method (i.e. by (4)) be

$$N = N_1 N_2, \quad N_1 = N_2 \cdot N_3, \quad N_3 \geq 1. \quad (8)$$

Besides, let the constants k and m be arbitrarily chosen so that $0 \leq k \leq N_2 - 1$, $1 \leq m \leq N_2 - 1 - k$. In this case the subsequences $\{u_k(j)\}_{j=0}^{N_1-1}$ and $\{u_{k+m}(j)\}_{j=0}^{N_1-1}$:

$$u_k(j) = u(k + jN_2), \quad j = 0, 1, \dots, N_1 - 1 \quad (9)$$

$$u_{k+m}(j) = u(k + m + jN_2), \quad j = 0, 1, \dots, N_1 - 1 \quad (10)$$

are orthogonal.

Proof: According to (4) the PCCF of the subsequences $\{u_k(j)\}_{j=0}^{N_1-1}$ and $\{u_{k+m}(j)\}_{j=0}^{N_1-1}$ can be evaluated as follows:

$$\begin{aligned} P_{kk+m}(r) &= \sum_{j=0}^{N_1-1} u_k(j) u_{k+m}^*(j+r) = \\ &= \sum_{j=0}^{N_1-1} u(k+jN_2) u^*(k+m+(j+r)N_2) = \\ &= \sum_{j=0}^{N_1-1} e^{\{2\pi i[(k+jN_2)^2 - (k+m+(j+r)N_2)^2]\}/M} = \\ &= e^{\{(-2\pi i)[2km+m^2+2r(k+m)N_2+(rN_2)^2]\}/M} \times \\ &\quad \times \sum_{j=0}^{N_1-1} e^{\{(-2\pi i)[2(mN_2+rN_2^2)j]\}/M} \end{aligned} \quad (11)$$

Let us consider the last term in (11), supposing that N is even:

$$\begin{aligned} \sum_{j=0}^{N_1-1} e^{\{(-2\pi i)[2(mN_2+rN_2^2)j]\}/M} &= \\ &= \sum_{j=0}^{N_1-1} e^{\{(-2\pi i)[2(mN_2+rN_2^2)j]\}/(2N_1N_2)} = \\ &= \sum_{j=0}^{N_1-1} e^{\{(-2\pi i)[(m+rN_2)j]\}/N_1} \end{aligned} \quad (12)$$

Now it should be seen that N_1 never divides exactly (i.e. ever the remainder is nonzero) the term $(m+rN_2)$ in (12). This statement follows from the analysis of the congruence

$$N_2 \cdot r \equiv -m \pmod{N_1}. \quad (13)$$

As N_2 divides N_1 ($N_1 / N_2 = N_3 \geq 1$) exactly, (13) can have a solution for some r if and only if N_2 divides m exactly. This is impossible as $1 \leq m \leq N_2 - 1$. In other words

$$N_2 \cdot r + m \equiv q \pmod{N_1}, \quad q \neq 0 \pmod{N_1}, \quad (14)$$

which allows the last term in (12) to be evaluated as follows

$$\begin{aligned} \sum_{j=0}^{N_1-1} e^{\{(-2\pi i)[(m+rN_2)j]/N_1\}} &= \\ &= \sum_{j=0}^{N_1-1} e^{(-2\pi i)(qj)/N_1} = \frac{1-e^{[(-2\pi i)(qj)/N_1]N_1}}{1-e^{(-2\pi i)(qj)/N_1}} = 0 \end{aligned} \quad (15)$$

A truly analogous result can be easily obtained in the case of odd N . Consequently, $P_{kk+m}(r) = 0$ for $r = 0, 1, \dots, N_1 - 1$, which ends the proof of the Proposition 3.2. It should be mentioned that Proposition 3.2 remains true also if the construction (5) is used, but in this case the calculations are a bit tedious.

Now the main theorem of the paper can be presented.

Theorem 3.3: Let N , N_1 and N_2 be the same as in Proposition 3.2. Then at least an USPPACF $\{v(k)\}_{k=0}^{N-1}$ exists which all elements belong to the reduced set

$$\{\exp[(2\pi i l)/N_1]; l = 0, 1, \dots, N_1 - 1\} \quad (16)$$

Proof. Let us consider the USPPACF $\{u(k)\}_{k=0}^{N-1}$, synthesized by the Chu's method. Its perfect PACF can be described by means of the so-named polynomial representation [9]

$$\sum_{r=0}^{N-1} P_u(r)x^r = \left[\sum_{k=0}^{N-1} u(k)x^k \right] \left[\sum_{k=0}^{N-1} u^*(k)x^{-k} \right] \pmod{x^N - 1} \quad (17)$$

Here $P_u(r), r = 0, 1, 2, \dots, N-1$ are given in (3) and $x^{-k} = x^{N-k} \pmod{x^N - 1}$.

The USPPACF $\{u(k)\}_{k=0}^{N-1}$ can be separated into N_2 subsequences $\{u_k(j)\}_{j=0}^{N_1-1}$, $k = 0, 1, \dots, N_2 - 1$, which elements are defined by (9). As a result, the polynomials in the right hand of (17) can be rearranged as follows

$$\sum_{k=0}^{N-1} u(k)x^k = \sum_{k=0}^{N_2-1} x^k \left[\sum_{j=0}^{N_1-1} u_k(j)x^{jN_2} \right] \quad (18)$$

$$\sum_{k=0}^{N-1} u^*(k)x^{-k} = \sum_{k=0}^{N_2-1} x^{-k} \left[\sum_{j=0}^{N_1-1} u_k^*(j)x^{-jN_2} \right] \quad (19)$$

After taking into account (18) and (19) in (17), the result is

$$\begin{aligned} \left[\sum_{k=0}^{N-1} u(k)x^k \right] \left[\sum_{k=0}^{N-1} u^*(k)x^{-k} \right] &= \sum_{k=0}^{N_2-1} F_k(x^{N_2}) F_k^*(x^{-N_2}) + \\ &+ \sum_{k=0}^{N_2-1} \left[\sum_{m \neq k, m=0}^{N_2-1} x^{k-m} F_k(x^{N_2}) F_m^*(x^{-N_2}) \right] \pmod{(x^N - 1)} \end{aligned} \quad (20)$$

Here for brevity the substitutions

$$F_k(x^{N_2}) = \sum_{j=0}^{N_1-1} u_k(j)x^{jN_2}, \quad (21)$$

$$F_k^*(x^{-N_2}) = \sum_{j=0}^{N_1-1} u_k^*(j)x^{-jN_2}, \quad (22)$$

are used.

From (17) and Proposition 3.2 the relations issue

$$0 = \sum_{r=0}^{N_1-1} P_{km}(r)x^{rN_2} = F_k(x^{N_2}) F_m^*(x^{-N_2}) \pmod{x^N - 1}, \quad (23)$$

$$k = 0, 1, \dots, N_2 - 1, \quad m = 0, 1, \dots, N_2 - 1, \quad k \neq m.$$

Consequently

$$\sum_{r=0}^{N-1} P_u(r)x^r = \sum_{k=0}^{N_2-1} F_k(x^{N_2}) F_k^*(x^{-N_2}) \pmod{x^N - 1} \quad (24)$$

Now it should be seen that according to (4), the polynomial (21) can be presented in the form

$$\begin{aligned} F_k(x^{N_2}) &= \sum_{j=0}^{N_1-1} e^{2\pi i(k^2 + 2kjN_2 + N_2^2)/M} x^{jN_2} = \\ &= e^{2\pi i(k^2 + N_2^2)/M} \sum_{j=0}^{N_1-1} e^{2\pi i(2kjN_2)/M} x^{jN_2} = \\ &= e^{2\pi i(k^2 + N_2^2)/M} G_k(x^{N_2}). \end{aligned} \quad (25)$$

Here the coefficients of the polynomial

$$G_k(x^{N_2}) = \sum_{j=0}^{N_1-1} v_k(j)x^{jN_2}, \quad (26)$$

belong to the set (16) because

$$v_k(j) = \begin{cases} e^{2\pi i k j / N_1}, & N \text{ even}, \\ e^{4\pi i k j / N_1}, & N \text{ odd} \end{cases} \quad (26)$$

Analogously, the following relations take place:

$$F_k^*(x^{N_2}) = e^{-2\pi i (k^2 + N_2^2)/M} G_k^*(x^{-N_2}), \quad (27)$$

$$G_k^*(x^{-N_2}) = \sum_{j=0}^{N_1-1} v_k^*(j)x^{-jN_2}. \quad (28)$$

After taking into account (25) and (27) in (24), the result is

$$\sum_{r=0}^{N-1} P_u(r)x^r = \sum_{k=0}^{N_2-1} G_k(x^{N_2})G_k^*(x^{-N_2}) \pmod{x^N - 1} \quad (29)$$

Now it should be seen that

$$G_k(x^{N_2})G_k^*(x^{-N_2}) = 0 \pmod{x^N - 1}, \quad k \neq m, \quad (30)$$

because

$$0 = F_k(x^{N_2})F_m^*(x^{-N_2}) = e^{2\pi i (k^2 - m^2)/M} \times \\ \times G_k(x^{N_2})G_m^*(x^{-N_2}) \pmod{x^N - 1}, \quad k \neq m. \quad (31)$$

From (29) and (30) follows that the sequence

$$\{v(l)\}_{l=0}^{N-1} = \{v(k + jN_2)\}_{k=0, j=0}^{N_2-1, N_1-1} \quad (32)$$

satisfies the relation

$$\left[\sum_{k=0}^{N-1} v(k)x^k \right] \left[\sum_{k=0}^{N-1} v^*(k)x^{-k} \right] = \sum_{l=0}^{N_2-1} G_k(x^{N_2})G_k^*(x^{-N_2}) + \\ + \sum_{k=0}^{N_2-1} \left[\sum_{m \neq k, m=0}^{N_2-1} x^{k-m} G_k(x^{N_2})G_m^*(x^{-N_2}) \right] = \\ = \sum_{r=0}^{N-1} P_u(r)x^r \pmod{x^N - 1} \quad (33)$$

This proves the Theorem 3.3, because (33) shows that the sequence (32) has a perfect PACF, according to (3).

From Theorem 3.3 the following conclusion can be made.

Conclusion: The method, proved in the Theorem 3.3 extends the possibilities of the Chu's method and gives analogous results

in cases, where the Frank-Zadoff-Heimiller's and Milewski's methods are applicable.

Indeed, according to the Theorem 3.3, an USPPACF $\{u(k)\}_{k=0}^{N-1}$, synthesized by the Chu's method, can be separated into N_2 the subsequences, defined by (9). The elements of every subsequence can be "corrected" by multiplication with an "individual" coefficient. This fact generalizes the Chu's method. Besides, if

$$N_1 = N_2, \quad N = N_1^2, \quad (34)$$

and if the individual coefficients for correcting of the subsequences are chosen to be

$$t_k = e^{-2\pi i (k^2 + N_1^2)/M}, \quad k = 0, 1, \dots, N_1 - 1 \quad (35)$$

then the elements of all subsequences will belong to the set (16). In addition, the subsequences can be corrected by multiplication with arbitrary individual coefficients which are complex numbers with modulus 1. More over, the sequence (32) is truly equivalent to the sequence, synthesized by the Frank-Zadoff-Heimiller's method if $N_3 = 1$. At the end it should be seen that (8) is equivalent to $N = N_3 \cdot N_2^2$. Consequently, an USPPACF analogous to the sequence, constructed by means of Theorem 3.3 can be synthesized by the Milewski's method. Anyway the method, proved by Theorem 3.3, has this advantage that it gives directly the wanted USPPACF, while the Milewski's method is applicable only if an USPPACF of length N_3 is initially known.

Theorem 3.3 and the above general conclusion will be explained by the following example.

Example 3.4: Let $N = 16$. In this case it is not hard the following USPPACF $\{u(k)\}_{k=0}^{15}$ to be synthesized by the Chu's method

$$\begin{aligned} \{u(k)\}_{k=0}^{15} = & \{u(0) = 1, \quad u(1) = h, \quad u(2) = h^4, \quad u(3) = h^9, \\ & u(4) = h^{16}, \quad u(5) = h^{25}, \quad u(6) = h^4, \quad u(7) = h^{17}, \\ & u(8) = 1, \quad u(9) = h^{17}, \quad u(10) = h^4, \quad u(11) = h^{25}, \\ & u(12) = h^{16}, \quad u(13) = h^9, \quad u(14) = h^4, \quad u(15) = h \end{aligned} \quad (36)$$

where $h = \exp(2\pi i / 32)$, $h^8 = i$, $h^{16} = -1$. First if we choose $N_1 = 8, N_2 = 2, N_3 = 4$, the direct examination shows that the subsequences

$$\begin{aligned} \{u_0(0 + jN_2)\}_{j=0}^7 = & \{u(0) = 1, u(2) = h^4, u(4) = h^{16}, \\ & u(6) = h^4, u(8) = 1, u(10) = h^4, u(12) = h^{16}, u(14) = h^4\} \end{aligned} \quad (37)$$

$$\begin{aligned} \{u_1(1 + jN_2)\}_{j=0}^7 = & \{u(1) = h, u(3) = h^9, u(5) = h^{25}, \\ & u(7) = h^{17}, u(9) = h^{17}, u(11) = h^{25}, u(13) = h^9, u(15) = h\} \end{aligned} \quad (38)$$

are orthogonal. As a result, they can be corrected by multiplication with the individual coefficients, calculated by (35)

$$t_0 = 1, \quad t_1 = h^{-1}. \quad (39)$$

This leads to the modified orthogonal subsequences

$$\begin{aligned} \{v_0(0+jN_2)\}_{j=0}^7 &= \{v(0) = 1, v(2) = h^4, v(4) = h^{16}, \\ &\quad v(6) = h^4, v(8) = 1, v(10) = h^4, v(12) = h^{16}, v(14) = h^4\} \end{aligned} \quad (40)$$

$$\begin{aligned} \{v_1(1+jN_2)\}_{j=0}^7 &= \{v(1) = 1, v(3) = h^8, v(5) = h^{24}, \\ &\quad v(7) = h^{16}, v(9) = h^{16}, v(11) = h^{24}, v(13) = h^8, v(15) = 1\} \end{aligned} \quad (41)$$

The subsequences (40) – (41) now can be reassembled, according to (32), and the result is

$$\begin{aligned} \{v(k)\}_{k=0}^{15} &= \{v(0) = 1, v(1) = 1, v(2) = h^4, v(3) = h^8, \\ &\quad v(4) = h^{16}, v(5) = h^{24}, v(6) = h^4, v(7) = h^{16}, \\ &\quad v(8) = 1, v(9) = h^{16}, v(10) = h^4, v(11) = h^{24}, \\ &\quad v(12) = h^{16}, v(13) = h^8, v(14) = h^4, v(15) = 1\} \end{aligned} \quad (42)$$

The elements of the sequence (42) belong to the reduced set

$$\begin{aligned} \{1, f, f^2, f^3, f^4, f^5, f^6, f^7\}, \\ f = h^4 = \exp(2\pi i / 8) = \sqrt{i} \end{aligned} \quad (43)$$

The direct examination shows that the sequence (42) possesses perfect PACF which demonstrates an significant extension of the possibilities of the Chu's method, obtained on the base of Theorem 3.3.

Now if we choose $N_1 = N_2 = 4$, $N = N_1^2$, $N_3 = 1$, the USPPACF (36) can be separated into $N_2 = 4$ orthogonal subsequences:

$$\begin{aligned} \{u_0(0+jN_2)\}_{j=0}^3 &= \\ &= \{u(0) = 1, u(4) = h^{16}, u(8) = 1, u(12) = h^{16}\} \end{aligned} \quad (44)$$

$$\begin{aligned} \{u_1(1+jN_2)\}_{j=0}^3 &= \\ &= \{u(1) = h, u(5) = h^{25}, u(9) = h^{17}, u(14) = h^9\} \end{aligned} \quad (45)$$

$$\begin{aligned} \{u_2(2+jN_2)\}_{j=0}^3 &= \\ &= \{u(2) = h^4, u(6) = h^4, u(10) = h^4, u(14) = h^4\} \end{aligned} \quad (46)$$

$$\begin{aligned} \{u_3(3+jN_2)\}_{j=0}^3 &= \\ &= \{u(3) = h^9, u(7) = h^{17}, u(11) = h^{25}, u(15) = h\} \end{aligned} \quad (47)$$

The subsequences (44) – (47) can be corrected by multiplication with the individual coefficients, calculated by (35)

$$t_0 = 1, \quad t_1 = h^{-1}, t_2 = h^{-4}, \quad t_3 = h^{-1}. \quad (48)$$

This leads to the modified orthogonal subsequences

$$\begin{aligned} \{v_0(0+jN_2)\}_{j=0}^3 &= \\ &= \{v(0) = 1, v(4) = h^{16}, v(8) = 1, v(12) = h^{16}\} \end{aligned} \quad (49)$$

$$\begin{aligned} \{v_1(1+jN_2)\}_{j=0}^3 &= \\ &= \{v(1) = 1, v(5) = h^{24}, v(9) = h^{16}, v(14) = h^8\} \end{aligned} \quad (50)$$

$$\begin{aligned} \{v_2(2+jN_2)\}_{j=0}^3 &= \\ &= \{v(2) = 1, v(6) = 1, v(10) = 1, v(14) = 1\} \end{aligned} \quad (51)$$

$$\begin{aligned} \{v_3(3+jN_2)\}_{j=0}^3 &= \\ &= \{v(3) = h^8, v(7) = h^{16}, v(11) = h^{24}, v(15) = 1\} \end{aligned} \quad (52)$$

The subsequences (49) – (52) can be reassembled again, according to (32), and the result is

$$\begin{aligned} \{v(k)\}_{k=0}^{15} &= \{v(0) = 1, v(1) = 1, v(2) = 1, v(3) = h^8, \\ &\quad v(4) = h^{16}, v(5) = h^{24}, v(6) = 1, v(7) = h^{16}, \\ &\quad v(8) = 1, v(9) = h^{16}, v(10) = 1, v(11) = h^{24}, \\ &\quad v(12) = h^{16}, v(13) = h^8, v(14) = 1, v(15) = 1\} \end{aligned} \quad (53)$$

The elements of the sequence (53) belong to the reduced set

$$\{1, i, i^2, i^3\}, i = h^8 = \exp(2\pi i / 4). \quad (54)$$

The direct examination shows that the sequence (53) possesses perfect PACF. In fact, the sequence (53) is a version of the corresponding Frank-Zadoff-Heimiller's sequence with the same length, shifted cyclically in two positions to the left. This shows that the general method, proved by Theorem 3.3, leads to USPPACF truly equivalent to the sequences, obtained by the Frank-Zadoff-Heimiller's method if $N_3 = 1$.

In addition, the individual coefficients for correcting of the subsequences can be arbitrary complex numbers, which modulus is 1. Indeed, it is not hard to verify that the sequence

$$\begin{aligned} \{w(k)\}_{k=0}^{15} = & \{w(0) = 1, \quad w(1) = 1, \quad w(2) = g, \quad w(3) = h^8, \\ & w(4) = h^{16}, w(5) = h^{24}, w(6) = g, \quad w(7) = h^{16}, \\ & w(8) = 1, \quad w(9) = h^{16}, \quad w(10) = g, \quad w(11) = h^{24}, \\ & w(12) = h^{16}, w(13) = h^8, w(14) = g, w(15) = 1\} \end{aligned} \quad (55)$$

is an USPPACF. The sequence (55) is obtained from the sequence (53) by multiplication with the correcting coefficients

$$t_0' = 1, \quad t_1' = 1, \quad t_2' = g, \quad t_3' = 1, \quad |g| = 1. \quad (56)$$

It should be stressed that the sequence (56) can not be synthesized by any of Chu's, Frank-Zadoff-Heimiller's, Milewski's and Ipatov's methods.

IV. CONCLUSION

In the paper a general method for synthesis of USPPACF is proved in Theorem 3.3. In fact it essentially extends the possibilities of the Chu's method and as a result the Frank-Zadoff-Heimiller's and Milewski's methods can be viewed by a common theoretical base.

The proved in the paper method could be used in the following areas.

First, as the subsequences (9) of an USPPACF are orthogonal, they form a family of sequences with optimal correlation properties. In other words, the subsequences (9) of an USPPACF can be used as signature sequences in the communication systems with code division of the users. In this direction some obstacle could be the defects of the PACFs of the subsequences. This problem could be solved by multiplication of the subsequences with appropriate USPPACF, according to the Ipatov's theorem [10].

Second, from (24) it follows that the subsequences (9) of an USPPACF form a set of the so-named generalized Golay sequences [4], [6]. Consequently, the proved in the paper method can be exploited for a direct synthesis of these sequences.

Third, Theorem 3.3 gives some evidences that the used Q -PSK restricts strongly the maximal possible length N of the USPPACF. Namely, the following inequality may take place

$$\max N \leq Q^2. \quad (57)$$

We obtained a proof of (57) and hope to present it in a future paper soon. It is not hard to see that from (57) it issues that Barker sequences with even length do not exist if $N > 4$, which closes an still open problem in the theory of the signals.

ACKNOWLEDGMENT

The authors wish to thank Prof. Dr Kunchev, Prof. Dr Kabakchiev and Prof. Dr Lazarov. Finally, the authors appreciate the thoughtful critique by the referees.

REFERENCES

- [1] J. J. Benedetto and J. J. Donatelli, "Ambiguity function and frame-theoretic properties of periodic zero-autocorrelation waveforms," *IEEE J.of Selected Topics in Signal Processing*, vol.1, No.1, pp. 6-20, June 2007.
- [2] D. C. Chu, "Polyphase codes with good periodic correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-18, pp. 531-532, 1972.
- [3] H. Chung and P. V.Kumar, "A new general construction for generalized bent functions," *IEEE Trans. Inf. Theory*, vol. 35, pp. 206-209, 1989.
- [4] F. Fiedler, J. Jedwab and M. G. Parker, "A framework for the construction of Golay sequences," *IEEE Trans. Inf. Theory*, vol. 54, No. 7, pp. 3114-3129, July 2008.
- [5] R. L. Frank and S. A. Zadoff, "Phase shift codes with good periodic correlation properties," *IRE Trans. Inform. Theory*, vol. 8, pp. 381-382, 1962.
- [6] M. J. E. Golay, "Complementary series," *IRE Trans. Inform. Theory*, vol. 7, pp. 82-87, 1961.
- [7] S. W. Golomb, "Two-valued sequences with perfect periodic autocorrelation," *IEEE Trans. Aerosp. Electro. Syst.*, vol. 28, pp. 383-386, 1992.
- [8] R. C. Heimiller, "Phase shift pulse codes with good periodic correlation properties," *IRE Trans. Inform. Theory*, vol. 7, pp. 254-257, 1961.
- [9] D. A. Huffman, "The generation of impulse-equivalent pulse trains," *IRE Trans. Inform. Theory*, vol. 8, pp. S10-S16, Sept. 1962.
- [10] V. P. Ipatov, "Contribution to the theory of sequences with perfect periodic autocorrelation properties," *Radio Engineering and Electronic Physics*, vol. 25, pp. 31 - 34, Apr. 1980.

Using Support Vector Machines for Passive Steady State RF Fingerprinting

Georgina O'Mahony Zamora & Susan Bergin
Department of Computer Science
National University of Ireland, Maynooth
Maynooth, Co. Kildare
Ireland

Irwin O. Kennedy
Bell Laboratories
Alcatel-Lucent
Blanchardstown, Dublin 15
Ireland

Abstract—Passive steady state RF Fingerprinting has recently been proposed as a promising new method for identifying a radio transmitter. In essence, the algorithm detects the differences imbued on a signal as it passes through the analogue stages of a transmit chain. In this paper we improve the algorithms performance and scalability by proposing a new more sophisticated classification engine. The classifier engine is based on a one-against-one multi class support vector machine. We measure the improved system's performance in the largest, most representative case study of its kind – 73,000 measurements across 41 models of UMTS user equipment (UE). We achieve 94.2% classification accuracy. In addition we provide detailed misclassification analysis and outline how the analysis can be used to considerably further improve overall classification accuracy.

I. INTRODUCTION

Identification of a radio transmitter at the physical layer would enjoy many applications. Gerdes et al [1] provide a diverse list of possible applications including intrusion detection, authentication, forensic data collection and defect detection monitoring. More recently we have been involved in a cellular wireless application of femto base stations [2] that would considerably benefit from such identification. This application is a special case of authentication. It involves reducing the core network signalling load due to location update management in Universal Mobile Telecommunications System (UMTS) femto cellular networks. If we can accurately identify a UE (User Equipment) at first contact with the base station using Radio Frequency (RF) fingerprinting, we can provide an elegant solution to the challenge of suppressing signalling traffic to the core network at higher layers as outlined in [3].

Earlier this year a pilot study was carried out to determine if it was possible to accurately distinguish between different radio transmitters using a novel passive steady state RF fingerprinting based technique [3].

This technique exploits the aggregate effect of differences introduced during transmitter manufacturer. These differences were found in component design (filters, power amplifiers, inductors, capacitors), same component manufacturing tolerance spread, Printed Circuit Board (PCB) materials and PCB soldering etc. These differences are imbued in the transmitted signal and the effect can be detected at the receiver. The only differences in the digital baseband samples produced

by the receiver's radio are due to different transmitters, noise and interference.

The pilot study attempted to correctly discriminate between seven UMTS models. The results were encouraging with discrimination accuracy of 91% being achieved. This study and its strong result received much interest; however, concern was raised as to whether our approach and the accuracy achieved would hold on a truer representation of the UMTS models currently in use. A second study was proposed that would employ data from a large representative sample of the wide variety of mobile phones currently in use and would aim to maintain or indeed improve the high level of accuracy achieved in the pilot study. This paper describes this study in detail and is organized as follows.

First, a detailed review of previous related work is provided. Next the experimental setup is outlined followed by a description of our method of transmitter identification. Our results are presented and a detailed misclassification analysis is provided. Finally, suggestions to further improve our technique are briefly discussed.

II. BACKGROUND AND PREVIOUS WORK

In this work a transient signal is described as a short signal (typically microseconds) that occurs during transmitter power on. This is the time during which the power amplifier ramps its power output and in most cases, where the frequency synthesizer makes the transition to steady state frequency generation. Once this transition period is complete we refer to the rest of the transmission as the steady state signal.

Previous work in radio identification has been dominated by transient signal amplitude variation analysis. The reason for this is that the transient occurs consistently upon transmitter power on. In contrast, the steady state signal is dependent on the data being transmitted. That is the signal changes from one transmission to the next and hence is unsuitable for identification purposes. However this is not strictly true. Modern wireless systems make use of preambles to simplify receiver implementation. These preambles are well defined steady state signals that are consistent between transmissions and radios. We are aware of only one other publication that has investigated the use of steady state signals [1]. They focus on the preamble of wired Ethernet 802.3. Their method employs a bank of matched filters and a threshold based decision unit. Whilst encouraging, the discriminatory performance is unclear.

The authors do not give an overall classification performance figure. Also, they appear to have a large number of false positives. Their system also requires many ad hoc steps to tune the performance. For example, the discriminatory performance was manually refined through a combination of bandpass filtering, creating an ensemble of matched filters and time domain trimming.

As mentioned above, the amplitude variation transient signals have been extensively studied [4], [5], [6], [7], and [8].

They have been shown to offer good identification performance – in excess of 90% [6] - however we observe the following challenges and problems:

- Transient analysis offers good classification performance only when the beginning and end of the transient can be reliably identified [4], [7], and [8].
- It has been reported in [1], [9] that transient analysis is not always able to distinguish between same manufacturer and same model variants.
- The very high over sampling rates (50GS/s) [6] and 500MS/s [4]) demanded by transient analysis requires sophisticated and expensive receiver architectures.

In summary, steady state signals offer a relatively unexplored alternative to transient signals for transmitter identification. We note that if identification is possible in the frequency domain, the use of standard low cost Analogue to Digital Converter (ADC) sample rates and receiver architectures will be made possible.

III. DATA OVERVIEW AND EXPERIMENTAL SETUP

Currently, four UE manufacturers, Nokia, Samsung, Sony Ericsson and Motorola together enjoy 75% market share, as depicted in Fig. 1. In order to represent this market share in our study, 54 mobile UEs spanning 41 different models were purchased and included. The list of UEs and the number of each purchased is provided in Table 1.

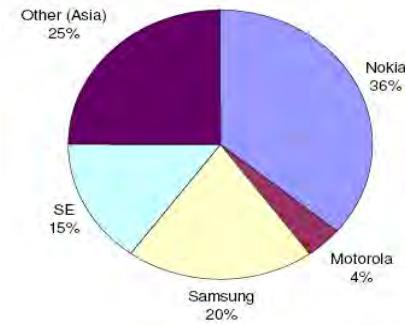


Fig. 1: Outline of UMTS UE manufacturer market share [16].

The test equipment used for capturing the digital I/Q samples is a Rhode and Schwarz FSQ26 signal analyser. All captures are performed at 20MSamples/s.

All measurements are performed in an anechoic chamber. The base station is configured to transmit with very low power (less than 100mW). We have full access to the software load on an Alcatel-Lucent 2100 MHz UMTS base station. In the UMTS standard, system information blocks (SIBs) are broadcast in the cell down link channels. The UE reads the SIBs and uses them to configure its operation. Of particular interest to us in this work is the ability to restrict the UE to use

only a single combination of Random Access Channel (RACH) preamble signature and scrambling code. This means that every RACH preamble transmission from each of the UEs contains the same digital Inphase/Quadrature (I/Q) content at the transmitter.

Table 1: Breakdown of UEs by model included in this study.

Model name	No. of handsets included in study
Motorola KRZR K3	1
Motorola RAZR maxx v6	1
Nokia 6288	1
Nokia 6500 Classic	1
Nokia 6555	1
Nokia 6630	1
Nokia 6650	2
Nokia 7900 Prism	1
Nokia E61i	1
Nokia E65	1
Nokia N70	1
Nokia N78	1
Nokia N91	1
Samsung Softbank 707SCII	1
Samsung F700	1
Samsung i450	1
Samsung L170	1
Samsung SGH i600	1
Samsung Z107	2
Samsung Z170	1
Samsung Z500	1
Samsung Z720	1
Sony Ericsson K530i	1
Sony Ericsson K610i	1
Sony Ericsson K618	1
Sony Ericsson K800i	1
Sony Ericsson W880i	1
Sony Ericsson Z610iR	1
Other PCMCIA: Sierra Wireless (3), Option & Globetrotter (1) & Novatel Wireless (12). Handset: LG (3), Sharp (1), Toshiba (2) & HTC (2).	24

We also edited the base station software load so the base station would never respond to a RACH preamble. This meant the UE would never receive a response to its RACH preamble, therefore it would continue to retransmit its RACH preamble ramp sequence. This was done to make it straightforward to capture the examples required for classification.

The UMTS preamble occupies a bandwidth of 5MHz and consists of 4096 chips at a rate of 3.84Mcps. The result is a 4096 chip pseudo random quadrature phase shift keying (QPSK) signal. It is root raised cosine filtered with an excess bandwidth $BT = 0.22$. Measurements were automated by controlling the signal analyzer with a custom written program running on a laptop that was connected to the analyzer via Ethernet. Measurements are repeated until enough RACH preambles have been captured. We captured approximately

1350 preambles for each UE, 73608 preambles in total. The preamble power ramp means that each preamble in a ramp sequence will have higher power than the previous. This means Additive White Gaussian Noise (AWGN) must be added to higher power RACHs to normalize the Signal to Noise ration(SNR). Finally, the raw data file was written to disc in ASCII format for use by our identification methodology.

IV. METHOD

Our technique uses frequency domain feature extraction combined with a discriminatory classifier to perform device identification. The feature extraction method was similar to that used in our initial pilot study [3]. In essence, the technique detects differences imbued upon the signal as it passes through the analogue stages of a radio transmitter. Fig. 2 depicts the difference between two UMTS UE transmit chains. The graph plots the normalized power spectral density of two UEs transmitting exactly the same digital RACH preamble signal. This section will review the feature extraction method before describing the new classifier engine in detail.

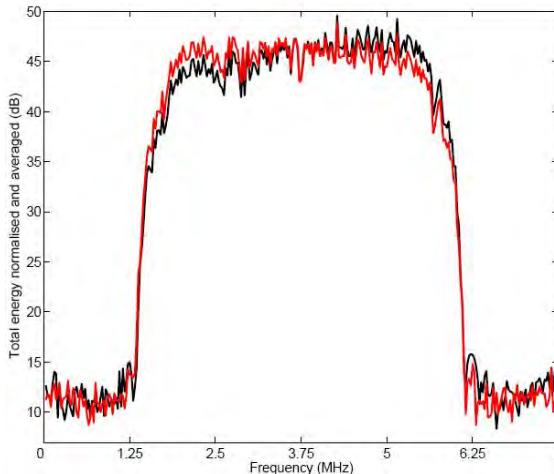


Fig. 2: Example of Power spectral density for two UEs used in this experiment.

Fig. 3 illustrates the processing steps involved in device identification. The input to the pre-processing stage is the received RF signal from the transmitter.

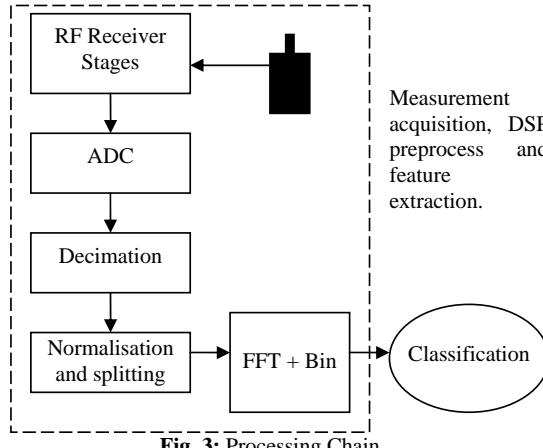


Fig. 3: Processing Chain

A standard radio receiver architecture is employed, down converting the transmit band to baseband, before being band pass over sampled by the ADC at twice the Nyquist rate.

Next the signal is down sampled to Nyquist rate. Captured preambles are separated in time by a period of no transmission. The preamble sequences are split from the signal using a sum of the absolute values window function. The window has length equal to the number of samples in a preamble. It is shifted across the file in 10 sample increments, with the total energy recorded for each window. For every set of samples between two periods of no transmission, the window with the maximum energy is extracted as the preamble.

To remove amplitude variations between transmissions, the time domain samples are energy normalized. We do not apply carrier frequency correction since the UMTS handset disciplines its local quartz source to the down link broadcast carriers.

Next, the frequency domain representation of the complex baseband preamble signal is obtained using Fast Fourier Transform (FFT). To reduce the dimensionality and to construct the feature set presented to the classifier, we reduce the number of bins by taking the mean value of multiple FFT bins to form a single new bin. A set of log-spectral-energy features is finally output to the classifier.

The output of the spectral analysis stage feeds into the final device identification stage in Fig. 3. We feed the output features of the feature extraction stage into a Support Vector Machine (SVM) a state-of-the art supervised machine learning algorithm.

SVMs are a relatively recent set of supervised machine learning algorithms that have been shown to have either equivalent or significantly better generalization performance than other competing methods on a wide range of classification problems [10]. They can be used to classify linearly separable data using the original input space or non-linearly separable data by mapping to a higher dimensional feature space in which a linear separator can be found.

In a typical binary classification problem composed of a training dataset $\{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_m, y_m)\}$ where $\mathbf{x}_i \in \mathcal{R}_d$ and $y_i \in \{\pm 1\}$, SVMs seek a solution to the following Lagrangian optimization function:

$$W(\alpha) = \sum_{i=1}^m \alpha_i - \frac{1}{2} \sum_{i,j=1}^m \alpha_i \alpha_j y_i y_j K(\mathbf{x}_i, \mathbf{x}_j) \quad (1)$$

subject to the following constraints:

$$C \geq \alpha_i \geq 0 \quad \forall i \text{ and } \sum_{i=1}^m \alpha_i y_i = 0. \quad (2)$$

C is an optional parameter that controls the trade off between allowing training errors and forcing rigid margins.

That is, it represents a soft margin that allows some misclassifications which can be beneficial in noisy datasets. Where a soft margin is not allowed, the constraint is simply $\alpha_i \geq 0$. K represents the kernel function and numerous choices exist, including:

$$\text{linear: } K(\mathbf{x}_i, \mathbf{x}_j) = (\mathbf{x}_i^T \cdot \mathbf{x}_j + 1) \quad (3)$$

$$\text{Polynomial: } K(\mathbf{x}_i, \mathbf{x}_j) = (\mathbf{x}_i \cdot \mathbf{x}_j + 1)^d \quad (4)$$

Radial Basis Function:

$$K(\mathbf{x}_i, \mathbf{x}_j) = \exp(-\gamma \|\mathbf{x}_i - \mathbf{x}_j\|^2), \gamma > 0. \quad (5)$$

Once an optimal solution is found, the decision function for a new point \mathbf{z} is given by

$$f(\mathbf{z}) = \text{sign}\left(\sum_{i=1}^m y_i \alpha_i K(\mathbf{x}_i, \mathbf{z}) + b\right). \quad (6)$$

\mathbf{z} is a training example, b is the bias and non-zero α_i values represent support vectors, the points that lie closest to the hyperplane.

In this study a Radial Basis Function (RBF) SVM was implemented. RBF SVMs are currently the most popular choice of non-linear SVM and thus are an appropriate algorithm for a first experiment in this problem space [10], [11].

A number of approaches have been proposed to extend SVMs to handle multi-class classification problems, for example, one-against-all, one-against-one and directed acyclic graph SVM (DAGSVM). 'One-against-one' [12] is implemented in this study as it has been shown to have comparable if not better generalized accuracy than alternative techniques and requires considerably less training time [13], [14].

The method consists of constructing an SVM for each pair of classes. Thus for a problem with n classes $n(n-1)/2$ SVMs are trained to distinguish between the samples of one class from the samples of another class. For an unknown pattern, each SVM votes for one class and the class with the highest number of votes is chosen.

The procedure taken to implement the RBF SVMs was as follows. First the attributes are scaled to avoid attributes in greater numeric ranges dominate those in smaller numeric ranges. Then an extensive grid search using 10-fold stratified cross validation was performed to find the best γ and C parameters using 66% of the data. In this procedure, data is randomly split into 10 parts, with each part representing the same proportion of each class or wear state. Each part is held out in turn and the learning scheme is trained on the remaining nine parts. The error rate is calculated on the holdout (test) set. The procedure is executed 10 times on different training sets and the results are averaged over all of the testing datasets. Although this approach is more computationally intensive than the commonly used 'hold out' method, all examples in the dataset are used for training and testing and thus confidence on the generalisability of the results is increased. In addition the stratification process improves the representativeness of each fold as the process seeks to represent the same proportion of each class in a fold as is in the original full dataset. Finally the optimized SVMs are used to predict model type for each of the unseen samples (34% of the data).

V. RESULTS AND DISCUSSION

The pilot study for this project [3] used a Nearest Neighbour algorithm to predict seven different categories of UE models (4,000 preambles in total) with 91% accuracy. The goal of this study was to achieve the same performance on a larger sample reflecting a fairer representation of the current mobile

market. This goal was achieved. With over 73,000 preambles used for training and testing spanning 41 models a prediction accuracy of 94.2% was achieved. A breakdown of the data is shown in Table 2. We believe a similar performance can also be achieved in an indoor wireless propagation environment. For example, our pilot study's measurements [3] were performed in such an environment and the typical maximum delay spread is comparable to the UMTS symbol period.

In total 1456 preambles were misclassified in the test set. Although this result is very good, further efforts to understand and improve the misclassification error were undertaken. In particular attention was focused on the misclassification of Nokia, Samsung, Sony Ericsson and Motorola handsets given their dominant market share.

Nokia UEs account for 36% of current UMTS UEs in use. However, our approach has achieved the smallest amount of error for this class of UE, with less than 5% of Nokia handsets being misclassified. Similarly, Samsung ranks as the next highest selling manufacturer with 20% of the market share and again our approach results in Samsung being misclassified with the second smallest amount of error with 5.9% of Samsung handsets being misclassified. The same inverse relationship holds true for Sony Ericsson (6.7% error rate) and Motorola (10.62% error rate). Thus our approach has effectively minimised error in direct proportion to market share.

To further examine the error two supplementary investigations were carried out. First, the misclassification errors were examined in detail to establish the extent of each type of error and specifically to examine, for each misclassification, how often the classifier actually predicted a different model by the same manufacturer. The results of this analysis are outlined in Table 3.

Arguably, such an error is not as critical as the classifier choosing a different model by a different manufacturer and an ensemble-model that allowed subsequent algorithms to filter from manufacturer to model could greatly improve performance. This is outlined further below.

Nokia handsets are correctly classified as a type of Nokia handset 93% of the time. As a proof-of-concept we extended our approach into an ensemble learning environment where handsets detected to be any Nokia model were filtered to a dedicated Nokia only classifier. This classifier used a simple Nearest Neighbour algorithm to separate the Nokia handsets by model with 97% accuracy, thereby reducing the error considerably. Such an approach could also improve the error rate within each of the other manufacturer categories. In addition, our intuitive observation suggests that an alternative voting mechanism could again improve performance however further investigation is required to examine this.

A second investigation was carried out on the misclassifications to determine how confident the classifier was of the model predicted. Although SVMs typically only output a target label for each input, an extension to the algorithm is possible to generate probability estimates for each sample. The estimates are based on the distance each test point is from the separating hyperplane, the further the point is from the hyperplane, the higher the probability it belongs in the

class, that is the more confident the classifier is that it belongs to the predicted class [15].

Table 2: Breakdown of misclassifications by UE manufacturer, ordered by percentage market share.

Handset	No. of Errors	Misclassified preambles per manufacturer	% Error per manufacturer	% Market share
Nokia 6288	71			
Nokia 6555	15			
Nokia 6630	2			
Nokia 6650	1			
Nokia 790	35			
Nokia E61i	63			
Nokia E65	49			
Nokia N70	10			
Nokia N78	27			
Nokia N91	5			
Samsung L170	112			
Samsung Softbank 707SCII	26			
Samsung SGH i600	20			
Samsung Z170	17			
Samsung i450	10			
Samsung Z500	1			
Samsung Z107	1			
Samsung F700	2			
Samsung Z720	34			
SE K610i	91			
SE K800i	40			
SE K530i	35			
SE Z610iR	19			
SE K618	5			
SE W880i	2			
Motorola K3	54			
Motorola v6	44			
Others	665	665	71.82	25

In 87% of the misclassified cases, the classifier was less than 90% confident that it had predicted the correct class. This suggests that setting a high threshold of how confident the classifier must be to reach a final decision could greatly improve performance. Furthermore, detailed analysis found that in over 80% of the misclassified test instances, the model with the second highest probability was correct, as illustrated in Table 5. Again an ensemble learning mechanism optimised for these findings could be developed.

Finally, it is worth noting that the goal of this study was to achieve similar results to the pilot study but using a considerably more representative sample. Although the authors spent considerable time on the classification stage, the feature extraction techniques remained relatively similar to those used in the pilot study. It is likely that further improvements could be achieved using alternative feature

extraction techniques. A revisit of this stage is planned as a next step.

Table 3: Analysis of Error where predicted model belonged to same manufacturer as actual mode.

	Nokia	Motorola	SE	Samsung
No. of Errors where model predicted belonged to same manufacturer	257	85	68	60
% of Error where model predicted belonged to same manufacturer	93	87	35	27

Table 4: Confidence of misclassifications.

	Nokia	Motorola	SE	Samsung
No. of Errors where probability > 90%	43	20	13	19
% when >90% confident	16	20	7	9

Table 5: Analysis of class with second highest predicted probability.

	Nokia	Motorola	SE	Samsung
No. of Errors where next highest probability correct	253	97	163	183
% of Error where next highest probability correct	91	99	85	82

VI. CONCLUSIONS

This paper reports on the largest study of its kind into radio transmitter identification using passive RF steady state fingerprinting. The study was based on approximately 73,000 RACH preambles and 41 different UE models. A pilot study using our novel approach had achieved very good accuracy however it involved a significantly smaller sample of handsets and related preambles.

The results of this new study are very encouraging with an overall generalisation accuracy of 94.2%. Furthermore, detailed supplementary investigations on misclassification and probability based analysis were carried out and suggestions for using these findings to further improve classification performance were described.

ACKNOWLEDGMENTS

The authors wish to acknowledge Henry Liu for the measurements used in this work. This work was in part supported by the IDA Ireland.

REFERENCES

- [1] R.M. Gerdes, T.E. Daniels, M. Mina and S.F. Russell, “Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach”, *ISOC Network and Distributed, System Security Symposium*, February 2006.
- [2] L.T.W. Ho and H. Claussen, “Effects of User-Deployed, Co-Channel Femtocells on the Call Drop Probability in a

- Residential Scenario”, *IEEE International Symposium on Personal, Indoor and Mobile Communications*, September 2007.
- [3] I.O. Kennedy, P.Scanlon and M. Buddhikiot, “Passive Steady State RF Fingerprinting: A Cognitive Technique for Scalable Deployment of Co-channel Femto Cell Underlays”, *Proceedings IEEE Conference on Dynamic Spectrum Access Networks*, October 2008.
- [4] J. Hall, M. Barbeau and E. Kranakis, “Detecting rogue devices in Bluetooth networks using Radio Frequency Fingerprinting”, *Proceedings of the International Conference on Communications and Computer Networks*, October 2006.
- [5] D. Shaw and W. Kinsner, “Multifractal Modelling of Radio Transmitter Transients for Classification”, *Proceedings Conference on Communications, Power and Computing*, pp. 306-312, May 1997.
- [6] H. Tekbas, N. Serinken and O. Ureten, “An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions”, *Canadian Journal Computer Engineering*, 2004.
- [7] O. Ureten and N. Serinken, “Bayesian detection of transmitter turn-on transients”, *Proceedings NSIP99*, pp. 830-834, June 1999.
- [8] O. Ureten and N. Serinken, “Detections of radio transmitter turn-on transients”, *Electronic Letters*, vol. 35, pp. 1996-1997, November 1999.
- [9] K. Ellis and N. Serinken. Characteristics of radio transmitter fingerprints. *Journal of Radio Science*, pp. 585-597, 2001.
- [10] C.J. Burges, “A Tutorial on Support Vector Machines for Pattern Recognition”, *Knowledge Discovery and Data Mining*, vol. 2, pp. 121 – 167, 1998.
- [11] B. Schoelkopf and A. J. Smola, *Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond*. MIT Press, 2002.
- [12] S. Knerr, L. Personnaz and G. Dreyfus, “Single-layer Learning Revisited: a Stepwise Procedure for Building and Training a Neural Network”, *Neurocomputing: Algorithms, Architectures and Applications*, 1990.
- [13] C.-W. Hsu and C.-J. Lin, “A Comparison of Methods for Multiclass Support Vector Machines”, *IEEE Transactions on Neural Networks*, vol. 13, pp. 412- 425, 2002.
- [14] J. Milgram, M. Cheriet and R. Sabourin, “‘One Against One’ or ‘One Against All’: Which One is Better for Handwriting Recognition with SVMs?”, *Tenth International Workshop on Frontiers in Handwriting Recognition*, 2006.
- [15] J. Platt, “Probabilistic outputs for support vector machines and comparison to regularized likelihood methods”, *Advances in Large Margin Classifiers* , pp. 61-74, 2000.
- [16] T. Luke, A.M. Gardiner, J. Kvall, “Global Wireless Semiconductor Update”, *Lehman Brothers Equity Research Note*, April 29th 2008.

Genetic Optimization for Optimum 3G Network Planning: an Agent-Based Parallel Implementation

Alessandra Esposito, Luciano Tarricone, Stefano Luceri, Marco Zappatore
Dept. Innovation Eng., University of Salento
Via Monteroni
73100 Lecce - Italy

Abstract- The continuous evolution of wireless networks, as well as the attention paid by the public opinion to human exposure to electromagnetic fields radiated by basestation antennas, render the development of software tools to support optimum design and planning of 3G networks highly desirable. Though many tools are already available, open problems are still on the table. One key issue is represented by optimization methods adopted to solve the problem of identifying optimum locations and electrical parameters for basestation antennas. In this paper, the recent technology of software agents is adopted, in conjunction with genetic algorithms and parallel computing, in order to perform effective and efficient optimization of 3G networks. Results demonstrate the appeal of such a strategy, tested on standard real cases. Impressive results are achieved for both the accuracy and the performance attained, with the use of low-cost computing platforms and freeware tools.

I. INTRODUCTION

The design of efficient third-generation (3G) wireless networks is a complex task, deserving the convergence of several different skills in areas such as telecommunication systems, radiopropagation, information systems. Moreover, the optimum design of 3G networks must take into account both constraints coming out from quality of service, coverage, etc., and issues related with human exposure to electromagnetic (EM) fields generated by basestation (BS) antennas. Indeed, safety standards cast some limitations to field levels, and the public opinion is usually extremely sensitive to the possibility of controlling (or, better, reducing) human exposure to EM fields.

In such a many-folded scenario, the setting up of software tools and models to support optimum design and planning of 3G networks is highly desirable. A crucial role is played by optimization methods adopted to solve the problem of identifying optimum locations and electrical parameters for BS antennas. The problem is computationally intensive and must be attacked by using methods able to guarantee global search.

As a matter of fact, Genetic Algorithms (GAs) have proven to be an attractive optimization technique in a wide range of applications, including the optimum planning of wireless networks [1]-[4]. These works demonstrated the need to scale GAs towards parallel computing environments, in order to attack large real-life problems, as well as the importance of performing this at affordable costs.

In this paper, a very recent information technology, *Software Agents*, is adopted in conjunction with parallel (*grid*) computing in order to set up a very efficient and effective

genetic optimizer, suitable to solve the problem of optimum planning of 3G wireless networks.

The paper is structured as follows. Section II proposes the formulation of the optimization problem of 3G network design. Section III recalls basic concepts on GAs, on their parallel implementation and their application in the specific problem. Section IV introduces agents and their adoption in the specific application. Section V describes the agent based-architecture and framework. Results are given in Section VI, proving the efficiency and effectiveness of the method on real cases. Finally, conclusions are drawn.

II. THIRD GENERATION WIRELESS SYSTEM PLANNING

Planning tools for wireless networks are becoming essential for offering a high-quality service network with appropriate use of resources and minimal EM exposure.

To build a planning tool, different aspects have to be accounted for, such as geographical data management, antenna technical data storage, EM fields estimation and network parameter optimization [5].

Among these aspects, one of the most crucial is the appropriate evaluation of the EM field levels generated by network antennas. Several radiopropagation methods can be used to estimate the mean intensity value of the received signal in a specific point. Such methods evaluate the attenuation as the transmitted-to-received power ratio, accounting also for possible wave interactions with the obstacles between transmitter and receiver. The EM simulator employed in this paper adopts Free Space Loss (FSL), the empiric COST231-Okumura-Hata and the semi-empiric COST231-Walfisch-Ikegami model [6]. Obviously, these approaches, are not suitable to address situations of near-field exposure and suffer from a limited accuracy especially in very complex urban scenarios. In such a case the potential user could identify areas of uncertainty in order to adopt dedicated strategies and models [7] on demand.

The other important module of a planning tool is the optimization one. It optimizes BS locations and antenna parameters in order to design high-quality networks, with reduced EM emissions. The network parameter optimization requires the formulation of the problem, specifying the objective function and the constraints, and the choice of the solution method (as described in Section III). The optimum 3G network planning problem (3GNPP) can be formalized as follows: *once the geographical area to be covered has been*

discretized into points where the traffic demand and the EM levels are estimated, given a set of possible BS positions and antenna parameters range, find the best network configuration to minimize a function of the EM field values and to satisfy EM exposure, handover and downlink capacity constraints.

For the sake of brevity, we address the reader to a recent paper [4] for a complete analysis of the variables, constraints and objective functions concerning the problem. We just recall now some relevant issues.

The area is discretized by means of two different set of points. *SDP*: set of Demand Points (DPs), where the total traffic demand is partitioned. *STP*: set of Test points (TPs), where the EM field levels are estimated.

Concerning network parameters, each BS antenna (sector) is characterized by variable parameters such as azimuth, tilt, height-above-ground, total emitted power and few fixed parameters, such as gain, frequency and radiation pattern. In this work we choose to fix these parameters in order to limit the computational cost of optimization, and mainly because, in real network configurations, only a very limited range of antenna types is used.

The BS locations are grouped into subsets, and a maximum of one BS can be activated for each group. A network configuration is defined when each BS is located and all the parameters of each BS sector are set up. The network configuration feasibility is enforced by constraints that provide a realistic representation of a 3G cellular network and compliance with upper limits of EM field values on the TPs.

The specific target of 3GNPP is the achievement of the required quality of service (traffic coverage in this case), while pursuing a policy of control of the human exposure to EM fields (according to safety limits existing in several countries). Therefore, the objective function must take into account the EM levels detected at the TPs. Several scalar functions can be implemented to achieve this goal, i.e.

- the minimization of the sum over the total E field levels in STP (*MinSum*) to provide a global decreasing of the total observed level;
- the minimization of the maximum E field level in the area (*MinMax*) to prevent the formation of peak values;
- the minimization of the difference among the total E field levels in two TP subsets with the highest and lowest values (*MinDiff*) to lead toward solutions with a relatively smooth field distribution.

These objective functions are not monotone with respect to all the variable parameters: their behavior when a BS is moved or if sector tilt or power level are changed is not trivially predictable. In this work only downlink capacity and handover have been considered [8]-[10]. Downlink capacity is expected to be particularly relevant in the presence of asymmetrical communication and it gives us relevant indications about the amount of traffic that can be covered [11]. Other objective functions and models taking into account more network parameters (as accepted users, effective load, etc. [12]) and

uplink direction [11] could be considered but this is outside of the scope of this work.

III. THE PARALLEL GENETIC ALGORITHM

GA is an iterative optimization method that exploits the analogies with genetic processes, in particular natural selection and heredity principles. The EM community is rather familiar with GA approach, and we address the interested reader to [13] for a tutorial introduction to GAs and to [14] for a more specific application to planning problems of wireless networks.

The strength of GAs lies on their robustness and large applicability to different classes of problems since they are capable of performing an efficient search also when the apriori knowledge of the problem is limited.

However, in some problems, the fitness evaluation and/or the feasibility check of each individual of the population can be very time consuming. The consequences are either the slowing down of the entire process or, fixing a reasonable execution time, a shallow exploration of the solution space. The necessity to overcome these limitations and the high modularity of the GA has led toward parallel GA (PGA) implementations.

The parallel approach can be applied to a GA in different ways, depending on how the population is distributed and on how information is shared among parallel instances. A basic classification of PGA has been reported in [15]. In the present paper, taking advantage from the strategies proposed in some recent papers [16][17], we propose an island-based PGA to solve the 3GNPP.

Our implementation of island-based PGA consists of a predefined number of sequential GA threads (instances), each processing a portion of the entire population.

The chromosome migration mechanism follows an adaptive ring topology, thus ensuring ring continuity in case of one or more threads fail or prematurely terminate their execution.

IV. SOFTWARE AGENTS AND PGA

In this section, software agents, and their amenability for an efficient implementation of PGA, are discussed. Software agents are autonomous entities capable of "flexible, autonomous action in their environment in order to meet their design objectives" [17]. In simpler terms, they are computational entities capable of autonomously taking initiative and of communicating with their peers to pursue a goal. Agent-based genetic optimizers have been implemented by several authors [18]-[20]. In most cases, a multi-agent framework is implemented, where each agent carries its own genetic material and interacts with other agents to reach the global optimization goal. This is also the case of the unique (at our best knowledge) work in the computational electromagnetic field [19]. A different approach is proposed here: an *island-based* model, obtained by embedding existing serial code into software agents. The software agent paradigm was chosen for this model for two major reasons:

- 1) agents intelligence can be used to manage global search behaviour (by controlling topology and migration parameters);

- 2) agents are considered the most suited programming paradigm for parallel applications in computational grids (CG) [20], CG being a very low-cost parallel computing environment (see Fig. 1).

Indeed, software agents have several features making them amenable to CG environments. First of all, they can migrate during the execution from one host to another in a network. This is particularly useful in dynamic and unstable environments, such as CGs, where load on computing resources may change enormously during execution time.

Moreover, agents can be dynamically created and destroyed and the computing application is highly transparent with respect to the hardware platform, the number of computers and the configuration of the computer network. This renders agent-based systems very flexible with respect to other libraries commonly used in CGs, such as MPICH-G2, which needs the previous installation and compilation of executables at each node.

On the other hand, performance of distributed agent-based applications can be low as communication between agents generally consumes more bandwidth than other communication models (such as MPI) [22].

Luckily, our problem requires very limited data exchange. Indeed chromosomes migration is sporadic with respect to frequency of generations. Moreover, messages that allow the dynamic adjustment of communication path and framework administration (e.g. keep-alive signal) require a very low bandwidth. Furthermore, since the time needed for exchanging messages between agents is hidden by the time needed for the generation of new chromosomes, the system is expected not to suffer too much from the enhanced communication burden of agent-based paradigm.

V. PGA ARCHITECTURE

The parallel genetic application framework is depicted in Fig. 2, showing a master-worker architecture.

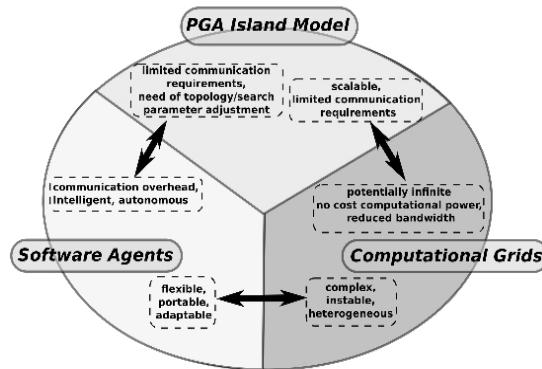


Fig. 1. PGA enabling technologies: the choice for agent-based paradigm is reinforced by suitability of computational grids to support parallel problems with limited communication needs

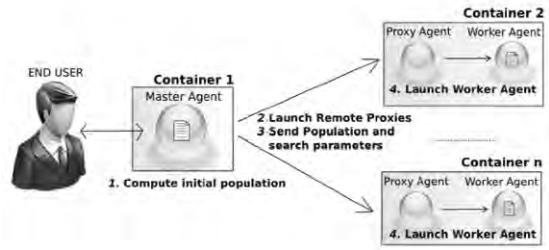


Fig. 2. The PGA framework is based on a master-worker model. The master is responsible for initializing the search, collecting outputs and monitoring search evolution. Worker agents perform searches in islands. Each worker is associated to a proxy agent, that maintains the communication with the master during the search

The *master* agent, apart from being the interface to the end user, is in charge of initializing the environment and of managing and controlling the execution of the framework itself. It launches the worker agents, collects their outputs and ranks them. It is also responsible of adjusting parameters related to search status, topology, and environment conditions change (node fault, unbalanced load, etc.).

The *worker* agents are obtained by embedding GA native C code into a Java method. They carry out a GA search in the sub-population they have been assigned, and exchange individuals at every generation producing an improvement (or after a predefined number of iterations if no improvement is obtained). Each worker agent is associated with a special agent, namely the *proxy*, having the responsibility of managing the interaction between the worker and the rest of the world (master or other workers) during the search. Proxies perform the following actions: forward chromosomes to other proxies and viceversa; inform the master agent about the current status of the associated worker; inform the worker about changes on the execution parameters.

The master/proxy/worker structure allows one to distinguish between local searches (carried out by worker agents) and global search management (carried out by the master which takes into account information provided by the proxies). Substantially, two communication paths are followed (see Fig. 3). The former is performed by workers and proxies and is finalized to perform the exchange of individuals: each time a worker wants to send individuals to other workers, it sends the chromosomes to its proxy, which is in charge of sending the individuals to the correct destination (according to the current network topology). The latter is pursued by the master and the proxies, and is finalized to the monitoring and control of the overall search.

This configuration is flexible and adaptable, featuring the key requirements needed to cope with the instability and unbalance of CG environments and providing (transparently to end-user) the dynamic adjustment of the communication path, (which may be due to network/node failure or, in the most common case, to search completion by one of the worker agents).

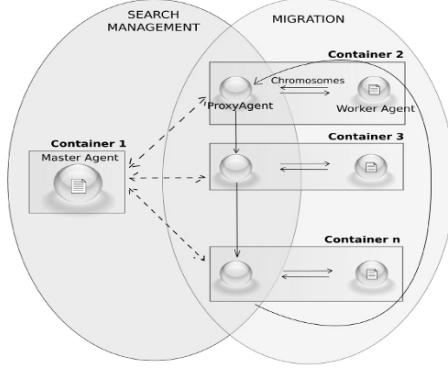


Fig. 3. The two agents communication paths (dashed and continuous lines), ensure asynchronous search management and migration of chromosomes

Software agents need a suited execution environment able to support communication, localization and migration. The de facto standard platform is JADE [22], adopted in our experimentation, which follows the official standard for communication named FIPA [23] and provides a robust framework for hosting agent-based systems.

VI. RESULTS

The PGA applied to 3GNPP has been tested using data from The Hague city scenario prepared by the IST-2000-28088 project MOMENTUM [24]. The considered area, a mix of urban and suburban zones, is 4 Km x 4 Km wide with 76 possible BS sites, each with a different height range. We have divided these potential sites into subgroups of 4 locations and have considered 16 possible values for emitted power (between 0 and 30 W) and sector azimuth, 8 alternative choices for height (each range associated to the relative BS location) and for mechanical tilt (between 0 and 8°) and sector azimuth. The parameters involved in the optimization process have been codified as explained in Fig. 4, using binary strings (chromosomes) to store their numerical values.

All services are considered: speech telephony, file download, Location-based Services, streaming multimedia, video telephony, web surfing, email, MMS. The corresponding traffic data are provided through average and busy hour traffic for each service and traffic snapshots. A *snapshot* is a photo of the traffic demand in a given instant, represented by a set of points, each using a specific service.

In the reported trials, the traffic associated with a snapshot is subdivided among 400 DPs, counting how many snapshot points are in the cell grid of a DP and reporting the different services to speech telephony (according to Tab. I [25]).

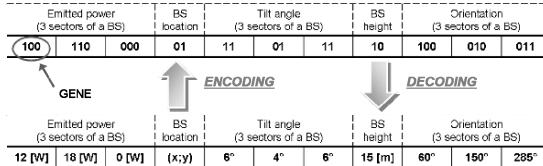


Fig. 4. A bitstring excerpt and the corresponding encoded values.

TABLE I
CONVERSION FOR THE DIFFERENT SERVICES WITH RESPECT TO SPEECH SERVICE

Traffic Type	Effective Downlink Capacity
Speech telephony	1.0
File download	6.9
Location base services (LBS)	1.0
Streaming multimedia	5.7
Video telephony	9.3
Web sharing	3.1
Email	3.6
MMS	3.6

In the following tests, (*MinSum*) has been chosen as objective function and, without loss of generality, the STP has been taken coincident with SDP. The used radiopropagation method is COST231-Okumura-Hata for urban case.

Tests have been performed within a network of 8 computers connected by a TCP/IP-based 100Mb/s network. Computer characteristics are

- CPU: P-IV 3.0Ghz - RAM: 1GB;
 - CPU: AMD Athlon 1.6Ghz - RAM: 256MB
- running under Linux and Windows operating systems.

The platform on which agents reside has to be up and running before the developed PGA framework execution. It includes one main-container and 7 remote containers (one on each host) connected to it. The framework starts once the master agent is launched in one of the available containers. Then the master agent, according to input data given by the user, copies all files and libraries on the other containers and orders the framework to start all agents needed for the simulation. It can be noticed that no previous installation of software is required apart from JADE.

Three instances with a different number of individuals of the global population (400, 800, and 1600 individuals) have been considered. For each of them the following trials have been tested:

- 1 sequential GA with the entire population;
- 2 GA threads running on half the whole population with and without chromosome migration;
- 4 GA threads running on 1/4th of the whole population with and without chromosome migration;
- 8 GA threads running on 1/8th of the whole population with and without chromosome migration.

Table II displays the best objective function value and the wall clock time of each trial with a randomly generated initial population for the 800 individuals instance. In details, the table columns represent: *Seed*, the seed for the random number generator used for the initial population; *n_host*, the number of used hosts (*islands*); *migr_size*, number of chromosomes to migrate; *n_pop*: number of individuals of each subpopulation; *Best*, objective function value of the best resulting solution and *Time*, wall clock time required for the entire execution, including preprocessing and postprocessing phases.

Concerning the migration case, a series of trials with different *migr_size* values have been carried out. The results (not reported here for the sake of brevity) show that in almost every case better results are reached when *migr_size* is the 10%

of the island population. This is the *migr_size* value used in trials described in Figures 5 and 6.

Trials executed with a randomly generated initial populations for the 400 and 1600 individuals instances (not reported here) show similar trends in objective function values and wall clock time. On the basis of data in Tables II, we can observe that (in agreement with [15]) the parallel implementation with or without migration leads in almost every trial to better results than the sequential case. Moreover, Fig. 5, shows that: 1) when exchange of individuals is permitted, the framework succeeds in getting better solutions than in the no-migration case, and in this specific case 2) the solution improves as the host number increases. This behavior is coherent with the island-based population idea: a set of smaller distributed subpopulations with individuals moving from one group to another generates better individuals than a single large static population.

As described in Sec. V, sequential GA is given by the execution of the original C implementation, while PGA consists of the original C code embedded inside a Java agent. Looking at the wall clock time column in Tab. I (also displayed in Fig. 6 for the 800 individuals case) and comparing the execution time of the sequential GA with the execution time of the two-hosts PGA, the overhead due to this kind of implementation can be noticed. The impact of such an overhead is more and more smoothed when more hosts are added. Indeed, a substantially linear trend with respect to the host number is featured by the PGA instances. Such a linear trend is justified by the following considerations:

- preprocessing time (generation of the entire population and distribution of individuals to the hosts) and postprocessing time (sorting of the solutions from the single GAs) is similar for 2, 4, and 8 hosts;

TABLE II
RESULTS FOR THE 800 INDIVIDUALS INSTANCE

Seed	n_host	migr_size	n_pop	Best	Time(s)
1	1	0	800	0.81519	9420
1	2	0	400	0.84803	7465
1	4	0	200	0.77555	4109
1	8	0	100	0.80308	2215
1	2	40	400	0.76244	7589
1	4	20	200	0.71829	4197
1	8	10	100	0.66089	2322
2	1	0	800	0.79037	9628
2	2	0	400	0.82898	7423
2	4	0	200	0.83449	4052
2	8	0	100	0.75772	2224
2	2	40	400	0.76561	7701
2	4	20	200	0.67473	4501
2	8	10	100	0.66542	2299
3	1	0	800	0.80542	9551
3	2	0	400	0.76923	7457
3	4	0	200	0.80294	4052
3	8	0	100	0.77710	2238
3	2	40	400	0.73768	7641
3	4	20	200	0.67838	4312
3	8	10	100	0.63350	2238

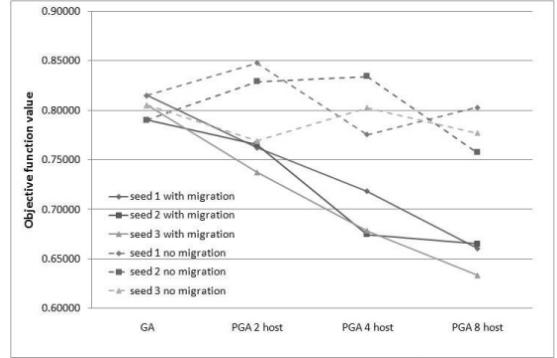


Fig. 5. Migration (solid lines) vs. non-migration (dashed-lines) case for three different initial population for the 800 individuals instance

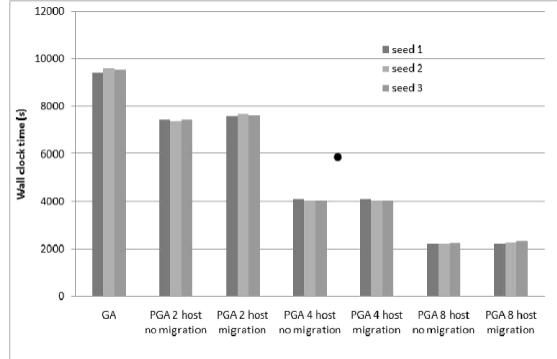


Fig. 6. Wall clock times in seconds of the 800 individuals instance.

- the *migr_size* value and the migration frequency do not influence the wall clock time, thanks to the asynchronous solution exchange mechanism.

Concerning the last issue, a series of tests executed by modifying the migration frequency (ranging from every 20 to every single generation) returns practically the same wall clock time, proving that the solution exchange time (carried out by the Java agent) is hidden by the time needed for the generation of new chromosomes (carried out by the C genetic algorithm implementation).

In conclusion, we observe that:

- agent-based GA is efficiently parallelized;
- the use of agents peculiar features is crucial to achieve high quality solutions in a very reduced time (linear speed-up is attained in a very low-cost local grid).

From the network planning point of view, since it is not straightforward to deduce the meaning of the best objective function values, a comparison between the average traffic distribution in The Hague and the EM distribution of two of the obtained solutions has been reported (see Fig. 7). The EM levels are represented in $dB\mu M/V$. As it can be seen, the resulting solution shows a good match among the BS positions and the areas with higher traffic values.

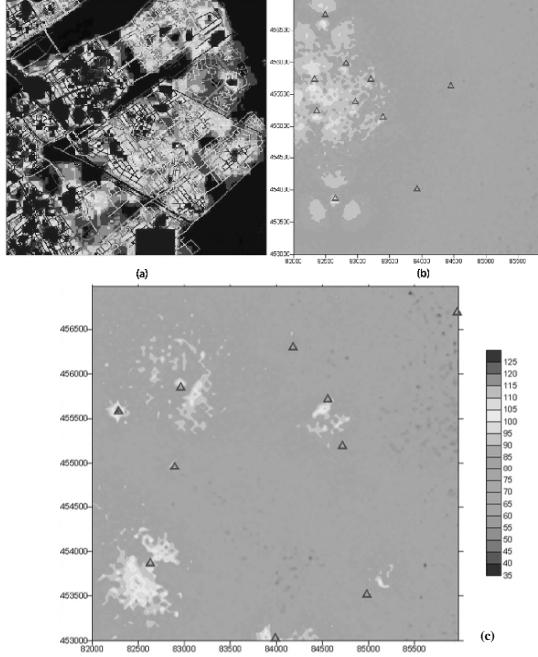


Fig. 7. Average traffic distribution in The Hague city scenario (a) vs. EM field distribution of two resulting solutions with different objective function values ((b) 1.2481), (c) 0.066542).
Markers identify BS location.

Therefore, the optimum planning has produced a high quality network configuration with low EM impact (the maximum EM values are around $120 \text{ dB}\mu\text{M/V} = 0.316 \text{ V/m}$). While guaranteeing a high quality of service.

VII. CONCLUSIONS

In this paper the problem of optimizing locations and electrical parameters of BS antennas in a 3G wireless network has been attacked and solved by using GAs, in conjunction with the technology of software agents and adopting parallel computing strategies.

The adoption of suitable algorithmic choices, namely gene migration, rendered extremely natural and efficient by agents, has produced impressive effectiveness and high-performance in the solution of real cases. Quasi-linear speed-ups are achieved, with a high scalability of the application.

Moreover, software agents are intrinsically open to computational grids, thus paving the way to the adoption of very cost-effective computing platforms, as well as to the setting up of open and scalable software tools for 3G network optimum planning.

REFERENCES

- [1] Pantoja, M.; Bretones, A. and Martin, R.: "Benchmark Antenna Problems for Evolutionary Optimization Algorithms," *IEEE Trans. on Antennas and Propagation*, vol. 55, no. 4, pp. 1111–1121, Apr. 2007.

- [2] Brunetta, L.; Di Chiara, B.; Mori, F.; Nonato, M.; Sorrentino, R.; Strappini, M.; Tarricone, L.: "Optimization Approaches for Wireless Network Planning," in *Proc. 2004 URSI EMTS, Int. Symp. on Electromagnetic Theory*, Pisa (Italy), May 2004, pp. 182–184.
- [3] Di Chiara, B.; Nonato, M.; Strappini, M.; Tarricone, L.; Zappatore, M.: "Hybrid Meta-heuristic Methods in Parallel Environments for 3G Network Planning," in *Proc. EMC Europe Workshop 2005, EM Comp. of wireless Systems*, Rome (Italy), Sept. 2005, pp. 199–202.
- [4] Crainic, T.; Di Chiara, B.; Nonato, M. and Tarricone, L., "Tackling Electrosmog in Completely Configured 3G Networks by Parallel Cooperative Meta-heuristics," *IEEE Wireless Comm., Special Issue 3G/4G/WLAN/WMAN Plann. and Optim.*, vol.13, no.6, pp.34–41,2006
- [5] Angelucci, M.; Di Chiara, B.; Sorrentino, R.; Strappini, M. and Tarricone, L.: "Genetic Optimization of Radiobase-Station Sizing and Location using a GIS-based Framework: Experimental Validation," in *Proc. IEEE AP-S Int. Symp. and USNC/CNCURSI National Radio Science Meeting*, Columbus (Ohio), June 2003, ISBN 0-7803-7847-4.
- [6] Saunders, S. R.; *Antennas and Propagation for Wireless Communication Systems*. New York: John Wiley & Sons Ltd, 1999.
- [7] Catarinucci, L.; Palazzari, P. and Tarricone, L.: "Human Exposure to the Near Field of Radiobase Antennas - a Full-Wave Solution Using Parallel FDTD," *IEEE Trans. on MW Theory and Tech.*, vol. 51, no. 3, pp. 935–940, 2003.
- [8] Jamaa, S. B.; Altman, Z.; Picard, J. M. and Fourestie, B.: "Combined Coverage and Capacity Optimisation for UMTS Networks," in *Proc. Telecommunications Network Strategy and Planning Symp. NETWORKS 2004, 11th International*, 2004, pp. 175 – 178.
- [9] Maple, C.; Guo, L. and Zhang, J.: "Parallel Genetic Algorithms for Third Generation Mobile Network Planning," in *Proc. Int. Conf. on Parallel Computing in Electrical Engineering*, 2004, pp. 229–236.
- [10] Amaldi, E.; Capone, A. and Malucelli, F.: "Base Station Configuration and Location Problems in UMTS Networks," in *Proc. 9th Int. Conf. on Telecommunication Systems, Modelling and Analysis*, 2001.
- [11] Amaldi, E.; Capone, A.; Malucelli, F. and Signore, F.: "Optimization Models And Algorithms For Downlink UMTS Radio Planning," in *Proc. IEEE Wireless Comm. and Networking*, vol.2,2003, pp.827–831.
- [12] Golberg, D. E.: *Genetic Algorithms in Search, Optimization and Machine Learning*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc, 1992.
- [13] S. Datta, Aragon, A and Saunders, S. R.: "Automatic optimisation for UMTS indoor coverage using distributed antenna systems," in *4th IEE Int'l. Conf. on 3G Mobile Comm. Tech.*, vol. 494, 2003, pp. 42–47.
- [14] Han, J.; Park, B.; Choi, Y. and Park, H.: "Genetic Approach with a New Representation Base Station Placement in Mobile Communications," in *Proc. 54th IEEE Conf. on Vehicular Technology*, vol. 4, 2001, pp. 2703–2707.
- [15] Cantú-Paz, E.: "A Survey of Parallel Genetic Algorithms," University of Illinois at Urbana-Champaign, Tech. Rep., 1997.
- [16] Calegari, P.; Guidec, F.; Kuonen, P. and Kobler, D.: "Parallel Island-based Genetic Algorithm for Radio Network Design," *Journal of Parallel and Distributed Computing, Special issue on parallel evolutionary computing*, vol. 47, no. 1, pp. 86–90, Nov. 1997.
- [17] Wooldridge, M.: "Agent-based software engineering," *IEEE Proc. Software Engineering*, vol. 144, pp. 26–37, 1997.
- [18] Cardon, A.; Galinhos, T. and Vacher, J.: "Genetic Algorithms Using Multi-Objectives in a Multi-Agent System," *Robotics and Autonomous Systems*, vol. 33, pp. 179–190, 2000.
- [19] Lymeropoulos, D.; Tsitsas, N. L. and Kaklamani, D. I.: "A Distributed Intelligent Agent Platform for Genetic Optimization in CEM: Applications in a Quasi-Point Matching Method," *IEEE Trans. on Antennas and Propagation*, vol. 55, no. 3, pp. 619–628, 2007.
- [20] Foster, I.: "Brain Meets Brawn: Why Grid and Agents Need Each Other," in *AAMAS'04*, New York, USA, July 2004.
- [21] Lymeropoulos D. et al.: "Software Agents for Parametric Computational Electromagnetic Applications," in *Advances in Information Technologies for Electromagnetics*, A.Esposito and L.Tarricone, Eds. Springer, 2006, pp. 345–379.
- [22] Jade web site. [Online]. Available: <http://jade.cselt.it>
- [23] Fipa web site. [Online]. Available: <http://fipa.org/repository/index.html>
- [24] Ist momentum web site. [Online]. Available: <http://momentum.zib.de>
- [25] Eisenblätter, A.; Fügenschuh, A.; Fledderus, E. R.; Geerdes, H. F.; Heideck, B.; Junglas, D.; Koch, T.; Kürner, T. Martin, A.: "Mathematical Methods for Automatic Optimization of UMTS Radio Networks," IST-2000-28088 MOMENTUM, Tech. Rep. D4.3, 2003.

A Survey about IEEE 802.11e for better QoS in WLANs

Md. Abdul Based

Department of Telematics, NTNU, Norway

based@item.ntnu.no

Abstract-The demand for Quality of Service (QoS) is increasing day by day in many multimedia applications with the rapid implementations of Wireless Local Area Networks (WLANs). The task group 802.11e of the Institute of Electrical and Electronic Engineers (IEEE 802.11e) is working to improve the QoS in WLAN by introducing two new functions namely Enhanced Distributed Coordination Function (EDCF) and Hybrid Coordination Function (HCF) since these two offer some enhancements beyond the original two functions Distributed Coordination Function (DCF) and Point Coordination Function (PCF) of IEEE 802.11 WLAN. To provide better QoS, Differentiated Service (DiffServ) is coupled with the IEEE 802.11e. This paper briefly describes QoS issues and concepts in general, the DCF and PCF of 802.11, the EDCF and HCF of IEEE 802.11e, and the coupling between the IEEE 802.11e and DiffServ.

I. INTRODUCTION

WLANs are becoming more and more popular in homes, businesses, industry, and public areas due to its less expensive network infrastructure and flexibility of connection. QoS is a set of network performance characteristics [1] like delay, jitter, bit error rate, and packet loss. QoS involves not only the network but also the end systems for multimedia services. Now-a-days, QoS is required in many applications like voice over WLAN, Real time communication, Audio and Video stream. Applications have different QoS requirements. Video-on-demand (VoD) can tolerate moderate end-to-end delay, but requires high throughput and very low error rate [1]. Internet telephony demands very low end-to-end latency [1], but needs moderate throughput and a slightly higher error rate than VoD.

In this paper, the fundamental concepts for implementing QoS are discussed in section II. The two modes of operation standardized by IEEE 802.11 are described in section III. The first mode is DCF and the other mode is PCF. The DCF is mandatory and it is based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). To support time bounded service PCF is used. PCF has higher priority than DCF and is coordinated by a station called Point Coordinator (PC). The EDCF and HCF are explained in section IV. The EDCF introduces Traffic Categories (TCs) to support QoS and is designed to provide differentiated, distributed channel accesses for frames with different priorities (0 to 7). EDCF is used in the Contention Period (CP) only. The HCF combines functions from the DCF and PCF with some enhanced QoS-specific mechanisms and QoS data frames in order to allow a uniform set of frame exchange sequences to be used for QoS data transfers [2, 3]. However, IEEE 802.11e can not provide QoS alone. Hence, the DiffServ protocol is coupled with

IEEE 802.11e. DiffServ is the dominant protocol in the network layer that supports different network interfaces. The coupling of DiffServ with IEEE 802.11e is shown in section V. This paper concludes with section VI, where the summary of the paper and future plans are discussed.

II. FUNDAMENTAL CONCEPTS OF QoS

QoS is the ability of a network element to assure that its traffic and service requirements can be satisfied. QoS is often accomplished by providing different prioritization for different types of traffic over a network. According to International Telecommunications Union (ITU), QoS is the collective effect of service performance, which determines the degree of satisfaction of the use of a service. The Internet Engineering Task Force (IETF) gives another definition of QoS. The IETF approach to QoS is, QoS is a set of service requirements to be met by the network while transporting a flow. The goals of a communication system that guarantees QoS is the effective utilization of the bandwidth, bounds on delay and jitter, acceptable error rate, low processing overhead for the underlying communication and end systems, and adaptability to dynamically changing network and traffic conditions [1]. This provides benefits in voice over WLAN, real time communication, and audio and video stream.

There are three levels of QoS measures. They are application QoS that provides bandwidth control and traffic policing for individual traffic stream accessing servers, access QoS that provides bandwidth control and traffic policing for individual traffic stream, and backbone/core QoS to provide network resource allocation and control on aggregate traffic. There is no single technique that provides efficient, dependable QoS in an optimum way. Many techniques [1] have been developed, with practical solutions such as Overprovisioning, Buffering, Traffic Shaping, the Leaky Bucket Algorithm, the Token Bucket Algorithm, Resource Reservation, Admission control, Proportional Routing, and Packet Scheduling. Of these the only one that does not add additional delay is overprovisioning. The goals of the scheduling techniques to support QoS are [1] to share bandwidth and to provide fairness to competing flows. The scheduling techniques also meet bandwidth, loss, and delay guarantees while reducing delay variations at the cost of increased delay. There are different scheduling techniques with different criteria. The most prominent scheduling techniques [1] in the Internet are First Come First Serve, Priority Queuing, Generalized Processor Sharing, Round Robin, Weighted Round Robin, Deficit Round Robin, Weighted Fair Queuing, and Virtual Clock.

III. QoS IN ORIGINAL IEEE 802.11 STANDARD

The 802.11 MAC sublayer protocol is quite different from Ethernet and supports two modes of operation [4-7]. The first mode is called DCF that does not use any kind of central control. The other mode is called PCF that uses the base station to control all activities in its cell. IEEE 802.11 specifies access mechanisms that support both contention and contention-free access. The contention mechanism is supported by CSMA/CA protocol. There are two cases for contention-free transmission. The first case is the Request to Send/Clear to Send (RTS/CTS) based handshaking to avoid the hidden terminal problem. The second case is the implementation of the PCF for the time-bounded applications. The CSMA/CA operation uses virtual channel sensing [7] that reduces the hidden station problem. The 802.11 standard allows frames to be fragmented into smaller pieces [7], each with its own checksum to increase the throughput by restricting retransmissions to the bad fragments rather than the entire frame. The Network Allocation Vector (NAV) [7] mechanism keeps other stations quiet only until the next acknowledgment. Since, there is no central control in DCF; stations compete for airtime, just as they do with Ethernet [6, 7].

A. Distributed Coordination Function

The Distributed Coordination Function (DCF) allows sharing of the wireless medium between compatible physical layers through the use of a CSMA/CA protocol and this mechanism is mandatory for all stations, including 802.11e QoS-supporting stations. DCF performs carrier sense by using both physical and virtual mechanisms [3]. When a station senses the channel condition and the wireless medium (to see if it is idle for a certain period of time), it is called physical carrier sense. This time period is called DCF Inter-Frame Space (DIFS). The DIFS varies. DCF uses a backoff algorithm to avoid collision between two simultaneously transmitting stations. This is also used as deferral of transmission for DIFS time. Normally, a station waits until the wireless medium is idle for DIFS time after detecting the channel as busy and if there is pending transmission request. After that it draws a random number to calculate an additional time period that it has to wait. The random number is chosen from a range of values called Contention Window (CW), which varies depending on the number of previous retransmission attempts [3]. The count down is suspended if the wireless medium is busy during backoff and resumed when the wireless medium is detected to be idle subsequently for DIFS time [9]. DCF operation is shown in Fig. 1.

Collision Avoidance is achieved by a virtual carrier sense mechanism. The NAV indicates the time when the wireless medium is busy for each station. A duration value is included in each frame that is transmitted by a station, which indicates how long the transmission lasts, including any subsequent acknowledgments and fragments. All stations in the vicinity receive the frame and use the duration value to update its own NAV [3]. Every station checks whether its NAV is zero to start transmission. If the NAV is not zero, it

must wait until NAV is zero. The reason is that, NAV indicates that another station has access to the wireless medium. Thus, after winning contention to the wireless medium a station can transmit one MAC Service Data Unit (MSDU) and waits for a time period called Short Inter-Frame Space (SIFS) for the acknowledgment (ACK) from the MSDU recipient. Generally, SIFS is shorter than DIFS to give the ACK frame highest priority for accessing the wireless medium. So, any other station would not start transmission while the ACK is expected. When no ACK is received after SIFS, retransmission is attempted until either the number of retransmission has exceeded certain thresholds or the lifetime of the MSDU has expired; if this is the case, the MSDU is discarded. Sometimes, MSDUs can be fragmented to increase the probability of success transmission, but it increases transmission overhead since each fragment of the MSDU is acknowledged individually.

B. Point Coordination Function

The Point Coordination Function (PCF) is optional (Shown in Fig. 2) and was designed to support time-bounded services. PCF has a Point Coordinator (PC) to control the contention free access to the wireless medium. The PC is co-located with the Access Point (AP). Two periods namely Contention Free Period (CFP) and Contention Period (CP) are defined by IEEE 802.11 between two consecutive beacon frames. The beacon frames are Delivery Traffic Indication Message (DTIM) beacon frames. These beacon frames are sent periodically by the AP, although it can be delayed by a busy wireless medium, and they carry synchronization and network Basic Service Set (BSS) information. PC uses DTIM to

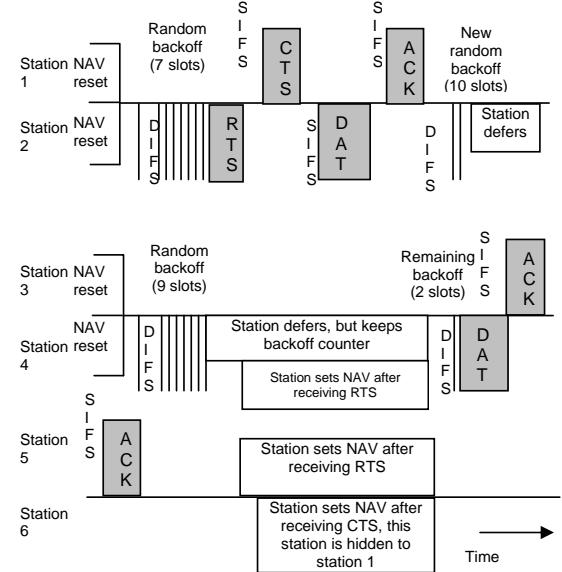


Fig. 1: DCF Operation [3]. Station 6 can not detect the RTS frame of the transmitting station 2, but can detect the CTS frame of station 1.

indicate the start of a CFP. All the stations contend for the wireless medium using DCF during contention period. The AP schedules transmissions to individual station or transmissions from individual station during CFP. There is no contention between stations during CFP. So, when the AP obtains access to the wireless medium using PCF Inter-Frame Space (PIFS) timing [3] at Target Beacon Transmission Time (TBTT), the CFP starts. The value of PIFS is shorter than DIFS, but longer than SIFS. This implies that the priority of PCF is higher than DCF without interrupting any DCF transmissions [3]. During CFP, SIFS is used to exchange frames when PCF obtains access to the wireless medium.

The PC starts polling by sending a CF-Poll frame to one of the pollable stations and uses a data frame piggybacking a CF-Poll frame if the PC itself has a pending transmission. The polled station responds with a Data + CF-ACK frame or with a CF-ACK frame if there is no pending transmission in the station. If the frame exchange sequence with one station is completed, the PC sends CF-Poll to another station in its list of pollable stations. After finishing polling of all pollable stations or the CFP duration has expired, the PC broadcasts a CF-End frame to announce the end of the CFP [8]. This time the NAV of all stations are set to maximum at TBTT to protect the CFP from unwanted transmissions and the AP broadcasts the actual CFP duration in the beacon to update the NAV accordingly. Thus, all stations reset their NAV to zero when either they have received a CF-End frame or the CFP duration expires and contend for the wireless medium using DCF until the next DTIM beacon.

C. Limitations of DCF and PCF

There is no provision to support QoS in DCF because all data traffic is treated in a first come first serve manner. In DCF, all stations in the BSS contend for the wireless medium with the same priority and thus it causes asymmetric throughput between uplink and downlink. Here, AP has the same priority as other stations, but often has much higher throughput requirement. In DCF, there is no differentiation between data flows to support traffic with QoS requirements, so the probabilities of collisions become higher when the number of stations in a BSS increases [3]. This results in frequent retransmissions and decreases QoS and throughput in the BSS. The inefficient and complex central polling scheme reduces the performance of PCF high-priority traffic when traffic load increases. Though PCF was designed to support time-bounded traffic [3], it shows many inadequacies such as unpredictable beacon delays due to incompatible cooperation between CP and CFP [9-13]. A station is allowed to send a single frame if it has been polled by the PC. The frame may be fragmented and of arbitrary length (maximum of 2304 bytes or 2312 bytes with encryption) [3]. The duration of the MSDU delivery is not under the control of the PC. This destroys any attempt to provide QoS to other stations that are polled during the rest of CFP [3]. To setup and control PCF operations, there is no management interface, so it is not possible to setup a PCF policy according to the requirements of higher layer protocols such as

Differentiated Service or Integrated Service [3, 6]. To optimize the performance of the polling algorithm in the PC, stations need to communicate QoS requirements to the AP. But, there is no mechanism for this in PCF. So, performance optimization is not possible. Thus, we can say that neither DCF nor PCF provide sufficient facility to support traffic with QoS requirements.

IV. QoS IMPROVEMENTS IN IEEE 802.11e

The HCF is used only in QoS enhanced BSS (QBSS). HCF has an EDCF which is a contention-based channel access function that operates concurrently with HCF based on a polling mechanism controlled by the Hybrid Coordinator (HC). The HC is co-located with the QoS supporting Access Point (QAP) [10, 12]. HCF and EDCF (Shown in Fig. 3 and Fig. 4, respectively) enhance or extend functionality of the original access methods DCF and PCF. EDCF has been designed for support of prioritized traffic similar to DiffServ, whereas HCF supports parameterized traffic similar to Integrated Service (IntServ) protocols [2, 3]. The basic concept of EDCF and HCF is the Transmission Opportunity (TXOP). "A TXOP is a bounded time interval in which the QoS station is allowed to transmit a series of frames. A TXOP is defined by the start time and a maximum duration [12]". If a TXOP is obtained using the contention-based channel access, it is called an EDCF-TXOP. If a TXOP is granted through HCF, it is called a HCF (polled) TXOP [3]. The duration of the EDCF-TXOP is controlled by the QAP and is distributed to non-AP QoS stations in the beacon frames along with other EDCF related parameters [9]. Though HCF can be operated during both CFP and CP, EDCF is used only during CP. IEEE 802.11e recommends to use HCF during CP only and discourages its use during CFP, because it is very difficult to implement CF-Poll and QoS CF-Poll at the same time and also, QAP delivers multicast and broadcast frames during either CP or CFP under EDCF or PCF respectively.

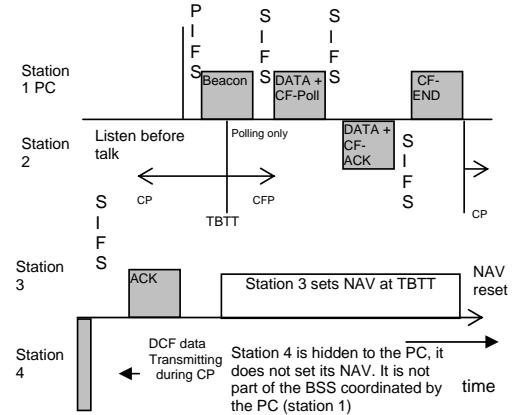


Fig. 2: PCF Operation [3]. Station 1 is the PC polling station 2. Station 3 detects the beacon frame and sets the NAV for whole CFP. Station 4 is hidden to the PC, it does not set its NAV. It is not part of the BSS coordinated by the PC (station 1).

A. Enhanced Distributed Coordination Function

The EDCF introduces Traffic Category (TC) to realize QoS. When the channel is idle for a new kind of inter frame space called Arbitration Inter-Frame Space (AIFS), each TC starts a backoff. EDCF introduces three parameters, namely, AIFS, CWMin (minimum initial value of the CW), and CWMax (maximum value of the CW) which can be determined and announced by the AP via beacon frames. Depending on the network conditions, the AP can adapt these parameters. AIFS is at least as DIFS and can be chosen individually for each TC to provide a deterministic priority mechanism between the TCs. For this purpose, the CWMin can be selected on a per TC basis and the subsequent CW is doubled when collisions occur [2]. The CWMax sets the maximum possible value [2] for the CW and is intended to be the same for all TCs as in DCF. Generally, the smaller AIFS and CWMin, the shorter the channel access delay [2] and hence the more bandwidth share for a given traffic condition. EDCF also provides differentiated and distributed channel access for frames with 8 different priorities (from 0 to 7).

The 8 TCs used in EDCF have independent transmission queues within a station. There is a scheduler inside each

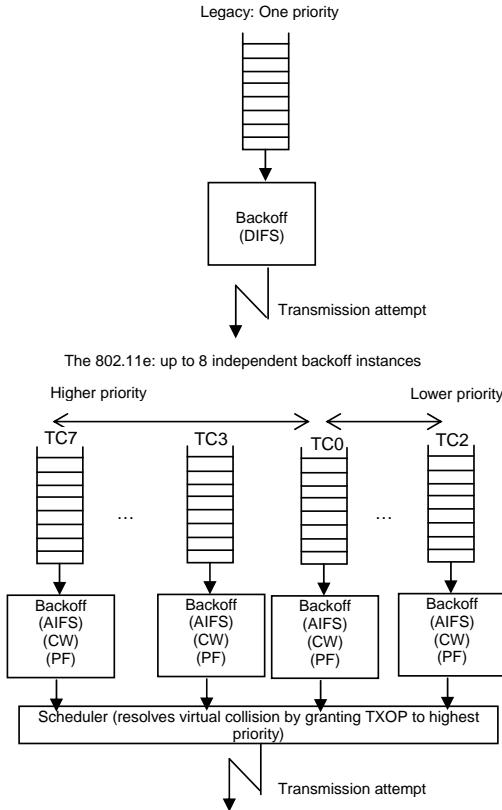


Fig. 3: Virtual backoff of eight traffic categories [3].

station. When the backoff counter of two or more TCs in a single station is zero, the scheduler treats the event as a virtual collision without recording a retransmission. In this way, the TXOP is given to the TC with the highest priority of the colliding TCs and others backoff as if a collision on the medium occurred.

B. Hybrid Coordination Function

The Hybrid Coordination Function is an extension of the polling data in PCF. As in PCF, under HCF, the superframe is divided into the CFP and CP. CFP starts with every beacon and access is governed by EDCF during CP though the HC can initiate HCF access at any time. The HC issues a QoS CF-Poll to a particular station to give it a TXOP, specifying the start time and the maximum duration during the CFP. No station attempt to gain access to the medium at this time, and so when they receive a CF-Poll, they assume a TXOP and transmit any data they have [2, 3, 7]. The beacon frame or a CF-End frame determines the time to end a CFP. A station is expected to start responding with data within a SIFS period if it is given a CF-Poll frame. After a PIFS, the HC can take over the medium and allocate another CF-Poll to another station if it does not start to respond. Thus, the use of the medium is very efficient during the CFP. If the base station desires to initiate a CF-Poll based transmission sequence within the CP, the HCF allows the base station to do so. The HC has a snapshot view of per TC per station queue length information in the cell including that of the AP sent by the stations via the new QoS control field added to the MAC frame [10]. This information is important for the HC to decide to which station (including itself) to allocate TXOPs during CFP. To allocate TXOP during CFP, the HC considers priority of the TC, required QoS for the TC, queue length per TC, queue length per station, duration of TXOP available and to be allocated, and past QoS seen by the TC.

The HC does not specify a particular TC for the TXOP when a wireless station receives a TXOP from the HC; rather it leaves this decision up to the wireless station. This choice depends on the same factors as the HC scheduler, except for the multistation cell-wise aggregation that the HC scheduler uses. For fast collision resolution, the HC polls stations for MSDU Delivery. To do this, the HC requires information that has to be updated by the polled stations from time to time [3]. The HC maintains a way called controlled contention to learn which station needs to be polled, at which time, and for which duration [3, 8, 9].

C. Impact of EDCF and HCF

The EDCF is updated from DCF by making some of the parameters of the CSMA/CA MAC protocol variable on a per TC basis. The introduction of the TCs performs virtual collisions within a wireless end-point and backoff accordingly affects the behavior of EDCF compared to DCF [3, 7]. EDCF provides significant improvements for high priority QoS traffic, however these improvements are typically provided at the cost of worse performance for power priority traffic and the EDCF parameters can require significant tuning to

achieve these performance goals. Also, EDCF does not improve channel utilization over DCF, which means it has significant overhead. Despite these problems, we find EDCF attractive because of its simplicity and decentralized nature [3]. The HCF provides much more efficient use of the medium when the medium is heavily loaded. HCF does a fairly good job of channel utilization. Due to reduced overhead, HCF can provide better QoS support for high priority streams while allocating reasonable bandwidth to lower priority streams [3, 7, 8, 9]. HCF involves state at the access point and is centralized, making for a less robust protocol [7-9].

V. DiffServ AND IEEE 802.11e

The end-to-end QoS is required for the multimedia applications [2] to work properly. One of the major architectural approaches in Internet to support QoS is DiffServ. The DiffServ architecture provides a QoS framework for service providers to support differentiated services in heterogeneous network. When a station simultaneously services multiple sessions under different applications like Voice over Internet Protocol (VoIP), video streaming, and email, according to the type of the service the traffic should be treated differently at the network node. Based on this concept the architecture can be divided into two parts. The first part is Direct Mapped QoS architecture that maps between Differentiated Services Code Point (DSCP) and Traffic Category Identifier (TCID) [2]. The second part of the architecture is Hierarchical QoS that uses the hierarchy from Per Hop Behavior (PHB) to the IEEE 802.11e Prioritized QoS.

A. Direct Mapped QoS

This architecture maps between DSCP and TCID via interface between IEEE 802.2 Logical Link Control (LLC) Service Access Point (SAP) and PHB. Every Internet Protocol (IP) packet is placed into 802.11e MAC priority queues with no preemption. IP packets are arrived to MAC layer with non-preemptive mode. Then IP packets are forwarded to the 802.11e MAC layer according to the arrival times regardless the DSCP values of IP packets [2]. The arrival times are in order of Assured Forwarding 2(AF2), AF4, Extended Forwarding (EF), and default. Each frame is allocated to a priority queue or an access category in MAC layer according to its TCID value when the IP packets are encapsulated in MAC frames. The TCID of 802.11e MAC is 3-bit long and the DSCP field of DiffServ is 6-bit long. So, a single TCID value may represent multiple DSCP values [2].

B. Hierarchical QoS

The main element in this architecture is the DiffServ engine. The DiffServ engine is a logical entity that performs packet classification and conditioning in the network layer [2]. The engine consists of classifier, meter, marker and shaper/dropper used for traffic shaping and policing. When the IP packets arrive at this engine, they are classified and marked into DSCP values and shaped in accordance with the priority of the DSCP values. The engine is called Traffic Conditioner (TrC). When TrC completes the traffic shaping, it encapsulates IP packets into IEEE 802.11e MAC frames and forward them to 802.11e priority queues in accordance with the TCID values. When the IP packets arrive at DiffServ TC in order of DSCP values, AF4, AF2, EF and default, they are shaped to EF, AF4, AF2 and default according to the priority

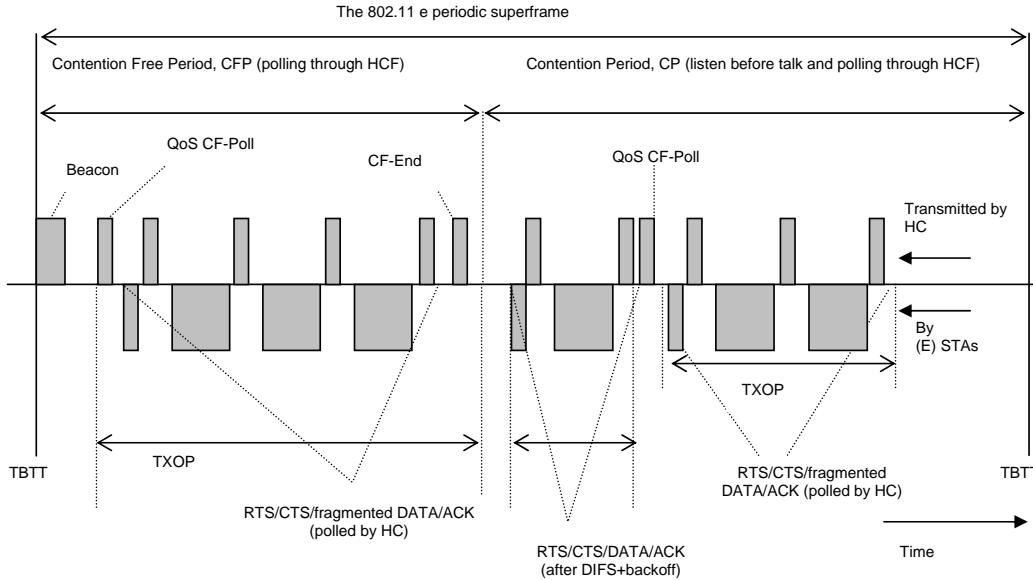


Fig. 4: 802.11 superframe [3]. The concept relies on TXOPs. Polled TXOPs may be located in CP and CFP.

[2]. After completing the traffic shaping, IP packets are encapsulated in 802.11e MAC frame and placed into the 802.11e priority queue. Since IP packets are policed and shaped in the network layer, traffic control can support full range of DiffServ QoS as well as 802.11e. This enables the network system to manage accurate end-to-end QoS traffic control required by user applications [2].

VI. CONCLUSIONS AND FUTURE WORK

The EDCF provides provisions for relative priorities by configuring time to access the channel once it is sensed idle and by changing the size of the contention window. The priority of each traffic category can be changed by the contention window in EDCF. This ensures that high priority class will be able to transmit first than the low priority class by assigning a short contention window to high priority class [3]. The AIFS in EDCF for a given class should be a DIFS plus some time slots. This facilitates that a class with a small AIFS has a higher priority. In EDCF, a station is allowed to send as many frames it wishes as long the total access time does not exceed a certain limit and no collision occurs after getting access to that channel. This improves the QoS of real time traffic though the performances are not optimal since EDCF parameters cannot be adapted to the network conditions [2, 3].

The HCF combines the advantages of PCF and DCF. The HC provides both contention free and contention based channel access mechanisms in the CP. HC uses PC's highest priority to access the wireless medium, initiate frame exchange sequences and allocate TXOPs. HC traffic delivery and TXOP allocation may be scheduled during both CFP and CP in order to meet the QoS requirements of particular traffic categories. QoS guarantee is based on the traffic specification negotiation between the QoS AP and the QoS stations prior to frame transmission [8]. The EDCF and HCF have the ability to fulfill their goals of better QoS & higher channel efficiency. HCF reduces channel contention and allows better channel utilization; thus provides greater net throughput. Both EDCF and HCF are highly sensitive to protocol parameters. The effectiveness of these functions also depends on the scheduling algorithms. They enable differentiated treatment of traffic streams and can be tuned to meet the QoS requirements of low latency and jitter. To provide QoS in multimedia applications the DiffServ protocol is coupled with the IEEE 802.11e. The hierarchical QoS interface between DiffServ and IEEE 802.11e performs end-to-end traffic control like traffic classification, traffic shaping and traffic policing. For offering multimedia services via WLAN the interface between DiffServ and 802.11e plays the role to provide better QoS.

In this paper, the analysis is based on theoretical descriptions. Better analysis, simulations, and experiments are to be done in the future. There may have some other important issues and information related to DiffServ and IEEE 802.11e, that were left due to shortage of time. Many open issues and research work can be done to validate the QoS mechanisms for 802.11e WLANs. After implementation, performance verification will be necessary.

ACKNOWLEDGMENT

I would like to thank Professor Gerald Maguire, Royal Institute of Technology (KTH), Stockholm, Sweden and Dr. Khaled Mahmud, Assistant Professor, Department of CSE, North South University, Bangladesh for their support and fruitful discussions.

REFERENCES

- [1] Sanjay Jha and Mahbub Hassan, "Engineering Internet QoS", Artech House, Boston, London, 2002.
- [2] Seyong Park, Kyuntae Kim, Doug C. Kim, Sunghyun Choi and Sangjin Hong, "Collaborative QoS Architecture between DiffServ and 802.11e Wireless LAN", Vehicular Technology Conference, 2003. VTC 2003-Spring, April 2003, pp 945-949, vol. 2.
- [3] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz, L. Stibor, "IEEE 802.11e WLAN for Quality of Service", European Wireless 2002, Italy, February 2002.
- [4] Kaveh Pahlavan and Prashant Krishnamurti, "Principles of Wireless Networks", Prentice Hall PTR, 2002.
- [5] Theodore S. Rappaport, "Wireless Communications", Second Edition, Pearson Education Asia, 2002.
- [6] William Stallings, "Data & Computer Communications", Sixth Edition, Prentice Hall International, Inc, 2000.
- [7] Andrew S. Tanenbaum, "Computer Networks", Fourth Edition, Prentice-Hall of India, 2002.
- [8] Qiang Ni, Lamia Romdhani, Thierry Turletti, and Imad Aad, "QoS Issues and Enhancements for IEEE 802.11 Wireless LAN", INRIA, No. 4612, November 2002.
- [9] Qiang Ni and Thierry Turletti, "QoS support for IEEE 802.11 Wireless LAN", Technical report, PLANETE Group, INRIA Sophia Antipolis, 2004.
- [10] P. Garg, R. Doshi, R. Greene, M. Baker, M. Malek, and X. Cheng, "Using IEEE 802.11e MAC for QoS over Wireless", Computer Science Department, Stanford University, USA, April 2003, pp 537-542.
- [11] Jeff Thomas, "802.11e bring QoS to WLANs", Network World, 23 June, 2003.
- [12] Simon Chung and Kamila Piechola, "Understanding the MAC impact of 802.11e", EE times, 30 October, 2003.
- [13] Heegard, C. Coffey, J.T. Gummadi, S. Murphy, P. A. Provencio, R. Rossin, E. J. Schrum, S. Shoemaker, M. B., "High-Performance Wireless Ethernet", IEEE Comm. Magazine, vol. 39, no. 11, Nov. 2001.

Method of a Signal Analysis for Imitation Modeling in a Real-Time Network

TeNe 2008 Conference

Igor Sychev
Amur State University
21 Ignatevkoe shosse
Blagowestschensk, Amur Region, 675027 Russia
(igor.sychev@hpi.uni-potsdam.de, sychov@tfh-berlin.de)

Irina Sycheva
Amur State University
21 Ignatevkoe shosse
Blagowestschensk, Amur Region, 675027 Russia
(irina.sycheva@gmx.de)

Abstract- The main goal of presented research is to discover a new method of process analysis for predicting, testing and modeling network traffic.

Presented method is applicable not only for learning traffic behavior, but also for many industrial tasks, for instance mechanical products testing.

I. INTRODUCTION

This research was planned as an extension for the research published in [1]. Having a sufficient mathematical mechanism for traffic analysis and modeling we need to expand our theory from some specific cases to a general case. This paper is a significant step towards for the purpose of generalizing the theoretical knowledge based on the Laplace-Stiltes transform for predicting packets transmitting delays, in a network based on the Internet technology [1].

The paper also reflects some use-cases that was not planned and appeared after formalizing a method that is presented in section IV of the paper. Section IV is the key part of this paper.

Using an accurate and trusted method for traffic measurement in real-time it is possible to get a general picture of networking traffic behavior. For accurate measurement purposes we use a special installation, the installation presented in publication "The Problem of Accurate Time Measurement in Researching Self-Similar Nature of Network Traffic" [2].

Traffic analysis consists of following levels:

- learning experiment methodology and tools;
- synthesis of an actual mathematical model, that describes the real process most accurate;
- an experimental proof for the model.

Creating a mathematical model of a network data transmitting process is rather challenging task, since, as any real engineering solution it has different environmental sources of influence; all this factors can't be reflected by the deterministic mathematical model, so this model must take into account a random property of the process. For our task, methodology of learning random-nature processes and signals divides into two blocks:

- Methods for finding math law of incoming signal. Typically, the law is a cumulative distribution function (CDF) or a probability density function (PDF) [5-19], [23].

- An approach for obtaining quality characteristics, which we are interested in. This block consists of a set of methods

for obtaining concrete values that required for technical system (for example, frequency characteristics after Laplas transform).

In most cases, network traffic is described by the following mathematical laws, that have fundamental differences:

- network traffic as a Poisson flow [3];
- network traffic as a self-similar process [4].

In the both cases the law of input signal depends on a random value. An experiment methodology for traffic measurement and definition of networking process is presented in [2]. Analysis methods and examples of an apparatus usage for getting quality characteristics are presented in [1].

Dealing with random-nature process, we assume CDF as a most informative characteristic of a process.

In [1] a method for obtaining CDF in common case is not revealed (when input flow law is given as analytic function of a random value). Method of getting CDF from given analytic function is the main result of presented research.

Prerequisites for the research are presented in section II. Section II tells about our motivation and provides basic understanding of the problem. An idea of implementing Plutenko theory [3] to a problem from Fraunhofer Institute Computer Architecture and Software Technology (Fraunhofer FIRST) is discussed.

Section III describes the problem-related solutions. This section is focused on autocorrelation function (ACF) for signal analysis in a linear system with stationary input process. The apparatus has a wide use in control theory and designed for similar to our purposes.

The content of section IV is the main contribution of the paper. Section IV has a formal definition of the problem and the mathematical solution - CDF transformation algorithm.

Section V is about networking traffic tests and about the physical meaning of CDF transformation algorithm.

Section VI is a manual for computation experiments. We propose MATLAB Simulink scheme as a most effective and convenient tool for simulating a system with researched properties.

And general conclusions are presented in section VII. We would like to thanks many people for a great help in the "acknowledgment" section.

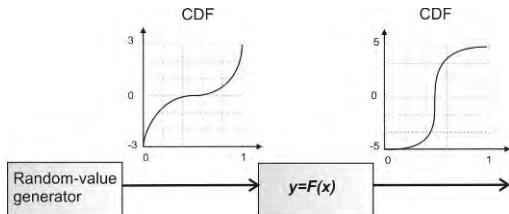


Fig. 1. An example of CDF shape before and after a signal passes through the system.

II. PREREQUISITES FOR RESEARCH

The research was started from the theory and a mathematical apparatus of Plutenko [3]. The major idea of [3] – is to use Laplas-Stiltes transform for obtaining frequency characteristics instead of time values. The transform applied for computer systems. To get practical application and to verify theoretical research of Plutenko we use the problem from Fraunhofer Institute Computer Architecture and Software Technology (Fraunhofer FIRST), “the problem of predicting the data transmitting delay in the network with the self-similar nature of traffic, for the purpose of improving the real-time conferencing” [1]. Plutenko apparatus was formalized in the algorithm “A” (“algorithm for determination of the time of receiving-transmitting a data block”)[1].

First step of the algorithm “A” gives us the following instruction:

“A1. Find the cumulative distribution function (CDF) $F(t)$; where $F(t)$ is the CDF of random time of one packet transmitting.”

The solution for the step “A1” is trivial if we assume that CDF for the traffic is known (having a sufficient proof). However, in real technical systems it might be difficult to measure data for computing CDF without influencing on a system. It might be also impossible to prove CDF of a process that we are interested in.

Our second motivation is: improving networking systems. For this purpose we have to define a specific entity for technical systems. In this paper a *system* is a “black box” with one or more *inputs*, one or more *outputs* and a set of the *internal states* (the definition is classical for most of technical systems). Using this definition we separate a random-value *generator* and a *system*. A random-value generator produces a *signal*. Generator is a *source* of a signal for the system input. The signal passes through the system. And it is possible to measure the signal on the output. We assume that the distribution of the generator is known. Thus, we get a problem of CDF transformation after signal transference through a system.

First, we encountered the problem trying to apply Plutenko [3] apparatus for mathematical modeling of self-similar traffic. In this case, a system for self-similar traffic production depends on random-value generator with the given (known) distribution. This problem is illustrated in Fig. 1.

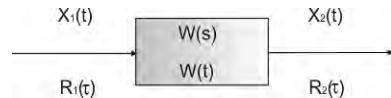


Fig. 2. Transfer of a random signal in a linear system.

III. THE PROBLEM-RELATED SOLUTIONS

At the present moment, there are a lot of research papers and books about probability theory methods [5-19]. There is a great amount of publications about probability theory applied for networking, among others [20-22]. Additionally, a set of publications about probability theory applied for synthesis of effective algorithms [23-24] exists.

After examination of abovementioned literature, we came to a conclusion that autocorrelation function ACF for random signals analysis is the most similar method to our purposes. It is possible to find ACF usage in control theory for random processes [25-26]. It's proposed to use following entities:

- $x_1(t)$ – random stationary process on the input;
- $x_2(t)$ – random stationary process on the output;
- $R_1(\tau)$ – input ACF of the process;
- $R_2(\tau)$ – output ACF of the process;
- $W(s)$ – image of transfer function (after Laplas transform);
- $W(t)$ – original transfer function.

Where $R_2(\tau)$, $x_2(t)$ – unknown and should be found.

Transfer of a random signal in a linear system is presented in Fig. 2. In the problem $x_1(t)$, $R_1(\tau)$ is known, also $W(s)$ and(or) $W(t)$ is known. To find $R_2(\tau)$ we have to find $x_2(t)$ first. The solution for the problem of getting output ACF of the random stationary process is presented in [25-26]. Using properties of ACF it is possible to get expected value $R(0)=M[x^2(t)]$, $R(\infty)=M^2[x(t)]$, and dispersion $D[x(t)]=M[x^2(t)] - M^2[x(t)]$.

Disadvantages of this method:

- it is not possible to use self-similar model of input process, because input signal must be stationary;
- the method is designed for linear model of system that is not adequate for real technical systems.

We did not find published method for getting CDF in case when analytically represented function depends from the argument and the distribution of the argument is known.

IV. CDF TRANSFORMATION ALGORITHM

Let's determine the formal problem:

To obtain the distribution of values of analytical function $y(x)$, if a distribution of random value x on $[a, b]$ range is given.

We assume that it is possible to solve the problem if it is possible to get the back function $x(y)$ analytically.

Let's x – random value with the given CDF. Let's the source random value ξ has a density $S_x(x)$ on $[a, b]$. Let's define the random value generating function as $y(x)$.

If on the $[a, b]$ range back function $x(y)$ has only one single value and $\frac{dy}{dx}$ never has zero value then density of result value v is proportional to:

$$S_y(y) \propto S_x(x(y)) \frac{dx}{dy} \quad (1)$$

Using normalization, let's find an absolute value of S_y :

$$S_y(y) = \frac{S_x(x(y)) \frac{dx}{dy}}{\int_{[a,b]} S_x(x(y)) \frac{dx}{dy} dy} \quad (2)$$

The result of (2) is a probability density function (PDF). First derivative from CDF is PDF.

The integral in (2) is the Lebesgue integral [27-28] on the range y on $x \in [a, b]$ (it is not necessary that the range is equal to $[y(a), y(b)]$, since $y(x)$ might have a discontinuity. For example $y=x^2$ has the discontinuity on $[-1, 1]$).

If $x(y)$ is not uniquely defined and (or) $\frac{dy}{dx}$ becomes equal to zero on $[a, b]$ we use another method, except for the case when $x(y)$ is uniquely defined and it is possible to take the improper integral in the denominator (2). For y which is not the values $y(x)$ in points $\frac{dy}{dx}=0$ works the following method:

Let's y_0 – is the point where S_y should be found.

1. We get a set of ranges: $[a_1, b_1], [a_2, b_2], \dots, [a_n, b_n], \dots$

on each range $y(x)$ is monotonous and continuous, $\frac{dy}{dx}$ has no zeros and there is only one solution for the equation $y(x_n)=y_0$. In the worst case an amount of ranges is countable.

2. To obtain a fragment $[a_n, b_n]$, get a probability P_n that ξ belongs to the fragment (it is $\int_{a_n}^{b_n} S_x(x) dx$), and obtain the particular density:

$$S_{yn}(y_0) = P_n \frac{S_x(x(y_0)) \left(\frac{dx}{dy} \right)_{y_0}}{\int_{y(a_n)}^{y(b_n)} S_x(x(y)) \frac{dx}{dy} dy} \quad (3)$$

3. Common density is the sum of the particular density

$$S_y(y_0) = \sum_n S_{yn} \quad (4)$$

4. The density and the value of integral in (3) are significant positive values.

5. The result of (4) is a probability density function (PDF). First derivative from CDF is PDF.

V. NETWORKING TRAFFIC TESTS AND THE PHYSICAL MEANING OF CDF TRANSFORMATION ALGORITHM.

Authors of the paper use section IV for the problem predicting data transmitting delay. However, it is possible to use presented apparatus for other problem-related purposes.

For example, it is possible to test an optimal set-up for Internet protocol (IP) packets transmitting. It is possible to

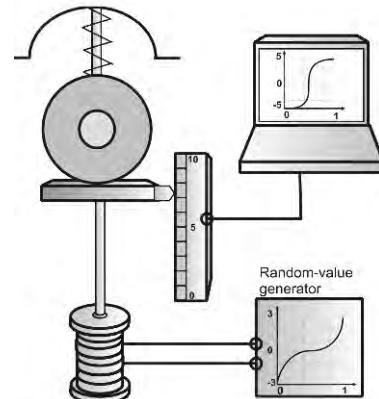


Fig. 3. Conceptual scheme of the mechanical experiment.

build CDF and PDF for packets loss with the different maximum transfer unit (MTU). Packet transfer time is also an interesting object for studying, synthesis of CDF and PDF might help improving quality of service (QoS). Most of Real-Time networking systems strongly depend on packets delays [1-2], effective tests and simulations is a key for the problem solution.

The meaning of proposed testing with the algorithm from section IV might be interpreted not only in terms of networking technologies. Let's draw analogy with mechanical testing. Let's describe an example of testing damping system in a car. Conceptual scheme of the experiment is presented in Fig. 3. The car body is fixed. The wheel of a car (or directly the fastening of the damper) is fixed on a platform. The platform is able to move independently up and down. A generator of random signal with the known distribution makes the platform move*. Transference sensor registers vertical moving of the wheel. Statistical data, collected during the experiment, will be computed and rendered. Then it is possible to see transformed CDF. CDF is the most informative description of the random process.

VI. COMPUTATIONAL EXPERIMENT.

Taking into account following engineering needs:

- to demonstrate the method from section IV;
 - to get an additional practical verification;
 - to get a graphical visualization;
 - to implement new methodology in technical devices;
- we present an experiment in this section.

Our experiment consists of two principal parts:

- Experimenting with a real system, where CDF of a random-value generator is known (As it shown in Fig. 1.); in this case, we collect statistical data and observe statistical values. The result depends on number of experiments and accuracy of measurements.

*In the example we assume that the platform moves perfectly according to generator signals if the platform is not loaded and the force is constant. In this case we do not reflect the reality absolutely accurate. For this purpose we have to add an additional function-block for the platform behavior.

- Computing the CDF transformation algorithm. This part might be defined as “an etalon CDF producing mechanism” (if we have an adequate analytical model of researched system).

In order to save time and resources we propose computational simulation for both parts of the experiment. Our main environment is MATLAB v.6.5 and Simulink.

Let's define common conditions for the both phases of the experiment.

Common conditions.

Let's a system, which transfers a signal, is described by the following analytical equation:

$$y(x) = \sqrt{x} \quad (5)$$

We use a simple analytical function to make the demonstration easy for understanding*.

Let's assume the normal distribution for our random-value generator**. PDF of normal distribution is published in most books about probability theory and statistics, among others in [5-19]. PDF of normal distribution represented by the following equation:

$$P(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\left(\frac{(x-\mu)^2}{2\sigma^2}\right)} \quad (6)$$

where x – is a random value, $\sigma > 0$ is the standard deviation, the real parameter μ is the expected value (σ and μ are parameters). Down the paper $\mu = 5$, $\sigma = 1$.

First phase.

For this phase we don't use (6) directly. To get a vector of random values, we use trusted random-value generator from MATLAB package. We assume that the generator is trusted if it is always possible to prove similarity to the normal distribution using one or more than one of normality tests (Kolmogorov-Smirnov, Pearson's chi-square, Anderson-Darling, Jarque-Bera, Shapiro-Wilk and other tests) [5-19].

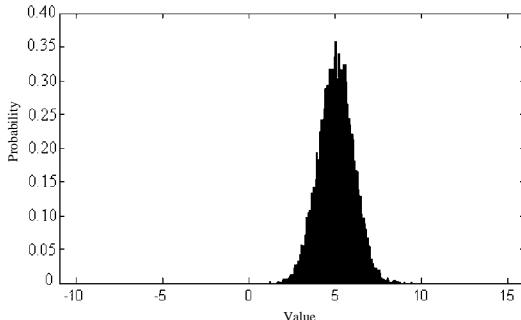


Fig. 4. Experimental PDF

*To a great regret of authors, an experiment with a process as in section V runs out from this paper frames, but it might appear in our next publication.

** Obviously, it is possible to use any other known distribution.

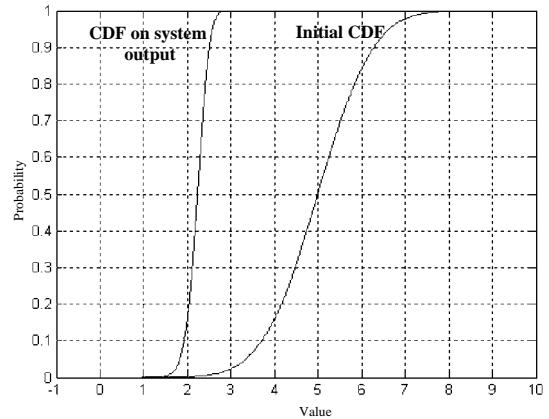


Fig. 5. Initial CDF and CDF on system output.
The first phase of the experiment

PDF of 10^4 normal distributed random values is presented in Fig. 4. We use the values for transferring though the system, described by (5). CDF before and after values transference is presented in Fig. 5. On the right side of Fig. 5. the function graphic built on the same data as the PDF on Fig. 4. On the left side of Fig. 5 distribution of values on the system output is presented.

On the first step of the experiment all graphics built on statistical data; let's compare those graphics with the analytical solution on the second step of the experiment.

Second phase.

For the second step of the experiment we designed so called “S-model” or “S-schema” which is a set of graphically represented library blocks. Those blocks reflect ideal technical primitives. Designed S-model presented in Fig. 6. One of great advantages of S-models is an ability to implement S-schema into electronic schema.

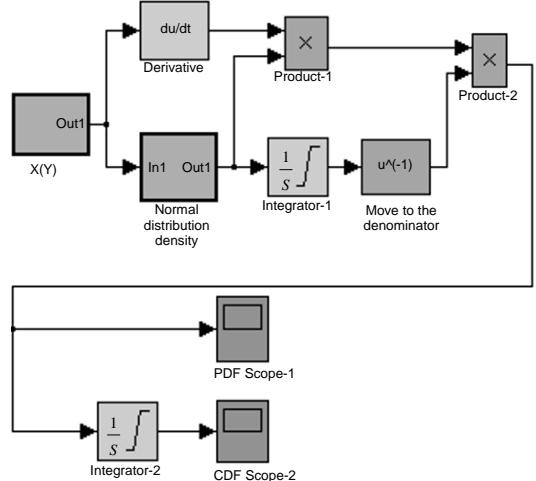


Fig. 6. The S- schema for CDF transformation algorithm.

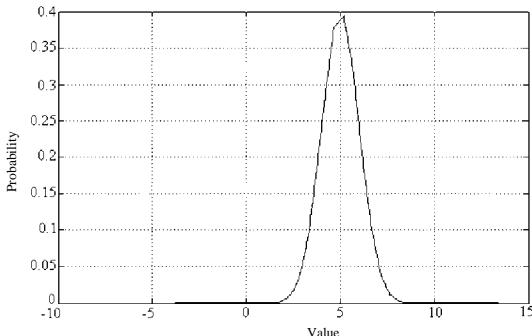


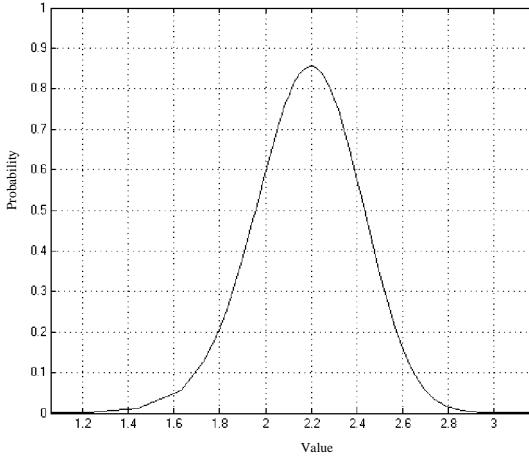
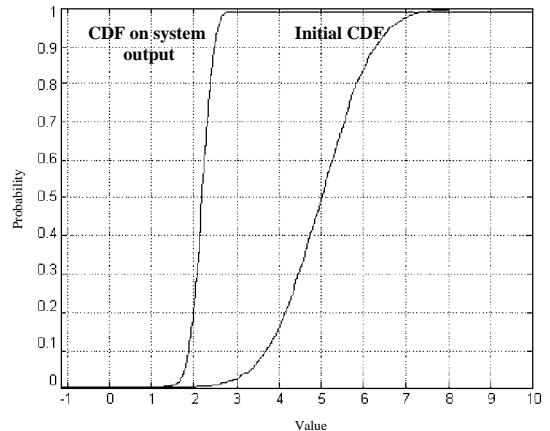
Fig. 7. PDF of the normal distribution.

Blocks “ $x(y)$ ” and “normal distribution density” are not basic Simulink blocks; both blocks have an internal realization (subsystem), which might be also represented in Simulink basic blocks (in our case, the subsystem is a formula for the MATLAB command line). Our main results it's - PDF and CDF on the system output; this results will be rendered by “PDF Scope-1” and “CDF Scope-2”.

If we add an additional “scope” block to the “out1” of the “normal distribution density” block, we get a graphic for (6); this graphic is presented in Fig. 7. If we add an additional integrator to the “out1” of the “normal distribution density” block and then connect to a “scope” (this is the same fragment as “Integrator-2” connected to “CDF Scope-2”) we get the initial CDF (presented on the right part of Fig. 9.). We combine initial CDF and output CDF in the same space, using “Mux” block before “CDF Scope-2”.

It is possible to see how PDF shape changes after transference through the system (after the analytical solution) in Fig. 8 (PDF Scope-1).

The experiment shows us identical results on both phases (Fig. 5. and Fig. 9.). Now it is easy to observe how CDF transformation algorithm works.

Fig. 8. PDF on the system output.
The second phase of the experiment.Fig. 9. Initial CDF and CDF on the system output.
The second phase of the experiment

VII. CONCLUSIONS.

The key part of this paper is section IV where CDF transformation algorithm is presented. Obtained knowledge can be effectively applied for:

- modeling self-similar traffic;
- improving a real-time networking;
- mechanical modeling.

Obtained mathematical method allows analyzing traffic with non-trivial distributions. It gives an opportunity to find and to simulate many properties of a network connection easily. For example, to simulate a “bottle neck” of a network.

It is possible to produce mechanical imitation tests more accurate, using random signals (and to observe probabilities of examined characteristics from CDF). Besides practical application we have done a significant step for generalizing from special case published in [1] to a wide range of processes.

ACKNOWLEDGMENT.

Our research group of Amur State University thanks Raul and Natalia Nakhmanson-Kulish for professional help and effective discussion; Sergey Sayanovich Ohotnikov for a great help with technical equipment; Prof. Dr. Evgeniy Leonidovich Eremin and Dmitriy D. Gazzaev for reviewing research values, Prof. Dr. Andreas Polze for collaboration.

REFERENCES

- [1] I.Sychev, Prof. Dr. A. Polze, D. D. Gazzaev, Prof. Dr. C. Kordecki, I. A. Sycheva, “The Problem of Predicting the Data Transmitting Delay in the Network With the Self-Similar Nature of Traffic, for the Purpose of Improving the Real-Time Conferencing”, IEEE Conference Publishing, ISBN 978-1-4020-8736-3, 2007.
- [2] I.V.Sychev, “The Problem of Accurate Time Measurement in Researching Self-Similar Nature of Network Traffic”, IEEE Conference Publishing, ISBN 978-1-4020-6265-0, 2006.
- [3] A.D.Plutenko, “Execution time assessment of subqueries to relational databases”, Computational Technologies vol. 5 no 4 Novosibirsk, ISSN 1560-7534, 2000 [Reviewed by “Zentralblatt für Mathematik” and by “Mathematical Reviews”].

- [4] Will E. Leland, Murad S. Taqqu, Walter Willinger, Daniel V. Wilson, "On the Self-Similar Nature of Ethernet Traffic", 1993.
- [5] Henk Tijms, *Understanding Probability*, Cambridge University press, ISBN 978-0-521-70172-3, 2007.
- [6] J. S. Wentzel, *Probability theory*, Vysshaya Shkola Publishres, Moscow, ISBN: 5-06-005688-0, 2006.
- [7] William Feller, *An Introduction to Probability Theory and Its Applications*, Volume 1, John Wiley & Sons Inc, ISBN: 0471257087, 1968.
- [8] Gut Allan, *Probability: A Graduate Course*, Springer-Verlag, ISBN 0387228330, 2005.
- [9] Patrick Billingsley, *Probability and Measure*, New York, Toronto, London, ISBN 0471804789, 1986.
- [10] Andrej Nikolaevic Kolmogorov, Nathan Morrison, *Foundations of the theory of probability*, Chelsea publ. co., New York, OCLC:185529381,1950 [originally published in German, 1933].
- [11] Walter Ledermann, Emlyn Lloyd, *Handbook of Applicable Mathematics: Statistics*, Vol 6, John Wiley & Sons, ISBN: 0471902748,1980.
- [12] Walter Ledermann, *Probability: Handbook of Applicable Mathematics*, Volume 2, John Wiley & Sons Ltd, ISBN: 0471278211, 1981.
- [13] Edwin Thompson Jaynes, G. Larry Bretthorst, *Probability Theory: The Logic of Science*, Cambridge University Press, ISBN 0521592712, 2003
- [14] Kai Lai Chung, *A Course in Probability Theory*, Academic Press, ISBN 978-0121741518, 2000.
- [15] Leonid Koralov, Yakov G. Sinai, *Theory of Probability and Random Processes*, Springer, ISBN 978-3540254843, 2007.
- [16] Alvin W. Drake, *Fundamentals of Applied Probability Theory*, McGraw-Hill College, ISBN 978-0070178151, 1967
- [17] Harold Jeffreys, *Theory of Probability*, Oxford University Press, USA, ISBN 978-0198503682, 1998.
- [18] Henry Stark, John W. Woods, "Probability, Random Processes, and Estimation Theory for Engineers", Prentice Hall, ISBN 978-0137287918, 1994.
- [19] Arnold O. Allen, "Probability, Statistics, and Queueing Theory With Computer Science Applications", Academic Press, ISBN 978-0120510511, 1990.
- [20] T. Mikosch, S. Resnick, H. Rootzen, A. Stegeman, "Is network traffic approximated by stable Levy motion or fractional Brownian motion?", *the Annals of Applied Probability* Vol. 12 No. 1, p. 23–68, 2002.
- [21] Vern Paxson, "Experiences With Internet Traffic Measurement and Analysis", ICSI Center for Internet Research International Computer Science Institute and Lawrence Berkeley National Laboratory, 2004.
- [22] Peter Haga, Peter Pollner, Gabor Simon, Istvan Csabai, Gabor Vattay, "Self-generated Self-similar Traffic, Communication Networks Laboratory", Eotvos Lorand University, 2004.
- [23] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, *Introduction to Algorithms*, second edition, MIT Press, ISBN 0-07-013151-1, 2002.
- [24] Donald E. Knuth, *The Art of Computer Programming*, Third Edition vol. 2 Seminumerical Algorithms, Addison-Wesley, ISBN 0-201-89684-2, 1998.
- [25] Katsuhiro Ogata, *Modern Control Engineering*, Prentice Hall, ISBN 978-0130609076, 2001.
- [26] William L. Brogan, *Modern Control Theory*, 3rd Edition, Prentice Hall, ISBN 978-0135897638, 1990.
- [27] H. Lebesgue H, *Leçons sur l'intégration et la recherche des fonctions primitives*, Paris: Gauthier-Villars, 1904.
- [28] G. Bartle, *The elements of integration and Lebesgue measure*, Wiley Classics Library, New York: John Wiley & Sons Inc., ISBN 0-471-04222-6, 1995.

Simple yet efficient NMEA sentence generator for testing GPS reception firmware and hardware.

V. Sinivee MSc

Department of Physics

Tallinn University of Technology

Ehitajate tee 5

19086,Tallinn, Estonia

Keywords: GPS, binding data to geographic coordinates, positioning, spectrometer, NMEA, SIRF-Star, test pattern, test sequences generator, testing, DUT.

Abstract- A simple device for generating NMEA sequences for testing embedded GPS reception firmware and hardware is described. Device can work in standalone mode and also in conjunction with control software. Configuration program can be used to generate test strings without tester hardware as well.

I. INTRODUCTION

It is often desirable to bind measured (field-) data with exact time and coordinates, especially in handheld mobile environmental instruments. Geographic data is usually obtained from a GPS-receiver. Modern GPS engines have lots of attractive features: they are small and economic, output data could be read easily. Due to minute power consumption use of such receiver in battery powered apparatus is justified.

GPS is very useful mean of positioning in a simple case when measurement sensors spatial orientation is not important.

Cases exist where 3 coordinates are not enough to guarantee needed accuracy and repeatability of measurements. A good example is measuring moisture contents of various materials. Since the 30 cm range moisture sensor of „Moist 200” instrument uses polarized microwave radiation, it is essential to determine probe's spatial orientation. If the tested sample/object has a fibrous structure, results depend much of sensor's rotation angle around its longitudinal axes. Described effect is clearly visible when measuring, for example, moisture of paper. For such cases a more precise 6-DOF positioning system like described in [6] could be used.

Author of present thesis used GPS engine to bind spectral data from an experimental portable gamma spectrometer-datalogger „GammaMapper” with geographic coordinates. In this device coordinates from the GPS receiver are stored together with every preset amount of gamma events thus allowing the experimenter build radiation maps of his/her everyday environment [3].

Data from a standard GPS-receiver is output in form of various so-called NMEA sentences. In NMEA mode data is presented as a stream of ASCII characters. A „SIRF-Star” binary format also exists.

Receiver's output stream combines lot of information divided into different protocols. Device description is usually also transmitted on engine power-up.

On start-up or in poor visibility acquired coordinates could be not valid. For example in protocol \$GPRMC (Recommended minimum specific GPS/Transit data) a special character – letter ‘V’ or ‘A’ indicates fitness of data. More information about protocols used in GPS data transactions and their meanings could be obtained from [1,5,8].

Part of designing process of state-of-art instruments with embedded GPS engine involves writing routines for decoding receivers output stream. For testing those routines one must have some kind of test data source. Unfortunately GPS data is usually not available indoors.

Another problem is simulating validity of data and erroneous stream reception. Good firmware must be able to handle errors occurred due to poor signal level, problems in link between GPS engine and main processor of instrument under test (protocol and hardware errors) etc. Using data output by standard GPS-receiver even with many satellites in view does not offer means for testing all mentioned situations.

Numerous excellent programs have been written for decoding NMEA and binary messages of GPS receivers.

There are not so many reverse converters i.e. programs simulating a GPS receiver. „GPSSIMUL” [9] is a good freeware (30-day trial version) NMEA sentence simulator that could prove to be practical in many cases. Unfortunately it (like multiple other programs author could find) simulates only correct and only NMEA sentences.

In some situations a stand-alone configurable (low-power) test generator with a wide range of supply voltage and possibility to simulate errors is more preferable.

Present thesis describes a prototype GPS data simulator designed and built in Department of Physics of Tallinn University of Technology. First version of the device was limited to generating only one NMEA message and enabled simulation of communication errors (see fig.4.). Later versions were developed to a more universal device with control via a GUI running on an ordinary PC.

II. SIMULATOR HARDWARE

First solution of described problem was writing a simple firmware for a low-cost and readily available microcontroller generating only needed NMEA sentences (see fig.1.).

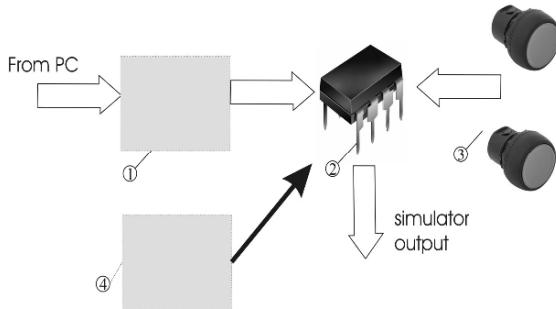


Fig. 1. GPS simulator's block-diagram. 1 –optional USB or RS232 interface, 2 – microcontroller, 3 – control buttons, 4 – optional adjustable power supply.

Core of the circuit is a small microcontroller (2). Two modifications of the output data stream were made available via jumper/pushbutton (3) settings: simulation of a „position not valid” flag and erroneous sentence (one that was prematurely terminated).

Optionally an adjustable power supply (4) could be added to circuit for using it with processors with a non 5V supply voltage.

For configuration the board must be connected to a PC via USB or serial interface (1).

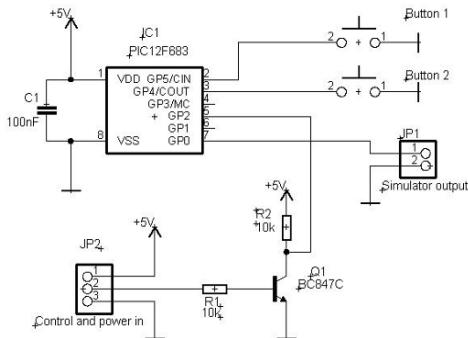


Fig. 2. Test sequences generator's electrical circuit.

Prototype of the GPS tester was built on Microchip's popular PIC series processor [4] due to it's availability, low power consumption, wide range of supply voltage and also due

to author's experience in writing software for them.

Heart of the simulator is IC1 (see fig.2.). Microcontroller generates all needed test protocols. Data is output from a bit-banged serial port [7] via pin GP0.

Above mentioned jumpers were replaced in present version with buttons. External pull-up resistors were not used since PIC micro controller can be configured to use internal pull-ups.

Capacitor C1 is a standard mean of suppressing noise generated more or less in all digital circuits.

Transistor Q1 together with R1 and R2 form a level shifter circuit to connect the device with a PC via standard serial port. If the device will be used in standalone mode only, mentioned components except resistor R2 may be omitted.

Since PIC12F683 used in described circuit lacks internal USART, reception of control commands is realized via a “bit-bang” software serial port [7] working at a fixed baud rate of 4800 bd.

A standard USB port is a very convenient and handy mean for powering the device and communicating with PC since serial ports are nearly extinct. One could use an off-shelf USB to RS232 converter together with a MAX232 level shifter IC or build one on a special chip – FT232RL manufactured by FTDIchip [10].

Powering the PIC microcontroller from a separate adjustable supply allows using the tester circuit for debugging hardware with supply voltage in range of 2,7...5,5V. A standard LM317 voltage regulator (not shown on circuit) could be used for this purpose.

Full digital control of devices features might include adjusting supply voltage. A MAX518 digital to analog converter is suitable for this purpose since the PIC microcontroller operates in nanowatt power mode.

The D/A chip could get it's instructions from PIC microcontrollers outputs dedicated normally to switches (since control commands and button press events usually do not occur simultaneously) or a controller with different I/O count could be used.

Author of present thesis implemented I²C control of the D-to-A chip using mentioned switch outputs (GP0 and GP1 on figure 2).

PIC-microcontroller's internal brown-out control's voltage threshold should be set below minimum operational voltage in that case (2,0V is recommended).

Figure 4 showing the control program does not yet reveal possibility of supply voltage control of the board.

III. SIMULATOR FIRMWARE

Main work mode of the GPS simulator described in present thesis is a standalone mode without control from PC. At first start there will be no saved test sequences in device's EEPROMmemory. Therefore the device defaults to emulating only a correct “\$GPRMC” sentence every second.

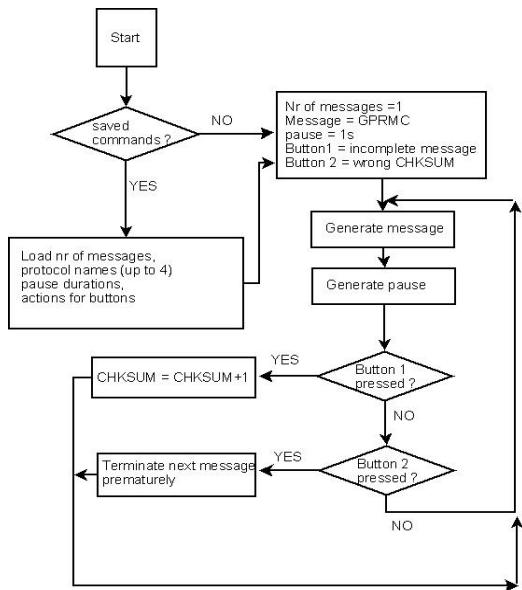


Fig. 3. Test sequences generator's work flow.

Pressing button 1 sets flag “position not fixed” in output message and pressing button 2 terminates next message prematurely. Normal messages will be generated if both buttons are released (see fig.3.).

High-speed operation and compact code of the device is achieved by using assembly programming language.

IV. CONTROL GUI

In order to make described device more universal, major changes were made to its firmware and a small control program was written.

Figure.3 shows utility’s working screen. This program uses Windows platform and allows sending different NMEA protocols to the simulator micro controller. One can select number of simultaneously generated different sentences. Also a device ID could be sent on start-up. Since it differs from ordinary data stream, it could cause crashing of firmware of the device under test. Device ID could be of arbitrary length and contents.

Pause between emitting different protocols is also configurable.

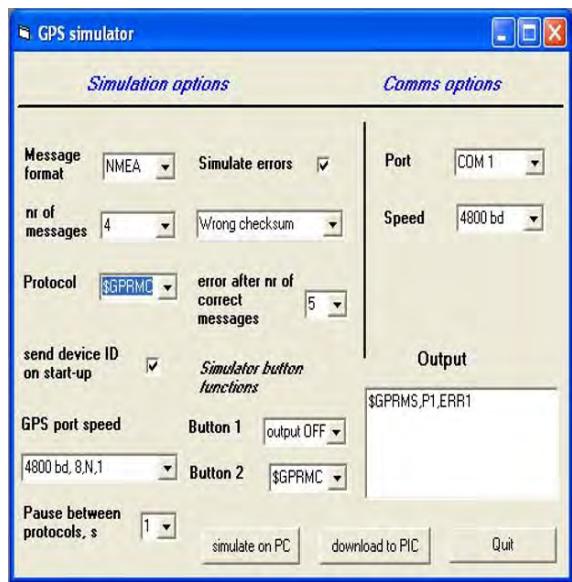


Fig. 4. Main screen of control utility.

Baudrate of the GPS-engine simulated is selectable between 4800 bd up to 115200 bd. Other parameters of communication port could be configured as well.

Control GUI lets user define different actions undertaken on button press event on the simulator board. Actions could be selected form a drop-down list. Both buttons could be configured separately.

Selections are:

- sending selected standard protocol,
- switching output off or on again,
- simulating error in communication,
- changing port speed (simulation of error case)
- sending a device ID etc.

It must be noted that user composed messages or device ID-s could be sent to DUT form the “Output” text box. If there is a message in text box, corresponding option appears to all relevant drop-down selection lists.

Freely composable messages make the device more universal not limiting it’s use to the field of GPS systems only.

Comm’s options menu controls connecting the simulator board to PC. Simulators own input baud rate is fixed to 4800 bd due to lack of resources for autobauding in used microprocessor.

Button “download to PIC” sends configuration data to the simulator board where it is saved to controllers on-chip EEPROM memory. Settings are applied immediately for the next message generated.

For users having no resources to build described simulator board, option of generating test strings straight from PC’s own comm port was added to the GUI code.

V. CONCLUSION

Described in present thesis simple GPS signals simulator proved to be practical and useful. It has already saved author hours of debugging time in writing firmware for his portable spectrometer, the "GammaMapper" [3]. This was especially true while debugging the device described in [2].

Due to very compact hardware the device could be useful to other programmers working in field of instruments making use of embedded GPS engines.

In order to improve precision of timing of output test string a crystal resonator could be added to the circuit.

Author plans to write a new firmware version which supports SIRF binary format messages as well.

Custom messages typed into the output box enables using the device as a universal test pattern generator not limiting to GPS applications only.

Parameters of described GPS-simulator's board are as follows:

- power consumption: 0,8 mA@5V;
- power supply range: 2,7...5,5V;
- output port speed: 4800...115200 bd;
- output format: NMEA;
- standard NMEA sentences simulated (in present firmware version): \$GPGGA, \$GPRMC, \$GPGLL, \$GPGRT, \$GPRMB, \$GPZDA;
- option of custom messages;
- option of simulating errors in output stream;
- configurable via control program running on an ordinary PC.

REFERENCES

- [1]<http://home.mira.net/~gnb/gps/nmea.htm>
- [2] V.Sinivee, "A Simple Data Filter for the GPS Navigator," Instruments and Experimental Techniques, Vol. 49, No. 4, 2006 , p.511.
- [3]Sinivee, V. A prototype gamma spectrometer-datalogger binds data to geographical coordinates and offers protection of measurement results. In International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE 07), Bridgeport, CT, USA. December 3 - 12, 2007.
- [4]http://ww1.microchip.com/downloads/en/DeviceDoc/41211D_.pdf
- [5]<http://www.circuitcellar.com/library/print/0899/Cyliax109/2.htm>
- [6]V. Sinivee, L. Kurik and U. Kallavus, "Combined positioning system for mapping measured properties of objects of arbitrary shape" In 6th International DAAAM Baltic Conference INDUSTRIAL ENGINEERING (TTU, Tallinn, Estonia, April 2008), pp 183-188.
- [7]<http://www.rentron.com/Myke7.htm>
- [8]<http://aprs.gids.nl/nmea/>
- [9]<http://www.sailsoft.nl/gpssimul.htm>
- [10]<http://www.ftdichip.com/Products/FT232R.htm>

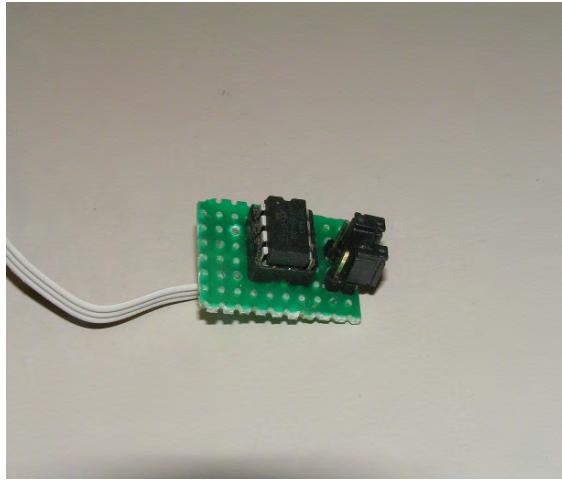


Fig. 5. First prototype of the simulator board.

Game Theoretic Approach for Discovering Vulnerable Links in Complex Networks

Mishkovski Igor, Sonja Filiposka, Sasho Gramatikov, Dimitar Trajanov and Ljupco Kocarev

*Dept. of Computer Sciences
Faculty of Electrical Engineering and Information Technology
University Ss. Cyril and Methodious Skopje
Skopje, R. Macedonia
{igorm, filipos, saso.gramatikov, mite, lkocarev}@feit.ukim.edu.mk*

Abstract – Complex networks have been an up-and-coming exciting field in the realm of interactions. With their widespread use appearing on the horizon it is ever more vital to be able to measure their vulnerability as a function of their topology. Precisely, discovering vulnerable links, disposed to attacks, can help in hardening these links and by that providing more secure and reliable network structure. This paper addresses the link vulnerability of different topologies of complex networks such as: random networks, geographic random networks, small world networks and scale-free networks. We introduce measure for vulnerability of complex networks, and prove by simulations that network vulnerability heavily depends on the network topology.

Index Terms – Complex Networks, Vulnerability, Game Theory, Network Topology.

I. INTRODUCTION

Shielding a link from malicious attacks is a key challenge to network security and management. Identifying and hardening the key links in a certain network will increase the network reliability but also it will decrease the amount of time needed to wield a reliable network. The emergence of terrorist attacks opened a new direction in the vulnerability analysis. Now the engineers must also be aware of intentional network attacks by the terrorists. The impact of these intentional link failures on the performances of the network depends on the routing strategy and the topology of the network. One way to deal with these intelligent attacks is to make the network more robust, i.e. to have more alternative routes. Thus, the original concept behind the Internet was that of a network that would withstand a nuclear attack [1]. But, no matter how much the network is robust there is always an open hole for the intelligent attackers.

In order to analyze these intelligent attacks on complex and man-made networks we use the game theoretic approach, proposed in [1].

Game theory introduces mathematical background for different analysis of the interactive processes for decision making. This theory enables tools that can leverage the prediction of what might happen in an environment where there is interaction between agents with conflict interests, i.e. non-cooperative environment. The traditional applications of the Game Theory try to find out the equilibrium point, i.e. set of strategies in which it is almost impossible for the individuals to change the current strategy.

This theory was introduced in [2] and its further development was due to the Nash Equilibrium concept in

[3]. The games that were studied during the evolution of this theory were well defined mathematical objects. The games are consisted of players, a set of strategies, and specification of the profits for every combination of the strategies.

In the game presented in this study the players are the router, which seeks minimum cost paths for the packets, and a tester, whose aim is to maximize the trip cost. The solution of the game is the mixed strategy Nash equilibrium where the path selection probabilities are optimal for the router and the link failure probabilities are optimal for the tester. The overall vulnerability of the complex network is measured by the statistically expected trip-cost and the critical links for the network performance are indicated by the link failure probabilities.

There have been many uses of the proposed game theoretic approach by Bell in [1]. In [4] Bell quantifies the risk in transporting hazardous materials across a road network. In [5] using this approach the authors quantified the reliability of communication in mobile ad hoc network (MANET). In [6] authors propose a new vulnerability identification method in multicommodity stochastic networks.

This paper is an extension of the work by Bell [1] in the way that it analyzes the vulnerability of different topologies of complex networks. Thus, four generators were implemented for the different network topologies: random (Erdos Renyi - ER), geographic random (GER), small world (SW) and scale-free (SF). We introduce a new measure for vulnerability of the networks, and prove by simulations that the vulnerability of a network largely depends on its topology. Additionally the game theoretic approach was used in order to seek out the most vulnerable links in these topologies and to compare the topologies in terms of vulnerability.

The rest of the paper is as follows. In Section 2 we give a survey of the complex networks. In this survey we analyzed the: random networks, geographic random networks, small world networks and scale free networks. Section 3 presents the game theoretic tool which we used to measure the vulnerabilities of these types of networks. In Section 4 we give the topology-dependent properties of the observed networks. Section 5 presents the results obtained from the vulnerability analysis. Section 6 concludes the paper.

II. COMPLEX NETWORKS

Complex network is a complex graph-based structure made of nodes (which can be individuals, computers, web pages, power grid plants, organizations, cities, proteins in the human body, etc.) that are connected by one or multiple

types of interdependence (i.e. friendship, network links, power transport network, trade, roads, chemical reactions, etc.) These graphs or networks have certain properties which limit or enhance the ability to do things with them [22]. For example, small changes in the topology, shutting down only small number of links between the nodes, may lead to serious damage to the network capabilities.

A. Random Graphs

The Euler's introduction of the graph theory, was the initial step to uncover the properties of large, but ordered graphs.

Major breakthroughs are eight papers authored by Erdos and Renyi [7] laying down the foundation of the theory of random networks. They took on the challenge of explaining a very complex phenomenon by proposing an elegant mathematical answer to describe complex graphs within a single framework. By deliberately discarding the fact that different systems follow disparate rules in building their own networks, they follow the simplest solution: connect the nodes randomly.

Although Erdos and Renyi say that we need only one link per node to stay connected, real networks (like the worldwide net) are not only connected but are well beyond the threshold of one. Consequently, the networks in nature are very dense networks within which every node is navigable.

Start with a large number of isolated nodes. Then randomly add links between the nodes. If this continues, inevitably pairs of connected nodes will connect together forming clusters of several nodes. When enough links are added such that each node has an average of one link, a unique cluster emerges. That is, most of the nodes will be part of a single cluster such that, starting from any node, any other node can be reached navigating along the links between the nodes.

If the network is large, despite the links' completely random placement, almost all nodes will have approximately the same number of links. The result shows that the distribution of the number of links in a random graph is according to the Poisson distribution, which predicts that it is exponentially rare to find a node which deviates from the average by having considerably more or fewer links.

B. Geographic Random Networks

A geographic random network consists of set of points randomly scattered over a region according to some probability distribution, and these nodes are connected by an edge only if the distance between the nodes is less than specified value [16].

These types of networks are different from random networks in a way that they do not follow the property of independence or near-independence between the status of different edges. In geographic random networks triangular property is more realistic, which means if X_i is close to X_j , and X_j is close to X_k , then X_i will be fairly close to X_k .

With the advances in wireless communication technology geographic random topology is more and more present in the real complex and man-made networks. The ad hoc networks and mesh networks follow the properties of the geographic random graphs. This model can also represent a

network of randomly placed sensors, each equipped with a limited communication capability.

In geographic random networks the average number of neighbors the node has, or the average node degree of the node depends on the transmission range of the node and the density of the nodes in the terrain, it can be calculated as:

$$k = \frac{N \cdot r^2 \cdot \pi}{a^2} \quad (1)$$

where N is the number of nodes in the terrain, r is the transmission range of the nodes and a is the size of a square terrain.

C. Small World Networks

The random network theory has dominated network thinking since its introduction in 1959. In 1967, Stanley Milgram [8] turned the concept of "six degrees of separation" into a much celebrated, groundbreaking study on interconnectivity.

A repeated characteristic of complex networks is the small-world phenomenon, defined by the co-existence of two apparently contrary conditions:

- (i) the number of intermediaries between any pair of nodes in the network is quite small - i.e. six-degrees of separation phenomenon and
- (ii) the large local "cliquishness" or redundancy of the network - i.e., the large overlap of the circles of neighbors of two network neighbors. The latter property is typical of ordered lattices, while the former is typical of random graphs [9].

When one says that the network has "small world" topology, it means that almost every pair of nodes is connected by a path with an extremely small number of steps.

This kind of topology can be mostly seen in the social networks but there are also some technology, man-made and complex networks that have these characteristics. The Web falls in the same class of networks, where it has been shown that any document is on average only nineteen clicks away from any other [10]. Taken together these two networks suggest that behind the short observed distances of the enormous networks there is a fundamental property. This suspicion was later confirmed by subsequent discoveries which demonstrated that small separations are common in just about every network scientists have had a chance to study. The Internet, a network of hundreds of thousand of routers, has a separation of ten. The networks composed of proteins [11] with connections that indicate the physical interaction of the proteins exhibit small-world properties. Other examples are the road maps, electric power grids, neural networks etc. The highly interconnected nature of these networks is the reason for this small separation.

If you consider a network in which the nodes have on average k links, there are however k^2 nodes two links away and roughly k^d nodes d links away. So if k is large, for even small values of d , the number of reachable nodes can become very large. If you have N nodes in the network, k^d must not exceed N . Thus, using $k^d=N$, a simple formula is obtained that works well for random networks, showing that the average separation follows the equation:

$$d = \frac{\log N}{\log k} \quad (2)$$

“Small worlds” are a generic property of networks in general. Most networks obey it since it is rooted in their structure. In Granovetter’s paper [12] a new proposition for the structure of complex network emerges. The structure of the complex network around an arbitrary node is rather generic. In his view the graph is structured into highly connected clusters, or close-knit circles of nodes, in which every node has link to everybody else.

Watts [13] answered the question concerning the likelihood of forming clusters of nodes. To achieve this Watts and Strogatz introduced a quantity called the clustering coefficient. This coefficient tells how closely knit the circle of neighboring nodes is. A number close to 1.0 means that all neighbor nodes of one node are also neighbors with each other. Working on available networks, it has been shown that real networks like the network of mathematicians’ co-authorship, or the collaboration graph of scientists are showing evidence of high clustering.

D. Scale-free Networks

Malcolm Gladwell’s [14] conclusion has shown an altogether new property of complex networks: Connectors – nodes with an anomalously large number of links – are present in very diverse complex systems, ranging from the Internet to the cell. They dominate the structure of all networks in which they are present, making them look like small worlds. Indeed, with links to an unusually large number of nodes, hubs create short paths between any two nodes in the system.

Power laws mathematically formulate the fact that in most real networks the majority of nodes have only a few links and that these numerous tiny nodes coexist with a few big hubs, nodes with an anomalously high number of links. In a random network the peak of the node degree distribution implies that the vast majority of nodes have the same number of links and that nodes deviating from the average are extremely rare. Therefore, a random network has a characteristic scale in its node connectivity, embodied by the average node and fixed by the peak of the degree distribution. In contrast, the absence of a peak in a power law degree distribution implies that in a real network there is no such thing as a characteristic node. There is no intrinsic scale in these networks. This is why Albert Barabasi and his group described the networks with power law distribution as scale-free networks [10]. For scale-free networks the number of nodes with exactly k links follows a power law, each with a unique degree exponent that for most systems varies between two and three:

$$N(k) \sim k^{-\gamma} \quad \gamma=(2,3) \quad (3)$$

The first proposal for generation of scale-free networks is the Albert Barabasi model [15] which draws from the fact that scale-free topology is a natural consequence of the ever-expanding nature of real networking. Starting from two connected nodes, every time a new node is added to the network, it prefers to attach to the more connected nodes. The expansion of the network means that the early nodes

have more time than the latecomers to acquire links. Thus growth offers a clear advantage to the senior nodes, making them richest in links.

After the first model appears making it possible to create a scale-free network using growth and preferential attachment, several additions to the model follow. An important addition to the model is the possibility for creating a competitive environment [10]. Here each node has certain fitness f_i , a quantitative measure of a node’s ability to stay in front of the competition. The introduction of fitness changes what is considered attractive in a competitive environment. In the original model it is assumed that node’s attractiveness is determined solely by its number of links. In a competitive environment, nodes with higher fitness are linked to more frequently. A simple way to incorporate fitness is to assume that preferential attachment is driven by the product of the node’s fitness and the number of links it has. Later it is shown that the fitness distribution can lead to two cases: the rich get richer scale-free topology, and the-winner-takes-all network where only one huge hub exists and all nodes are connected to it.

There are many networks that obey the scale-free characteristics, such as: protein-protein interaction networks., the World Wide Web, semantic networks etc.

III. LINK VULNERABILITY ANALYSIS USING GAME THEORY

Game theoretic approach for measuring the vulnerability of stochastic networks was introduced in [1]. The players in the game are a “router” which seeks minimum cost paths throughout the network and a virtual tester which aim is to maximize the cost of the trip. The game is with mixed strategies, where the path selection probabilities are optimal for the router and the link failure probabilities are optimal for the tester. Also an overall measure, statistical – trip cost, for the vulnerability of the network is introduced. By using this approach and one can identify the critical links for the network performance.

The objective of the game is to seek links whose failure would damage the performance of a complex network the most.

In this game it assumed that one link can fail at a given time and each failure scenario corresponds to 1 failed link.

When a link fails, some penalty must be introduced. The queue on each link is assumed to be a $M/M/1$ (random arrivals/random service times/single server). The degree of saturation on link i equals p_i , giving an s-expected delay of:

$$d_i = \frac{p_i}{1 - p_i} \quad (4)$$

Initially, the failure penalty is assumed to be the same for all links and equal to 10 units. Thus, cost of the link i under failure scenario j is equal to:

$$c_{i,j} = \begin{cases} 10, & \text{if } i = j, \\ d_i, & \text{otherwise} \end{cases} \quad (5)$$

Because the cost of the link in the complex networks is traffic dependent MSA (Method of Successive Averages) algorithm, can be used [1]. The procedure is as follows.

Step 1: Link failure probabilities (q_i) for all scenarios are initialized to $1/n$ Links.

Step 2: Link use probabilities (p_i) for all links are initialized to 0 and $n \leftarrow 1$.

Step 3: s-Expected link-costs are calculated as a function of link-use probabilities and the path with the minimum s-expected cost is sought (we used the Dijkstra algorithm [17]); $x_i \leftarrow 1$ if link i is on the shortest path, 0 otherwise.

Step 4: Update link use probabilities:

$$p_i \leftarrow (1/n) \cdot x_i + (1 - (1/n)) \cdot p_i \text{ for all links } i.$$

Step 5: Find the j which maximizes $\sum_{i,j} p_i \cdot c_{i,j}(p_i)$, and $y_j \leftarrow 1$; for all scenarios, $k \neq j$, $y_k \leftarrow 0$.

Step 6: Update link failure probabilities:

$$q_j \leftarrow (1/n) \cdot y_j + (1 - (1/n)) \cdot q_j, \text{ for all scenarios } j.$$

Step 7: $n \leftarrow n + 1$; return to *Step 3* until satisfactory convergence is reached.

The vulnerability measure for the whole network, s-expected trip cost, can be calculated as:

$$C = \sum_{i,j} p_i \cdot c_{i,j} \cdot q_j \quad (6)$$

This algorithm is a heuristic one and there is no guarantee for convergence. And when it occurs is one of possibly many solutions to the problem. The convergence can be ensured using convergence criteria which measures the distance to a solution explicitly.

IV. TOPOLOGY DEPENDENT PROPERTIES OF THE OBSERVED COMPLEX NETWORKS

The game theoretic approach used in [1] and also explained here was tested on four topologies of complex networks: random topology, geographic random topology, small world topology, and scale free topology. For the purpose of the simulations we implemented network generators, in Matlab [18], for each network topology. The number of nodes (N) in the network was 500 and the average node degrees (k_{av}) of the networks were close to 6.

The generator for the small world network was based on the Watts-Strogatz model with probability of reconnection of 0.1.

The generator for the Scale-Free networks was based on the BA model were at the beginning the network was consisted of 4 entirely connected nodes.

The generator for random networks was based on the Erdos-Renyi model. The nodes were randomly connected where the probability for a link between nodes i and j was:

$$p_{i,j} = \frac{k_{av}}{N-1} \quad (7)$$

The geographic random generator was invented by us. The algorithm is as follows. At first the nodes were randomly scattered along a $1m^2$ square terrain and their connectivity radius was calculated using (2) as:

$$r = \sqrt{\frac{k_{av}}{N \cdot \pi}} \quad (8)$$

All of the networks need to be connected, i.e. starting from any node; any other node can be reached navigating along the links between the nodes. For this purpose we used eigenanalysis [19]. We checked the connectivity of the networks by finding that the second eigen value of the Laplacian matrix was bigger than 0 [19]. In the case of the geographic random network generator if this is not the case the giant component was found and the nodes from the islands were again randomly scattered, this process last until the giant component is consisted of all the nodes in the network.

Table 1 gives the topology dependent properties of the observed network topologies, such as the average node degree [21], clustering coefficient [13] and normalized betweenness centrality [21], obtained by Ucinet [20].

Table 1 Topology dependent properties of the observed complex networks

Measure/Network	ER	GER	SW	SF
Average node degree	6.27	6.26	6.00	5.98
Clustering coefficient	0.014	0.627	0.447	0.055
Average normalized node betweenness	0.521	3.352	0.894	0.445

V. VULNERABILITY ANALYSIS

The MSA algorithm and network generators were implemented in Matlab. In the simulation there were 1500 OD (origin-destination) commodity pairs. The nodes in commodity pairs were chosen randomly. The game specified used in the simulation allows the virtual network tester to fail only 1 link at a time. This is suitable where the probability of 2 or more concurrent failures is very small.

The first analysis was related to the vulnerability of the whole network. Figure 1 shows the convergence of the MSA method for the four topologies of complex networks. One can see that this method converges very fast despite the network topology.

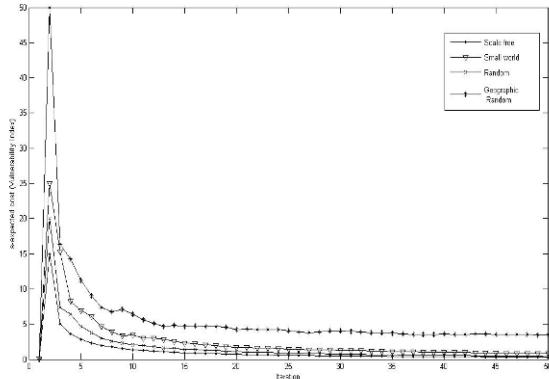


Fig. 1 Convergence of the Vulnerability index for the four topologies of complex networks

The value to which it converges as a function of the network topology is shown in fig. 2. As we can see the poorest performance gives the geographic random topology with index of 3.4189, then small world network (index: 0.8001), then the random network topology (index: 0.4279) and then scale free network topology (index: 0.3163).

In reality, these results mean that the scale free topology (for example the Internet network) is more resistant to link failure than network with geographic random topology, i.e. ad hoc network.

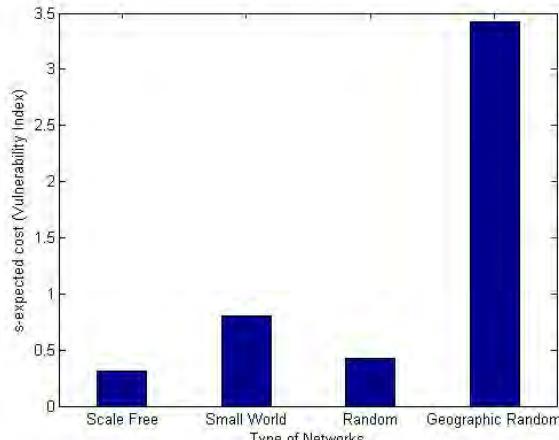


Fig. 2 Vulnerability index for the four topologies of complex networks

The second analysis consisted of finding the most vulnerable links in the networks, i.e. find the link with the greatest link failure probability. We seek out the weakest link for the most resistant topology, scale free, and the least resistant topology, geographic random. In fig. 3 the scale free network is shown with the weakest link (with bold line) between nodes 1 and 2. This is the link that connects the two biggest hubs in the network. The link failure probability of this link is around 0.95 and obviously it must be the most protected and robust link in the scale free network. Thus, its

successful attack and removal will dramatically degrade the network performances.

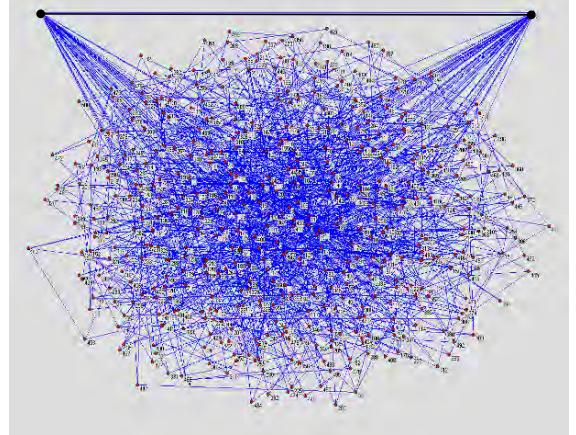


Fig. 3 Scale free network. The weakest link is the link connecting the two biggest hubs, node 1 and node 2

In fig. 4 the geographic random network is shown with the weakest link (with bold line) between the nodes 80 and 371. From the figure one can see that if this link is attacked and destroyed then the path length of its neighbors will increase dramatically. The link failure probability of this link is around 0.80 and it is much bigger than any other link in the geographic random network.

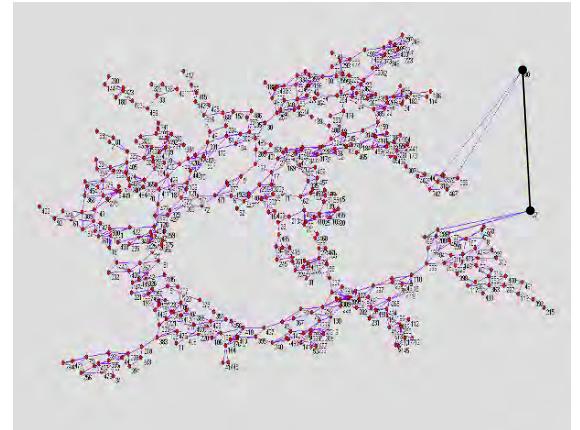


Fig. 4 Geographic random network. The weakest link is the link connecting the nodes 80 and 371

VI. CONCLUSION

The contribution of this work is twofold. Firstly, we use game theoretic approach to measure the vulnerability of complex networks with different topologies. We have studied vulnerability index in networks with four network topologies: random network, geographic random network, small-world network and scale free network. Our results show that the vulnerability of a network heavily depends on its topology. Concretely, we show that the scale free topology is the most resistant network topology to

intelligent link attacks and geographic random is the most vulnerable network to this kind of attacks. Secondly, using this approach we identify the weakest links in complex networks.

Our future work will be focused on using this approach for identifying vulnerability of different kind of real complex and other types of networks. Furthermore, we want to measure how the vulnerability of different network topologies changes after failure of certain nodes. These nodes can be chosen randomly or using some algorithm for choosing the most influent node, i.e. pageRank algorithm.

Another direction is to measure the vulnerability of the network by using the graph theory and network analysis to measure centrality of an edge, i.e. the edge betweenness.

REFERENCES

- [1] M.G.H. Bell, *The use of game theory to measure the vulnerability of stochastic networks*. Reliability, IEEE Transactions on Volume 52, Issue 1, March 2003 Page(s): 63 – 68.
- [2] John von Neumann, Oskar Morgenstern, *Theory of Games and Economic Behavior*. Princeton University Press, 1944.
- [3] J. Nash, *Equilibrium point in n-person games*. Proceeding of the National Academy of Science, 36, 1950.
- [4] M.G.H. Bell, *Mixed Route Strategies for the Risk-Averse Shipment of Hazardous Materials*, Netw. and Spat. Econ., vol. 6, no. 3, pp. 253-265, 2006.
- [5] H. Karaa, and J.Y. Lau, *Game Theory Applications in Network Reliability* in Proc. Communications, 23rd Biennial Symposium, 2006, pp. 236-239.
- [6] Satayapiwat, P.; Suksomboon, K.; Aswakul, C, *Vulnerability analysis in multicommodity stochastic networks by game theory*, ECTI-CON 2008, pp. 357-360.
- [7] Michael Karonski and Adrzej Rucinski: *The Origins of the Theory of Random Graphs*, The Mathematics of Paul Erdos, Berlin, Springer, 1997
- [8] Milgram S.: *The small world problem*, Psychology today 2, pp. 60-67,1967.
- [9] L.A.N. Amaral and J.M. Ottino, *Complex Networks, Augmenting the framework for the study of complex systems*, Eur. Phys. J. B 28, 147-162, 2004.
- [10] Albert Laszlo Barabasi: *Linked*, Penguin Group, London, May, 2003
- [11] P. Bork et al. "Protein interaction networks from yeast to human", Current Opinion in Structural Biology, 14(3):292-299, 2004.
- [12] Mark S. Granovetter: *The Strength of Weak Ties: A Network Theory Revisited*, Sociological Theory 1, 1983
- [13] D. J. Watts: *Small Worlds: The Dynamics of Networks between Order and Randomness*, Princeton University Press, 2003
- [14] Malcom Gladwell: *The Tipping Point*, New York, Little, Brown, 2000
- [15] Albert B., Barabasi A.L.: *Statistical mechanics of complex networks*, Reviews of modern physics, Vol. 74, January 2002.
- [16] Mathew Penrose: *Random Geometric Graphs*, Oxford University Press, New York, 2004
- [17] E. W. Dijkstra: *A note on two problems in connexion with graphs*. In Numerische Mathematik, 1 (1959), S. 269–271.
- [18] THE MATHWORKS, INC. 1997. MATLAB: *The Language of Technical Computing*. The MathWorks, Inc. Using MATLAB (Version 7).
- [19] Keith Briggs, *Graph eigenvalues and connectivity*, july 2003.
- [20] Borgatti, S., Everett, M. & Freeman, L. (1996a). *UCINET IV Version 1.64*. Natick, MA: Analytic Technologies.
- [21] Freeman, L. C. (1979). *Centrality in social networks: Conceptual clarification*. Social Networks, 1(3), 215-239.
- [22] Sonja Filipska, Dimitar Trajanov and Aksenti Grnarov, Survey of Social Networking and Applications in Ad Hoc Networks, ETAI 2007, Ohrid, R.Macedonia, 2007.

Modeling Trust in Wireless Ad-Hoc Networks

Tirthankar Ghosh, Hui Xu
tghosh@stcloudstate.edu,hxu@stcloudstate.edu
Department of Statistics and Computer Networking
College of Science and Engineering
St. Cloud State University
St. Cloud, Minnesota 56301, U.S.A.

Abstract—A model for computing trust in wireless ad-hoc networks has been proposed. The model is based on the societal approach towards building a trusted community, where trust is built up slowly, but decreases to zero on a single detectable misbehavior. Successive trust build-ups depend on past behavior. Wireless channel loss probability has also been considered in the model. Extensive simulation has been conducted to evaluate the model under different conditions. A system level approach for incorporating the model in a real-life ad-hoc network testbed has also been discussed.

I. INTRODUCTION

Modeling and computing trust in ad-hoc networks has always been a challenging problem. It is very difficult to form a true and honest opinion about the trustworthiness of the nodes in such applications where the network is formed with near-strangers relying on one another for normal network operation without any prior knowledge of trustworthiness; these near-strangers can be engaged in malicious activities in different ways. This intricacy in trust computation, together with frequent topology change among nodes, quite often causes the whole network to get compromised or disrupted. Different malicious activities of the nodes can very well be misinterpreted as the regular erratic behavior of the wireless networks in general and ad-hoc networks in particular, thus making trust computation even more difficult.

II. STATE-OF-THE-ART

Modeling and computing trust for a distributed environment has been actively researched for quite a long time. Most of these distributed trust models combine direct and recommended trusts to come up with trust computations. A similar approach has been taken by the authors in [1]. They have suggested a recommendation protocol to formalize the propagation of trust information by issuing *recommendation request* and *recommendation messages*. However, the proposed model lacks any mathematical basis to calculate the trust values. The authors have not discussed how the trust values are computed and updated. In addition, the suitability of the model can be questioned when extended to a ad-hoc network.

A policy-based approach has been proposed in [2], based on a simple language to specify trust actions and relationships. The authors proposed a trust management system called PolicyMaker which binds Public Keys to the predicates

defining actions for which they are used. PolicyMaker accepts as input a set of policy statements, a collection of credentials and a description of a proposed trusted action. It then evaluates the proposed actions by interpreting the policy statements and credentials.

Watchdog mechanism [3], based on promiscuous mode operation of the ad-hoc nodes, has been the fundamental assumption in any trust computational model. In [4] the authors have proposed a trust evaluation-based secure routing solution. The trust evaluation is done based on a trust matrix stored at each ad-hoc node. The matrix consists of several parameters on which the final trust evaluation is computed. However, the mechanism for collecting the required parameters was not discussed by the authors. They also did not discuss the means of measuring communication success or failure pertaining to the parameter *experience statistics*. In [5] a similar concept has been proposed. The authors have defined different trust categories based on the effectiveness of the protocol functionalities.

Trust model based on subjective logic has been proposed in [8]. The concept of subjective logic was first proposed by Josang [9]. Subjective logic is “*a logic which operates on subjective beliefs about the world, and uses the term opinion to denote the representation of a subjective belief*” [9]. An opinion towards another entity x is represented by three states: *belief* [$b(x)$], *disbelief* [$d(x)$] and *uncertainty* [$u(x)$], with the following equality:

$$b(x) + d(x) + u(x) = 1 \quad (1)$$

The concept of subjective logic has been extended to propose a trusted routing solution in [8]. The opinion of a node about another node is represented in a 3-dimensional matrix representing *trust*, *distrust* and *uncertain opinions*. The opinions are updated by a positive or a negative feedback from the node in question. The proposed model, however, fails to protect the network from an internal attack, where a malicious node either refuses to forward the packets and duly authenticates itself to the source, or it cooperates with the source node and acts as a black hole.

In some of the earlier works on trust computation, incentive mechanisms have been proposed to prevent selfish behavior among the nodes. These mechanisms can be either reputation-based incentive mechanisms [10, 11], or price-based incentive mechanism [12]. In both mechanisms, nodes are given incentives to suppress their malicious intention in favor of the network. But nodes with malicious intentions always try

to find ways to bypass these incentive mechanisms. In our previous work we proposed a framework for modeling and computing trusts that take into account different malicious behavior of the nodes. Interested reader may refer to [13].

Recently there has been an effort to represent trust and confidence on a node by using Bayesian approach. Several statistical distributions have been considered to represent the belief or trust on a node, like Gaussian, Poisson, binomial, and beta. Out of all these, beta distribution has been used by some researchers as it is characterized by two parameters, which in this case, are the number of successful interaction and the number of failed interaction [6,7]. A standard Bayesian approach has been adopted by many where trust is represented as:

$$p(\text{belief}|\text{observation}) = \frac{p(\text{observation}|\text{belief}) * p(\text{belief})}{\text{normalizing constant}} \quad (2)$$

Where, $\theta = p(\text{belief})$ is assumed to follow beta distribution and is characterized by

$$\text{Beta}(\theta, s, f) = \frac{\Gamma(s+f)}{\Gamma(s)\Gamma(f)} \theta^{s-1} (1-\theta)^{f-1} \quad (3)$$

Where, s and f denote the number of successful and failed interactions respectively.

III.PROPOSED TRUST MODEL

One fundamental assumption underlying the above solution has been frequently questioned by experts. Since all proposed trust models rely on watchdog mechanism, they all assume the existence of symmetrical and bidirectional wireless channels. In practice, given the well-established fact that wireless channels are unstable, lossy, asymmetric, and more prone to interference and background noise, this assumption is far from reality. We carried out a series of simple experiments on a real-life ad-hoc network testbed that has proved beyond doubt the unrealistic nature of the assumption. Interested reader may refer to [16] for more details.

In this paper we have proposed a trust model that takes into account the probability of channel loss in a wireless medium. Our model is based on the social perspective of trusted community where it takes time for an individual to build up trust, while one single detectable misbehavior can bring it down. Successive trust build-ups depend on past experience, and several parameters should be taken into consideration. Although probabilistic distributions can be used to represent trust build-up and decay, it is always a concern how to interpret and use the trust values in making communication decisions. The following are the characteristics of the model:

- Slow trust build-up
- Fast decay
- Successive build-ups depend on past experience about the node behavior

Before presenting the model, let us take some time to revisit what is meant by trust. Trust has been defined as a belief level on another entity for performing a specific action.

However, when applied in the context of ad-hoc networks, trust can be perceived as a belief level on another entity for performing actions. So, the trust notation that we are going to use is $(\text{subject}, \text{object})$. The most fundamental issue when creating a trust computational model is how to incorporate the belief level in making communication decisions. More fundamentally, if an entity has belief levels of 0.8 and 0.7 on its two neighboring entities, can it be concluded that the entity with belief level of 0.8 can be more trusted? Furthermore, in the context of using probabilistic distributions to model trust, how will an entity interpret same trust values, one on the leading side and the other on the trailing side of the graph?

The basic principle behind the trust formulation depends on the watchdog mechanism proposed by Marti et al. in [8]. Each node, after forwarding a packet to its next hop neighbor, keeps a watch to find out whether the later is forwarding the packet. Each successful observation on the part of the neighbor's behavior is denoted by s , and each failed observation when the neighbor fails to forward the packet is denoted by f . Each failed observation can be the result of malicious behavior or because of the loss of the packet due to channel loss. Trust is assumed to be a continuous value between 0 and 1.

The trust model is shown below: (4)

$$T_n = \begin{cases} \min \left\{ 0.5, 0.5 \exp \left(-\frac{1}{\sqrt{d_n+1}} \sum_{i=i_0}^n x_i - f_n \right) \right\}, & \text{if } T_{n-1} < 0.5 \\ \max \left\{ 0.5 + 0.5 \frac{f_n}{n} \left(\frac{1}{n} \sum_{i=1}^{n-2} T_i \right), \right. \\ \left. \frac{s_n}{n} \left(1 + \exp \left(-\frac{1}{\sqrt{d_n+1}} T_{n-1} - \sum_{i=i_0}^n x_i \right) \right)^{-1} + \frac{f_n}{n} \left(\frac{1}{n} \sum_{i=1}^{n-2} T_i \right) \right\}, & \text{if } T_{n-1} \geq 0.5 \\ 0, & \text{if } (100p-1) \text{ consecutive failures, or } 100 \left(p + 2\sqrt{\frac{p(1-p)}{100}} \right) \\ & \text{failures out of 100.} \end{cases}$$

where,

n = total number of observations

T_i = Trust at the i^{th} observation, $i=1, 2, \dots, n$.

s_n = number of successful interactions till the n^{th} observation.

f_n = number of failed interactions = $n - s_n$

d_n = number of times in the past trust decreased to zero till the n^{th} observation

x_i = the i^{th} observation

i_0 = the position where T_n drops to 0

p = probability of channel loss

IV.SIMULATION AND ANALYSIS

There are three options for trust initialization when a node joins the network: a trust-your-neighbor approach where all nodes are initially trusted; a paranoid approach where no

node is trusted in the beginning; and a neutral approach. We selected the third approach, and started from an initial trust of 0.5.

Each observation x_i is either 1 or 0. It is a mixture of two distributions; one is Bernoulli with success probability p and the other is a degenerated distribution at 0, that is $x_i \sim (1-p_a) * \text{Bernoulli}(p) + p_a * 0$. In other words, with probability $(1-p_a)$, x_i is a Bernoulli realization with success probability p , and with probability p_a , x_i is 0, where p is the probability of channel loss and p_a is the probability of attack.

We used two sets of random numbers set.seed(128) and set.seed(256) in statistical software R to simulate 1000 independent observations $x_i, i = 1, 2, \dots, 1000$. The two conditions that make trust drop to zero are based on the empirical rules. Let us suppose that the failure is only caused by channel loss assuming channel loss is $(100*p)\%$. First, the probability of observing $(100p-1)$ consecutive failures is $p^{(100p-1)}$, which is very small. For example, if $p=0.05$, then $p^{(100p-1)}=6.25 * 10^{-6}$. Secondly, with roughly 95% chance, the observed proportion of failures among 100 observations is between $p - 2\sqrt{p(1-p)/100}$ and $p + 2\sqrt{p(1-p)/100}$.

The key idea in T_n is that if $T_n < 0.5$, it grows like an exponential function, and if $T_n \geq 0.5$ it grows like a logistic function. When trust is greater than 0.5, we use the weighted average of the logistic function and the average of the previous trust. The weight is the proportion of successes in the n observations. The simulation results show that if trust becomes 0, it either stays at 0 or grows slowly until enough successful interactions are observed. Even if trust is close to 1, if there are suspected attacks, instead of dropping slowly, trust drops to 0 immediately. If there is no attack, most of the time trust stays very high, and in the face of continuous attacks, will remain at 0.

We considered four cases: 3% channel loss without malicious behavior; 3% channel loss with 5% chance of malicious behavior; 5% channel loss without malicious behavior; and 5% channel loss with 5% chance of malicious behavior.

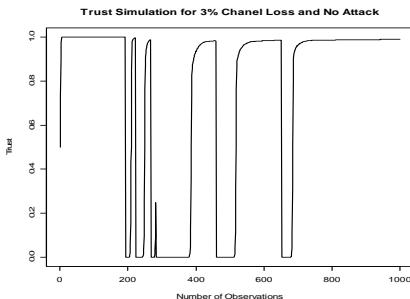


Fig. 1. Trust variation with 3% channel loss and no attack under random seed 128

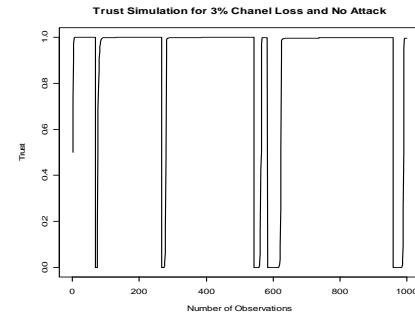


Fig. 2. Trust variation with 3% channel loss and no attack under random seed 256

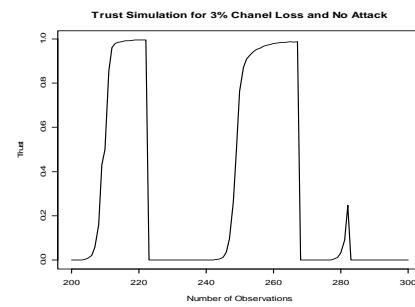


Fig. 3. Trust variation with 3% channel loss and no attack between 200 and 300 observations

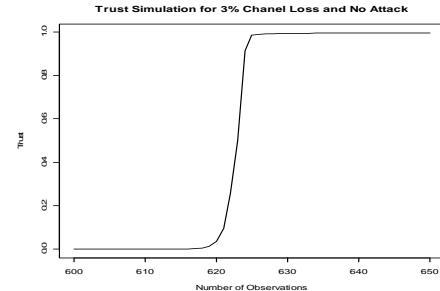


Fig. 4. Trust variation with 3% channel loss and no attack between 600 and 650 observations

Figs. 1 and 2 show the trust variation assuming 3% channel loss and without malicious behavior under two different random seeds. The drops are due to packet loss satisfying the drop conditions that we discussed earlier. Figs. 3 and 4 show the corresponding trust variations under similar conditions between 200 and 300 observations and 600 and 650 observations respectively. It can be seen that trust grows exponentially from 0 when it is less than 0.5, and it increases slowly when it is close to 1. The trust drops to zero when the drop conditions are satisfied.

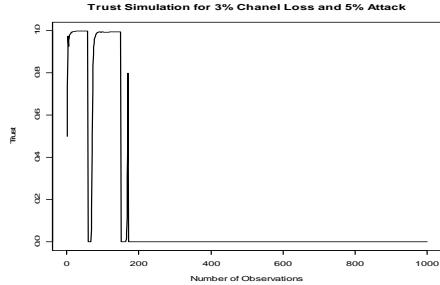


Fig. 5. Trust variation with 3% channel loss and 5% chance of attack under random seed 128

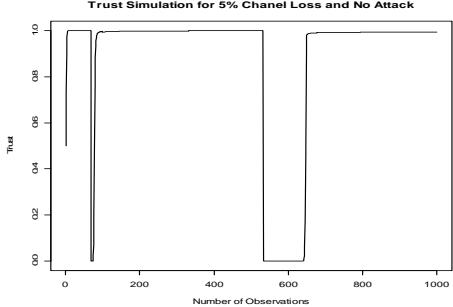


Fig. 8. Trust variation with 5% channel loss and no attack under random seed 256

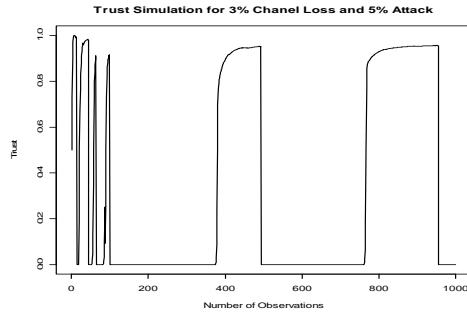


Fig. 6. Trust variation with 3% channel loss and 5% chance of attack under random seed 256

Figs. 5 and 6 shows that trust variation under 3% channel loss and 5% chance of malicious behavior under two different random seeds. It can be seen that under such condition the trust of a node remains zero most of the times going up occasionally after large number of successful interactions.

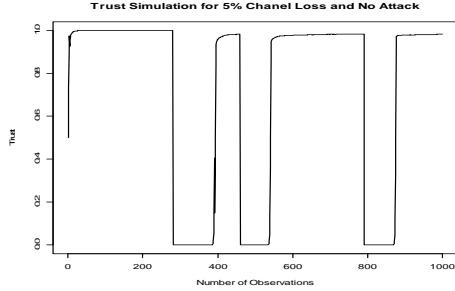


Fig. 7. Trust variation with 5% channel loss and no attack under random seed 128

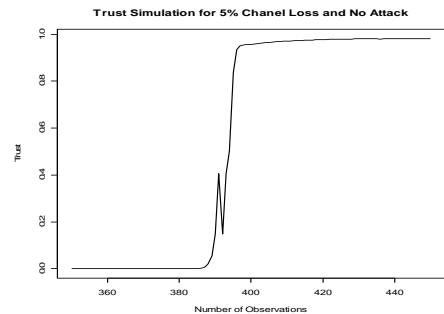


Fig. 9. Trust variation with 5% channel loss and no attack between 300 and 500 observations

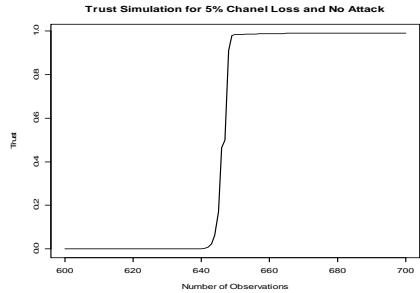


Fig. 10. Trust variation with 5% channel loss and no attack between 600 and 700 observations

Figs. 7 and 8 show trust variation under 5% channel loss and without malicious behavior under two different random seeds. Trust grows exponentially from 0, then increases slowly, and occasionally drops to zero under packet drops due to channel loss, and going up subsequently. Figs. 9 and 10 show the increase under similar conditions.

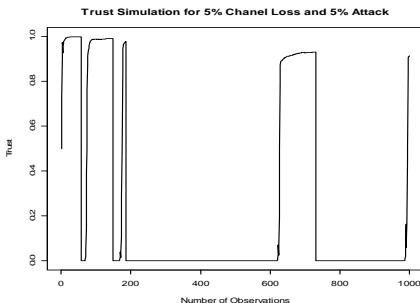


Fig.11. Trust variation with 5% channel loss and 5% chance of attack under random seed 128

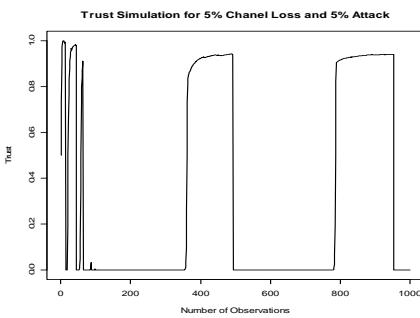


Fig. 12. Trust variation with 5% channel loss and 5% chance of attack under random seed 256

Figs. 11 and 12 show trust variation under 5% channel loss and 5% chance of malicious behavior under two different random seeds. It can be seen that under such situation trust of a node remains at zero most of the times.

V.CONCLUSION

We have proposed a trust model for wireless ad-hoc networks in this paper. A societal approach has been taken where trust is built up slowly, but decreases to zero on a single detectable misbehavior. Wireless channel loss probability has been taken into the model. Currently we are working towards a system-level implementation of the model on a wireless ad-hoc network testbed that we have created on our campus, as has been discussed earlier.

REFERENCES

- [1] Alfarez Abdul-Rahman & Stephen Hailes, "A Distributed Trust Model", ACM New Security Paradigm Workshop, 1997.
- [2] Matt Blaze, Joan Feigenbaum, Jack Lacy, "Decentralized Trust Management", inProc. IEEE Conference on Security and Privacy, Oakland, CA, May 1996.
- [3] Sergio Marti, T.J. Giuli, Kevin Lai and Mary Baker, "Mitigating Routing Misbehavior in MobileAd-hocNetworks", inProceedings of the 6thAnnual International Conference on Mobile Computing and Networking (MobiCom), Boston, Massachusetts, United States, August 06 - 11, 2000.

- [4] Zheng Yan, Peng Zhang, Teemupekka Virtanen, "Trust Evaluation Based Security Solution in Ad-hoc Networks", inProc. of NordSec 2003, Norway, 2003.
- [5] Asad Amir Pirzada and Chris McDonald, "Establishing Trust in Pure Ad-hoc Networks", appeared in 27thAustralian Computer Science Conference, The Univ. of Otago, Dunedin, New Zealand, 2004.
- [6] J. Li, R. Li, J. Kato, "Future Trust Management Framework for Mobile Ad-hoc Networks", IEEE Communications Magazine, April 2008.
- [7] Y. L. Sun, Z. Han, W. Yu, K.J.R. Liu, "Attacks on Trust Evaluation in Distributed Networks", inProc. of the 40thannual conference on Information Science and Systems (CISS), Princeton, NJ, March 2006.
- [8] Xiaoqi Li, Michael R. Lyu, Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad-hoc Networks", Proceedings 2004 IEEE Aerospace Conference, Big Sky, Montana, U.S.A., March 6-13 2004.
- [9] A. Josang, "A Logic for Uncertain Probabilities", International Journal of Uncertainty, Fuzziness and Knowledge-based Systems, vol.9(3):pp.279-311, 2001.
- [10] Sonja Buchegger and Jean-Yves Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Ad-hoc Networks)", inProceedings of the Third ACM International Symposium on Mobile Ad-hoc Networking and Computing (MOBIHOC '02), Switzerland, June 9-11, 2002.
- [11] Pietro Michiardi and Refik Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad-hoc Networks", inProceedings of the 6th IFIP Communications and Multimedia Security Conference, Portoroz, Slovenia, 2002.
- [12] JL. Buttyán and J.P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad-hoc Networks", Mobile Network and Applications (MONET), vol.8(5), pp 579-592, 2003.
- [13] T. Ghosh, N. Pissinou, K. Makki, A. Farhat, "A Framework for Computing Trust in Mobile Ad-hoc Networks", Mobile and Wireless Network Security and Privacy, by Makki, K., et al (Eds.), Springer, ISBN: 978-0-387-71057-0, July 2007.
- [14] AODV Implementation, (AODV-UU), Department of Information Technology, Uppsala University (Sweden), <http://core.it.uu.se/core/index.php/AODV-UU>.
- [15] Peter Reiher, et al., "Research Direction in Security and Privacy for Mobile and Wireless Networks", Technical Report to National Science Foundation, July 2006.
- [16] T. Ghosh, B. Pratt, "Routing Table Instability in Real-world Ad-Hoc Network Testbed", Advances in Computer and Information Science and Engineering, by Sobh, T. (Ed). Springer, ISBN 978-1-4020-8740-0, 2008.
- [17] S. Buchegger, C. Tissieres, J.L.Boudec, "A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks-How Much Can Watchdogs Really Do?", inProceedings of IEEE WMCSA '04, English Lake District, UK, December 2004.

Address Management in MANETs Using an Ant Colony Metaphor

A. Pachón, Universidad Icesi, M. Veiga, Universidad de Vigo, J.M. Madrid, Universidad Icesi

Abstract— Address management is a critical process in a network. Any node wishing to make part of a network must first obtain an address. Address management in MANETs poses particular challenges, due to their operation conditions, their dynamic topology and the unique events that take place inside them. This article presents an approach for solving the address management problem in this environment, using the self-organization and emergency principles governing the behavior of social insect colonies, particularly ant colonies.

Keywords—Address management, MANETs, Ant colony algorithms

I. INTRODUCTION

A MOBILE ad-hoc network (MANET) is an autonomous system, comprised by a set of mobile nodes using wireless links in order to communicate among themselves [1]. These nodes constitute a temporary network without the need of centralized management, and without the supporting services found in a conventional network.

Nodes move in a random pattern, and are able to organize themselves in an arbitrary fashion. Thus, the network topology can change in a very dynamic, fast and unpredictable manner.

A node must have a valid address in order to recognize other nodes, and be recognized by them as a valid peer, thus being able to participate in all the processes in the network. Approaches used to solve the address assignment problem in wired networks, or in infrastructure-mode wireless networks are not directly applicable in the MANET realm.

This article presents an approach to solve the address assignment problem in MANETs. First, it explores the node

A. Pachón is a titular professor with the ICT Department at Universidad Icesi, Colombia (email: alvaro@icesi.edu.co). M. Veiga is a titular professor with the Department of Telematics Engineering at Universidad de Vigo, Spain (email: mveiga@det.uvigo.es). J.M. Madrid is an associate professor with the ICT Department at Universidad Icesi, Colombia (email: jmadradi@icesi.edu.co)

roles in the proposed approach. Next, we analyze the lifecycle of a MANET. Then, the addressing strategy is discussed. The next section addresses the maintenance processes running in the MANET nodes. Finally, we present the experiments done in order to validate the approach, and their results. The article ends with an overview of other applications for the proposed approach.

II. NODE ROLES

A. Swarm Intelligence.

Nature has been an inspiration source for breakthrough solutions to several problems in engineering. In [2], the *swarm intelligence* concept is defined as a computational and behavioral metaphor, based in the group behavior of social insects (such as termites, bees and ants) and certain animals (such as birds and fish). This metaphor is used to develop several forms of “intelligence” (useful behaviors), which emerge to the colony level as a result of local interactions among the individuals making part of the colony.

In particular, we will study the behavior and the dynamics of an ant colony. As a result of the mutual cooperation happening among the colony members, the whole colony exhibits complex behavioral patterns, enabling it to carry on tasks that would be very difficult from an individual point of view. For example, when ants of some species require leaving the anthill in order to search for food, they move towards the source of food laying down a chemical substance known as a *pheromone*. That pheromone enables ants to communicate indirectly, by modifying the perception of the physical space they are in. This way of communication is known as *stigmergy*. When ants find no trace of pheromones along their path, they move randomly; on the other hand, when a trace of pheromone is found, ants tend to follow that trace. Thus, we can state that ants select the path to follow by using a probabilistic decision mechanism, biased by the pheromone amount present. As more and more ants follow the same path, they lay down more pheromone, generating a self-reinforcement effect, ultimately marking that path as the optimal trajectory towards the food source. This effect is

known as the *self-catalytic effect*. The process is completed by the action of the environment, which causes the evaporation of the pheromone after some time. This whole process (stygmergy, pheromone laying-down, pheromone evaporation) is being used in the telecommunications field, in order to solve the routing problem in a network.

B. Swarm Intelligence-based Systems: Design Characteristics.

The social behavior of the individuals making part of the colony can be emulated in a computational environment, in order to solve different kinds of problems. In [2], the author identifies the characteristics of a system designed after the swarm intelligence principles. Such characteristics will be used as design premises for an approach to handle address self-configuration in a MANET. In this environment, each colony member is implemented as a computational agent.

In [3], the author states that two terms, *self-organization* and *emergency*, define and characterize the self-organization methodologies needed for MANETs. Self-organization is defined as a process in which a system acquires a global behavior, as a consequence of multiple interactions in its lower levels. In addition, rules specifying interactions among the system components are executed based solely in local information, without any reference to a global pattern. In turn, the author defines emergency as the emergent behavior of the system, as a result of cooperation among its components.

The following are the most salient characteristics in a self-organized system, according to [4]: a) Control in a self-organized system is distributed and localized; b) Individual behavior (microscopic behavior) determines the system's resulting structure and operation (macroscopic behavior); c) Application of a simple conduct at the microscopic level causes a sophisticated system organization (emergent behavior); d) The system is able to adapt in a coordinated fashion to changes inside itself, or in the environment; e) The system tries to converge towards beneficial structures while avoiding undesirable ones; f) The system is reliable against failures, as a consequence of its intrinsic adaptability and distributed nature. This reliability implies the system is able to detect and correct failures without external help, and, in case of a component failure, the system degrades slowly; and g) A self-organized system is highly scalable. Thus, if a network is modeled as a self-organized system, the result will be a more scalable, flexible, failure tolerant network. At the same time, it will take less effort to manage and configure such a network, as a result of self-organization.

In our context, a MANET will be known as a *colony*. One or several colonies may exist in a determined geographical area. Network nodes move in a random pattern, thus generating a dynamic (time-varying) topology. These nodes may assume any of the following roles: a) Node in pre-birth status. A node

will assume this role just after its initialization, when it has no network address and is not participating in any process in the MANET; b) Queen ant. A node will assume this role when it has the responsibility of assigning network addresses. In our metaphor, the queen ant will create a new worker ant for the colony, each time she assigns a new address; c) Worker ant. A node will assume this role when it takes part in the collective, distributed process for network address assignment (working as an intermediary for the queen ant in the address acquisition process), and in the collective process for topology maintenance. In our metaphor, message exchanges will be used to spread information about the colony. Explorer ants will be used to search for information on ants of neighboring colonies, on the queen ant or on worker ants.

III. LIFECYCLE OF A MANET

In our context, a MANET will come to life once its first node completes its initialization. Colony initialization happens once the queen ant (the first ant in the colony) assumes the following responsibilities: a) Give an identity to the colony, by selecting a network identifier (NETID), and b) assume all the tasks of the colony. Later, as other nodes acquire addresses and thus, are "born" in the colony, the first worker ants are born, and functional specialization begins. When reaching this stage, the queen ant's sole responsibility becomes creating new individuals. The colony then begins its growth phase, with the birth of new working ants (as network addresses are assigned) and the death of old ones (when a node decides to leave the network). In this phase, it's possible for the colony to undergo unstable periods, as a consequence of network merge or partition processes, or as a result of the queen ant's death. Once these events are resolved, the colony will return to the growth phase, or it will become extinct if the queen ant is dead. Each time an ant dies in the colony, it has the possibility to be reborn as a new queen ant or as a new worker ant in other colony, and repeat its lifecycle.

IV. NETWORK ADDRESSING

As a design goal, our approach will operate independently of the chosen addressing scheme. However, we will use IPv4 without losing generality. It's worth noting here that mechanisms implemented in IPv6 favor the implementation of the proposed model. When obtaining a network address, a node undergoes two processes [5, 6]: a) Generation of a temporary address; b) Assignment of a permanent address.

Any new node wishing to make part of the network must use a temporary address first, in order to communicate with its direct neighbors. In the acquisition of a new address, a direct neighbor (a node already configured in the network) will play a crucial role, since it will be an intermediary between the

queen ant (responsible for assigning new addresses) and the node willing to get an address.

Our proposal assumes a centralized scheme for network address management. The queen ant will be responsible for managing the network address assignment table. However, the network address assignment process and the table maintenance process have a distributed, cooperative nature. In nature, the queen ant is ultimately responsible for creating new worker ants for the colony. Nevertheless, the worker ants are responsible for the collective, distributed execution of all the other tasks in the colony. Thus, the queen ant and the worker ants must be in communication with each other permanently. After the worker ants are born, the queen ant will need to know about their status, and eventually, repopulate the colony.

V. EVENT MANAGEMENT

A. Querying for Neighbors

Querying for neighbors is a key element in our approach. By means of this process: a) A new node trying to acquire a network address will find a node already configured in the network, which in turn will act as an intermediary to the colony's queen ant, and thus will allow the new node to acquire a permanent address; b) An already configured node will recognize and confirm, or otherwise correct the knowledge about its surrounding nodes.

B. Network Merge.

In our approach, each network is uniquely identified by means of a network identifier (NETID). This identifier is propagated in the neighbor reconnaissance process. When a node detects a NETID different from its own, it triggers a network merge event. Such event must be executed in a distributed, gradual fashion.

C. Network Partition

Worker ants are in charge of detecting network partitions. A worker ant sends explorer ants periodically, in order to check for the presence of the queen ant. If the queen ant does not respond when executing this procedure, that might mean: a) the queen ant has died, or b) the network has been partitioned. Both cases trigger a network partition event. This partition is executed in a distributed fashion, with incomplete and imprecise information.

VI. PROCESSES ASSOCIATED WITH A NODE

Once the node has acquired a role (as a worker or queen ant), it will: a) Listen to information requests from other ants in the colony; b) send information to the colony, by answering queries directed to it and/or generating queries on its own; c) respond to network merge or network partition events.

VII. EXPERIMENTAL RESULTS

The conducted experiments were aimed to fulfill three objectives: First, to verify the model's functionality; second, to verify the efficiency of the proposed solution; and third, to quantify the impact of the solution to the performance of user applications.

The verification of the approach functionality included tests for all the basic transactions in the model: a) colony initialization; b) a node checking for neighbor existence; c) a worker ant checking for the presence of the queen ant in the colony; d) a node in the colony detecting and managing a network merge event; e) a node in the colony detecting and managing a network partition event; f) the worker ants in the colony detecting and managing the event of the death of the queen ant; and g) the model's capability to assign a permanent address to a node striving to become a worker ant in the colony, in a cooperative and distributed fashion.

For the efficiency verification, we selected two metrics: a) Latency for network address self-configuration, i.e. the average time needed by a node in order to obtain an unique IP address in the network; and b) The scalability of the proposed solution, i.e. the impact on the performance of user applications as the number of nodes in the network increases.

To be able to evaluate the impact of the model on a typical user application, two tasks need to be conducted: First, to establish a baseline in order to have a reference point for comparisons; and second, to quantify the impact.

Several scenarios were defined in order to establish the baseline. In the first set of experiments, the *ping* command was used to quantify the network delay, in the following scenarios: a) Self-ping, using the same network interface; b) Ping to another node in a wired network; and c) Ping to another node in a MANET. The second set of experiments used a typical client/server application, and information exchange over TCP and UDP in a MANET. Finally, the third set of experiments was run in the NCTUns simulation tool [8], and simulated the exchange of information between two nodes. The obtained results for the TCP protocol are summarized in Fig. 1.

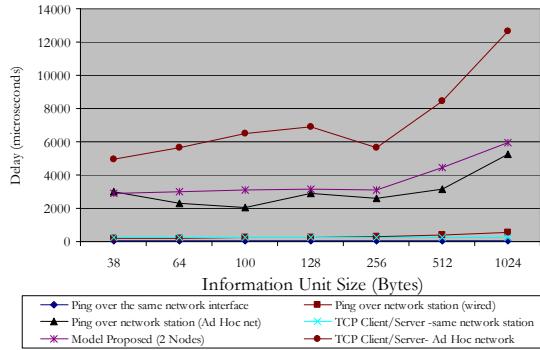


Fig. 1. TCP Delay in baseline scenarios.

In order to evaluate the impact of the proposed model on user applications, we used a typical client/server application implementing an echo service, and a set of nodes behaving according to the model. The TCP and UDP protocols were used in the transport layer, and several simulation runs were executed using different message sizes in the client/server exchanges. The sizes used were: 38 bytes (same size as the explorer ants, i.e. the messages exchanged by the nodes), 64, 128, 256, 512 and 1024 bytes. Finally, the number of nodes in the scenario also was adjusted, from 2 to 100.

In order to be able to correctly evaluate the model, its behavior should be well known. The proposed model has different behaviors in its initialization and stable states.

During the initialization phase: a) the nodes wishing to obtain a permanent network address generate a temporary address at random, and verify it for uniqueness. During the verification process, each node sends broadcast messages to all its neighbors; b) once they have a temporary address, the nodes may enter a contest in order to choose the queen ant. In this contest, one of the ants will be selected as the queen, and all the others will become worker ants, and will ultimately contact the queen ant in order to get a permanent network address. The contest is conducted by means of broadcast messages among all the involved nodes, so the traffic between such nodes is comparatively high in the initialization phase of the network.

During the stable operation phase: a) the nodes, now acting as ants, make a reconnaissance sweep in their coverage range, to search for neighbors. Through this process, ants are able to recognize other ants in their own colony, and ants in other colonies (which will trigger network merge events); b) the queen ant makes an inventory of the worker ants, and recovers the addresses of those ones who have left the colony and whose pheromone level has dropped to zero (this event does not generate network traffic); and c) worker ants query the

queen ant, in order to reinforce their pheromone amount, thus reaffirming their presence in the colony, and detecting the presence or absence of the queen ant. When a worker ant is unable to detect the presence of the queen ant, it assumes a network partition event has occurred. Traffic in this phase is considerably smaller than in the initialization phase. Thus, we propose three verification scenarios: a) initialization phase, b) a representative operation cycle in stable state, and c) sampling in some particular time instants during the simulation run.

In conclusion, the battery of verification tests considers: a) Three variables: Information unit size, number of nodes in the simulation run, and protocol type; and b) Three different time perspectives: Initialization phase, operation in stable state, and sampling in some particular time instants during the simulation run.

The activation of a node in the simulation scenario triggers three events: Acquisition of a temporary address, election of the queen ant, and acquisition of the permanent address, once the queen ant is elected. Considering the average time taken for each one of those three events, we can calculate the time elapsed in the contest for choosing the queen ant, and the average time elapsed for assigning an address to a worker ant. Knowing these values, the network address self-configuration latency can be calculated. Fig. 2 shows these results in graphical form. In first place, we can see the time elapsed for assignment of a temporary address grows slowly with the number of nodes. Applying a linear regression, we found that the presence of each additional node only poses a 0.61 ms overhead in the temporary address assignment process.

In second place, and considering the time elapsed for the queen ant election, we can see the relationship between the number of nodes and the time for election of the queen ant grows also linearly, with a slope somewhat higher than the previous event. The slope increases when 35 nodes or more are considered.

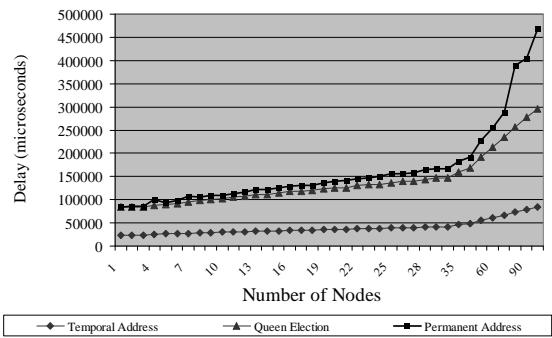


Fig. 2. Events in the initialization phase.

In third place, and considering the elapsed time for the assignment of a permanent address, the graph represents the workload of the queen ant during the massive node initialization process. This graph is very similar to the second one. However, the slope becomes even higher when 35 nodes or more are considered in the scenario. Another aspect considered to verify the model's efficiency is the overhead on user applications. In order to measure such overhead, we propose a scenario in which two nodes exchange information units, using a set of nodes running the proposed address management scheme as a middle tier. We use a client/server application implementing an echo service. As stated before, TCP and UDP protocols are used, and several information unit sizes are tested for each protocol. Each scenario is run with an increasing number of nodes in the middle tier. The overhead verification test is run once the colony ends its initialization phase and enters its stable phase. Results for TCP and UDP are shown in Fig. 3 and Fig. 4, respectively. Both graphs show that delay remains relatively stable for a fixed message length, and it has a slight increase as the size of the information unit increases. Thus, we can conclude the overhead our solution imposes over the network is low, and it remains stable along the different scenarios tested. Since low overhead on user applications was one of the design premises of the model, we can state the model behaves as desired.

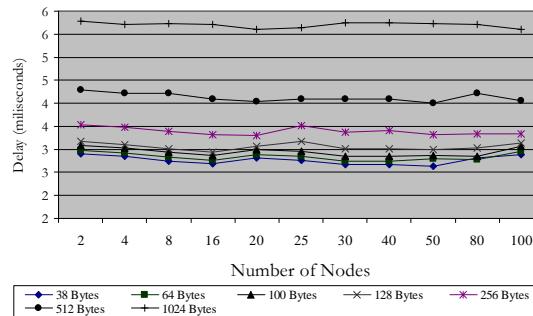


Fig. 3. Delay vs. Number of Nodes - TCP.

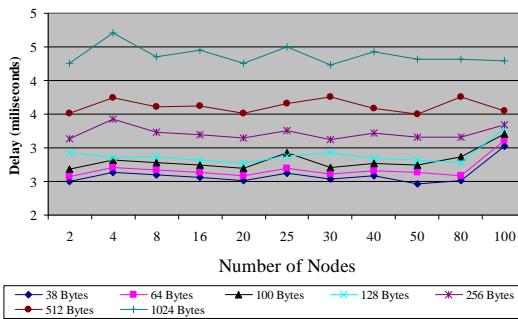


Fig. 4. Delay vs. Number of Nodes - UDP.

In order to see the difference in traffic in the model's initialization phase and stable state, we ran a simulation scenario consisting of 50 nodes, and checked the delay in a client/server exchange, both in the initialization phase and the stable state. TCP and UDP protocols were used, and 50 samples were taken. Obtained results for TCP are shown on Fig. 5; a similar behavior was observed in UDP.

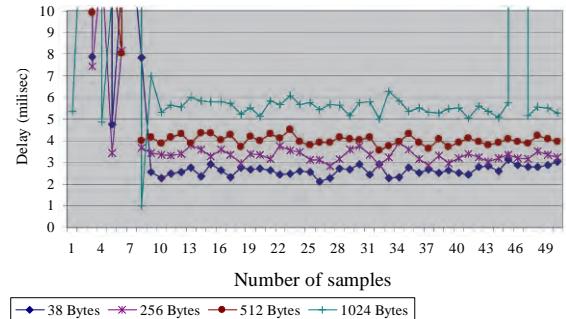


Fig. 5. Delay in Initialization Phase - TCP.

The graph shows a high peak on the first instants of network operation, and then a relatively constant behavior once the stable state is reached. The undesirable overload effect of the initialization phase remains confined in a very short time interval. It's worth noting the same behavior can be observed in the worst-case scenario (simultaneous, massive initialization of all nodes in the scenario). Results for the stable state phase (a typical operation cycle of the proposed model) is shown in Fig. 6.

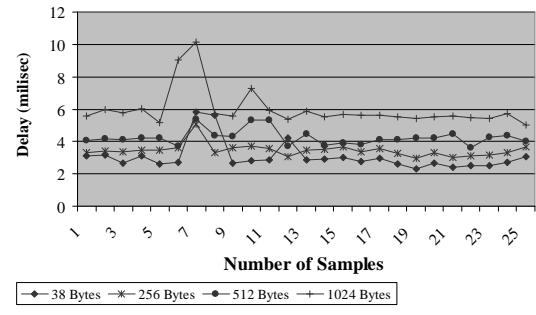


Fig. 6. Delay in Stable State - TCP.

The graph shows there is no significant impact on the delay a user application experiences once the stable state phase of the model is reached. The delay increases slightly with the increase in the information unit size. We ran additional tests in scenarios with 80 and 100 nodes; both showed the same behavior as above.

We also tested the model's capability to return to a stable state (a state such that only one queen ant exists in each one of the colonies deployed in the simulation scenario), after a queen ant dies, or a node initializes in the vicinity of multiple networks, triggering a massive network merge event. This allows us to study convergence to a desirable situation, one of the most prized features of self-organized systems.

We executed the proposed model in several scenarios, each one with a different node population. The event sequence that took place in all the scenarios was as follows: a) Simultaneous initialization of all the nodes; b) election of the queen ant in the colony; c) death of the queen ant (by inactivating the simulation scenario of the node in the queen ant role); d) election of a new queen ant; e) operation in stable state; f) death of the queen ant; g) election of a new queen; and h) operation in stable state. Table II shows these scenarios, along with the time of death (TOD) of the queen ants, and the convergence time for the model, in each case. Times are given in seconds.

Table II.
MODEL CONVERGENCE EVALUATION.

Number of nodes	TOD for first queen ant	Convergence time	TOD for second queen ant	Convergence time
3	10	t<2	-	-
5	5	t<1	25	t<1
10	5	t<2	25	t<2
15	5	t<2	25	t<2
25	5	t<2	20	t<2
30	5	t<2	20	t<2
40	5	t<2	20	t<2
50	5	t<2	25	t<2
100	5	t<2	30	t<7

In the event of the queen ant death, we can see the convergence time for the model stays almost constant as the number of nodes in the scenario increases. The convergence time increases only with a significant increase in the number of nodes (from 50 to 100).

Other initialization and movement scenarios were tested, in order to evaluate the capability of the approach to detect and manage network merge and partition events, ultimately returning to the stable state. The model complied with all the design premises in all the evaluated scenarios, converging in a relatively short time to a stable state after detecting the network partition / merge events.

VIII. OTHER APPLICATIONS

The proposed model may have many other applications, because of its capacity for generating spontaneously a node with unique features. For example, it could be used in the information security area for session key generation, digital

certificate generation, etc. The model's distributed management feature enables it to quickly reconfigure its behavior, using only local information. These features enable it to work in dynamic, changing environments, such as MANETs.

REFERENCES

- [1] Siva Ram Murthy, C.; Manoj, B.S. *Ad Hoc Wireless Networks: Architectures and Protocols*. Prentice Hall. May 2004.
- [2] Di Caro, Gianni. *The Ant Colony Optimization (ACO) Metaheuristic: A Swarm Intelligence Framework for Complex Optimization Tasks*. IDISIA, USI/SUPSI. Lugano.
- [3] Dressler, Falko. *Self-Organization in Ad Hoc Networks: Overview and Classification*. Autonomic Networking Group. Dept. of Computer Science, University of Erlangen. Germany. 2006.
- [4] Prehofer, Christian; Bettstetter, Christian. *Self-Organization in Communication Networks: Principles and Design Paradigms*. DoCoMo Euro-Labs. IEEE Communications Magazine. July 2005.
- [5] Perkins, Charles E.; Waikaka, R.; Malinen, J.; Belding-Royer, Elizabeth; Suan, Y. *IP Address Autoconfiguration for Ad Hoc Networks*. November 2001.
- [6] RFC 2462. Thomson S.; Narten, T. *IPv6 Stateless Address Autoconfiguration*
- [7] Jeong, Insu; Choi, Hyunjung; Joongsoo Maa. *Study on Address Allocation in Ad-Hoc Networks*
School of Engineering Information and Communications University. Daejeon, Korea. Proceedings of ICIS '05. IEEE 2005.
- [8] *NCTUns 4.0 Network Simulator and Emulator*.
<http://ns1.csie.nctu.edu.tw/nctuns.html>

Elitism Between Populations For The Improvement Of The Fitness Of A Genetic Algorithm Solution

Dr. Justin Champion, Staffordshire University
j.j.champion@staffs.ac.uk

Abstract – The use of Elitism within Genetic Algorithms is well documented allowing the best solution from any generation to be carried across to the new population allowing it to survive intact. This paper is looking at a similar concept of using Elitism across solutions rather than just each of the generations. The consideration is to use previous solutions to improve the fitness of the current population when applied to a similar problem. Usage within our context is for the placement of data object replicas within a cellular phone network for the benefit of the user base.

I. INTRODUCTION

Evolutionary computing as discussed in this paper relates to the use of Genetic Algorithms (GA) as considered by Holland [1] as a potential method of solving a defined problem. Genetic Algorithms will not generally produce an optimal solution in relation to the problem but they will usually generate a satisfactory solution within a prescribed timeframe. It is possible however that a GA solution does produce the optimal one via the nondeterministic nature of the algorithm having the correct solution initially, or results from an evolutionary process. They are particularly adapted to problems in which a guaranteed optimal solution can not be found within a short time scale

The use of GA focuses on an evolutionary solution to a problem whereby over time use of cross breeding procedures provides insight into current solutions. The initial concern involves encoding the information. This is required in order to produce a successful format capable of being used to evaluate the solution; also to store enough information to be meaningful. A useful illustration is provided by considering the problem encoded into a chromosome which, as in life, stores all relevant information. The most common form of encoding is binary, whereby a value is either '1' or 0. In this form numerous problems can be represented and evaluated for the best solution, e.g. light a street to a defined level whilst using the minimum amount of power. Each position in the chromosome can take one of two values, 0 or '1'. Refer to Figure 1 below which illustrates a chromosome having 23 positions. Each position of the chromosome '1' can be thought of a light turned on; conversely 0 indicates off.

001010101011010101110

Figure 1 Example Chromosome

Other methods of encoding information do exist which allow more information to be placed at each position at the expense in terms of complexity of evaluation. These encoding methods can use the alphabet, or a real number, indeed basically anything which can be used to represent information in a coherent manner. Hence a number of chromosomes will be generated to give a population, thus allowing crossover to occur between selected results. As discussed in [2] the number of items in the population has an effect upon the quality of the final result. Therefore the larger the population the more likely it is that an optimal result will be discovered. This larger population however will subsequently increase the complexity of evaluating each chromosome impacting upon the work of cross breeding. Nonetheless ultimately a point should be reached whereby the benefits and costs of calculation are evened out.

Clearly the evaluation needs to be carried out in an efficient manner to ensure a timely resolution to the problem. In the event of each chromosome taking '1' minute to evaluate with a population of 10 and a maximum of 100 generations, this could give maximum evaluation time of approximately 16 hours, 40 minutes. Hence this would remove the efficiency of using the GA in the first place. GA will produce a large number of results during the life of the algorithm needing evaluation. This evaluation allows for a fitness score (based on the quality) to be attached to each of the solutions. Therefore this means that the 'better' results can survive into the new population. The evaluation method utilised will depend on the problem being solved, with certain algorithms attempting to gain the minimum fitness score, whilst others are attempting to maximise the fitness. In addition, crossbreeding (also referred to as Crossover) focuses on swapping some of the genetic information from one chromosome to another. A number of methods are specified for the selection of the chromosome for crossover. One of the widely used methods is roulette wheel selection [3], where each member of the population has a probability of being crossed over which is proportional to the fitness score. In addition to the use of Elitism, detailed in DeJongs PhD thesis [4]. In this method, 'best' scoring pair will remain unaltered and copied into the new population. In the event of pairs of parents continuously breeding without one of them having an optimal solution the generations will then converge on a single answer early in the population. However the introduction of mutations to the current populations helps

to prevent this. Furthermore, in each of the generations some of the bits will be randomly mutated to a new value.

Genetic Algorithms are used for problems in which an optimal solution cannot be derived within a reasonable timeframe. Thus they utilise an alternative algorithm which considers all parts individually. This is discussed further in a paper by Braun [5], with regard to a comparative study of a number of algorithms inside a distributed environment for the placement of jobs. Within this study it was found that Genetic Algorithms consistently provided better results within a lower timescale.

PROBLEM DOMAIN

As discussed GA are useful when a quick solution needs to be discovered to a problem, in which using exhaustive searching would be prohibitive. The example previously used of street lighting is an example of this where a solution can be evolved quickly and the lights will be turned on. This may not be the optimal solution to the lighting but it is more than adequate to the needs. These quick solutions to problems can come from a large number of domains and example can be seen within [6], where a solution is required to a placement problem. The increased usage of data within cellular networks can be seen with the increased use of non voice services within the cellular network. The cellular networks as a new revenue stream are increasingly successfully being pushed towards increased data usage with the MDA recording a 25% growth in mobile internet usage in 2008 [7]. Within the work that is being looked at a controlling node would monitor the state of the network from the point of view of standard metrics such as error rate or latency. The controlling node could be a dedicated node as seen in Figure 2, or simply an additional task of an existing node such as the Serving GPRS Support Node (SGSN). Once this decision has been made that a monitored threshold has been reached with an object then a solution needs to be attempted in terms of placing objects within the network. The context for the network of this work is discussed further within [6] with cellular networks which are being used for data usage. The issue is that based on the current state of object requests a number of replicas could be placed within the network and the requests will then be pushed towards these.

The cellular network is a privately owned large scale network giving the possibility of placing replicas at suitable locations for the benefit of the end users. This is considered against a network such as the Internet which does not have a single owner of all hardware. Relocation of replicas within the Internet would require a potentially large number of organisations to agree and allows this on there hardware.

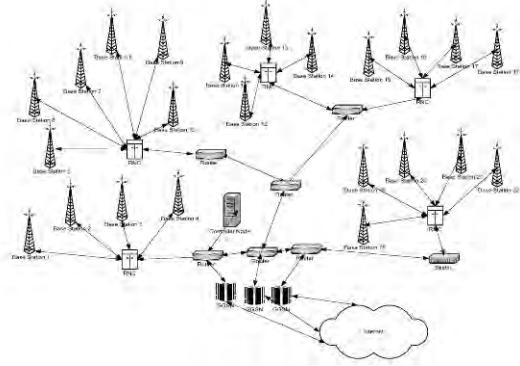


Figure 2 Example Cellular Network

Given a number of locations and requests taking place within this infrastructure a number of replicas should be located. The future requests then can be forwarded to this new source. The obvious example to use for this is small movie downloads which are transferred to your mobile such as movie trailers. The issue of placing these objects taking into account the benefits to the network and the overhead added to the infrastructure are given in [8]. GA is used in this context to quickly evolve a solution to the problem based on the state of the network at a time interval quickly to avoid any loss of satisfaction by the user base. Although the use of exhaustive searching would produce an optimal solution the time interval taken would be prohibitive. Due to the changing nature of data communications a long time spent calculating a solution would probably indicate that the pattern had changed again forcing a repeat of the process.

ELITISM

Within GA Elitism is popular way of keeping the best solution intact with no crossbreeding taking place. Within Elitism the best (Fittest) solution from each of the generations is copied across to the new population to prevent being lost with the cross breeding being run on this chromosome. The advantage of this is that the population can not get any worse in terms of the fittest solution as this will always be copied across unaltered. As discussed as part of the paper by [9] the use of Elitism allows for faster convergence to a result, by retaining the best solutions from the previous generation, although the result may be sub-optimal. The issue with the faster convergence upon a result is that the population moves towards solutions which may not be optimal, but no longer contains enough divergence to allow any change of to the chromosome. The use of mutation will allow some changes to the population, but at the low rate in which mutation is used it is unlikely to

have a significant effect on the final result, with $1/N$ given as the de facto standard used in most implementations [10].

ELITISM ACROSS SOLUTIONS

As discussed GA are ideal for a situation where a good solution is required within a short time frame but may not be optimal. Elitism is used within the generations with the best solution of each generation never being lost meaning that the population gets at least equal or fitter each generation. Taking the example given previously of placing the data objects within a network infrastructure, this is carried out based on the state of the network at a defined time, after this the network continues to operate. In the event of the controlling node then recording that the network has changed in terms of the patterns of requests which are being made then the controlling node will evolve a new solution based on the updated conditions.

This same consideration though can be given in a number of fields where a GA has been used to generate the solution and the conditions have changed slightly, such as queue processing or traffic management on a motorway network. The consideration of this paper is to look at using Elitism not only within the generations to achieve a quick convergence on a solution but also to use that Elite solution in any new problem which is defined. The first stage of the GA is to generate a randomised population to start off the problem and then to evolve these into a good solution at the end. The intention here is to copy into the population the unaltered solution from the last time that algorithm run. In the event of nothing changing since the last run in any environment then the end solution will be at least as good as previous result and could potentially be better due to the additional randomised population potentially having the capability of an improved result within it. The more interesting consideration though is what happens when the problem changes by a threshold. In an article by [11] there is a similar consideration given within it that a solution to a placement problem is evolved. This solution is based on access logs from a previous day with replicas placed within the network infrastructure. In the event of the access patterns changing from the previous days log a new solution would be evolved. In the article it is discussed about using an Adaptive Genetic Replication Algorithm (AGRA) which would use the previous solution to run a small number of generations given as 10 in an attempt to improve the solution.

A. GA Parameters

To look at this problem of using a previous solution to generate a new improved solution a GA was created with the following settings configured:

Population Size = 200
Number of Generations = 200

CrossOver Type = Roulette Wheel, Single Point
Mutation Rate = $1/N$
Elitism Used – Best chromosome pair copied across

The problem which is being looked for the purposes of this paper is a simple pattern matching problem. The program generates a random 1000 bit binary pattern. The number of generations has been kept small to allow the algorithms to run in a reasonable time and to prevent the problem being solved purely as a result of using a GA method. The fitness score is given as the number of bits which match the pattern generated. The originally generated pattern is then adjusted by a percentage as can be seen in the following figures and tables. Once the adjustment is made the GA method is then used to evolve a solution to match the new updated pattern.

B Results

The graphs below show the Elite and “Non Elite” results. Within the Elite algorithm the best result which is generated for matching the first pattern (0% change) is then copied across unaltered into all of the proceeding attempts with the pattern changing by a percentage. Within the “Non Elite” method just as normal GA methods a new population is randomly generated at the start of the problem and is then evolved into a solution.

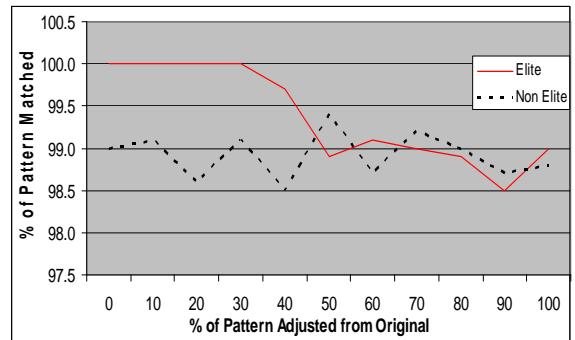


Figure 3 Highest Fitness Score Evolved

Figure 3 shows the best fitness score which was achieved by the methods across all of the attempts at pattern matching. As can be seen in Figure 3 the Elite method of using the best chromosome from the original pattern still produces the best result with up to 40% of the pattern changed from the original which is being copied into population. After this point the algorithm produces a similar result to the normal (“Non Elite”) method of generating a new randomised population at the start.

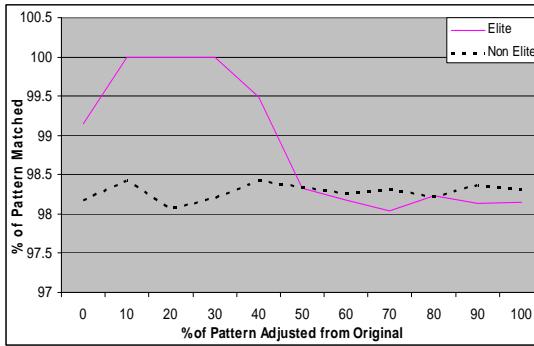


Figure 4 Average Fitness Score across all of the Populations

Figure 4 shows the average fitness score for each of the pattern adjusted sizes. The 0% adjustment for the Elite solution is less than 100% as can be seen below in Table 1, that two attempts were used to evolve the 100% solution. The first attempt matched 983 (98.3%) bits of the pattern.

Each of the runs had a number of attempts to match the pattern and the table below shows the number of the attempts which were used by each method up to the maximum of 10.

Table 1 Number of Attempts at Matching the Pattern (Max 10)

% of Pattern Adjusted	Elite	Non Elite
0	2	10
10	1	10
20	1	10
30	1	10
40	10	10
50	10	10
60	10	10
70	10	10
80	10	10
90	10	10
100	10	10

The work of [11] as shown earlier is similar to the consideration which is discussed here, with a previous good solution being used to feed into the population for the new problem. As can be seen in Table 2 the number of generations required depends upon the change within the problem domain, rather than a fixed small amount. Although with a small change only a small number of generations are needed as seen here with a 10% change a solution was discovered within one generation. The issue is that the change to a problem can not be predicted in a real world scenario such as the cellular network placement problem. A small change such as a

different read pattern may well end up adjusting the majority of the solution which was generated. As shown below in Table 2 with the 100% matched only results displayed as the problem changes the number of generations which are needed to match the pattern again increases.

Table 2 Average number of Generation to Match the Pattern using Elite Method

% of Pattern Adjusted	Attempts	Average Generations to Achieve 100% Pattern Match
0	2	130.5
10	1	1
20	1	59
30	1	165

As stated even a small change may have a large effect change on the actual solution and as such this paper would recommend leaving the maximum number of generations the same as you would with a standard GA ("Non Elite"). Table 3 shows the average fitness score which achieved for all of the population changes for 40% onwards. This value was selected as Elitism after 30% did not achieve a 100% pattern match. Although Elitism still produced the best result up to 50% where it produced a similar result to the "Non Elite" method.

Table 3 Average Population Matched across all solutions after 30% changed

	Elite	Non Elite
Average % Population Matched	98.36	98.32

As shown in Table 3 which is table version of the data which is shown in Figure 4 the overall average between the methods after 30% adjustment produces similar results. The Elite method only shows a 0.04% improvement which could easily be lost or improved due to the nondeterministic nature of the GA algorithm.

CONCLUSION

This short paper has shown that a previous good result can be used not only within the proceeding generations (Elitism) but also between solutions. As the problem changes the use of Elitism from a previous solution has been shown within the context of pattern matching to produce an improved result in terms of an optimal solution. This was shown in the paper if less than 40% (400) of the bits had changed. The use of this method still produced a good set of results even if the problem had changed to a further extent with a large change in the problem domain. The GA method then reverts to its normal operation in terms of removing the result after the 1st generation if it was not one of the fittest solutions. The work which is shown here will be useful for problems where the use of GA has been applied to a dynamic environments. The

particular context of this work is the placement of objects based on read patterns observed and replicas placed based on these logs.

FUTURE WORK

The work here will be built upon taking the same consideration of looking at the use of GA within placement decisions. A number of considerations can be built upon for this work with the implementation of the algorithm within a simulation environment such as OPNET [12] allowing for changes to the usage patterns to take place within the environment. The continuation of this work will look at the current solution to a problem and the previous solution and carry out a comparative analysis rather than accepting the answer which has been evolved. The overall consideration of all of this work is the usage of a GA which will carry out replica placement decisions within a dynamic network reacting within a time context which would allow a suitable network satisfaction for the majority of users. The satisfaction of the user base allows continued usage and ultimately the expansion of the network to exciting new services.

REFERENCES

- [1] Holland, 1975, "Adaptation in Natural and Artificial Systems", University of Michigan press, ISBN 0262581116
- [2] Gotshall, Rylander, 2002, "Optimal population size and the Genetic Algorithm", WSEAS 2002, February 11-15, 2002, Interlaken, Switzerland
- [3] Goldberg, Deb, 1991, "A comparative analysis of selection schemes used in genetic algorithms", Foundations of Genetic Algorithms, G. J. E. Rawlins, ed., pp. 69--93.
- [4] De Jong, 1975, "An analysis of the behaviour of a class of genetic adaptive Systems" Doctoral Dissertation, University of Michigan Microfilm 76-9381
- [5] Braun, T.D., Siegal, H.J., Beck, N., Boloni, L.L., Maheswaran, M., Reuther, A.I., Robertson, J.P., Theys, M.D., Biu Yao, Hensgen, D., Freund, R.F., 1999, "A comparison study of static mapping heuristics for a class of meta-tasks on heterogeneous computing systems", Heterogeneous Computing Workshop, 1999. (HCW '99) Proceedings. Eighth, 12 April 1999 Pages15 - 29
- [6] Champion, Yu, Sunley, 2006, "Ordering of Replicated objects within a cellular 3rd Generation Network using a Genetic Solution to place the Data", Proceedings of the Seventh Informatics Workshop, ISBN: 1-8514-3232-9
- [7] MDA , 2008, "MDA Stats Reveal Mobile Data Growth", <http://www.mobilemarketingmagazine.co.uk/2008/07/mda-stats-revea.html>
- [8] Champion, Rees, Sunley, 2003, "Placement of Data within a Third Generation network using a Genetic solution", PGNET 2004 Evolutionary Computation, I (1), pp. 25-49, 1993.
- [9] Chang, Ramakrishna ,2002, "Elitism-based compact genetic algorithms" Evolutionary Computation, IEEE Transactions on Volume 7, Issue 4, Aug. 2003 Page(s):367 - 385
- [10] Mühlenbein, H. and Schlierkamp-Voosen, D.: Predictive Models for the Breeder Genetic Algorithm: I. Continuous Parameter Optimization.
- [11] Loukopoulos, Ahmad ,2004, "Static and adaptive distributed data replication using genetic algorithms", Journal of Parallel and Distributed Computing archive, Pages 1270 - 1285 , ISSN:0743-7315
- [12] <http://www.opnet.com>, 2008

Adaptive Genetic Algorithm for Neural Network Retraining

C.I.Bauer; H.Yu; B.Boffey

Faculty of Computing, Engineering and Technology, Staffordshire University, Stafford, England

C.I.Bauer@staffs.ac.uk; H.Yu@staffs.ac.uk; boffey@liverpool.ac.uk

Abstract—Within cellular systems prediction has proven to be a potential solution to enhancing the handover procedure to guarantee constant Quality of Service to mobile users. By using historical route information, the future movement of mobile devices is predicted in advance with the aim to reserve resources prior to arrival of the device in a new cell. However, as the traffic patterns of devices in this environment change over time this needs to be taken into consideration when designing a prediction system. This paper presents a Neural Network-based movement prediction system for a cellular environment with a Genetic Algorithm-based retraining scheme using layer-based adaptive mutation to enhance the system performance in the presence of changing traffic patterns.

Index Terms—Cellular systems, genetic algorithms, handover, prediction

I. INTRODUCTION

Genetic algorithms (GAs) have over the years been applied to a variety of problems with great success. One area of application is the use of GAs for initial training and tailoring the weights of neural networks (NN) to a given problem. Research in this field has clearly shown that the use of GAs can be beneficial, providing equally good results in the fraction of the time required by conventional NN training techniques through backpropagation algorithm. Hence, they hold the potential to widen the field of applications NNs can be applied to. Traditional applications of NNs are based on systems that are likely to encounter information with the same characteristics that are fed to the NN for processing. During training of a NN this information is used to adjust the weights accordingly to produce the required response. While in most NN based systems the characteristics of the information are not likely to change much, retraining is rarely a consideration. However, depending on the problem to which a NN is applied, this may not necessarily be the case. This paper presents a GA based retraining scheme using a layer-based adaptive mutation approach for a NN based movement prediction systems in a cellular environment to enhance system performance under changing traffic patterns. Starting with a review of related research work combining GAs and NNs, the following sections will provide details of the NN-based prediction scheme, followed by the details and experimental results of a GA with layer-based adaptive mutation for NN retraining to the given problem.

II. RELATED WORK

GAs have been investigated and applied to a large variety of problems over the years due to their ability to search the

solution space efficiently delivering optimal solutions to problems to be solved. This ability has been exploited by numerous authors through combining GAs with other approaches including NNs and applications found in publications are manifold. The concept of NN retraining within this is not entirely new and was also recognised previously by authors in other subject areas, including NN-based prediction systems resulting in a variety of schemes suggested for different scenarios. Schemes that fall into this category include the approach by Nastac and Matei [1], as referred to and detailed in [2] and [3], that proposes a NN retraining scheme based on scaling the reference weights by a defined scaling factor. They can then be used as initial weights for a new training cycle to improve the network accuracy and the adaptable NN model for recursive non-linear traffic predictions of communication networks proposed in [4] that is based on estimating the NN weights to change them according to the current network conditions. However, the majority of authors concentrate on using GAs for implementing feature selection algorithms to reduce the amount of training data fed to the NN to shorten training times and enhance the network response as proposed in [5]; for the initial training of the NN weights as discussed in [6] and [7]; to identify a suitable network design for a given problem and periodically redesign the network structure and determine the network weights such as the load forecasting model [8] and the short-term traffic flow forecasting scheme in [9] for intelligent transportation systems (ITS). Although there are a large number of GA-based NN schemes for a variety of problems, the possibility of using GAs to retrain a network with a fixed network structure to maintain performance levels in the presence of changing conditions appears so far to have been mostly overlooked.

III. NEURAL NETWORK MOVEMENT PREDICTION

For the implementation of the NN-based movement prediction scheme, a cellular network with hexagonally shaped cells is assumed, with each cell within the network grid being surrounded by six neighbouring cells.

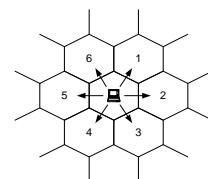


Fig. 1. 6-cell architecture

To identify individual cells within the network grid each cell has been assigned a unique index number. User movement in this environment can be expressed as a sequence of visited cells during an on-going call with the first cell being the cell in which the mobile initiated the call and the last one as being the cell in which the mobile terminated the call. As such, an active connection path can be presented as follows with $c(k)$ representing a cell in a path and with $k=0,1,2,3,\dots, n$, n being the cell in which the call was terminated:

$$\text{path} = c(0) + c(1) + c(2) + \dots + c(n)$$

$$\text{path} = \sum_{k=0}^N c(k) \text{ with } k = 0,1,2,3, \dots, n$$

In general each cell in a cellular environment that is part of an active call can be assigned a set of probability values that expresses the likelihood of a mobile device transferring to any of the six surrounding cells. In addition to this there is also the probability of the mobile device terminating the connection in the current cell without transferring to another cell. This can be represented by a probability vector \mathbf{p} with the components p_1, p_2, p_3, p_4, p_5 and p_6 for the transfer probabilities to the six surrounding cells and p_0 for the probability of terminating the call in the current cell. The probability values can be determined using knowledge of the movement pattern of either individual mobile users or all mobile users that have been accumulated over a period of time and reflect the user behaviour sufficiently.

$$\mathbf{p} = (p_0, p_1, p_2, p_3, p_4, p_5, p_6)$$

$$\text{with } p_n \geq 0 \leq 1, \forall n \text{ and } \sum_{n=0}^6 p_n = 1$$

Taking into consideration the previous movement of a mobile device during an active call by incorporating the previously visited cell that is part of the path, this can be adapted to include the probabilities of a mobile device moving from the previously visited cell into the current cell. Similar to the previous definition the probability of the mobile device moving from the previous cell into the current cell and then moving on to the next cell can be expressed as $p_{p,n}$, with p denoting the previously visited cell and n the next visited cell. For example, following the scenario with a mobile device moving to cell #80 from cell #79 and then moving towards cell #95 as depicted below can be expressed as $p_{2,1}$.

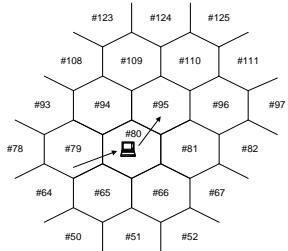


Fig. 2. Example of cell movement probabilities $p_{2,1}$

Following the previous notation using the numbers of the surrounding cells and including all possible movement probabilities this can be converted into a matrix containing 49 values that reflects the probability distribution of the mobile's movement:

$$p(p,n) = \begin{pmatrix} p_{0,0} & p_{0,1} & p_{0,2} & p_{0,3} & p_{0,4} & p_{0,5} & p_{0,6} \\ p_{1,0} & p_{1,1} & p_{1,2} & p_{1,3} & p_{1,4} & p_{1,5} & p_{1,6} \\ p_{2,0} & p_{2,1} & p_{2,2} & p_{2,3} & p_{2,4} & p_{2,5} & p_{2,6} \\ p_{3,0} & p_{3,1} & p_{3,2} & p_{3,3} & p_{3,4} & p_{3,5} & p_{3,6} \\ p_{4,0} & p_{4,1} & p_{4,2} & p_{4,3} & p_{4,4} & p_{4,5} & p_{4,6} \\ p_{5,0} & p_{5,1} & p_{5,2} & p_{5,3} & p_{5,4} & p_{5,5} & p_{5,6} \\ p_{6,0} & p_{6,1} & p_{6,2} & p_{6,3} & p_{6,4} & p_{6,5} & p_{6,6} \end{pmatrix}$$

with $p_{p,n} \geq 0 \leq 1, \forall p, n$ and $\sum_{p=0}^6 \sum_{n=0}^6 p_{p,n} = 1$

For the implementation of the NN movement prediction scheme this matrix is used to provide information on the previous movement history to a NN based on accumulated route information over a period of time. As this information will be different for each cell within the grid, the system has to maintain a separate probability distribution matrix for each cell. In order to allow the system to predict where the mobile device is moving to, two additional parameters are required, which are provided through previous movement steps for the current route. These values are expressed through two binary vectors to code the previous two directions of movement in accordance with the numbering scheme used for the probability values of the matrix as illustrated in figure 2. The seven possibilities were coded through a vector $\mathbf{v} = (v_0, v_1, v_2, v_3, v_4, v_5, v_6)$ with v_0 to indicate whether a call started in the current cell and $v_1 \dots v_6$ to indicate the previous direction of movement, with a value of 1 denoting activity and a value of 0 denoting no activity. As the previous movement is a known factor, each of the two previous movement vectors should only have one of the values set to the value 1. A similar vector was used for the prediction output of the NN with the slight modification that the value v_0 indicating whether the call ends in the current cell, $v_1 \dots v_6$ indicating the future movement direction, and that more than one value of the vector could be set to 1. The basic structure of the NN movement prediction system is depicted in the diagram below:

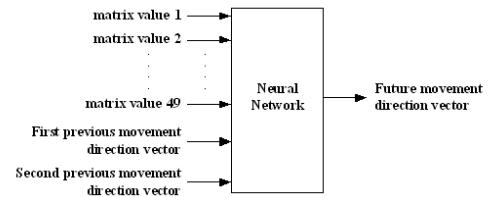


Fig. 3. NN prediction system with binary vectors

The network is trained with mobile device route information that has been accumulated over time and reflects the device's regular movement. Using this for training enables the NN-based movement prediction system to predict future movement, through the information in the distribution

probability matrix and the previous movement step, with a certain level of accuracy. However, as the movement patterns of mobile devices change over time this will affect the prediction success rate of the system. Without retraining with new route information that reflects the updated movement pattern of mobile devices the prediction success rate will drop over time. However, as this can be very time-consuming and inconvenient at times, GAs could be the solution to the problem, or at least provide a temporary measure to allow the system to continue with acceptable performance levels until full retraining is possible. This algorithm could be employed once the prediction success rate has dropped below a defined threshold to improve the prediction success rate.

IV. GENETIC ALGORITHM RETRAINING SCHEME

When applying GAs to a problem there are two main requirements as defined in [10]: firstly, a suitable way to represent the problem/solution needs to be found. Secondly, in order to be able to evaluate the solutions of each generation, a fitness function needs to be defined that allows for selecting the best solutions from each generation with which to continue the evolutionary process. In addition to this parameters such as population size, number of generations, how to implement the genetic operations and apply them to the defined chromosomes as well as any additional parameters that arise due to the scenario-specific implementation have to be identified. In the case of the given scenario using NNs in combination with GAs, two parameters are indirectly given through the design of the NN and the way its performance is evaluated. As the aim of the system is to successfully predict the next visited cell of a mobile device, the prediction success rate is used as the fitness function to evaluate individuals of a generation. In addition to the fitness function, elitism was used to carry across the best solution to the next generation without alteration. To represent the problem, the weight information provided through the trained network was encoded in a chromosome as depicted in the diagram below.

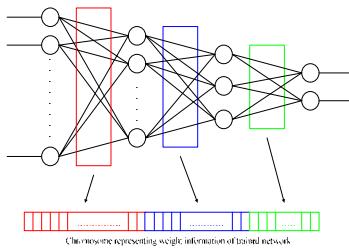


Fig. 4. Conversion of NN weight information into chromosome

This representation was chosen because the vital information of a trained network is stored in the weights for the connections between the different nodes and these are the parameters that determine the prediction success rate for a given traffic pattern. When the traffic patterns change this is the information that needs updating to maintain prediction performance levels.

To create the initial generation to start the GA the weight information of the trained and out-of-date NN was

used as a basis, as it can be argued that the ideal set of weights for the new traffic patterns are very close to the new optimal solution. Hence this holds the potential to further reduce training times. To generate the individuals of the initial population, each gene of the original set of weights was modified by a small, randomly selected value.

The remaining parameters used for the GA were a mutation rate of $1/N$ (with N being the length of the chromosome), single point crossover with a crossover rate of 50% using the roulette wheel selection algorithm with elitism as well as the population size of 180 individuals. The number of individuals selected for the next generations was set to 50% of the population size. These parameters were established through initial simulations to optimise the GA retraining approach. The simulations were run with 10, 20, 50 and 100 generations and the results for the parameter set optimised for the retraining approach compared against the standard settings as defined by DeJong [11]. The changing traffic patterns were simulated through data sets with varying levels of known regular route information ranging between 100%–50% in steps of 10% the NN had encountered during training. The remaining route information within the data sets consisted of unknown regular route information that had not been experienced previously. The results of the simulations can be seen in the diagram below which is showing the achieved fitness for the different number of generations averaged across the investigated data sets for ease of representation:

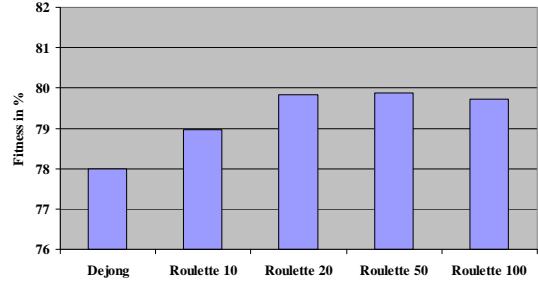


Fig. 5. Performance comparison

As can be seen from the diagram the results received for the customised parameter set using 10, 20, 50 and 100 generations for varying levels of new unknown regular route information within the data set clearly outperformed the standard DeJong settings for Neural Network retraining. However, although the simulation results showed that the GA retrained network can improve the fitness value compared to the original network without retraining, the results obtained were lower than expected. Therefore, the characteristics of the provided route information were investigated further to identify a reason for this. The weight information of networks trained with route information of 100%, 95% and 90% of regular known routes was investigated. It was observed that with each progressing layer of hidden nodes, the weight difference of the network trained with 100% regular routes compared to 95% and 90% as well as the network trained with 95% regular routes compared to 90%, increased, as depicted in the diagram below:

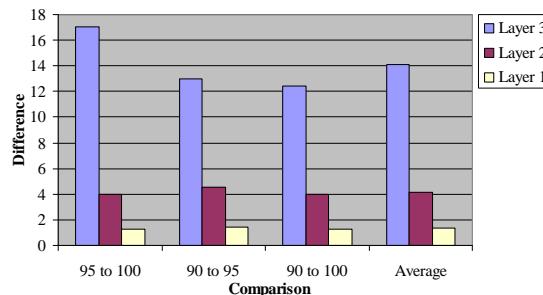


Fig. 6. Comparison of NN weight information

This suggests that when performing the genetic operations on the chromosomes it may be beneficial to distinguish between the different layers of hidden nodes contained within them. For this reason the application of the mutation operator was reconsidered to take into account the established pattern to investigate the effect of this on the GA results. The mutation operator was hence adjusted to reflect this by varying the amount the value of a gene is altered when mutation is applied. In the experiment if mutation was applied to a gene of the chromosome a random value ranging between 0 and 1 was multiplied by a multiplier value and then randomly added or subtracted after being scaled based on the hidden layer the gene belonged to. To investigate different multiplier values and identify the most suitable one this value was ranged between 1 and 200. The investigation showed that a value of 30 for the multiplier produced the best results. Based on this the previous simulations were rerun with 10, 20, 50 and 100 generations. The results of the simulations are depicted in the diagram below that is showing the performance in the same format as previously presented:

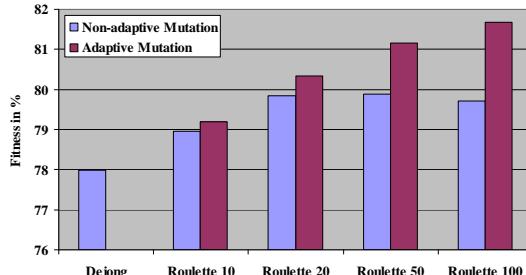


Fig. 7. Performance comparison with adaptive mutation

As can be seen from the graph, the layer-based adaptive mutation has provided significant improvement to the fitness. This indicates that there is a clear benefit to taking into consideration the structure of the weight information contained within a chromosome when applying the mutation operator.

V. CONCLUSION

In this paper a NN-based movement prediction algorithm for cellular systems was presented along with a GA-based retraining algorithm using adaptive mutation to assist the system in maintaining its performance levels in the

presence of changing traffic patterns. As simulation work has shown, the adaptive layer-based mutation approach provided further enhanced the system's capabilities to increase the prediction success rate (fitness) compared to the standard mutation approach. This is a strong indication that when applying genetic operators the structure of the weight information contained within a chromosome should be taken into account. So far only one of the two genetic operators has been investigated. It is expected, however, that using this gained knowledge on the crossover operator for this algorithm will yield equally good results to further enhance the GAs performance for the given problem. This research will therefore continue, in order to further investigate the potential of the layer-based genetic operators.

REFERENCES

- [1] Nastac, I.; Matei, R. "Fast retraining of artificial neural networks"; Rough Sets, Fuzzy Sets, Data Mining and Granular Computing, Springer-Verlag in the series of Lecture Notes in Artificial Intelligence; 2003; pp. 458.462; ISBN: 978-3-540-14040-5.
- [2] Nastac, I.; Costea, A. "A Retraining Neural Network Technique for Glass Manufacturing Data Forecasting"; International Joint Conference on Neural Networks", 2004; Proceedings 2004; Volume 4; 25-29 July 2004 Page(s): 2753 - 2758.
- [3] Nastac, I.; Cristea, P., "ANN Flexible Forecasting for the Adaptive Monitoring of Multi-Tube Reactor"; 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services; 14th International Workshop on Systems, Signals and Image Processing 2007; 27-30 June 2007; Page(s): 193 - 196.
- [4] Doulamis, A.D.; Doulamis, N.D.; Kollias, S.D., "An Adaptable Neural-Network Model for Recursive Nonlinear Prediction and Modeling of MPEG Video Sources"; IEEE Transaction on Neural Networks; Volume 14, Issue 1; January 2003 Page(s): 150 - 166.
- [5] Ichibuchi, H.; Nakashima, T.; Nii, M., "Learning of Neural Networks with GA-Based Instance Selection"; Joint 9th IFSA World Congress and 20th NAFIPS International Conference, 2001; Volume 4, 25-28 July 2001; Page(s): 2102 - 2107 vol.4.
- [6] Ling, S.H.; Lam, H.K.; Leung, F.H.F.; Tam, P.K.S., "A Genetic Algorithm Based Neural-Tuned Neural Network"; IECON '03; The 29th Annual Conference of the IEEE – Industrial Electronics Society, 2003; Volume 3, 2-6 Nov. 2003 Page(s): 2423 - 2428 Vol.3.
- [7] Zuo, Guoyu; Liu, Wenju; Ruan, Xiaogang, "Genetic Algorithm Based RBF Neural Network for Voice Conversion"; WCICA 2004; Fifth World Congress on Intelligent Control and Automation, 2004; Volume 5, 15-19 June 2004 Page(s): 4215 - 4218 Vol.5.
- [8] Zhangang, Yang; Yanbo, Che; Cheng, K.W. Eric, "Genetic Algorithm-Based RBF Neural Network Load Forecasting Model"; IEEE Power Engineering Society General Meeting, 2007; 24-28 June 2007 Page(s): 1 - 6.
- [9] Ji, Tao; Pang, Qingle; Liu, Xinyun, "Study of Traffic Flow Forecasting Based on Genetic Neural Network"; Sixth International Conference on Intelligent Systems Design and Applications – ISDA '06; Volume 1, Oct. 2006; Page(s): 960 - 965.
- [10] Núñez, Edwin; Banks, Edwin Roger; Agarwal, Paul, "High Performance Evolutionary Computing"; HPCMP Users Group Conference 2006, June 2006; Page(s): 354 - 359.
- [11] DeJong, K.A. and Spears, W.M. "An Analysis of the Interacting Roles of Population Size and Crossover in Genetic Algorithms," Proc. First Workshop Parallel Problem Solving from Nature, Springer-Verlag, Berlin, 1990. pp. 38-47

A New Collaborative Approach for Intrusion Detection System on Wireless Sensor Networks

Marcus Vinícius de Sousa Lemos ¹, Líliam Barroso Leal ¹, Raimir Holanda Filho ²

¹ {marvin, liliam}@edu.unifor.br

² raimir@unifor.br

Applied Computer Science Department
University of Fortaleza, Brazil

Abstract-Due to its characteristics, the Wireless Sensor Networks (WSN) are useful in a variety of applications such as environmental monitoring, surveillance, tracking, among others. Given the nature of such applications, where many are mission critical, the WSN become targets of possible attackers interested in harming the network. Among the defense mechanisms, the intrusion detection systems play important role in detecting attacks that can overcome the preventing techniques. This paper proposes a new collaborative and decentralized approach for intrusion detection system. Special nodes, called monitors, will be responsible for monitoring the behavior of neighbor nodes. The malicious activities evidences discovered by each monitor will be shared and correlated with the purpose of increasing the accuracy in detection of intruders. Experiment conducted by simulation show that our solution is effective in reducing the false positives.

I. INTRODUCTION

Typically formed by hundreds of small devices (called nodes) operated by batteries, the Wireless Sensors Networks (WSN) use a low-range wireless communication, besides severe restrictions in several other resources such as energy, bandwidth, and capacity processing. Often, these nodes are scattered in a wide area, making it difficult or even impossible to restore a damaged node or a depleted battery.

Because the sensing ability of the nodes, the WSN have applicability in several areas such as environmental monitoring, surveillance systems, health-care, among others. We realize that many of the applications of WSN are mission critical, making them a target to potential adversaries interested in harming the sensing level or even overthrow the entire network. This fact is exacerbated by the very nature of the deployed network. Often, nodes are deployed in a remote or hostile area, making them unprotected and susceptible to physical attacks [1]. Thus, the networks must be deployed with some security scheme. However, the extra consumption of energy caused by the implementation of security functions should be rewarded by the economy gained to treat and prevent attacks.

The solutions proposed in the literature generally fall into two main categories: prevention-based techniques and detection/retrieval techniques [2]. The preventing techniques try to prevent an intruder to access the network, usually through some encryption mechanism. In the category of detection, the nodes behavior are tracking in real time (or close

to real). Once the malicious node is discovered, a recovery mechanism could be used in order to remove the intruder and restore the normal network operation.

The prevention mechanism is the first line of defense in a WSN, ensuring some security principles, such as confidentiality, integrity and authentication. However, prevention, especially in WSN, is not sufficient to guarantee the security of the network. In many applications, the sensor nodes are deployed in open areas, making it possible an attacker to gain physical access to a sensor and retrieve the stored data, including cryptographic keys. Thus, it is clear the importance of an intrusion detection system (IDS) capable of detecting malicious nodes that have broken down the network prevention techniques. In addition to prevent greater damage on the network, the intrusion detection system can be used to collect information related to the attacks techniques, helping to develop prevent systems [3].

The standard procedure in the intrusion detection is to compare the behavior of the current system with the normal behavior in the absence of any intrusion [4]. Starting from this basic premise, three models of detection can be set. The first is based on anomalies. Through extensive training in order to characterize the network traffic, the system can detect when the network deviates from the normal behavior. However, it is a hard task characterizing the normal behavior and normally it generates a great number of false alarms (or false positives).

The second model, based on signatures, on the other hand, is based on known patterns of non-authorized behavior. This behavior is often determined by the network traffic. In networks systems, an intrusion detection system can analyze the traffic looking for packages or set of packages that, based on certain signatures, are classified as malicious. Signature-based detection is effective against attacks and produces few false alarms. However, a major problem in this kind of technique refers to the fact that it's unable to detect classes of attacks whose signature is unknown.

The third approach, actually a combination of previous ones, is called "based on the specification" [5]. This approach uses specifications that describe the behavior of the planned system. Thus, by monitoring the execution of programs, it is possible to detect malicious nodes by observing deviations in the behavior based on the specifications.

In an IDS, the nodes that are responsible for the monitoring functions are called monitors (or agents) and, within a wireless

network, behave themselves as watchdogs [6], receiving and processing the packages sent by their neighbors.

In our work, we used the model based on specification. Considering that the monitors are able to receive packets sent by their neighbors and using well-defined rules, they can identify which neighbors are performing tasks that are beyond the behavior expected.

However, since the monitors have only a partial view of the network (only their neighbors) it is higher the probability of false positive rates [3]. Aiming to reduce the amount of false positives, we propose a decentralized collaborative intrusion detection system. In this system, each monitor will share their inferences with other monitors, in order to increase the accuracy in detecting malicious nodes.

The rest of the paper is organized as follows. Section II presents the related works. Section III describes the operation of the proposed IDS in general, while section IV depicts the process of collaboration between monitors. In section V we have described the experiments of our simulation. Section VI analyses the results. Finally, section VII presents the conclusion and future work.

II. RELATED WORKS

In last years, many studies about intrusion detection systems in WSN were presented, however fewer of them treating collaboration between monitors.

In [7] was proposed a technique named as Spontaneous Watchdogs. This technique is effective in networks with high quantity of deployed sensor nodes in the region. For each package moving on the network, there are a number of nodes that are able to receive this package, in addition to the package relayed by their next hop. Consequently, all nodes have a chance to activate their global agents in order to track these packages.

Pires, Figueiredo, Wong and Loureiro [8] proposed a mechanism based on signal and power of geographic information to detect malicious nodes that are conducting Hello Flooding and Wormholes attacks. To perform the detection, the system compares the power of received signal with its expected value. The expected value is calculated using the geographic information and configuration of the transceiver. It also proposed a protocol to spread information about the malicious nodes. The great disadvantage of this proposal is because it is limited to only two types of attacks (Hello flooding and Wormholes).

A distributed IDS based on groups was proposed in [9]. The network is divided into several groups where each group is composed of nodes that are close to each other and share the same capacity of sensing. Each group will be chosen to execute the algorithm of IDS. During the execution of a particular group, each sensor will monitor the behavior of the nodes in the same group. If the sensor node sees a node performing an abnormal behavior, it will send a warning to all nodes about the suspicious node. If the amount of warnings about the suspicious node reach a limit, the network then concludes that the node actually are doing any illegal activity.

In [3] was proposed a decentralized intrusion detection system. The IDS uses the approach based on the specification, aiming to be adapted to a wide range of applications. From the unique features of WSN target, provided by the network designer, you can select rules that can detect possible attacks related to these characteristics. These rules will be executed by the monitors spread throughout the network in the packets sent by neighbors nodes. The main goal of this work is to create a methodology for the assembly of specific IDSs and that this methodology could be automated. Another main feature related to that IDS is the amount of attacks that can detect: Black Hole, Selective Forwarding, Repetition, Delay, Data Alteration, Interference, Wormhole, Negligence, and Exhaustion. However, there are some problems in this work such as not taking into account attacks to the monitors or the cooperation between the monitors. Through cooperation between the monitors it could be possible to obtain a correlation between the visions of each of the monitors, reducing thus the amount of false positives and negatives.

III. THE PROPOSED DESCENTRALIZED AND COLLABORATIVE IDS

In our IDS, special nodes called monitors nodes (or simply monitors) will be responsible for watch the entire network, in a distributed fashion. We use the work described in [3] as the main reference of our IDS. Each monitor, located somewhere in the network, will be in charge for monitoring a sub-part of the network, the nodes neighbors to it. From the traffic of the neighbor nodes, the monitor can infer which ones are behaving out of expected. This inference is possible because the system stores a set of rules that specify the nodes normal behavior. The intrusion detection is done in a time near to real. The monitor stores, in a fixed size buffer, each packet that it listen (Phase 1), and when this buffer is full, the rules are applied (Phase 2). In this phase, each package will be analyzed, taking into account the rules selected. Below, we list all the rules defined in [3] with a brief description.

1. **Interval Rule:** a failure is raised if the time past between the reception of two consecutive messages is larger or smaller than the allowed limits.
2. **Retransmission Rule:** a failure is detected if a node not forwarded a message when it should.
3. **Integrity Rule:** the data should remain unchanged in relay.
4. **Delay Rule:** the retransmission of a message by a monitor neighbor must occur before a defined timeout.
5. **Repetition Rule:** the same message can be retransmitted by the same neighbor only a limited number of times.
6. **Radio Transmission Range:** a failure is detected if the monitor receives a message from a node that does not have enough power radio.
7. **Valid Destination Rule:** verify if the destinations are valid ones.

8. **Valid Origin Rule:** verify if the origins are valid ones.
9. **Jamming Rule:** the number of collisions associated with a message sent by the monitor must be lower than the expected number in the network.

If any rule is violated at a frequency higher than expected due to natural failures of the network, an indication of abnormal behavior is generated (Phase 3). However, in our work, the monitor will publish the information generated in Phase 3, before inferring about a malicious node. Hence, the information can be correlated with the informations published by others monitors. In this way, the likelihood of false positives occurrences is lower. This collaboration is important because, by results of simulations in [3], it was shown the generation of false positives due to the lack of correlation between the visions of monitor nodes. Fig. 1. depicts a situation where a false positive was generated due to a lack of collaboration. Assuming that in the network there is no treatment for the repeated messages, the N node will be charged of running the Repetition attack by the monitor M1, although it is not performing the attack. Once node N is in the route of the real attacker, node I, the node N simply relay the repeated messages it receives. The monitor M2 is adjacent to I and is detecting it as malicious. If M2 could, in some way, inform the others monitors that the node I is also conducting the attack, it would be easy to infer that N is not malicious.

IV. COLLABORATION BETWEEN MONITORS

Based on the work defined in [10], the monitors nodes will be held together through a peer-to-peer architecture where the evidence of attacks will be shared among the participants in order to carry out a correlation between the visions of individual monitors. For every rule, there is a monitor responsible for the correlation of information generated by other monitors on that rule. In this way, we can define two type of monitor in our solution:

- **Common Monitor:** The monitor responsible for watch its neighbors, looking for broken rule evidences.
- **Supervisor Monitor:** A specialized monitor responsible in correlate the evidences discovered by other nodes. It is important to say that the supervisor monitor still execute the Common monitor functions.

For example, suppose a system where there is a supervisor monitor M1 responsible for the Repetition rule. If two other monitors, M2 and M3 discover a node that is violating the Repetition rule, they should forward such information to M1. Thus, M1 can check if there is any correlation between these attacks, detecting, more precisely, the source of the attack. In this paper we do not address how the network should react to the attacker detected. We left for future work the investigation of techniques of reaction that could be integrated in our IDS.

Communication between the monitors will be conducted using an encryption scheme (Snep [11], for example) in a way

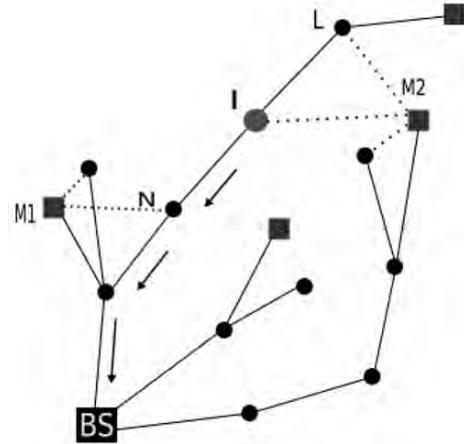


Fig.1. False Positive: Repetition Attack

that common nodes or intruder nodes do not have access to the content of the message.

Below we give more details about our collaboration system.

A. The Collaboration Process

Each WSN being monitored by an IDS will be formed by a set of monitors $M = \{m_i \mid i = 1, 2, \dots, p\}$, where each node monitors its neighbors. In this way, each monitor becomes a peer in a peer-to-peer system. Let R be the set of rules for the detection system, $R = \{r_i \mid i = 1, 2, \dots, q\}$ and R' a sub-set of R associated to each m_i . If there are more monitors than the amount of rules, some of them will not be responsible for any rules. If $R' = \emptyset$ than the monitor is a Common one, otherwise it is a supervisor. In our system, every node has the capability of play the supervisor role, but only if it has any rule associated to it.

When the phase of intrusion detection (Phase 3) ends, each Common monitor subscribes about the suspect node detected to the supervisor monitor (the one responsible for the violated rule). The subscriber monitor sends, along with the subscribe message, more information about the malicious activity. Thus, the supervisor will be able to correlate the received messages. After processing the rules of correlation, all supervisor monitors should publish a list of malicious nodes to the network (algorithm 1).

The sharing of information between the monitors will be done through a publish/subscribe mechanism due to its advantages in relation to our proposal [12]:

- **Decoupled in Space:** Publishers and subscribers do not need to be aware of the each other, indeed they can completely forget their identities.
- **Decoupled in Time:** Publication and reporting of data can occur at different periods of time.
- **Decoupled in Flow:** Interactions between peers may happen asynchronously without blocking.

Algorithm 1 – Subscribe processing algorithm

```

while message is received do
    if message == subscribe(my_type_of_attack) so
        buffer <= message
        if buffer is full so
            run correlating process
            subscribe malicious nodes
        end-if
    end-if
end-while

```

B. Communication through DHT

Each monitor must send informations about the malicious nodes detected to the supervisor monitor, responsible for the rule violated. However, how a monitor knows who is supervisor for a specific rule? Based on [10] we adopted a communication model based on Distributed Hash Table (DHT).

We use the Chord [13] protocol as the base of our DHT mechanism. We choose Chord because it can provide a mechanism to map a key to a node with *consistent hashing* [14].

During the establishment of the network, each monitor and selected rule for the IDS will receive a random ID (with k bits). The monitors must store the IDs of the rules in some internal data structure. The monitors in M must be organized on a logical ring based on the IDs of each monitor, in a clockwise order. When a monitor wish to send a report to the monitor responsible for the Repetition rule, with key a_i , the message is routed to the first monitor m_i whose identifier m_i is equal to or greater than the value of the rule key (a_i). The size of k must be sufficient to meet all the rules and monitors in the network.

Consistent Hash has several benefits [13]. First, all monitors are responsible for approximately the same number of keys so that a preliminary load balancing can be achieved. Moreover, when the m -th node join or leave the network, only a fraction $O(1/m)$ of the total load is moved. These benefits help to ensure the scalability of our system. For instance, if a supervisor crashes down (for any reason) another monitor will assume the rules associated with the previous monitor immediately.

C. Correlation Process

We saw in previous section that the supervisor monitor must correlate the subscribe messages in order to find some relation about them. This is done through a process called correlation.

For each rule, there are several steps that the supervisor must perform with the received subscribe messages.

The monitor stores every received subscribe message in a buffer. When the buffer is full, the monitor starts the steps of correlation between such information. These steps are specific to each type of attack. Algorithm 2 illustrates the correlation process of the repetition attack [3].

Due to the problem of storage, we use a minimum of

Algorithm 2 – Repetition Attack detecting algorithm

```

separate packets with the same id and origin in groups
for each group do
    for each packet in the group do
        if flag sure is true so
            store the node id in an array of malicious
        else
            node_id = packet.node_id
            mark_malicious(node_id)
            origin_id = packet.origin_id
        for each packet in the group do
            if element.destination_id = origin_id
                unmark_malicious(node_id)
            end-if
        end-for
        if node_id mark as malicious, so
            store the node id in an array of malicious
        end-if
    end-for
end-for

```

information to be exchanged between the monitors, such as: the message number, broken rule, immediate origin, immediate destination, source, and clock.

V. SIMULATION

In this section, we present comments about the scenario used, and the experiments held.

A. The Network

Here, we illustrated the main characteristics of the elements of the simulation held:

1) Features of the network

We consider a flat, fixed network, which nodes were distributed in random way. Each node has a unique identifier and a fixed range radio. There is no treatment for repetitive messages, allowing malicious nodes perform Repetition attack. We left for future work the analysis of the detection of other types of attacks.

2) Types of Nodes

The network is comprised of the following types of nodes:

- **Common:** Node that has the capability of sensing and routing. Captures information from the environment and forwards to the Base Station.
- **Monitor:** Node responsible for the monitoring of its neighbors by listening in promiscuous mode. Stores relevant information and applies rules to them.
- **Intruder:** Node that will carry out attacks inside the network. In this scenario, we are considering only the Repetition attack.
- **Base-Station:** In this proposed scenario, the base station works only as a destination for all messages

3) Messages: We consider only attacks on data messages.

We left for future work the analysis of attacks on other types of messages, such as configurations and routing establishment messages.

4) Distribution of Nodes: The scenario consists of a network with 100 nodes distributed in a random way, as illustrated in Figure 2.

The nodes with different functions are represented with different formats. In the scenario, there is a base station, two malicious node performing Repetition attack, 27 monitors and the rest are Common nodes. We are using only the Repetition rule from the rules defined in [3]. In Fig. 2 we have the base station labeled as BS. The intruder nodes are I1 and I2. Near the intruder I1, there are two monitors: M1 and M2. M1 is also neighbor from N1 (son of I1 in routing tree) while M2 is also neighbor from N2 (father of I1 in routing tree). There is no monitor neighboring to I2 and its father or son. There is also the monitor M3 neighbor to the father of I2 in the tree routing.

B. The Simulator

In our experiments, we used the simulator Sinalgo [15]. Sinalgo is a framework, written in Java, for testing and validation of algorithms for network. Unlike other tools such as NS2 [16] which allows the simulation of various layers of the stack of network protocols, Sinalgo focuses on the verification of algorithms and abstracts from the underlying layers.

C. The Experiments

To measure the effectiveness of our collaborative system we have defined two scenarios:

1) Detection Intruder I1: For this scenario, we highlight some nodes. M1 is adjacent to I1 and his son (N1) in the routing tree, as M2 is adjacent to I1 and his father (N2) in the routing tree. N4 is the father of N2. We consider, in our experiment, that N1 will send a package to the base station and the intruder node I1 will repeat this package continuously every 40 turns. First, we ran the simulation without the collaboration between the monitors and later with the collaboration active.

2) Detection Intruder I2: In this scenario, we are considering a message sent by node N5. I2 will repeat this package continuously every 40 turns. In the route between N5 and the base station there are 3 monitors (M3, M4, M5), but none of them are N5 neighbors. Like the previous experiment, we first ran the simulation without the collaboration, later with the collaboration active.

VI. RESULTS

In this section, we analyzed the results of our experiments in the two proposed scenarios.

1) Detection Intruder I1: First, we ran the simulation without the collaboration. In this case, two nodes were accused of performing the Repetition attack. M1, M2, M3 correctly detected the malicious node, while M4 and M5 falsely accused the node N2. This happened due to the fact that M4 and M5 were not able to listen the corresponding message heard earlier by N2 for not having enough radio range to node I1

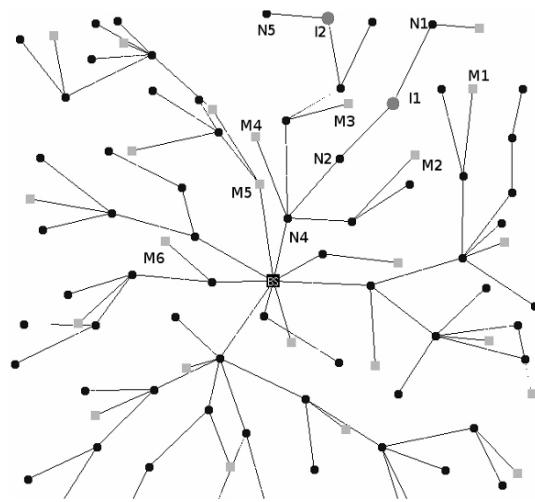


Fig. 2. Sensor Network with 100 nodes

(Fig.2). Then, we ran the simulation with the collaboration active.

In the proposed algorithm, a monitor will infer about the action of a possible malicious node only after the response of the supervisor monitor or if it does not reply, after a limited time. However, in this example, we have configured the monitors to inform the nodes detected as malicious while awaiting the response of the supervisor monitor. In the simulation, the monitor M6 is the Repetition rule supervisor. Initially, the result was similar to the previous case. M1, M2, M3 correctly detected the malicious node while M4 and M5 falsely accused the node N2. However, after the final of Phase 3, all the monitors subscribe, to M6, about the suspects. In this situation, as M1 is neighbor of the malicious node (I1) and the source of information (the son of I1) so it can inform, in a special field of package, the "certainty" that it must have about I1 be the malicious node. That certainty is due to the fact that M1 have listened a package sent by I1, whose origin is N1, but has not listened any packages originating from the N1 to I1. Thus, M6 can infer that any other node accused of repeating the same message reported by M1 is not the real attacker. At the end of the correlating process, M6 published to the monitors M1 to M5 information of the real attacker.

2) Detection Intruder I2: Detect the intruder I2 is a more difficult case, since there is no monitor node neighbor at the same time from I2 and the source of information, in this case N5 (son of I2). Here, the procedure for the M6 is trying to trace the route of the package to discover the node for which there is no message intended to it. After that, M6 can infer that this node is possible the attacker. In this situation, the detection was made possible by the presence of monitors (M3, M4 and M5) along the route traveled by the package to the base station. Based on the information sent by these monitors, M6 can trace the path traveled by the package (Fig. 3). As M6 received no

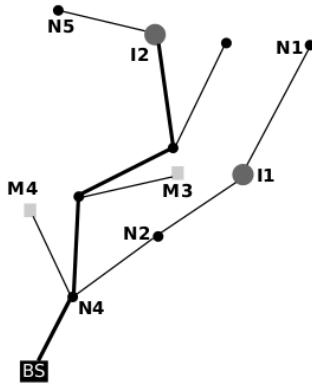


Fig. 3. Monitor M6 has traced the route followed by malicious packet

information about a package aimed to I2, it can then infer that this node is the possible attacker. It's important to say that M6 can only suspect about I2. If there were not enough monitors, M6 could not trace the route and a false positive could be generated. We left for future work how the monitors could react in a situation like that.

VII. CONCLUSION

The WSN have received considerable attention in the last few years due to its applicability in several areas. However, their characteristics and constraints make them very susceptible to attackers and malicious activities. Among the alternatives to address the issue of security, intrusion detection systems play an important role as they find malicious activities that were not thwarted by the prevention mechanisms. In such systems, special nodes, called monitors, has the task of watch its neighbors looking for evidence of malicious activities. However, without the correlation between the visions of each monitor, the likelihood of false positives occurrence is greater. This paper proposes a collaborative and decentralized intrusion detection system for WSN where the suspicious activity detected by each monitor will be correlated by special monitors, known as supervisors, in order to find the real malicious nodes. The proposed IDS proved to be very efficient in detecting Repetition attack. However, some points have not been addressed and will gain more attention in future works.

Among these items, we can cite: (1) The consumption of energy generated by the collaboration and how the system save by preventing the execution of an attack, (2) the behavior of monitors to detect other types of attacks, (3) how the network could react to the intruders and suspects detected, and (4) how a failure into a Supervisor monitor (node destruction, depleted batteries) would affect the system collaboration and how the remain monitors could react.

REFERENCES

- [1] H. Alzaid, E. Foo and J. G. Nieto, "Secure Data Aggregation in Wireless Sensor Network: a survey," *In 6th Australasian Information Security Conference, ACSC2008*, Wollongong, Australia, January 2008.
- [2] B. Parno, E. Gaustad, M. Luk and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," *CoNEXT 2006*, Lisboa, Portugal.
- [3] A. P. R. Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz and H. C. Wong, "Decentralized Intrusion Detection in Wireless Sensor Networks," *In Q2Swinet'05*. Montreal, Quebec, Canada, 2005.
- [4] R. Shorey, A. Ananda, M. C. Chan, and W. T. Ooi, *Mobile, Wireless and Sensor Networks: technology, applications, and future directions*. John Wiley & Sons. Hoboken, New Jersey, 2006
- [5] I. Balepin, S. Maltsev, J. Rowe, and K. Levitt, "Using specification-based intrusion detection for automated response," *In Proceeding of 6th International Symposium*, Pittsburgh, PA, September 2003. RAID 2003, Recent Advances in Intrusion Detection.
- [6] S. Marti, T. Giulii, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *In 6th ACM/IEEE Internacional Conference on Mobile Computing and Networking MobiCom' 00*, Agosto 2000.
- [7] R. Roman, J. Zhou and J. Lopez, "Applying Intrusion Detection Systems to Wireless Sensor Networks," *In Consumer Communications and Networking Conference 2006, CCNC 2006*. 3rd IEEE
- [8] W. R. Pires Jr., T. H. P. Figueiredo, H. C. Wong and A. A. F. Loureiro, "Malicious node detection in wireless sensor networks," *In Proceedings of the 8th International Parallel & Distributed Processing Symposium (IPDPS'04)*, Santa Fe, NM, USA. ISBN 0-7695-2132-0.
- [9] Guorui Li, Jingsha He, Yingfang Fu, "A Distributed Intrusion Detection Scheme for Wireless Sensor Networks," *Distributed Computing Systems Workshops, International Conference on*, vol. 0, no. 0, pp. 309-314, 2008 The 28th International Conference on Distributed Computing Systems Workshops, 2008.
- [10] C. V. Z. Zhou, S. Karunasekera and C. Leckie, "A peer-to-peer Collaborative Intrusion Detection System", *Networks*, 2005. Jointly held with the 2005, *IEEE 7th Malaysia International Conference on Communication*.
- [11] A. Perrig, R. Szewczyk, V. Wen, D. Culler and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," *In Mobile Computing and Networking 2001*, Rome, Italy.
- [12] K. Holger and W. Andreas, *Protocols and Architectures for Wireless Sensor Networks*. Jonh Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, England. 2008.
- [13] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications", *Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*. San Diego, California, United States. pp. 149 - 160. 2001.
- [14] D. Karger, E. Lehman, T. Leighton, M. Levine, D. Lewin, R. Panigrahy, "Consistent hashing and random trees: Distributed caching protocols for relieving hot spots on the World Wide Web," *Proc. 29th Annu. ACM Symp.*, May 1997, pp. 654-663.
- [15] Sinalgo. <http://dcg.ethz.ch/projects/sinalgo/>
- [16] NS2. http://nsnam.isi.edu/nsnam/index.php/Main_Page

A Dynamic Scheme For Authenticated Group Key Agreement Protocol

Yang Yu State Key Laboratory Of Information Security Graduate University Of Chinese Academy Of Sciences Beijing, P.R.China yuyang08@mails.gucas.ac.cn	Aixin Zhang School of Information Security Engineering Shanghai Jiao Tong University National Engineering Center of Information Security Shanghai, P.R.China axzhang@sjtu.edu.cn	Junhua Tang School of Information Security Engineering Shanghai Jiao Tong University National Engineering Center of Information Security Shanghai, P.R.China junhuatang@sjtu.edu.cn	Haopeng Chen School of Software Shanghai Jiao Tong University Shanghai, P.R.China chen-hp@sjtu.edu.cn
---	---	--	---

Abstract—Group communication mechanism provides several participants with a secure and credible communication environment by sharing a confidential group key within group members. Group Diffie-Hellman key exchange protocol (GDH) is an extension of two-party Diffie-Hellman key exchange. Many protocols based on GDH protocol have been proposed, among which AT-GDH protocol is an authenticated group key agreement protocol. AT-GDH2 protocol complements AT-GDH with a dynamic group key updating scheme. This paper proposes an improved dynamic scheme based on AT-GDH after analyzing the security flaws in AT-GDH2 protocol. We name this proposed group key management process as AT-GDH3. Then the security property of AT-GDH3 protocol is analyzed using the strand space and authentication test theory from the aspects of authentication, implicit key authentication, recency, backward security and forward security. The results show that AT-GDH3 protocol can overcome the security flaws in AT-GDH2 protocol, and can guarantee security properties of group key management.

Keywords-Authentication test, Authenticated group key agreement protocol, Group communication protocol, Strand space

I. INTRODUCTION

A rigorous group key management mechanism is the basic of ensuring security for group communication. A series of group key management techniques have been developed [1] [2]. All the schemes can be divided into two parts. One is the initial protocol, which is the initial instance for setting up a group communication session and for the first group key negotiation. The other is the dynamic protocol, which will be performed when the group membership changes dynamically. Authenticated Group Key Agreement Protocols (AGKAP) enable group principles to contributively generate a group key. The fundamental method in AGKAP is the Group Diffie-Hellman (GDH) key exchange which is based on two-party Diffie-Hellman key exchange [3], but extends to n parties [4]. A number of AGKAP have been proposed during the past years [5-12]. After analyzing several of them, Olivier Pereira, the author of [13], designed AT-GDH protocol in [13] and analyzed it using strand space theory. However AT-GDH protocol is only a static protocol. Li li complemented a

dynamic scheme and put forward AT-GDH2 protocol, an extension of AT-GDH protocol, in her doctor thesis [14]. She also verified the security properties using the strand space theory which was extended with the conception of cluster.

However, we noticed that AT-GDH2 protocol is not secure under some circumstances. In AT-GDH2 member joining protocol, the newcomer will be the key broadcaster automatically. But the newcomer may be a hostile intruder who wants to change the group key into another form for some baleful purposes, and the AT-GDH2 protocol cannot resist such attack. There is also a flaw in the member leaving protocol. The broadcaster is so powerful that he can force any member, whom he hopes not to participate in group communication any longer, to leave the group no matter whether the leaver intends to leave or not.

To solve these problems, we propose AT-GDH3 protocol in this paper. AT-GDH3 contains an improved dynamic scheme aiming at overcoming the security flaws of AT-GDH2 protocol in a more hostile environment where any member may be a spiteful person who may tamper the group key or illegally force a legitimate member to leave the group. The rest of the paper proceeds as follows. In Section 2, we first briefly introduce the strand space theory and its extension. Then some relevant AGKAP protocols, including GDH, AT-GDH and AT-GDH2, are introduced. In Section 3, we propose AT-GDH3 protocol with a new dynamic key agreement scheme for AT-GDH. In Section 4, we analyze security properties of AT-GDH3 from five aspects, which are authentication, implicit key authentication, recency, backward security and forward security. Finally, we conclude the paper in Section 5.

II. PRELIMINARIES OF AUTHENTICATED GROUP KEY AGREEMENT PROTOCOLS AND STRAND SPACE THEORY

In this section, we first review the notations of strand space which will be used to formalize and verify protocols, and then we briefly introduce some relevant AGKAP.

A. Review of Strand Spaces And Authentication Test

A strand is a sequence of message sent and received by legitimate participants or penetrators, where sending a term t is represented as $+t$ and receiving a term t is represented as $-t$. A strand element is called a node. If s is a strand, $\langle s, i \rangle$ is the i th node on s . The relation $n \Rightarrow n'$ holds between nodes n and n' if $n = \langle s, i \rangle$ and $n' = \langle s, i+1 \rangle$. Hence, $n \Rightarrow^+ n'$ (or $n \Rightarrow^* n'$) holds

* The project of this paper is supported by the National Science Foundation of China under Grant No.6070204 and the National High-Tech Research Development Program of China (863 program) under Grant No. 2007AA01Z139.

for node $n = \langle s_i \rangle$ and $n' = \langle s_j \rangle$ when $j > i$ (or $j \geq i$, respectively). A strand space is a set of strands consisting of strands for the protocol parties and penetrators. The relation $n \rightarrow n'$ represents inter-strand communication meaning term(n)= t and term(n')= t . Thus, the two relations \Rightarrow and \rightarrow jointly impose a graphic structure on the nodes of strand space. A bundle is a number of strands hooked together where one strand sends a message and another strand receives the same message and a bundle is sufficiently to formalize a session of a protocol with the nodes and the two relations. To make strand space easy to apply, three kinds of authentication tests were introduced based on the strand space structure, namely outgoing test, incoming test and unsolicited test. For more details, please refer to [15], [16].

Dynamic protocol is a quite complex and important portion of AGKAP. The biggest difference between static protocol and dynamic protocol is that a session in dynamic protocol contains several instances made up of different users, each instance is a bundle composed by strands of current users, and different bundles form a bundle sequence. Therefore in [14] Li li introduced a new definition ‘cluster’ for a session. Here we introduce some definitions of [14] which will be useful for our analysis in the next sections.

Definition 1: Let B be a bundle, then $M = \{princ(s) | s \in B\}$ is a set of members in bundle B , written as $M(B)$. $princ(s)$ means the owner of strand s .

Definition 2: For two strands s_1, s_2 in a bundle B , $height(s_1) < height(s_2)$, let Ns_1, Ns_2 be the node set of s_1, s_2 respectively, and Es_1, Es_2 be the edge set of s_1, s_2 respectively, s_1 is sub-strand of s_2 , if $Ns_1 \subset Ns_2$ and $Es_1 \subset Es_2$, written as $s_1 < s_2$.

Definition 3: For a user space M , S is a strand set in M , that is, for $s \in S$, $princ(s) \in M$. Let B be a set of bundles composed by strands in S , for $B_1, B_2 \in B$, $B_1 = (N_1, (\rightarrow_1, \Rightarrow_2))$ and $B_2 = (N_2, (\rightarrow_2, \Rightarrow_2))$ (where N_1 and N_2 are the node sets of B_1 and B_2 respectively), B_2 is a change of B_1 in M if they satisfy the following conditions concurrently:

$$(1) N_1 \subseteq N_2 \text{ and } (\rightarrow_1, \Rightarrow_1) \subseteq (\rightarrow_2, \Rightarrow_2)$$

$$(2) M(B_1) \cap M(B_2) \neq \emptyset \text{ and } M(B_1) \neq M(B_2)$$

(3) At least a pair of strands $s_1 \in B_1$ and $s_2 \in B_2$ exist, of which $princ(s_1) = princ(s_2)$ and $s_1 < s_2$

The changing relation can be written as $B_1 \mapsto B_2$.

The definition of “ \mapsto ” models the changing of dynamic instances in a group communication protocol session.

Definition 4: Cluster C is a set of bundles $C = \{B_1, B_2, \dots\}$, if it satisfies:

$$(1) \text{ for } B_i, B_j \in C \ ((i < j)), B_i \mapsto B_j;$$

(2) for $B_i, B_j \in C \ ((i < j))$, let B_C be the changing bundle from B_i to B_j , then B_C is finite.

From above we can see a session in a group protocol can be described as a cluster. If a cluster $C = \{B_1, B_2, \dots\}$, B_1 is the initial bundle of it, which identifies the initial protocol.

The authentication among different principals in a group communication is implemented in consecutive authentication. We have the following definition:

Definition 5: For strands $s_1, s_2 \in B$, if $n \in s_2$, and n is a negative node, term $t \subset n$, then a positive node n' must exist as $n' \in s_1$ and t originates uniquely on n' . We say that s_2 authenticates s_1 , n is the incoming authentication node of s_2 and t is the incoming authentication term of s_2 . Furthermore,

if n' is the l -th node of s_1 , we say that s_2 can authenticate s_1 with the height of l .

Please refer to [14] for more details of the dynamic extension of strand space. In general, the group communication protocol running in a user space M can be modeled formally as a cluster $C = \{B_1, B_2, \dots\}$, which is composed of bundles in M and changing relation “ \mapsto ”.

B. Relevant authenticated group key agreement protocols

We suppose p to be a prime integer and q a prime divisor of $p - 1$. G is the unique cyclic subgroup of \mathbb{F}_p^* of order q , and α is a generator of G . G and α are public. For a group M of n users M_1, \dots, M_n arranged into a ring to share a key, each group member M_i is assumed to select a new secret random value $r_i \in \mathbb{F}_p^*$ during each session of the following protocol.

First, let’s consider the Group Diffie-Hellman protocol (GDH) [4], which is the root for the following AGKAP.

1) Group Diffie-Hellman Key Exchange

In this protocol, each member M_i collects the intermediary values $\{\alpha^{r_j} | j \in [1, i-1]\}$, $\alpha^{r_{i-1}}$ sent by its predecessor M_{i-1} , then uses his own secret number r_i to generate new values, and appends them to the intermediary value set, forwards them to the next member M_{i+1} . That is,

$$M_i \rightarrow M_{i+1} : \{\alpha^{r_j} | j \in [1, i]\}, \alpha^{r_{i-1}}.$$

The last member M_n broadcasts the whole set

$$\{\alpha^{r_i} | i \in [1, n-1]\} \text{ to all the other members at the last round.}$$

Then, every member M_i can calculate the group key as:

$$S_n = \alpha^{\frac{r_1 \cdots r_n}{r_1 \cdots r_n}} = \alpha^{r_1 \cdots r_n}.$$

This protocol is a group key agreement protocol without authentication, however. Olivier Pereira designed an AGKAP which is called as AT-GDH using authentication tests [16].

2) AT-GDH Protocol

This protocol can be described in strand space as follows [13]:

$$SM_i[N, M, r_i, g_n[n-1]] =$$

$$< -N, +\{N, \alpha, \alpha^r\}_{S_i}, -\{|M_{<n}, g_n[n-1], H((g_n)_i^r)\}|_{S_n} > \quad (1)$$

$$SM_i[N, M, g_{i-1}[i], r_i, g_n[n-1]] = < -\{|N, g_{i-1}[i]\}|_{S_{i-1}},$$

$$+\{|N, M_{<i}, (g_{i-1})_i^r, (g_{i-1})_i, (g_{i-1})_i^r\}|_{S_i}, \quad (2)$$

$$-\{|M_{<n}, g_n[n-1], H((g_n)_i^r)\}|_{S_n} >$$

$$SM_n[N, M, g_{n-1}[n], r_n] = < +N, -\{|N, M_{<n-1}, g_{n-1}[n]\}|_{S_{n-1}}, \quad (3)$$

$$+\{|M_{<n}, (g_{n-1})_n^r, H((g_{n-1})_n^r)\}|_{S_n} >$$

Here the user space M contains n members, N is a nonce selected by the last group member M_n , g is the intermediate message, H is the hash value of g or group key.

The security properties of AT-GDH protocol are analyzed in [13] from three aspects, including Implicit Key Authentication, Resistance to Known Session-Secret Attacks and Individual Forward Secrecy. It showed that the protocol is secure.

3) AT-GDH2 Protocol

There are three sub-protocols in AT-GDH2 protocol: the initial protocol AT-GDH2-BP, the join protocol AT-GDH2-MA

and the leave protocol AT-GDH2-MS. The following are descriptions of AT-GDH2 protocol in strand space [14]. Here N' is a new session identifier and $\alpha[n]$ is a set of intermediate values.

AT-GDH2-BP:

$$SM_i[N, M, r_i, \alpha[n], K] = < -N, +[N, \alpha, \alpha']_{K_n^{-1}}, -[M_{<n}, \alpha[n], H(K)]_{K_n^{-1}} > \quad (4)$$

$$SM_i[N, M, r_i, \alpha_{i-1}, \alpha[n], K] (1 < i < n) = < -[N, M_{<(i-1)}, \alpha_{i-1}[i-1]]_{K_{n-1}^{-1}}, +[N, M_{<i}, (\alpha_{i-1}[i-1])^{r_i}, \\ (\alpha_{i-1}[i-1])_{r_i}]_{K_n^{-1}}, -[M_{<n}, \alpha[n], H(K)]_{K_n^{-1}} > \quad (5)$$

$$SM_n[N, M, r_n, \alpha_{n-1}, K] = < +N, \\ -[N, M_{<(n-1)}, \alpha_{n-1}[n-1]]_{K_n^{-1}}, +[M_{<n}, (\alpha_{n-1})^{r_n}, H(K)]_{K_n^{-1}} > \quad (6)$$

AT-GDH2-MA (M_{n+1} is the entrant):

$$SMA_{n+1}[N, N', M, L_n, r_{n+1}, H', K'] = < +N', -([N', M_{<n}, L_n, H']_{K_n^{-1}}), \\ +[N', M_{<(n+1)}, (L_n)^{r_{n+1}}, H(K'), H']_{K_{n+1}^{-1}} > \quad (7)$$

$$SMA_n[N, N', M, \alpha_n, r'_n, L'_{n+1}, K, K'] = < -N', +([N', M_{<n}, (\alpha_n)^{r_n}, [H(N, N', K)]_{K_n^{-1}}]_{K_n^{-1}}), \\ -[N', M_{<(n+1)}, (L_n)^{r_{n+1}}, H(K'), [H(N, N', K)]_{K_n^{-1}}]_{K_{n+1}^{-1}} > \quad (8)$$

$$SMA_i[N, N', M, L'_{n+1}, K, K'] (1 \leq i < n) = < -[N, N', M_{<(n+1)}, L'_{n+1}, H(K'), [H(N, N', K)]_{K_n^{-1}}]_{K_{n+1}^{-1}} > \quad (9)$$

AT-GDH2-MS (M_k is the leaver):

If the leaver is $M_j (1 \leq j < n)$, the protocol will be:

$$SMS_n[N, M, \alpha_n, r'_n, K'] = < +[N+1, M_{<(n)}_j, (\alpha_n)^{r_n}, H(K')]_{K_n^{-1}} > \quad (10)$$

$$SMS_i[N, M, L_i, K'] (1 \leq i, j \leq n \& i \neq j) = < -[N+1, M_{<(n)}_j, L'', H(K')]_{K_n^{-1}} > \quad (11)$$

If the leaver is the broadcaster M_n , the new broadcaster will be M_{n-1} , and the protocol goes like this:

$$SMS_{n-1}[N, M, \alpha_n, r'_{n-1}, K'] = < +[N+1, M_{<(n-1)}, (\alpha_{n-2})^{r_{n-1}}, H(K')]_{K_{n-1}^{-1}} > \quad (12)$$

$$SMS_i[N, M, L'', K'] (1 \leq i < n) = < -[N+1, M_{<(n-1)}, L'', H(K')]_{K_{n-1}^{-1}} > \quad (13)$$

In this protocol, $\alpha_i = \{\alpha^{\prod_{\{k \in [1, i] \wedge k \neq l\}}} | l \in [1, i]\}$, $(\alpha_i[i])$ is the j -th element of $\alpha_i[i]$, $M_{<i} = \{M_k | k \in [1, i-1]\}$, $M_{<(i)}_j = M_{<i} \setminus M_j$, $(\alpha_i)^{r_k} = \{a^{r_k} | a \in \alpha_i\}$, $\alpha_i[i] = \{\alpha_i, \alpha^{\prod_{\{k \in [1, i]\}}} \}$, $\alpha[n] = \alpha_{n-1}^{r_n}$, $L_n = (\alpha_n[n])^{r_n}$, $L_{n+1} = (\alpha_{n+1})^{r'_n}$, $L'' = (\alpha_n)^{r'_n}$, $L'' = (\alpha_{n-2})^{r_{n-1}}$, $H' = [H(N, N', K)]_{K_n^{-1}}$, N' is the next session identifier.

The hash value $H(N, N', K)$ is added into the key refresh message in the joining protocol to resist against the attack that the broadcaster M_n leaves and reenters a moment later using his old key refreshing message to act as broadcaster again and force M_{n-1} (once be a broadcaster after M_n leaves) to leave. But we notice that $H(N, N', K)$ can be easily got by applying to enter. Moreover, the hash value does not include any information about the secret value L_n calculated by the former broadcaster. Therefore, a baleful entrant may replace the new key with an unsafe and forbidden one, unknown by others. No one will realize that the group has been exposed.

As for the leave protocol, the broadcaster is so powerful that he can force any member to leave at his pleasure, and no one can stop him.

Aiming at overcoming the flaws discussed above, we put forward AT-GDH3 protocol which contains a new dynamic scheme for AT-GDH in the next section. The formal security analysis of this protocol will be given in section IV.

III. A NEW DYNAMIC SCHEME FOR AT-GDH PROTOCOL

In this section we will discuss a new group communication protocol based on AT-GDH protocol, called AT-GDH3 protocol.

Since the irrational disposal of broadcasters' power results in the vulnerability to attacks described in the preceding section directly, we must restrict the power of broadcaster in the dynamic protocol. Therefore in AT-GDH3 the broadcaster is chosen as the member who has been in the group for the longest time, and the newcomer will not be identified as broadcaster. That is, the broadcaster will be the same person until he leaves. We also require that a member must inform all the other members when he leaves. Here we present descriptions of AT-GDH3 protocol in strand space model.

AT-GDH3 protocol contains three parts: the static key-agreement protocol AT-GDH3-STATIC, the join protocol AT-GDH3-JOIN, the leave protocol AT-GDH3-LEAVE. We adopt the AT-GDH protocol which is described in eq. (4), (5) and (6) as AT-GDH3-STATIC protocol.

A. AT-GDH3-JOIN:

The join protocol can be described formally in strand space as:

$$SJM_{n+1}[N', M, a_n, L_{n+1}, K', r_{n+1}] = < +N', -[N', M_{<n}, a_n]_{K_n^{-1}}, +[N', M_{<n+1}, a_n^{r_{n+1}}]_{K_{n+1}^{-1}}, \\ -[N, N', M_{<n+1}, L_{n+1}(n+1), H(K')]_{K_n^{-1}}, +[N', M_{n+1}, H(K', M_{n+1})]_{K_{n+1}^{-1}} > \quad (14)$$

$$SJM_i[N, N', M, a_n, L_{n+1}, K', r'_n, r_{n+1}] = < -N', +[N', M_{<n}, a_n]_{K_n^{-1}}, -[N', M_{<n+1}, a_n^{r_{n+1}}]_{K_{n+1}^{-1}}, \\ +[N, N', M_{<n+1}, L_{n+1}, H(K')]_{K_n^{-1}}, -[N', M_{n+1}, H(K', M_{n+1})]_{K_{n+1}^{-1}} > \quad (15)$$

$$SJM_j[N, N', M, L_{n+1}, K'] (1 \leq i < n) = < -[N, N', M_{<n+1}, L_{n+1}(i), H(K')]_{K_n^{-1}}, \\ -[N', M_{n+1}, H(K', M_{n+1})]_{K_{n+1}^{-1}} > \quad (16)$$

Here $L_{n+1} = a_n^{r_{n+1}r'_n} = \{\alpha^{\prod_{\{k \in [1, n+1] \wedge k \neq l\}}} | l \in [1, n+1] \cap l \neq n\}^{r'_n}$, $L_{n+1}(i) = (\alpha^{\prod_{\{k \in [1, n+1] \wedge k \neq l\}}})_i^{r'_n}$ are the last intermediate values for computing group key, and $a_n = \{\alpha^{\prod_{\{k \in [1, n] \wedge k \neq l\}}} | l \in [1, n]\}$ is the value for computing group key in the last round session.

The purpose of the join protocol is to refresh the group key among members when there is a newcomer M_{n+1} . We set that M_n is still the broadcaster in the group.

B. AT-GDH3-LEAVE:

The leave protocol is more complex due to many possible situations, such as, whether the leaving person leaves on his own initiative or be forced to, whether the leaving person is the current broadcaster or not. We set a monitoring agent in the group to restrict the power of the broadcaster, he will monitor all members' behavior all along, order the member who compromises the security of the group to leave

and inform all the other members of the forcible leaving meanwhile. For those who leave in their intension, we require that they should not leave legally until they inform all other members and receive their feedback.

1) *Voluntary leaving.*

a) *AT-GDH3-LEAVE1: the leaver $M_j (1 \leq j < n)$ is not the broadcaster.*

$$\begin{aligned} SLM_j[N, M, A, N_a] = \\ < +[N, A, M_j, N_a]_{k_j^{-1}}, -[N, N_a + 1]_{k_j^{-1}}, +[N, N_a + 2]_{k_j^{-1}} > \end{aligned} \quad (17)$$

$$\begin{aligned} SLM_i[N, L'_n[i], M, A, N_a, K''] (1 \leq i < n, i \neq j) = \\ < -[N, A, M_j, N_a]_{k_j^{-1}}, +[N, N_a + 1]_{k_j^{-1}}, \\ -[N + 1, M_{(<n)}, L'_n(i), H(K''), H']_{k_n^{-1}} > \end{aligned} \quad (18)$$

$$\begin{aligned} SLM_n[N, L'_n, M, A, N_a, K'', r'_n] = \\ < -[N, A, M_j, N_a]_{k_j^{-1}}, +[N, N_a + 1]_{k_j^{-1}}, -[N, N_a + 2]_{k_j^{-1}}, \\ +[N + 1, M_{(<n)\setminus j}, L'_n, H(K''), [N, N_a + 2]_{k_n^{-1}}]_{k_n^{-1}} > \end{aligned} \quad (19)$$

$$H' = [N, N_a + 2]_{k_j^{-1}}$$

b) *AT-GDH3-LEAVE2: the leaver M_n is the broadcaster.*

$$\begin{aligned} SLM_n[N, M, A, N_a] = \\ < +[N, A, N_a, M_n, M_{n-1}]_{k_n^{-1}}, -[N, N_a + 1]_{k_n^{-1}}, \\ +[N, N_a + 2]_{k_n^{-1}} > \end{aligned} \quad (20)$$

$$\begin{aligned} SLM_i[N, L'_{n-1}[i], M, A, N_a, K''] (1 \leq i < n-1) = \\ < -[N, A, N_a, M_n, M_{n-1}]_{k_n^{-1}}, +[N, N_a + 1]_{k_n^{-1}}, \\ -[N + 1, M_{(<n-1)}, L'_{n-1}(i), H(K''), H']_{k_n^{-1}} > \end{aligned} \quad (21)$$

$$\begin{aligned} SLM_{n-1}[N, L'_{n-1}, M, A, N_a, K'', r'_{n-1}] = \\ < -[N, A, N_a, M_n, M_{n-1}]_{k_n^{-1}}, +[N, N_a + 1]_{k_n^{-1}}, -[N, N_a + 2]_{k_n^{-1}}, \\ +[N + 1, M_{(<n-1)}, L'_{n-1}, H(K''), [N, N_a + 2]_{k_n^{-1}}]_{k_n^{-1}} > \end{aligned} \quad (22)$$

$$H' = [N, N_a + 2]_{k_n^{-1}}$$

2) *Passive leaving.*

a) *AT-GDH3-LEAVE3: the leaver $M_j (1 \leq j < n)$ is not the broadcaster.*

$$SLM_n[N, M, L'_n, K'', r'_n] = < +[N + 1, M_{(<n)\setminus j}, L'_n, H(K'')]_{k_n^{-1}} > \quad (23)$$

$$\begin{aligned} SLM_i[N, M, L'_n[i], K''] (1 \leq i < n \cap i \neq j) = \\ < -[N + 1, M_{(<n)\setminus j}, L'_n(i), H(K'')]_{k_n^{-1}} > \end{aligned} \quad (24)$$

b) *AT-GDH3-LEAVE4: the leaver M_n is the broadcaster.*

$$\begin{aligned} SLM_{n-1}[N, M, L'_{n-1}, K'', r'_{n-1}] = \\ < +[N + 1, M_{(<n-1)}, L'_{n-1}, H(K'')]_{k_n^{-1}} > \end{aligned} \quad (25)$$

$$\begin{aligned} SLM_i[N, M, L'_{n-1}[i], K''] (1 \leq i < n-1) = \\ < -[N + 1, M_{(<n-1)}, L'_{n-1}(i), H(K'')]_{k_n^{-1}} > \end{aligned} \quad (26)$$

$$L'_n = \{\alpha^{\prod_{\{l_k | k \in [1, n] \cap l \neq i\}}} \mid l \in [1, n] \cap l \neq j\}_{r'_n}$$

$$L'_n(i) = (\alpha^{\prod_{\{l_k | k \in [1, n] \cap l \neq i\}}})_{r'_n}$$

$$L'_{n-1} = \{\alpha^{\prod_{\{l_k | k \in [1, n] \cap l \neq i\}}} \mid l \in [1, n-1]\}_{r'_{n-1}}$$

$L'_{n-1}(i) = (\alpha^{\prod_{\{l_k | k \in [1, n] \cap l \neq i\}}})_{r'_{n-1}}$ In passive leaving, all members must receive information from the monitoring agent.

IV. SECURITY ANALYSIS OF AT-GDH3 PROTOCOL

Only when static security and dynamic security can be guaranteed simultaneously, can we say the group key agreement protocol is secure.

A. Static Security.

In [13] Olivier Pereira proved static security from three aspects: implicit key authentication, resistance to known session- secret attacks and individual forward secrecy. A more detailed analysis and demonstration can be found in [13].

B. Dynamic Security.

Now we will use strand space model and authentication test defined in section II to analyze the security properties of dynamic AT-GDH3 protocol from the following five aspects. Due to the space limit, we will only give the final conclusions without proof.

1) Authentication.

The authentication here includes maintenance of authentication of changing bundles and authentication between the entrant or the leaver and other members. The process of authentication can guarantee confirmation of identity among members, confirmation of the source of message, and trust of information exchanged.

Proposition 1. Suppose a cluster \mathcal{C} is composed of all bundles of AT-GDH3 protocol. Consider any two bundles B_i and B_j in the cluster, and $B_i \mapsto B_j$, then B_j can keep the authentication of B_i .

Proposition 2. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. There are n members in B_1 ; M_n is the broadcaster. M_{n+1} applies to join. B_1 becomes B_2 with $n+1$ members. Suppose there is a strand $s_{n+1} \in SJM_{n+1}$ of \mathcal{C} -length ≥ 4 , then there exists a strand $s_n \in SJM_n$ of \mathcal{C} -length ≥ 4 , and the newcomer can authenticate the broadcaster M_n .

Proposition 3. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_n \in SJM_n$ of \mathcal{C} -length=5, then there exists a strand $s_{n+1} \in SJM_{n+1}$ of \mathcal{C} -length=5, the broadcaster M_n can authenticate the newcomer M_{n+1} .

Proposition 4. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SJM_i$ of \mathcal{C} -length=1, then there exists a strand $s_n \in SJM_n$ of \mathcal{C} -length=4, member M_i can authenticate the broadcaster M_n .

Proposition 5. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SJM_i$ of \mathcal{C} -length=2, then there exists a strand $s_{n+1} \in SJM_{n+1}$ of \mathcal{C} -length=5, member M_i can authenticate the newcomer M_{n+1} .

Proposition 6. Consider an AT-GDH3-LEAVE1-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. There are n members in B_1 ; M_n is the broadcaster; M_j is about to leave. B_1 becomes B_2 with $n-1$ members. Suppose a leaver's strand is $s_j \in SLM_j$ of \mathcal{C} -length=2, then there exists a strand $s_i \in SLM_i$ ($1 \leq i \leq n, i \neq j$) of \mathcal{C} -length=2, the leaver M_j can authenticate member M_i .

Proposition 7. Consider an AT-GDH3-LEAVE1-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ ($1 \leq i < n$, $i \neq j$) of \mathcal{C} -length=1, then there exists a strand $s_j \in SLM_j$ of \mathcal{C} -length=1, member M_i can authenticate the leaving person M_j .

Proposition 8. Consider an AT-GDH3-LEAVE1-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_n \in SLM_n$ of \mathcal{C} -length=3, then there exists a strand $s_j \in SLM_j$ of \mathcal{C} -length=3, the broadcaster M_n can authenticate the leaving person M_j .

Proposition 9. Consider an AT-GDH3-LEAVE1-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} -length=3, then there exists a strand $s_n \in SLM_n$ of \mathcal{C} -length=4, member M_i can authenticate the broadcaster M_n .

Proposition 10. Consider an AT-GDH3-LEAVE2-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. There are n members in B_1 , M_n is the broadcaster, M_n is about to leave, M_{n-1} becomes the new broadcaster. B_1 becomes B_2 with $n-1$ members. Suppose a leaver's strand is $s_n \in SLM_n$ of \mathcal{C} -length=2, then there exists a strand $s_i \in SLM_i$ ($1 \leq i \leq n-1$) of \mathcal{C} -length=2, the leaver M_n can authenticate member M_i .

Proposition 11. Consider an AT-GDH3-LEAVE2-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ ($1 \leq i < n-1$) of \mathcal{C} -length=1, then there exists a strand $s_n \in SLM_n$ of \mathcal{C} -length=1, member M_i can authenticate the leaving person M_n .

Proposition 12. Consider an AT-GDH3-LEAVE2-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand of broadcaster $s_{n-1} \in SLM_{n-1}$ of \mathcal{C} -length=3, then there exists a strand of the leaving person $s_n \in SLM_n$ of \mathcal{C} -length=3, the broadcaster M_{n-1} can authenticate the leaving person M_n .

Proposition 13. Consider an AT-GDH3-LEAVE2-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} -length=3, then there exists a strand $s_{n-1} \in SLM_{n-1}$ of \mathcal{C} -length=4, member M_i can authenticate the broadcaster M_{n-1} .

Proposition 14. Consider an AT-GDH3-LEAVE3-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. There are n members in B_1 , M_n is the broadcaster, M_j is forced to leave. B_1 becomes B_2 with $n-1$ members. Suppose there is a strand $s_i \in SLM_i$ ($1 \leq i < n$, $i \neq j$) of \mathcal{C} -length=1, then there exists a strand of broadcaster $s_n \in SLM_n$ of \mathcal{C} -length=1, member M_i can authenticate the broadcaster M_n .

Proposition 15. Consider an AT-GDH3-LEAVE4-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. There are n members in B_1 , M_n is the broadcaster, and is forced to leave, M_{n-1} becomes the new broadcaster. B_1 becomes B_2 with $n-1$ members. Suppose there is a strand $s_i \in SLM_i$ ($1 \leq i < n-1$) of \mathcal{C} -length=1, then there

exists a strand of broadcaster $s_{n-1} \in SLM_{n-1}$ of \mathcal{C} -length=1, member M_i can authenticate the broadcaster M_{n-1} .

2) Implicit Key Authentication.

Implicit key authentication means that group members can be reassured that only members in the group are able to get the group key. It can resist active attack. This security property can be proved by showing that the key share introduced newly is uniquely originating on regular strands, and that group key will not present on a penetrator strand.

Proposition 16. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_n \in SJM_n$ of \mathcal{C} -length ≥ 3 , then r_{n+1} is uniquely originating on $s_{n+1} \in SJM_{n+1}$.

Proposition 17. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_{n+1} \in SJM_{n+1}$ of \mathcal{C} -length ≥ 4 , then r_n' uniquely originates on $s_n \in SJM_n$.

Proposition 18. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_{n+1} \in SJM_{n+1}$ of \mathcal{C} -length ≥ 4 , then r_i uniquely originates on an SM_i -strand executed by M_i .

Proposition 19. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SJM_i$ of \mathcal{C} -length ≥ 2 , then r_n' uniquely originates on $s_n \in SJM_n$, r_{n+1} uniquely originates on $s_{n+1} \in SJM_{n+1}$.

Proposition 20. Consider an AT-GDH3-LEAVE1-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} -length=3, then r_n' uniquely originates on $s_n \in SLM_n$.

Proposition 21. Consider an AT-GDH3-LEAVE2-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} -length=3, then r_{n-1}' uniquely originates on $s_{n-1} \in SLM_{n-1}$.

Proposition 22. Consider an AT-GDH3-LEAVE3-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} -length=1, then r_n' uniquely originates on $s_n \in SLM_n$.

Proposition 23. Consider an AT-GDH3-LEAVE4-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} -length=1, then r_{n-1}' uniquely originates on $s_{n-1} \in SLM_{n-1}$.

Proposition 24. Suppose there is a bundle in an AT-GDH3-JOIN-cluster \mathcal{C} containing a strand $s \in SJM_i$ of \mathcal{C} -length=2, a strand $s \in SJM_n$ of \mathcal{C} -length=5, a strand $s \in SJM_{n+1}$ of \mathcal{C} -length=4, then there is no node $n \in \mathcal{C}$ such that $term(n) = \alpha^{s_1 \dots s_{n+2}}$ where $\{s_1, \dots, s_{n+2}\}$ is a permutation of $\{r_1, \dots, r_n, r_n', r_{n+1}\}$.

Proposition 25. Suppose there is a bundle in an AT-GDH3-LEAVE-cluster \mathcal{C} containing a strand $s \in SLM_i$ of \mathcal{C} -length=3, a strand $s \in SLM_n$ of \mathcal{C} -length=4(if it is passive leaving, then $length(SLM_i)=length(SLM_n)=1$), here n refers to the broadcaster, then there is no node $n \in \mathcal{C}$ such that $term(n) = \alpha^{s_1 \dots s_{n+1}}$, where $\{s_1, \dots, s_{n+1}\}$ is a permutation of $\{r_1, \dots, r_n, r_n'\}$.

3) *Recency*.

Recency is a necessary security property to resist against known session-secret attacks. This can be proved by affirming that the contributions newly introduced are recent.

Definition 6. [14] Consider a bundle B and a node n in B , suppose two regular nodes $m_0, m_1 \in B$ exist, satisfying $m_0 \Rightarrow^+ m_1$ and $m_0 \preceq n \prec m_1$, then we say n is recent for m_1 .

Proposition 26. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_n \in SJM_n$ of \mathcal{C} length ≥ 3 , then r_{n+1} originates on a node recent for $\langle s_n, 3 \rangle$.

Proposition 27. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_{n+1} \in SJM_{n+1}$ of \mathcal{C} length ≥ 4 , then r_n' originates on a node recent for $\langle s_{n+1}, 4 \rangle$.

Proposition 28. Consider an AT-GDH3-JOIN-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SJM_i$ of \mathcal{C} length ≥ 1 , then r_n' originates on a node recent for $\langle s_i, 1 \rangle$, and r_{n+1} also originates on a node recent for $\langle s_i, 1 \rangle$.

Proposition 29. Consider an AT-GDH3-LEAVE1-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} length $= 3$, then r_n' originates on a node recent for $\langle s_i, 3 \rangle$.

Proposition 30. Consider an AT-GDH3-LEAVE2-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} length $= 3$, then r_{n-1}' originates on a node recent for $\langle s_i, 3 \rangle$.

Proposition 31. Consider an AT-GDH3-LEAVE3-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} length $= 1$, then r_n' originates on a node recent for $\langle s_i, 1 \rangle$.

Proposition 32. Consider an AT-GDH3-LEAVE4-cluster \mathcal{C} containing two bundles B_1 and B_2 , $B_1 \mapsto B_2$, B_c is the changing bundle. Suppose there is a strand $s_i \in SLM_i$ of \mathcal{C} length $= 1$, then r_{n-1}' originates on a node recent for $\langle s_i, 1 \rangle$.

4) *Backward Security*.

For the join protocol, the old group key is not exposed, and the newcomer does not know random number r_1, \dots, r_n, r_n' , he can not recover the old group key from a_n . Therefore backward security is guaranteed, the newcomer has no possibility to learn the content of previous communications.

5) *Forward Security*.

For the leave protocol, the sub-key corresponding to the leaving person has been deleted in the update message, and the leaving person cannot recover the future group key from L_n' because he does not know random number $r_1, \dots, r_{j-1}, r_{j+1}, \dots, r_n$. Therefore forward security is guaranteed, and the leaving person can not learn the content of future communications.

V. CONCLUSION

In this paper, we proposed an authenticated group key agreement protocol AT-GDH3 which contains an improved dynamic scheme for AT-GDH and a static group key agreement protocol. Compared with AT-GDH2 which is

another extension of AT-GDH, the main contributions are as follows:

—The security of the join protocol is improved. Considering the fact that a newcomer may be hostile, AT-GDH3 does not allow the newcomer to be the broadcaster. Instead, only a reliable member who has been in the group for a long time can be the broadcaster. As a result, AT-GDH3 can resist the attack of tampering the new group key.

—AT-GDH3 overcomes the security flaw in the leave portion of AT-GDH2 protocol. We set a trusted third party to monitor members' behavior and determine whether they should be dislodged. By doing so we restrict broadcaster's power and illegal forced leave will not happen. It is worth noting that the trusted third party is an authority agent only to monitor each member's behavior, and the group key update process is implemented by the broadcaster not by him.

—The validity of active leave is enhanced. For those who want to leave on their own initiative, we require them to broadcast their notice of leaving to all other members in AT-GDH3 protocol. This information exchange process will guarantee initiative of the leaver adequately.

The formal analysis of AT-GDH3 protocol made it clear that the dynamic scheme designed in this paper can satisfy security requirements in terms of authentication, implicit key agreement, recency, forward security and backward security.

REFERENCES

- [1] S. Rafaeli, D. Hutchison, A Survey of Key Management for Secure Group Communication, ACM Computing Surveys. 35(2003)309-329.
- [2] Y. Amir, Y. Kim, C.Nita-Rotaru, G.Tsudik, On the Performance of Group Key Agreement Protocols, ACM Transactions on Information and System Security. 7(2004)457-488.
- [3] W.Difflie,M.E.Hellman, New directions in cryptography,IEEE Trans. on Information Theory. 22(1976)644–654.
- [4] M.Steiner,G.Tsudik,M.Waidner, Diffie-Hellman key distribution extended to group communication, In SIGSAC Proceedings of the 3rd ACM Conference on Computer and Communications Security.(1996)31-37.
- [5] M. Just, S. Vaudenay, Authenticated multi-party key agreement, In Advances in Cryptology-Proceedings of AsiaCrypt.1163(1996)36-49.
- [6] M. Steiner, G. Tsudik, M. Waidner, CLIQUES: A new approach to group key agreement, In Proceedings of IEEE ICDCS'97. (1997)380–387.
- [7] W. G. Tzeng, A practical and secure fault-tolerant conference key agreement protocol, In Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC'00. 1751(2000)1–13.
- [8] E. Bresson, O. Chevassut, D. Pointcheval, Provably authenticated group Diffie-Hellman key exchange - the dynamic case, In Advances in Cryptology - Proceedings of AsiaCrypt. 2248(2001)290–309.
- [9] Y. Kim, A. Perrig, G. Tsudik, Communication-efficient group key agreement, In Proceedings of IFFIP-SEC.(2001)229–244.
- [10] E. Bresson, O. Chevassut, D. Pointcheval, Dynamic group Diffie-Hellman key exchange under standard assumptions, In Advances in Cryptology - Proceedings of Eurocrypt. 2332(2002)321–336.
- [11] E. Bresson, O. Chevassut, D. Pointcheval, Group Diffie-Hellman key exchange secure against dictionary attacks, In Advances in Cryptology - Proceedings of AsiaCrypt. 2501(2002)497–514.
- [12] Y. Kim, A. Perrig, G. Tsudik, Tree-based group key agreement, ACM Transactions on Information and System Security(TISSEC).7(2004), 60-96.
- [13] O. Pereira, Modelling and security analysis of authenticated group key agreement protocols, PhD thesis,Universite catholique de Louvain, 2003.
- [14] Li li, Research on formal analysis and authentication technology of security protocol, PhD thesis, Wuhan university,2004.
- [15] F.Fabrega, J.Herzeg, J.Guttman, Strand spaces: why is a security protocol correct, In Proceedings of the 1998 IEEE Symposium on Security and Privacy. (1998)160-171.
- [16] J.Guttman, Security protocol design via authentication tests, In Proceedings of the 15th Computer Security Foundations Workshop, (2002)92-10.

Performance Evaluation of TCP Congestion Control Mechanisms

Eman Abdelfattah
University of Bridgeport
Bridgeport, CT 06604

Abstract- There are many congestion control mechanisms of TCP reported in the literature. Examples of these mechanisms are additive increase/multiplicative decrease, slow start, fast retransmit and fast recovery, and selective acknowledgement. Different versions of TCP have been implemented that include the previous mechanisms. Examples of these versions are TCP/Reno, TCP/Vegas, TCP/Sack, and TCP/Fack.

In this paper we have simulated different versions of TCP congestion control mechanisms. Extensive simulations are carried using NS Simulator to study the performance of the TCP congestion control mechanisms with different parameters such as the advertised window size, the initial size of congestion window on slow start, packet size, queue size, and bandwidth.

I. Congestion Control and Resource Allocation

A. Introduction

The term “congestion control” is used to describe the efforts made by the network’s nodes to prevent or respond to overload conditions. Congestion control is intended to keep a set of senders from sending too much data into the network because of the lack of resources at some point. Resource allocation means the process by which network elements try to meet the competing demands that applications have for the network’s resources.

A network is said to be congested when too many packets are contending for the same link, the queue overflows and the packets have to be dropped. Most networks provide a congestion control mechanism to deal with just such a situation.

The congestion control problem can be seen as how to effectively and fairly allocate resources among a collection of competing users. The resources being shared include the bandwidth of the links and the buffers on the routers or switches where packets are queued awaiting transmission.

Congestion control and resource allocation involve both hosts and network elements such as routers. Resource allocation and congestion control are not isolated to one single level of a protocol hierarchy. [1,2]

B. Evaluation of Mechanisms

A good starting point for evaluating the effectiveness of a congestion control scheme is to consider the two principle metrics of networking: throughput and delay. Throughput is the total data delivered over a given period of time. Delay is the total delay a data unit is subject to from the time it is sent to the time it is received. One way to increase the throughput is to allow as many packets into the network as possible, so as

to drive the utilization of all links up to 100%. The problem with this strategy is that increasing the number of packets in the network also increases the length of the queues at each router. Longer queues, in turn, mean packets are delayed longer in the network.

C. TCP congestion control

The essential strategy of TCP is to send packets into the network without a reservation and then to react to observable events that occur. TCP congestion control was introduced into the Internet in the late 1980s by Van Jacobson. At that time the Internet was suffering from congestion collapse where hosts would send their packets into the Internet as fast as the advertised window would allow, congestion would occur at some routers (causing packets to be dropped), and the hosts would time out and retransmit their packets, resulting in even more congestion. The idea of TCP congestion control is that each source determines how much capacity is available in the network, so that it knows how many packets it can safely have in transit. Once a given source has many packets in transit, it uses the arrival of an ACK as a signal that one of its packets has left the network, and that it is therefore safe to insert a new packet into the network without adding to the level of congestion. By using ACKs to pace the transmission of the packets, TCP is said to be self-clocking. Examples of TCP congestion control mechanisms that introduced in literature are Additive Increase/Multiplicative Decrease, Slow start, and Fast Retransmit and Fast Recovery.

II. The Testing Environment

In this section we are going to define a topology with six nodes which will be used in performance evaluation of TCP implementations in the following sections. Two nodes act as routers (r_1, r_2), which are labeled as nodes 2 and 3 in Figure 1. The routers forward the data that the source nodes (s_1, s_2), which are labeled as nodes 0 and 1, are sending to the destinations nodes (s_3, s_4), which are labeled as nodes 4 and 5. Figure 1 shows the topology of the network.

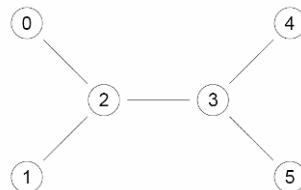


Figure 1: Network topology.

NS simulator [3,4] is used in carrying the simulations reported in this paper. The screen shot in Figure 2 shows the packets and acknowledgments flow in the network. The following packets are shown:

- a. Packets between node 0 and node 2.
- b. Packets between node 1 and node 2.
- c. Packets between node 2 and node 3.

The vertical line close to node 2 shows packets stored in the queue. In this particular case there are more packets waiting from node 1 than from node 0.

The screen shot in Figure 3 shows two TCP/Reno sessions for the network in Figure 1. The x-axis is the time while the y-axis is the number of packets. The left figure is for the TCP/Reno session between node 1 and node 4, and the right figure is for the TCP/Reno session between node 0 and node 4. In each figure, the upper trace represents the packets sent by the sender and the lower trace represents the acknowledgments sent by the receiver. For this example, we note the following:

- a. The traffic in both sessions did not pause due to any congestion.
- b. Both sessions have sent almost the same number of packets which keeps the traffic balanced between the two sources.
- c. There are no dropped packets in both sessions.

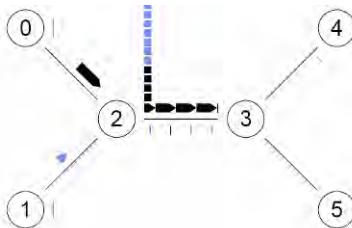


Figure 2: The screen shot of the packets and acknowledgments flow in the network.

III. Evaluation of different TCP implementations

A number of algorithms are used in modern TCP implementations aimed at controlling network congestion and maintaining good user throughput at the same time. In this section we will evaluate the following implementations of TCP: TCP/Tahoe, TCP/Reno, TCP/Newreno, TCP/Sack1 and TCP/Fack.

A. TCP

TCP or TCP/Tahoe includes slow start, additive increase/multiplicative decrease, and fast retransmit algorithms. With slow start, each ACK that is returned, two additional packets are sent, resulting in an exponential increase in the number of outstanding segments. With additive increase/multiplicative decrease, TCP opens the congestion window at a linear rate, but halves it when losses are

experienced due to congestion. With fast retransmit, a number of acknowledgements for the same sequence number (duplicate acknowledgments) triggers a retransmission without awaiting a timer expiration.

B. TCP/Reno

TCP/Reno includes fast recovery algorithm in addition to all algorithms included in TCP/Tahoe. With fast recovery, the congestion window is effectively set to half its previous value after the receipt of duplicate ACKs. However, the main weakness of TCP/Reno is that when multiple packets are dropped from one window of data, the sender has to wait for a retransmit timer before recovering.

C. TCP/Newreno

TCP/Newreno includes a small change to the Reno algorithm at the sender that eliminates the wait for a retransmit timer when multiple packets are dropped from one window, at the expense of retransmitting at most one dropped packet per round trip. The change concerns the sender's behavior during fast recovery when an ACK is received which acknowledges some but not all the packets that were outstanding at the start of that fast recovery period; we call this a "partial ACK". In TCP/Newreno partial ACKs during fast recovery are treated as an indication that the packet immediately following the acknowledged packet in the sequence space has been lost, and should be retransmitted.

D. TCP/Sack1 and TCP/Fack

TCP/Sack1 or Reno-Sack TCP implements Reno with selective acknowledgements and selective retransmission. With selective acknowledgements, the receiver could acknowledge exactly these frames that the receiver has received, rather than just the highest numbered frame received in order. This implies more information is given to the sender which makes it potentially easier for the sender to keep the pipe full. Also, these selective acknowledgment facilities increase the protocol overhead in proportion to the number of missing segments detected at the receiver.

TCP/Fack implements Reno with Forward Acknowledgement congestion control.

E. Performance parameters

In the following sections in our evaluation of TCP implementations the following parameters will be configured for the purpose of evaluation and comparison.

Queue size

The queue size for the duplex link between node(r1) and node(r2) and vice versa represents the maximum size of the queue in packets.

The advertised window

The advertised window size represents the upper bound on the advertised window for the TCP connection.

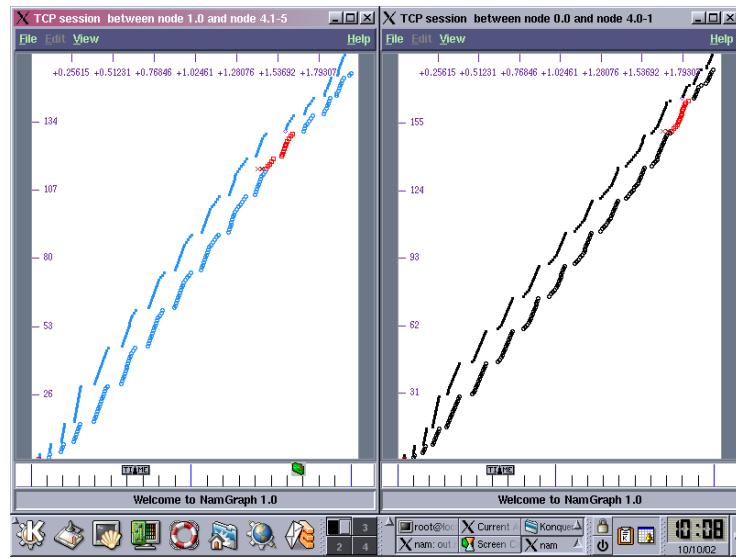


Figure 3: The screen shot for two TCP/Reno sessions for the network.

The packet size

The packet size represents the size in bytes to use for all packets from a specified source.

The initial window size

The initial window size represents the initial size of the congestion window on slow start.

The bandwidth

The bandwidth in Mbps for the duplex link between node(s1) and node(r1) and the duplex link between node(s2) and node(r1) is defined to be a measure of the capacity of the link.

Queue type

In our implementation we use drop tail queue. Drop-tail implements simple FIFO queue in which the first packet that arrives at a router is the first packet to be transmitted. However if a packet arrives and the queue is full, then the router discards that packet at the tail end of the queue

F. Evaluated parameters

For evaluation and comparison we calculated the throughput and counted the number of dropped packets. The throughput, which is defined as the observed rate at which data is sent through a link, is evaluated using the following formula.

$$\text{Throughput} = ((\text{number of send packets} - \text{number of dropped packets}) * \text{Packet size in bytes} * 8) / (\text{simulation time} * 1000)$$

The evaluated throughput is measured in Kbps.

IV. Case Study

We have evaluated the following implementations of TCP: TCP/Tahoe, TCP/Reno, TCP/Newreno, TCP/Sack1 and TCP/Fack. For the purpose of illustration we show results for TCP/Newreno.

A. Queue size

Figure 4 shows the throughput of the link between r1 and r2 versus the queue size and Figure 5 shows the number of dropped packets versus the queue size. The throughput does not change dramatically as the queue size decreases from 25 to 15 as shown in Figure 4 while there are no dropped packets in the same range as shown in Figure 5.

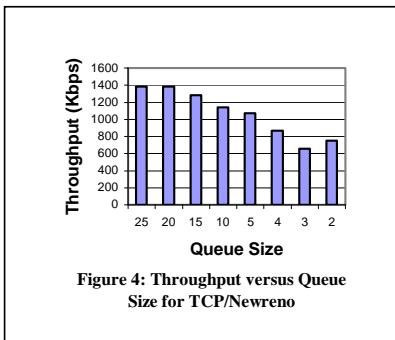
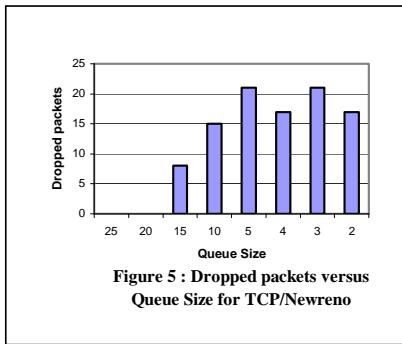
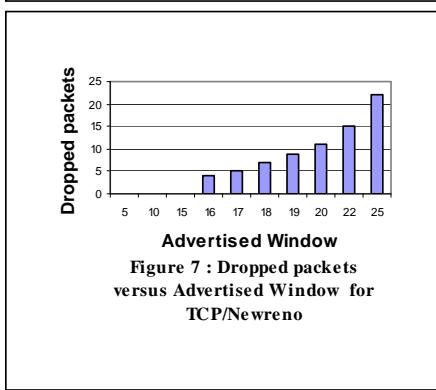
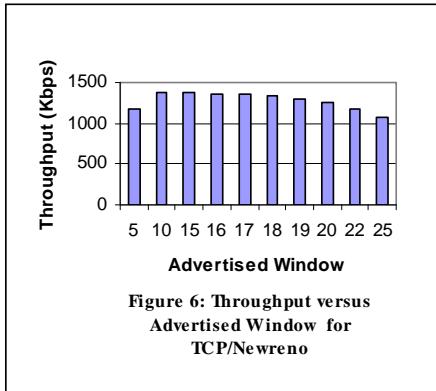


Figure 4: Throughput versus Queue Size for TCP/Newreno



B. Advertised Window size

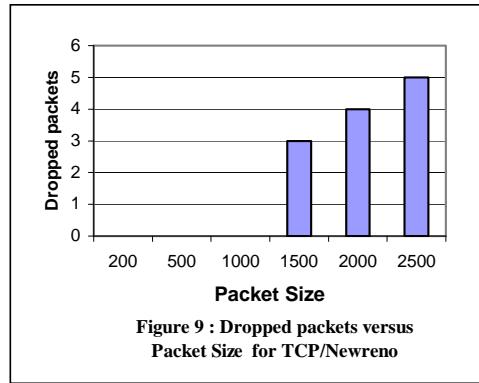
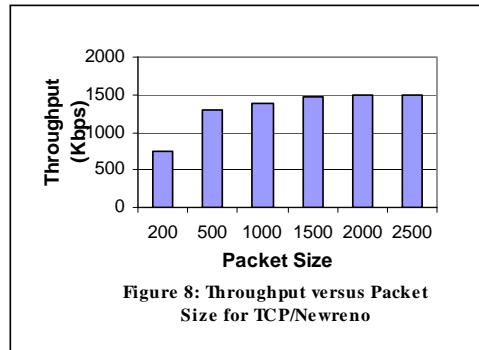
Figure 6 shows the throughput of the link between r1 and r2 versus the advertised window and Figure 7 shows the number of dropped packets versus the advertised window. For Tcp/Newreno there are no packets dropped for an advertised window less than or equal to 15. Furthermore, the throughput does not change dramatically as the advertised window increases from 10 to 19.



C. Packet Size

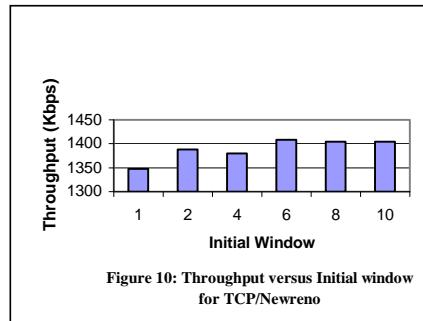
Figure 8 shows the throughput of the link between r1 and r2 versus the packet size and Figure 9 shows the number of dropped packets versus the packet size. As the size of the

packet increases above 1500, the throughput of the link between node r1 and node r2 is not affected as shown in Figure 8. The number of dropped packets is equal 0 for a packet size less than or equal 1000 bytes. As the size increases, the number of dropped packets increases as shown in Figure 9.



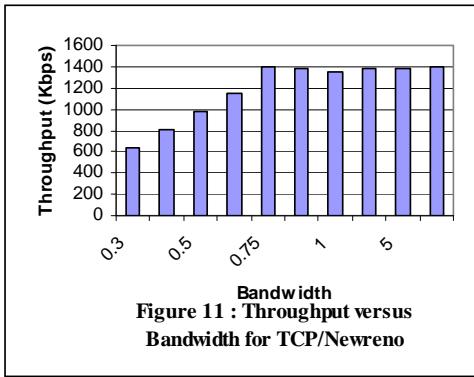
D. Initial Window size

Figure 10 shows the throughput of the link between r1 and r2 versus the initial window size of the congestion window on slow start. The throughput has not been changed significantly for all tested cases. It is important to keep the initial window at a small size which is typically 1 or 2 to avoid causing packets to be dropped in case the network is already congested.



E. Bandwidth

Figure 11 shows the throughput of the link between r1 and r2 versus the bandwidth of both the links of sources s1 and s2. As the bandwidth of the links of sources s1 and s2 increases, the throughput increases in a linear way until it reaches the highest value at a bandwidth 0.75 Mbps. As the bandwidth increases above 0.75 Mbps the throughput remains constant at about 1400 Kbps. The suggested bandwidth for each of the links of sources s1 and s2 is 0.75 Mbps.



V. Results and Conclusions

A. Effect of queue size

We investigate the effect of the queue size on the throughput with different implementations of TCP as shown in Table 1. The first column of the table shows the minimum queue size where a queue size larger than that value causes a significant reduction in traffic from first source. The second column shows the minimum queue size where a significant reduction in traffic from both sources is reported. The suggested queue size is chosen based on keeping a balanced traffic from both sources without reducing the throughput. The last column shows the number of dropped packets corresponding to the suggested queue size.

From the table we see that the throughput in all implementations is within 30% between the lowest throughput and the highest throughput. However, the queue size changes significantly from 5 in case of TCP/Newreno to 20 in case of TCP/Sack1 and TCP/Fack.

It is important from a design point-of-view to reduce the queue size, the best TCP implementation that satisfies this objective is TCP/Newreno with queue size of 5. We have to take into consideration this queue size of TCP/Newreno has

the highest drop packets which is 21 compared with 0 for TCP/Sack1 and TCP/Fack. This price of 21 dropped packets is a reasonable price if it reduces the queue size from 20 to 5.

B. Effect of the advertised window size

We examine the effect of the advertised window on the throughput with different implementations of TCP as shown in Table 2. The first column of the table shows the maximum queue size where a queue size smaller than that value causes a significant reduction in traffic from first source. The second column shows the maximum queue size where a significant reduction in traffic from both sources is reported. The suggested advertised window is chosen based on achieving the highest throughput for each implementation while minimizing the size of the advertised window.

From the table we see that the throughput in all implementations is within 1% between the lowest throughput and the highest throughput. The suggested advertised window is 10 for all implementations.

C. Effect of the packet size

We study the effect of the packet size on the throughput with different implementations of TCP as shown in Table 3. Point 1 is defined as a throughput close to the highest possible value with no dropped packets. Point 2 is defined as a high throughput with some possible dropped packets.

From the table we see that the throughput is within 0.8% for Point 1 and within 5.1% for Point 2. Increasing the packet size beyond Point 2 is not going to increase the throughput while it increases the dropped packets. The suggested packet size for Point 1 is 1000 bytes for all implementations. For Point 2 the suggested packet size is 1500 for TCP, TCP/Reno, and TCP/Newreno and 1400 for TCP/Sack1 and TCP/Fack.

Both TCP/Sack1 and TCP/Fack exhibit an anomalous behavior for packet sizes of 1500 to 1900. In other implementations as the packet size increases there is no significant change in throughput once it reached a saturated value close from the link's bandwidth. In TCP/Sack1 and TCP/Fack, for packet sizes between 1500 and 1900 the Explicit Congestion Notification (ECN) bits are sent to both sources, which cause them to halt the traffic for some period. This causes a major reduction in throughput from about 1400 Kbps to 800 Kbps in TCP/Sack1 and to 600 Kbps in TCP/Fack. Due to these anomalies of TCP/Sack1 and TCP/Fack with changes in the packet sizes, it is important to avoid the range(s) of packet sizes that causes major drop in throughput for these implementations. This range(s) of packet sizes change(s) as other parameters in the network change.

	Minimum Queue size for source S1	Minimum Queue size for both sources	Suggested queue size	Throughput corresponding to suggested queue size	Dropped packets corresponding to suggested queue size
TCP	7	2	8	1140	16
TCP/Reno	18	16	19	1396	2
TCP/Newreno	4	2	5	1072	21
TCP/Sack1	19	17	20	1392	0
TCP/Fack	19	17	20	1400	0

Table 1: Comparison of effect of queue size on different TCP implementations.

	Maximum Queue size for source S1	Maximum Queue size for both source	Suggested advertised window size	Throughput corresponding to suggested advertised window	Dropped packets corresponding to suggested advertised window
TCP	25	25	10	1388	0
TCP/Reno	17	19	10	1392	0
TCP/Newreno	25	25	10	1388	0
TCP/Sack1	16	16	10	1400	0
TCP/Fack	16	16	10	1396	0

Table 2: Comparison of effect of advertised window size on different TCP implementations.

	Point 1		Point 2		Anomalies
	Packet Size	Corresponding Throughput	Packet Size	Corresponding Throughput	
TCP	1000	1388	1500	1404	3
TCP/Reno	1000	1388	1500	1392	3
TCP/Newreno	1000	1388	1500	1464	3
TCP/Sack1	1000	1392	1400	1433.6	2
TCP/Fack	1000	1400	1400	1428	2

Table 3: Comparison of effect of packet size on different TCP implementations.

D. Effect of the initial window size

We investigate the effect of the initial window size of the congestion window on slow start on the throughput with different implementations of TCP as shown in Table 4.

From the table we see that the percentage increase in throughput in all implementations of TCP is within 5%. This insignificant increase in TCP performance as the initial

window size increases does not justify using an initial large window size because the network might be in a congested state. Also, in all the tested cases there are no dropped packets.

From the above analysis an initial window size of 1 or 2 is recommended.

	Minimum Throughput	Corresponding Initial window	Maximum Throughput	Corresponding Initial window	Percentage Difference %
TCP	1352	1	1404	6	3.8
TCP/Reno	1356	1	1408	6	3.8
TCP/Newreno	1348	1	1408	6	4.4
TCP/Sack1	1348	1	1404	6	4.1
TCP/Fack	1388	1	1396	4	.5

Table 4: Comparison of effect of the initial window size on different TCP implementations.

E. Effect of the bandwidth

All TCP implementations exhibit a linear increase in the throughput as the link's bandwidth increases till it reaches a constant value after a bandwidth of 0.75 Mbps.

At 0.75 Mbps bandwidth of the link, the number of dropped packets is zero for all implementations.

All implementations have a similar highest throughput which makes these implementations insensitive to changes in the links' bandwidth of the two sources.

References

1. Sally Floyd, "Promoting the Use of End-to-End Congestion Control in the Internet," IEEE/ACM Transactions on Networking, Vol. 7, No. 4, August 1999, pp. 458-472.
2. Ramesh Hohari and David Kim Hong Tan, "End-to-End Congestion Control for the Internet: Delays and Stability," IEEE/ACM Transactions on Networking, Vol. 9, No. 6, December 2001, pp. 818-832.
3. Kevin Fall and Kannan Varadhan, The ns Manual, The VINT Project, April 14, 2002. Available at: http://nsnam.isi.edu/nsnam/index.php/User_Information
4. Marc Geris, NS Tutorial, available at: <http://www.isi.edu/nsnam/ns/tutorial>

Optimization and Job Scheduling in Heterogeneous Networks

Abdelrahman Elleithy, Syed S. Rizvi, and Khaled M. Elleithy
Computer Science and Engineering Department University of Bridgeport, Bridgeport, CT USA
{aelleithy, srizvi, elleithy}@bridgeport.edu

Abstract— A heterogeneous network is a connected network of different platforms and operating systems. Job scheduling is a problem of selecting a free resource for unexecuted task from a pool of submitted tasks. Furthermore, it is required to find for every resource the best order of the tasks assigned to it. The purpose of this paper is to develop an efficient algorithm for job scheduling in heterogeneous networks. The algorithm should include parameters such as properties of resources and properties of jobs. The algorithm includes a cost function that is required to be optimized which includes parameters such as the total processing time, average waiting time. Our results demonstrate that the proposed algorithm can be efficiently used to determine the performance of different job scheduling algorithms under different sets of loads.

I. INTRODUCTION

JOB scheduling for heterogeneous networks has received significant attention in literature due to its significant effect on the overall performance of such networks [1, 2, 3]. An important component of the management system of a heterogeneous network is an optimal and sub-optimal scheduler. The scheduler should be able to create a schedule after analyzing the pending workload and the free computing resources. The efficiency of a distributed computing system depends on the quality and features of the scheduler. Scheduling in a heterogeneous networked environment involves scheduling over two dimensions, time and space, and on two levels, jobs and computing resources [1].

A. Problem Identification

The problem of job scheduling in heterogeneous network is a problem of identifying a resource for every task from the pool of unexecuted tasks. We define the problem using the following three dimensions:

(1) Constraints

There are three types of constraints

(A) Jobs constraints:

- Initial priority
- Time and data dependency
- Preemptability
- Memory size required
- Completion deadline
- Number of processing slots required

(B) Resources constraints.

- Memory size
- Number of processing slots available
- Processing speed

(C) Scheduling constraints:

- Job advance reservation
- Parallel job partitioning

(2) Load balancing

In order to balance the load among the network we assume that jobs are assigned to processors whenever they are free.

(3) Cost function

It is required to optimize a weighted cost function including with parameters such as total processing time, average waiting time, and average violation of completion deadline.

II. RELATED WORK

There are many approaches reported in literature for dynamic scheduling and load balancing in grid systems. Many of these involve some sort of centralized monitoring system, such as [4, 5, 6, 7], to collect up-to-date information on grid nodes. Such approaches suffer from the fact that the information needs to be kept up-to date as well as additional overhead which impacts negatively the performance. Such a phenomenon is obvious when the system is experiencing a heavy load [2].

Development in computational grid technologies has lead to high scale performances in distributed systems, wherein the grid resources are geographically dispersed and heterogeneous in nature. Nonetheless, a grid site uses a large scale of communication overhead to capture load information. Also, computational grid systems rely on load balancing to enhance the utilization of each node, and minimize the average response time of each jobs. A node in terms of a distributed system has “different processing speed and system resources.” These nodes control the decision making process in load balancing.

Since the load balancing decision is distributed; it is costly to let each node obtain the dynamic state information of the whole system. To address this problem, some algorithm developed a suitable work around; for instance, Mosix which uses a probabilistic approach to choose a random subset of hosted to talk to and cut down communication cost. Diffusion-based approach uses the

Contact author: srizvi@bridgeport.edu

near-neighbor load information to apportion surplus load from heavily loaded areas in the system. [1]

III. PROPOSED ANALYTICAL MODEL

In this section we discuss how we represent our problem in a three dimensional model. This mathematical representation is a new representation that is not reported in the literature.

A. Constraints Representation

There are three types of constraints

(A) Jobs constraints:

1. Initial priority is represented using two dimensional array IP of dimension n*3, IP[i,j], s.t. $1 \leq i \leq n$, $1 \leq j \leq 3$

IP [i, 1] represents the priority of the job which is a number between 1 and n.

IP [i, 2] represents the status of the job. Status equal 0 means the job did not start and it can be assigned to any free processor. Status equal 1 means the job started execution. Status equal 2 means the job is preempted and it can be assigned to any processor. Status equal 3 means the job finished execution.

IP [i, 3] represents the finished slots if the job is in preempted status.

2. Time and data dependency:

- a. Time dependency is represented using one dimensional array T of dimension n. T[i] = j, means that task number i can not be started before time j.
- b. Data dependency is represented using two dimensional array D of dimension n*n. D[i,j] = 1 means job i can not start before job j is finished, D[i,j] = 0 means job i can start before job j is finished.

Please note that D[i,i] = 0 for all values $1 \leq i \leq n$.

3. Preemptability: is represented using one dimensional array P of dimension n. P[i] = 1, means that task number i can be preempted during execution. P[i] = 0, means that task number i cannot be preempted during execution.
4. Memory size: is represented using one dimensional array M of dimension n. M[i] = j means job i requires memory of size j bytes.
5. Completion deadline: is represented using one dimensional array CD of dimension n. CD[i] = k means job i has to be finished by time k.

6. Number of processing slots required is represented using one dimensional array NPSR of dimension n. NPSR [i] = j means that job i requires j slots.

B. Recourses Constraints:

1. Memory size is represented using one dimensional array MP of dimension n. MP[i] = j means processor i has j bytes available for execution of tasks.
2. Number of processing slots is represented using one dimensional array NPS of dimension n. NPS[i] = j means processor i has j slots that can be used for processing tasks.
3. Processing speed is represented using one dimensional array PS of dimension n. PS[i] = j means processor i has a speed of j instructions per slot.

C. Scheduling Constraints:

1. Job advance reservation is represented using one dimensional array AR of dimension n. AR[i] = 1 means processor i allows advance reservation. AR[i] = 0 means processor i does not allow advance reservation.
2. Parallel job partitioning is represented using one dimensional array JP of dimension n. JP[i] = 1 means processor i allows partitioning. JP[i] = 0 means processor i does not allow partitioning.

(2) Load balancing

In order to balance the load among all processors, It is required to keep all processors busy. Instead of communicating the status of each processor to all processors, which requires exchanging large amount of data, processors get the next task to execute from the initial priority list (IP).

(3) Cost function

Our cost function will include the following parameters:

- | | |
|----|--|
| P: | total processing time |
| W: | average waiting time |
| V: | average violation of completion deadline |

The cost function is a weighted function. The following are the weights:

- | | |
|------------|---------------------------------|
| Ψ : | weighted cost function |
| α : | weight of total processing time |
| β : | weight of average waiting time |

γ : weight of average violation of completion deadline

$$\Psi = \alpha * P + \beta * W + \gamma * V$$

IV. PROPOSED PARALLEL ALGORITHM

The following is the parallel algorithm that will be executed by every processor. Figure (1) shows the initial status of the scheduler:

Select_task ()

{

Repeat for every free processor, p,

Select the highest priority job, k, from IP such that:

IP [k, 2] = 0 did not start, or

IP [k, 2] = 2 job was preempted

Check Time and data dependency:

- a. $T[k] \geq current_clock$
- b. $D[k, i]$ for all values are satisfied. This condition can be checked using IP
- c. $M[k] \leq MP[p]$: satisfy memory constraint

Case

- If all constraints are satisfied, set IP [K,2] = 1

- If any constraint is violated, select next available task
- If there is no available task, wait for next slot
- If $IP[i, 2] = 3$ for all values of I then
 - Finish_simulation_and_Produce_Statistics ();

Preemption ()

{

Repeat for busy processors (p) every time slot

- Check for the preemptability of the current task(T)

- If ($P[T] = 1$) and ($current_period = Preemption_period$) then

(a) $IP[T, 2] = 2$

(b) $IP[T, 3] = IP[T, 3] + current_period$

- Select_task ();

}

Finish_Task_and_Collect_Statistics ()

{

Repeat for busy processors (p) every time slot and for task (k)

- Check if task(T) has completed NPS(T)

- If task (T) finished execution then

(a) $IP[T, 2] = 3$

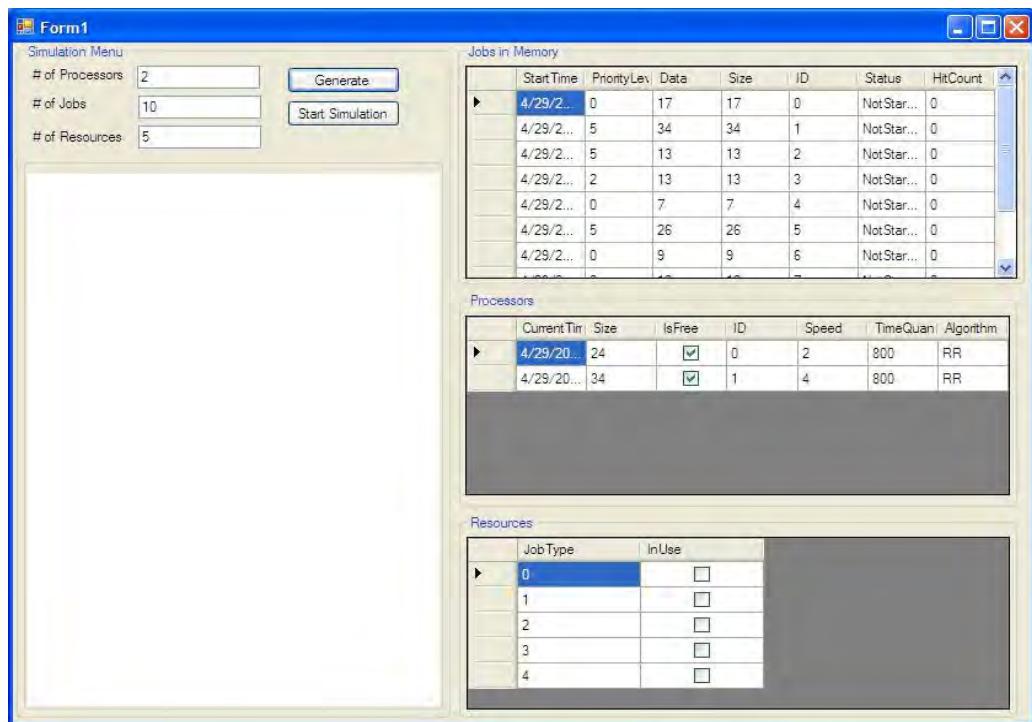


Figure 1: Status of the scheduler before run start for 2 processors, 10 jobs and 5 resources

```

(b) total processing time = total processing time +
current-period

(c) If (current_clock - CD [T])> 0 then
    average violation of completion deadline =
    average violation of completion deadline +
    (current_clock - CD [T] )
}

```

Finish-simulation-and-Produce-Statistics ()

```

{
- Update P, V, W
- Calculate  $\Psi = \alpha * P + \beta * W + \gamma * V$ 
- Print Statistics
}

```

V. IMPLEMENTATION AND EXPERIMENTAL VERIFICATIONS

We have implemented a simplified version of the algorithm using Visual Studio 2005 in C#. The following is a discussion of the implementation of the program. Figure (1) shows the initial status of the scheduler:

Inputs:

The user is allowed to use the visual interface for the following data:

- (1) Number of processors
- (2) Number of jobs
- (3) Number of resources

	StartTime	PriorityLe	Data	Size	ID	Status	HitCount
▶	4/29/2008...	4	0	17	0	Finish	1
	4/29/2008...	1	0	21	1	Finish	1
	4/29/2008...	4	0	28	2	Finish	1
	4/29/2008...	2	0	5	3	Finish	1
	4/29/2008...	5	0	8	4	Finish	2
	4/29/2008...	2	0	14	5	Finish	1
	4/29/2008...	4	0	27	6	Finish	3

Figure 2: Data about jobs in memory

Processor's Name : 2	
Job Info :	Name =2, Priority Level = 4, Hit Count =1
[Resource Type :	0
Resource Type :	1
Resource Type :	2
Resource Type :	3
Resource Type :	4

Figure 3: Data of the assigned task.

Processors							
	CurrentTim	Size	IsFree	ID	Speed	TimeQuan	Algorithm
▶	4/29/2008...	4	✓	0	1	800	PB
	4/29/2008...	13	✓	1	3	800	FIFO
	4/29/2008...	15	✓	2	2	800	LRU
	4/29/2008...	5	✓	3	1	800	PB
	4/29/2008...	18	✓	4	4	800	FIFO

Figure 4: Example of priority algorithms used by the scheduler.

The scheduler generates randomly the following data:

- (1) The start time
- (2) The priority level
- (3) The data size

During the run of the simulation the following data is displayed:

- (1) Data about jobs in the memory such as its status, speed and the allocated time. Figure 2 shows the data about jobs in memory.
- (2) The detailed status of every processor when ever a job is assigned such as the priority, the resources used for that specific job, and the hit count for that specific processor. Figure 3 shows the status of the assigned task.
- (3) The priority algorithm used for that specific processor. The following priority algorithms are supported by the scheduler: PB, FIFO, and LRU.

Figure 4 shows examples of priority algorithms used by the scheduler. Finally, Figure 5 provides the final results based on the proposed algorithm with the comprehensive amount of different statistics.

VI. CONCLUSION

In this paper we tackled the job scheduling problem in heterogeneous networks by developing a mathematical model and an efficient algorithm that takes into consideration the three types of constraints defined above, balancing load among processors in order to optimize the weighted cost function.

We have implemented a prototype of the scheduler for educational purpose. The implementation can be easily used as an educational tool for teaching concepts of scheduling in heterogeneous networks.

As a continuation of this study in a different course or an independent study, we are planning in the future to do a complete analysis of the algorithm and its performance in terms of different constraints:

- Initial priority
- Time and data dependency

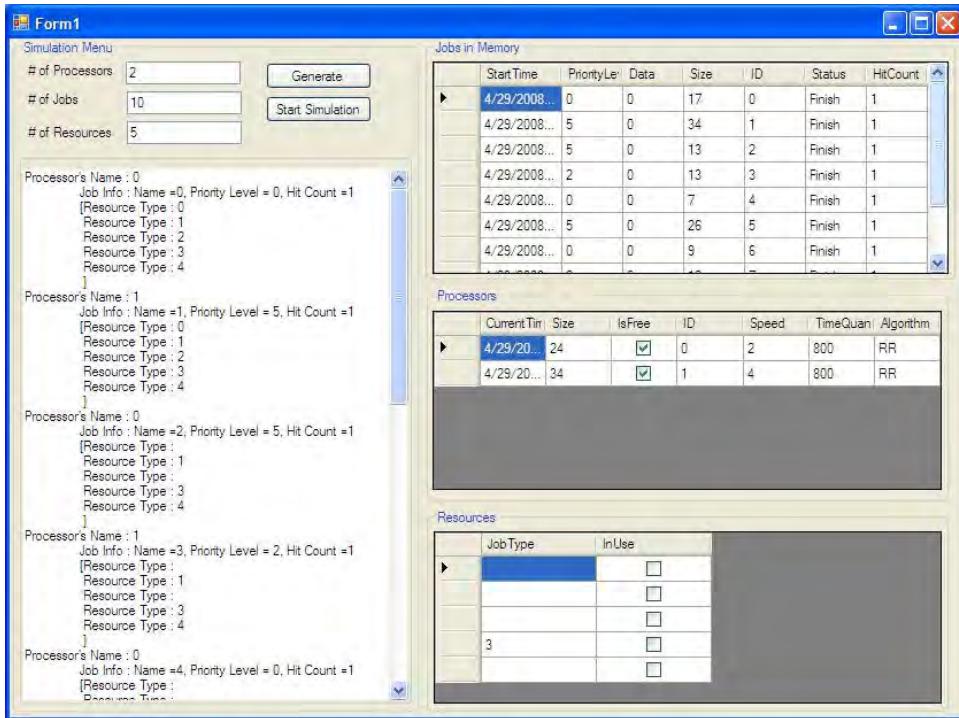


Figure 5: Final results of the simulation for 2 processors, 10 jobs and 5 resources

- Preemptability
- Memory size required
- Completion deadline
- Number of processing slots required
- Memory size
- Number of processing slots available
- Processing speed
- Job advance reservation
- Parallel job partitioning

REFERENCES

- [1] K. Lu , Y. Zomaya, "A Hybrid Policy for Job Scheduling and Load Balancing in Heterogeneous Computational Grids," *Sixth International Symposium on Parallel and Distributed Computing* (ISPDC'07), pp. 19-26, 2007.
- [2] L. Markov, "Two Stage Optimization of Job Scheduling and Assignment in Heterogeneous Compute Farms," *10th IEEE International Workshop on Future Trends of Distributed Computing Systems* (FTDCS'04), pp. 119-124, 2004
- [3] W. Homer, C. Lee, W. Chen, T. Lee, "A Job Schedule Model Based on Grid Environment," *First International Conference on Complex, Intelligent and Software Intensive Systems* (CISIS'07), pp. 43-49, 2007.
- [4] S. Fitzgerald, I. Foster, C. Kesselman, V. Laszewski, G. Smith, and S. Tuecke, "A Directory Service for Configuring High-Performance Distributed Computations," *Proc of 6th IEEE Symp. on High-Performance Computing*, 1997, pp.365–375, 1997.

- [5] J. Frey, T. Tannenbaum, I. Foster, M. Livny, and S. Tuecke,"A Computation Management Agent for Multi-Institutional Grids," *Proc. 10th IEEE Symp. on High-Performance Computing*, San Francisco, CA, USA, 2001
- [6] R. Buyya, J. Abramson, and J. Giddy, J. Nimrod, "Architecture for a Resource Management and Scheduling System in a Global Computational Grid," *4th IEEE Conf. on High-Performance Computing in the Asia-Pacific Region*, China, 2000
- [7] H. Casanova, A. Legrand, D. Zagorodnov, and F. Berman, "Heuristics for Scheduling Parameter Sweep Applications in Grid Environments," *Proceedings of the 9th Heterogeneous Computing workshop* (HCW2000), pp349-363, 2000.

Authors Biographies



Abdelrahman Elleithy has received his BS in Computer Science in 2007 from the Department of Computer Science and Engineering at the University of Bridgeport, Connecticut, USA . Abdelrahman is currently a MS student and expected to receive his MS in Computer Science in December 2008. Abdelrahman has research interests in wireless communications and parallel

processing where he published his research results papers in national and international conferences.



SYED S. RIZVI is a Ph.D. student of Computer Engineering at University of Bridgeport. He received a B.S. in Computer Engineering from Sir Syed University of Engineering and Technology and an M.S. in Computer Engineering from Old Dominion University in 2001 and 2005 respectively. In the past, he has

done research on bioinformatics projects where he investigated the use of Linux based cluster search engines for finding the desired proteins in input and outputs sequences from multiple databases. For last one year, his research focused primarily on the modeling and simulation of wide range parallel/distributed systems and the web based training applications. Syed Rizvi is the author of 45 scholarly publications in various areas. His current research focuses on the design, implementation and comparisons of algorithms in the areas of multiuser communications, multipath signals detection, multi-access interference estimation, computational complexity and combinatorial optimization of multiuser receivers, peer-to-peer networking, and reconfigurable coprocessor and FPGA based architectures.



DR. KHALED ELLEITHY received the B.Sc. degree in computer science and automatic control from Alexandria University in 1983, the MS Degree in computer networks from the same university in 1986, and the MS and Ph.D. degrees in computer science from The Center for Advanced Computer Studies at the University of Louisiana at Lafayette in 1988 and 1990, respectively. From 1983 to 1986, he was with the Computer Science Department, Alexandria University, Egypt, as a lecturer. From September 1990 to May 1995 he worked as an assistant professor at the Department of Computer Engineering, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. From May 1995 to December 2000, he has worked as an Associate Professor in the same department. In January 2000, Dr. Elleithy has joined the Department of Computer Science and Engineering in University of Bridgeport as an associate professor. Dr. Elleithy published more than seventy research papers in international journals and conferences. He has research interests are in the areas of computer networks, network security, mobile communications, and formal approaches for design and verification.

A New Methodology for Self Localization in Wireless Sensor Networks

Allon Rai, Sangita Ale, and Syed S. Rizvi
Computer Science and Engineering Department
University of Bridgeport
Bridgeport, CT USA
{Allonrai, Sale, Srizvi}@bridgeport.edu

Asia Riasat
Computer Science Department
Institute of Business Management
Karachi, Pakistan
Aasia.riasat@iobm.edu.pk

Abstract— With the tremendous applications of the wireless sensor network, self-localization has become one of the challenging subject matter that has gained attention of many researchers in the field of wireless sensor network. Localization is the process of assigning or computing the location of the sensor nodes in a sensor network. As the sensor nodes are deployed randomly we do not have any knowledge about their location in advance. As a result, this becomes very important that they localize themselves as manual deployment of sensor node is not feasible. Also, in WSN the main problem is the power as the sensor nodes have very limited power source. So, in this paper, we provide a novel solution for localizing the sensor nodes using controlled power of the beacon nodes such that we will have longer life of the beacon nodes which plays a vital role in the process of localization as it is the only special nodes that has the information about its location when they are deployed such that the remaining ordinary nodes can localize themselves in accordance with these beacon node. We develop a novel model that first finds the distance of the sensor nodes then it finds the location of the unknown sensor nodes in power efficient manner. Our simulation results show the effectiveness of the proposed methodology in terms of controlled and reduced power.

Keywords- *sensor nodes, localization, scaling, multi-path fading, AoA, TDoA, MDS, WSN*

I. INTRODUCTION

Wireless sensor network (WSN) is one of the growing issues in the field of wireless communication. Such sensor network consists of large number of sensor node having self organizing and computing capability. In various applications such as environmental monitoring, (e.g monitoring volcano activities), hard to reach areas such as natural disasters like earthquake and also in the battle fields, sensor nodes are deployed randomly as shown in Fig 1 and 4 a to get valuable information. Because of their random deployment, it is very necessary that they self localize themselves since the premature knowledge of their location is not possible in large sensor network. Thus, the concept of self localization came into existence and has become the area of great concern for the researchers. The other aspect of localization that has lured the researchers is the minimum power resource of these sensor nodes. All these sensor nodes have battery and radio so as soon as the battery is dead the sensor node is also dead which

will in turn hamper the network. So this has become one of the main problems in the localization process. As manual localization is not feasible for large sensor network, these nodes has to localize themselves in such a way that they can remain active for a longer period of time such that WSN can function properly for desired period of time. Fig. 1 and Fig. 4 shows a sensor network and also shows how sensor nodes convey the information after their localization (Fig.1). These nodes can be either data originator or data router.

The problem of localization has become the matter of interest as sensor nodes need to know their location in the sensor network in order to communicate and relay information to other neighboring sensor nodes as shown in Fig.1. Global Positioning System (GPS) is one of the solutions for this purpose but it is not applicable for large scale sensor network as it is expensive compared to common sensor nodes [3]. Moreover, GPS is limited to outdoor applications only as they are based on satellite communication. Many algorithms have been proposed for localization, but only those algorithms can be implemented that has self managing capability, ability to handle the node failure and range errors and takes into consideration the fact that power is of utmost importance when it comes to wireless sensor network as sensor nodes have a very limited amount of energy resources. Keeping these things

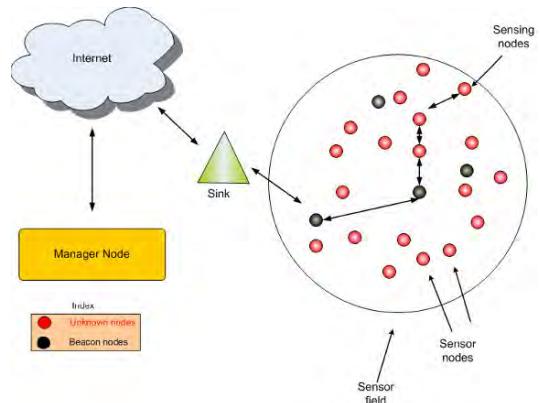


Fig 1:Showing sensor network

in mind, in this paper we present a solution to find the location of the sensor nodes using controlled power. In this paper, we have described an algorithm/method of calculating the location of sensor nodes which consists of mainly two parts. The first part is concerned with the evaluation of the distance of the sensor nodes in accordance with the beacon nodes and the second part is concerned with estimation of the location of the sensor nodes in the sensor network. In our model we have given emphasis to the fact that sensor nodes have limited power, and hence the localization has to be done accordingly.

II. METHODS OF SENSOR NODES LOCALIZATION

Localization has allured many researchers in the field of wireless communication. Since localization is one of the biggest challenges that one has to face in the wireless sensor network, many researches has been done and many are still going on. But still there are areas for improvement such as effective power management of the sensor nodes. Using GPS seemed to be the one of the solution to sort out the localization problem but it was not feasible for large sensor network as it is expensive and is not applicable for indoor applications. Here, we are listing some of the pre-existing methodology for the localization of the sensor nodes.

The RSSI model is based on the principle that signal strength diminishes with distance [1]. Thus, the distance between the source and the receiver could be found out by the strength of the radio signal received.

$$d = \left(\frac{Pr}{Pt} \right)^{1/2}$$

Here, d is the distance between the transmitter and the receiver, Pr is the received power, and Pt is the transmitted power. The demerits of RSSI method is that it is easily affected by multi-path fading, shadowing, scattering and also in the non line of sight condition.

The time difference of arrival method (TDoA) was also devised to calculate the distance of the sensor nodes [10]. This method used extra speaker and a microphone. The sender node sends the radio signal at first and after some time it again sends a sound 'chirp'. The receiver then detects the radio signal at time t_r and the sound at time t_s after some time delay td . It then uses this information to calculate the distance between the source node and the destination node.

$$d = (Sr - Ss) * (Ts - Tr - Td)$$

Here, d is the distance between the source and the receiver, Sr is the radio signal, Ss is the sound. This method was inconvenient because the sensor nodes required an extra microphone and speaker to be built in. The signal speed is also affected by humidity and temperature and for some condition the line of sight is difficult to meet.

The radio hop count method used the hop count to find the distance between the sensors nodes, [3]. Hop count is the shortest path between the two nodes. Fig.1 shows the hop count method. Mathematically, this can be expressed as:

$D = (\text{Avg hop distance } X \text{ no of hops})$ where D is the distance between the nodes a and b .

The disadvantage of this method is that it results in error of about $0.5R$ per measurement where R is the maximum range of the radio.

The Angle of Arrival (AoA) method was proposed to calculate the distance of the sensor nodes [11]. This method

used Radio and microphone arrays to calculate the distance. In this method, microphones hear the transmitted signal and analyze the phase or the time difference of the arriving signals at the microphone and then calculate the angle of the arriving signal. The demerit of this method is that the hardware used is expensive and bulky compared to TDoA. Moreover, this method is affected by the multi-path effects, shadowing, scattering and also when there is no line of sight condition.

Optimization algorithm was proposed for constraint-based localization scheme [11]. In this method, the feasible nodes were constrained by the data (RF communication, angular information) obtained from the optical device. Thus, Semi-Definite programming was used in finding the solution for the optimization problem.

For a centralized robust localization algorithm, Multidimensional Scaling (MDS) was proposed, which was a data analysis technique that displayed the data as a geometric picture [13]. Since it required the distance between all the nodes, distributed approach was proposed again that used parallelism and inter node communication to run the network.

III. AN IMPROVED METHODOLOGY FOR CALCULATING DISTANCE AND LOCATION OF SENSOR NODES

As it has already been stated above that the algorithms that are proposed for the localization must be energy efficient. After thorough research we have come up with a solution for this problem. Our model tries to find the location of the sensor nodes by saving the power of the nodes by controlling the amount of power that it requires to transmit the information. Thus our method is divided into two sections: a) distance calculation and b) location calculation

In our model, we control the transmission power of the beacon nodes such that we can conserve the energy of the beacon nodes as shown in Fig.2. When the nodes are deployed these beacon nodes are the only nodes that have the information regarding their location in the network and the other ordinary nodes find their location in accordance with the beacon nodes. The main objective of our model is to conserve the power of the beacon nodes and hence find the location of these randomly deployed sensor nodes.

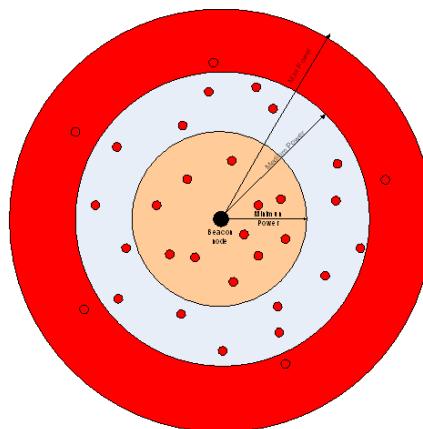


Fig 2. Showing the range of beacon nodes

A. Distance Calculation

Beacon nodes in a sensor network are the only special nodes that have the information about their location after they have been randomly deployed in the targeted area where as the other sensor nodes don't. They rely on the beacon nodes to find their location. Since all the nodes have radio within, what we do is that we control the power of the beacon nodes during the transmission of the information to the neighboring nodes, such that less power is used to transmit the information. Since the network is random i.e. the sensor nodes are randomly deployed, some sensor nodes align further from the beacon and some align nearer to the beacon. Thus the node that is near or in range with the beacon nodes gets the information first from the beacon. This scenario is presented in Fig. 3 where the sensor nodes are randomly deployed. The information consists of the identity of the beacon, its position and the path length is set to zero. Then the nodes calculate the distance based upon the signal strength received. After that the nodes add the path length and transfer the information to its neighboring nodes. The distance between the neighboring and the source nodes can be found by the received signal strengths. Now once the distance of the two neighboring nodes and the receiving/third node is known then the distance between the beacon nodes and the third or the receiving nodes can be found out by using the "voting process".

Fig. 4 shows a receiver nodes R which has two neighbors S1 and S2 and has a range of p and q respectively. The nodes S1 and S2 have the knowledge about their range from the Beacon B and also the range between themselves. Now if there is another node S3 that has the distance estimate to the beacon and is connected either to S1 or S2 and replaces the node S1 or S2, then we will have a pair of distance estimates. The correct distance from the receiver to the beacon is the part of both pairs. Thus the distance is selected by voting process. The selection process is more accurate if the density of neighbors is more.

In order to take care of the range errors we have to implement a safety mechanism. For this, the sum of the two smallest sides must exceed the largest side multiplied by a threshold value which is twice the range of the variance. In Fig. 4, the triangle R-S1-S2 must have $o + p > (1+V)q$, where V is the variance. The problem may occur when all the nodes are collinear. In this case, we select the distance that is $1/3^{rd}$ of the standard deviation of the other distance. Another problem may occur due to the wrong information of the neighbor node. In this case, we chose the distance whose standard deviation is at most 5% of that distance. Thus, in this way we can find the distance of the sensor nodes in the wireless sensor network.

IV. PROPOSED MATHEMATICAL MODEL

All system parameters along with their definition used in the proposed mathematical model presented in Table I. We have assumed that the power of the beacon node is conserved by controlling the transmitting power of the beacon node. Thus we have come up with the relationship as shown in Fig.5 between the transmitting power of the beacon node and the time span or the time till when the beacon is active. Our proposed model states that "more power (p) the beacon nodes transmit, lesser will be its time span (t)". Mathematically, this can be expressed as: $P \propto (1/t)$

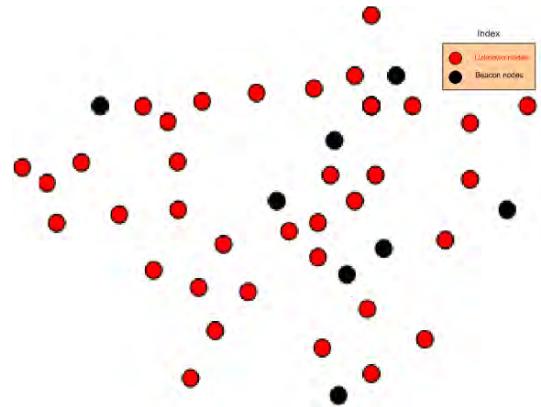


Fig.3. Random deployment of sensor nodes

Now the distance between the beacon node and the sensor node can be found out by using the path loss model;

$$d = (c / 4\pi f)(P_t / P_r)^{1/2}$$

Mathematically:
 d = distance between the beacon node and the neighboring sensor node

c = speed of light= 2.9979×10^8 (m/s)

f = Frequency of the signal (Hz)

P_t = Transmitted power

P_r = Received power

A. Location Calculation

To determine the position of the sensor nodes we use the lalteration method. With the known distance of the sensor nodes and the position of the Beacon nodes we can find the position of the sensor nodes. Let us see how a position of a sensor node is obtained.

Suppose,

- (a_i, b_i) : coordinates of beacon point i, r_i distance to anchor i
- (a, b) : unknown coordinates of node
- Using the distance formula
- $(a_i - a_0)^2 + (b_i - b_0)^2 = r_i^2$ for $i=1, \dots, 3$
- Subtracting eq. 3 from 1 and 2, we get,
- $(a_1 - a_0)^2 - (a_3 - a_0)^2 + (b_1 - b_0)^2 - (b_3 - b_0)^2 = (x_1)^2 - (x_3)^2$
- $(a_2 - a_0)^2 - (a_3 - a_0)^2 + (b_2 - b_0)^2 - (b_3 - b_0)^2 = (x_2)^2 - (x_3)^2$

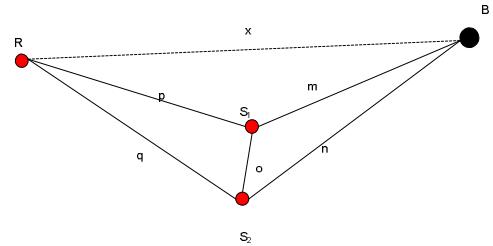


Fig.4: Voting Process

TABLE I
DIFFERENT PARAMETERS USED IN THE PAPER

Symbol	Definition
d	Distance between transmitter and receiver
Pr	Received power
Pt	Transmitted power
Sr	Radio signal
Ss	Sound signal
Ts	Time taken to hear the sound signal by receiver
Tr	Time taken to hear the radio signal by the receiver
Td	Time delay
R	Receiver node
S ₁ , S ₂	Neighboring node of R
p	Distance between R and S ₁
q	Distance between R and S ₂
o	Distance between S ₁ and S ₂
B	Beacon node
m	Distance between B and S ₁
n	Distance between B and S ₂
x	Distance between B and R
V	Variance
P	Power of Beacon node
t	Time span of Beacon node
c	Speed of light = 2.9979×10^8 (m/s)
F	Frequency of the signal(Hz)
a _i	X coordinate of Beacon node
b _i	Y coordinate of Beacon node
a _u , b _u	Unknown coordinates of node
r _i	Distance between Beacon and unknown node

Thus we get the linear equation after rearranging as below:

$$\begin{aligned} 2(a_i - a_1)a_i + 2(b_i - b_1)b_i &= x_i^2 - x_1^2 - a_i^2 + a_1^2 - b_i^2 + b_1^2 \\ 2(a_i - a_1)a_i + 2(b_i - b_2)b_i &= x_i^2 - x_2^2 - a_i^2 + a_1^2 - b_i^2 + b_2^2 \end{aligned}$$

Arranging the above equation in a matrix form, we get,

$$2 \begin{bmatrix} a_i - a_1 & b_i - b_1 \\ a_i - a_2 & b_i - b_2 \end{bmatrix} \begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} x_i^2 - x_1^2 - a_i^2 + a_1^2 - b_i^2 + b_1^2 \\ x_i^2 - x_2^2 - a_i^2 + a_1^2 - b_i^2 + b_2^2 \end{bmatrix}$$

For Example:

$$(a_i, b_i) = (3, 1), (a_1, b_1) = (6, 5), (a_2, b_2) = (9, 2), x_1 = 1, x_2 = 2, x_i = 3$$

Then,

$$2 \begin{bmatrix} 6 & 2 \\ 3 & -2 \end{bmatrix} \begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} 72 \\ 24 \end{bmatrix}$$

After calculation we get,

$$(a_u, b_u) = (5.3, 2.1)$$

This represents the location of unknown sensor nodes. Thus we are capable of finding the location of the sensor nodes using our proposed algorithm or method.

V. SIMULATION RESULTS AND EXPERIMENTAL VERIFICATIONS

In our proposed model, we have tried to come up with a power efficient method for the localization of sensor nodes. We have also tried to show the inverse relationship between the power transmitted by the Beacon nodes and the life span of the beacon nodes. We have proposed that when the beacon nodes transmit the information at maximum or at high power the life span of the beacon nodes will be shorter as compared

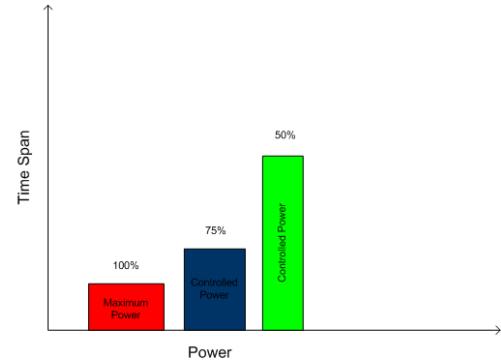


Fig.5. power Vs Time span

to the life span when it transmits at relatively low power. For this purpose, we have used the MATLAB for the simulation.

The simulation result in Fig. 6 and Fig. 9 shows that the activation time of the beacon nodes or the time for which the beacon node is active decrease with the increase in the transmitting power and vice versa. When the beacon nodes transmit at its maximum power then the time for which it is operational will be minimum and the time span will be maximum when it transmits at low power. The simulation results of Fig. 6 and 9 demonstrate the change in time span. Thus these results shows that the power can be conserved and help to increase the longevity of the beacon nodes which is the most important aspect in the process of localization

In our proposed model, the beacon node is allowed to transmit at relatively low power then its actual transmitting capacity as it is the only node that has the information in advance regarding its location after the nodes have been deployed. Thus it is important that these beacon nodes remain functional for a longer period of time. Once the beacon nodes transmit, the neighboring node receives the information that has been transmitted by the beacon nodes that consists the identity of the beacon nodes, location and the path length that is set to zero. Now, the distance calculation is done using the free path loss model: $D = (c/4\pi f)(Pt/Pr)^{1/2}$

Once the value of the distance is known the next step will be to find the location of the ordinary sensor nodes. For this

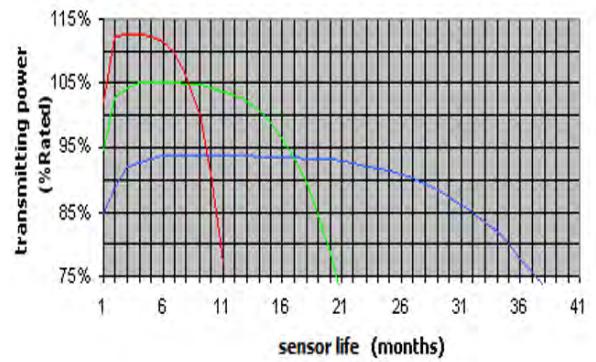


Fig 6 showing the relation between the life span and the power

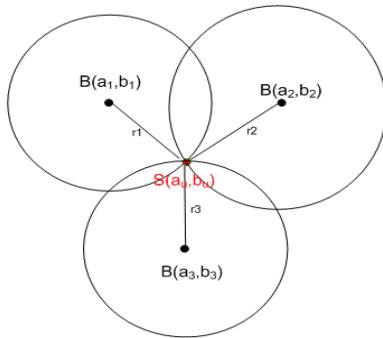


Fig.7 Calculation of location

purpose we use following method. We find the location of the sensor nodes with respect to the position of the beacon nodes. The calculation of location is represented in Fig. 7. Here we use three beacon nodes to find the location of unknown nodes. Using the distance formula between the beacon nodes and unknown nodes we find the location of the sensor nodes.

In the following example we find the location of the unknown nodes with reference to three beacon nodes.

Suppose,

- (a_i, b_i) : coordinates of beacon point i, r_i distance to anchor i
- (a_u, b_u) : unknown coordinates of node

Using distance formula:

- $(a_i - a_u)^2 + (b_i - b_u)^2 = r_i^2$ for $i=1, \dots, 3$
- Subtracting eq. 3 from 1 and 2, we get,
- $(a_1 - a_u)^2 - (a_3 - a_u)^2 + (b_1 - b_u)^2 - (b_3 - b_u)^2 = (x_1)^2 - (x_3)^2$
- $(a_2 - a_u)^2 - (a_3 - a_u)^2 + (b_2 - b_u)^2 - (b_3 - b_u)^2 = (x_2)^2 - (x_3)^2$

Thus we get the linear equation after rearranging as below:

$$\begin{aligned} 2(a_1 - a_u)a_u + 2(b_1 - b_u)b_u &= x_1^2 - x_3^2 - a_1^2 + a_3^2 - b_1^2 + b_3^2 \\ 2(a_2 - a_u)a_u + 2(b_2 - b_u)b_u &= x_2^2 - x_3^2 - a_2^2 + a_3^2 - b_2^2 + b_3^2 \end{aligned}$$

Arranging the above equation in a matrix form, we get,

$$\begin{bmatrix} a_1 - a_u & b_1 - b_u \\ a_2 - a_u & b_2 - b_u \end{bmatrix} \begin{bmatrix} a_u \\ b_u \end{bmatrix} = \begin{bmatrix} x_1^2 - x_3^2 - a_1^2 + a_3^2 - b_1^2 + b_3^2 \\ x_2^2 - x_3^2 - a_2^2 + a_3^2 - b_2^2 + b_3^2 \end{bmatrix}$$

This corresponds to $AX=B$. Using the MATLAB, we can solve the linear equation and get the corresponding value of X as $X=A^{-1}B$.

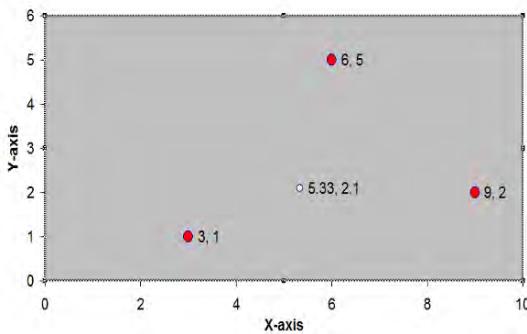


Fig.8. Plotting of the location of the beacon nodes and the unknown sensor nodes after calculating the location of the unknown nodes.

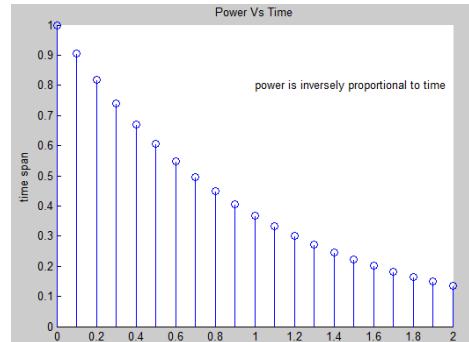


Fig.9. Power is inversely proportional to time span

For Example:

Let, $(a_1, b_1)=(3,1)$, $(a_2, b_2)=(6,5)$, $(a_3, b_3)=(9,2)$, $x_1=1$, $x_2=2$, $x_3=3$
Then,

$$\begin{bmatrix} 6 & 2 \\ 3 & -2 \end{bmatrix} \begin{bmatrix} a_u \\ b_u \end{bmatrix} = \begin{bmatrix} 72 \\ 24 \end{bmatrix}$$

After calculation we get,

$$(a_u, b_u) = (5.3, 2.1)$$

This represents the location of unknown sensor nodes. The same scenario is illustrated in Fig.8. Thus we are capable of not only finding the location of the sensor nodes but also successfully conserve the power at the same time to increase the longevity of the WSN using our proposed algorithm or method. The simulation result shows that the activation time vary inversely with the transmission power of the beacon nodes and with proper control of the power of the beacon nodes, we can find the location of the sensor nodes in a power efficient manner.

VI. CONCLUSION

In this paper, we present an algorithm that locates the location of the sensor nodes in a wireless sensor network in a power efficient manner. The simulation results show that the proposed model helps to improve the longevity of the WSN as the method helps to conserve the power which is the main problem in WSN as the sensor nodes have limited power resource and also shows that this method is a power efficient algorithm (i.e., it helps to conserve the power of the node and at the same time find the location of the sensor nodes in Wireless Sensor Network). In future we can make the localization process simpler by using sensors that will not have a battery as its power source i.e., we can use sensors without batteries.

REFERENCES

- [1] B. Krishnamachari, *Networking Wireless Sensors*, Cambridge University Press, New York, NY, 2005
- [2] S. Rappaport, *Wireless Communications*, Second Edition, Prentice Hall 2005.
- [3] B. Nath, D. Niculescu, "Ad-hoc positioning system," Proc. IEEE Global Communications Conf. (GLOBECOM'01), pp. 2926–2931, 2001.
- [4] L. Doherty, K. Pister, and L. El Ghaoui, "Convex position estimation in wireless sensor networks," in Proc. 20th Annual Joint Conf. of the IEEE Computer and Communications Society (INFOCOM 2001), Vol. 3, Piscataway, NJ: IEEE Press, 2001, pp. 1655–1663.
- [5] P. Bergamo and G. Mazzini, Localization in Sensor Networks with Fading and Mobility. In Personal, Indoor and Mobile Radio Communications, pages 750–754, 2002.

- [6] J. Hill, *System Architecture for Wireless Sensor Networks*. PhD thesis, UC Berkeley, May 2003
- [7] X. Ji, H. Zha, Sensor positioning in wireless ad-hoc sensor networks using multidimensional scaling, in: Proceedings of the IEEE INFOCOM, the Annual Joint Conference of the IEEE Computer and Communications Societies, March 2004
- [8] G. Balogh, M. Maroti, A. Ledeczi and J. Sallai, "Acoustic ranging in resource constrained sensor network" Technical Report, ISIS-04-504, February 25, 2004 (available at <http://www.isis.vanderbilt.edu/publications.asp>)
- [9] W. Su, I. Akyildiz, E. Cayirci, Y. Sankarasubramaniam, "A survey on sensor network" IEEE Communications Magazine, Vol.40, No.4, pp. 102-114, 2002
- [10] Y. Min, K. Won, K. Mechitov, S. Sundresh, W. Kim, G. Agha, "Resilient Localization for Sensor Networks in Outdoor Environment" Distributed Computing Systems, 2005. ICDCS 2005, Proceedings. 25th IEEE International Conference on 10-10 June 2005, pp. 643 - 652
- [11] L. Doherty, K. Pister, and L. Ghaoui, "Convex position estimation in wireless sensor networks". In Proceedings of the 20th Conference of the IEEE Communications Society (IEEE INFOCOM), pages 1655-1663, 2001.
- [12] D. Niculescu and B. Nath, "Ad-hoc positioning system using AoA". In Proceedings of the IEEE/INFOCOM 2003, San Francisco, CA, April 2003.
- [13] Y. Shang and W. Ruml, "Improved MDS-based localization," Proceedings of the 23rd Conference of the IEEE Communications Society (Infocom 2004); 2004 March 7-11; Hong Kong. Piscataway NJ: IEEE; 2004; 4: 2640-2651

Authors Biographies



SYED S. RIZVI is a Ph.D. student of Computer Engineering at University of Bridgeport. He received a B.S. in Computer Engineering from Sir Syed University of Engineering and Technology and an M.S. in Computer Engineering from Old Dominion University in 2001 and 2005 respectively. In the past, he has done research on bioinformatics projects where he investigated the use of Linux

based cluster search engines for finding the desired proteins in input and outputs sequences from multiple databases. For last one year, his research focused primarily on the modeling and simulation of wide

range parallel/distributed systems and the web based training applications. Syed Rizvi is the author of 45 scholarly publications in various areas. His current research focuses on the design, implementation and comparisons of algorithms in the areas of multiuser communications, multipath signals detection, multi-access interference estimation, computational complexity and combinatorial optimization of multiuser receivers, peer-to-peer networking, and reconfigurable coprocessor and FPGA based architectures.



AASIA RIASAT is an Associate Professor of Computer Science at Collage of Business Management (CBM) since May 2006. She received an M.S.C. in Computer Science from the University of Sindh, and an M.S in Computer Science from Old Dominion University in 2005. For last one year, she is working as one of the active members of the wireless and mobile communications (WMC) lab research group of University of Bridgeport, Bridgeport CT. In WMC research group, she is mainly responsible for simulation design for all the research work. Aasia Riasat is the author or co-author of several scholarly publications in various areas. Her research interests include modeling and simulation, web-based visualization, virtual reality, data compression, and algorithms optimization.



ALLON RAI is a MS student at University of Bridgeport. He received his B.E degree From Cosmos College of Management and Technology in 2006 and currently enrolled at University of Bridgeport, CT, USA in Electrical department. In the past he has done project in satellite communication. Right now his research area is focused on the Self-Localization of the Wireless Sensor Network, the Wireless Sensor Networks and the power management in the WSN.

A Novel Optimization of the Distance Source Routing (DSR) Protocol for the Mobile Ad Hoc Networks (MANET)

Syed S. Rizvi¹, Majid A. Jafri, and Khaled Elleithy

Computer Science and Engineering Department
University of Bridgeport
Bridgeport, CT 06601

{srizvi, majidals, elleithy}@bridgeport.edu

Asia Riasat

Department of Computer Science
Institute of Business Management
Karachi, Pakistan 78100
aasia.riasat@iobm.edu.pk

Abstract- This paper presents a new scheme for the Distance Source Routing (DSR) protocol which shows the improvement over the two major metrics of the DSR protocol: Route Discovery and Route Maintenance. In addition, we present a mathematical model that includes probability density function for these two observed metrics. Our simulation results demonstrate a significant improvement in the route discovery, transmission time, and the overall network utilization. As an interesting side result, our analysis also shows that the proposed model can be used to effectively reduce the packet losses.

Keywords- DS-CDMA, bit error rate, data throughput, multiuser communications

I. INTRODUCTION

The Dynamic Source Routing (DSR) protocol is dealt under On-Demand Routing (ODR) protocol which is just an exact opposite to the Table-Driven Routing (TDR) [2, 3]. Generally, there are two main phases use in the DSR protocol. One is the Route Discovery (RD) phase which discovers all the possible paths for the packets to be transferred from a particular source to a destination. It is essential to properly maintain the RD phase since maintaining a separate table for storing routing details involves cost issues. The second phase of the DSP protocol is the Route Maintenance (RM) phase which fixes all the possible paths from one particular source to a destination [5]. In DSR, the packets are transmitted only one time for each node. If the node does not receive the packet, the previous node is responsible to make attempts in order to transmit the packet. On the other hand, if the destination node receives the packet successfully, an acknowledgment is transmitted back to the source node for the received packet. Since the use

of the DSR protocol does not require the maintenance of a cache table, it allows us to avoid unnecessary updating works which results space and time saving advantages.

In the existing DSR scheme, the malfunctioning of one or more links along a certain route requires the retransmission of all packets back to the originating source node. This unnecessary amount of retransmission results a significant transmission overhead that can severely degrade the overall network performance by increasing the average time delay. In order to minimize the transmission overhead and maximize the network throughput, we present an alternative scheme that can be used to optimize the performance of DSR protocol. Specifically, our proposed scheme suggests improvement in the RD and the RM metrics of the DSR protocol. Based on the proposed optimization, we derive a mathematical model which proves the correctness of the proposed scheme.

II. PROPOSED OPTIMIZATION FOR THE DSR PROTOCOL

Our main goal is to maintain the original underlying architecture of the DSR protocol. Therefore, we consider the DSR scheme as a black box. The DSR protocol fails to maintain route consistency in the presence of broken links. When one of the links goes down, the DSR protocol locates an alternate route and transmits back the packet to the source node where the packet was originated. On contrary to the actual scheme of the DSR protocol, our proposed scheme uses a reserve direction search method. In our proposed scheme, the packets would be transmitted to the immediate prior node where the actual error was occurred. The proposed scheme then finds one or more alternative routes from the current location to the destination. This implies that the whole searching procedure of the proposed scheme will

¹Contact author: srizvi@bridgeport.edu,

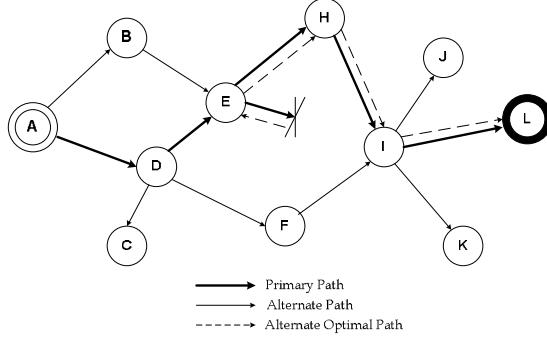


Fig. 1. Finding the alternate path in DSR protocol according to the proposed scheme

be done in the opposite direction starting from the destination node. Our simulation results demonstrate that the proposed scheme considerably increases the chance of finding a valid route for salvage packets that are typically stored in the send buffer.

For instance, consider an example for locating a route based on the reverse direction search scheme as shown in Fig. 1. It can be observed that the route finds by the RD procedure from node *A* (source node) to *L* would be: *A*→*D*→*E*→*I*→*L*. During transmission of the packets, it is detected at run time that the shortest link between node *E* and *I* goes down. Consequently, the proposed scheme immediately starts searching the best available alternate routes. In order to reach the destination node, the proposed scheme locates the neighboring nodes (i.e., node *B*, *D*, and *H* from node *E*). This process of finding the alternate route from the location of error results an optimal alternate route: *A*→*D*→*E*→*I*→*H*→*L*. This implies that our proposed scheme neither send any feedback to the destination node *A* nor it initiates the route discovery from the source point. Therefore, repeating this search in the reverse direction from the current location of error to the neighboring nodes results a significant increase in the chance of finding a valid optimized route.

A. Proposed Reverse Direction Search Scheme

In order to formulate the proposed scheme, we present a model that shows simple steps that need to be implemented for finding a valid and optimize route in the presence of link failures. The model is presented in Fig. 2. The model is typically divided into two parts. The upper part of the model represents the RD procedure where as the lower part represents the RM procedure. The RD procedure is based on an exhaustive search of an internal cache. During the transmission of a packet, if one of the links goes down, the proposed scheme mentions that the packet will be

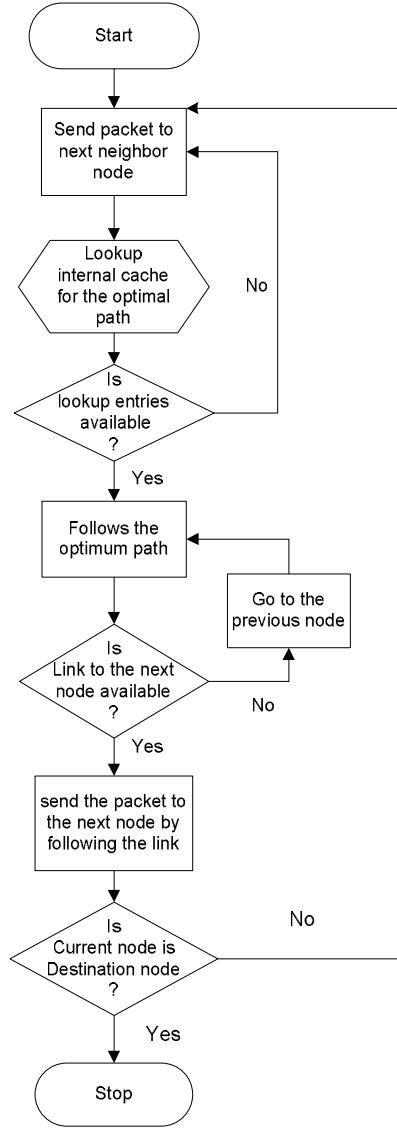


Fig. 2. Flow chart showing proposed model of DSR algorithm

immediately forwarded to the next available node and starts transmitting from the new location. Unlike the DSR protocol, the proposed scheme minimizes the transmission overhead by avoiding the unnecessary transmission of data to the source node in the presence of a faulty link. In other words, the proposed scheme does not provide any feedback to the source node that leads to a significant improvement in the network throughput. Since the RD can be done on the current node, we do not need to focus on the source node. This implies that the proposed scheme suggests the best

delivery of the packets even in the presence of link failure. In addition, the repetition of the packets due to the flooding will be cut down.

In the proposed model, we mainly focus on the RD and the RM. During the RD process, if the entries are found in the internal cache of the next node, the proposed scheme determines the optimal path that will be used to forward all the packets to the next node. At that current node location, the same procedure for searching the optimal path will be repeated over the passage of time in order to find the best path towards the destination. An empty entry in the internal cache represents that there is no valid route exist for a particular destination. In such a scenario, the proposed scheme will lookup into the next neighbor's cache and determine the best available route for the desired destination. Once the optimal route is discovered, the packet can then be transmitted. In the RM process, whenever there is a link failure along the path, the packet would not go further at the point of error and there is no need to send any feedback to the original source node. Instead, the proposed scheme determines and performs the RM process on the best available alternate path.

B. Mathematical Model

We derive our mathematical model based on the proposed reverse direction scheme. In our mathematical model, we show that the transmission of packets via an alternate route is more efficient as compared to transmitting packets from the source node using a primary route. This is especially true in the presence of error. All system variables, along with their definition, are listed in Table I.

The accuracy of the proposed scheme is essentially dependent on how efficiently we can discover the alternate routes in the presence of faulty links. In general, the accuracy is partially related to a certain interval by which we perform the RD procedure for a specific type of network traffic such as a stream of packets. In particular, we first need to derive an expression for a random variable, x , that can be used to characterize the behavior of RD process with respect to time. Therefore, in order to implement the proposed scheme, one must measure the frequency of route discoveries. In order to determine the interval between the route discoveries, the following mathematical expression can be derived for a random variable, x :

$$\int_{-\infty}^{+\infty} xf(x)dx \quad (1)$$

It should be noted that equation (1) is based on the PDF which is used to find the frequency of route discovery for a particular pair of source and destination.

Figure 4 represents the proposed scheme with the primary and the secondary paths along with their corresponding links. It can be seen in Fig. 3 that the node P represents the primary route whereas the node S represents the secondary

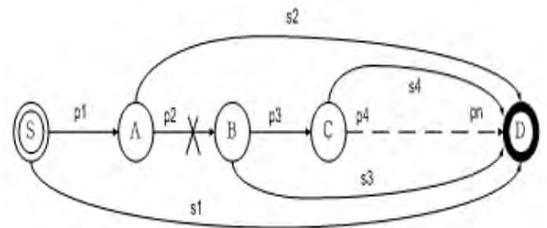
TABLE I
SYSTEM PARAMETERS AND DEFINITIONS

Parameters	Description
P_i	This represents the i th link in a primary path.
S_i	This represents the i th link in a secondary path.
X_{P_i}	Life time of the i th primary route.
X_{S_i}	Life time of the i th secondary route.
X_R	Minimum life time for the collection of all values in the primary path links
T	Intervals for route discovery
E_o	An event that shows any of the given link fails
$f_i(t)$	Frequency of route discovery
Z_i	Maximum life time among all available values.
\bar{P}_i	Represents the faulty primary link due to an event E
\bar{S}_i	Represents the faulty secondary link due to an event E

route. If an error occurs in the primary route, the proposed scheme will immediately discover an alternate route S_1 rather than going back to the source node A . In other words, in the presence of faulty links, the proposed scheme searches the internal cache and determines the alternative route S_1 which is typically stored in the local cache.

For this particular scenario, the success of the proposed scheme is heavily dependent on the rate at which one may need to execute the RD procedure. In addition, the success of the proposed scheme is not only dependent on the rate at which the RD procedure will be performed but also dependent on the accuracy and the efficiency by which the alternate routes will be determined. In order to find the frequency of an alternative RD, we assume that an event E might occur at a discrete point in time in the network which causes an error in one of the two types of routes (i.e., the primary P and the secondary S routes). Thus the transmission of an event can be mathematically described as:

$$E = \bar{P}_1 S_1 + (\bar{P}_2 (\bar{P}_1 + S_2) S_1) + (\bar{P}_3 (\bar{P}_1 (\bar{P}_2 + S_3) S_2) S_1) + \dots \quad (2)$$



Primary Path: P with links- $p_1, p_2, p_3, \dots, p_n$
Secondary Path: S with links- $s_1, s_2, s_3, \dots, s_n$

Fig. 3: Proposed scheme with primary and secondary path and their links

where \overline{P}_i represents the faulty primary-link where as \overline{S}_i represents the faulty secondary-link which caused due to the occurrence of an event E at discrete point in time within a network.

Equation (2) represents a generic equation that shows how the occurrence of an event in the network may cause an error in the alternate routes. Equation (2) can be further extended for the maximum K number of forwarding links within the available primary paths. It should be noted that the occurrence of an event E is representing a cause of malfunctioning in the currently used valid route. Taking these factors into account, one may write the following mathematical expression:

$$E = \langle \overline{P}_1 \overline{S}_1 \rangle + \langle \overline{P}_2 \overline{S}_2 \overline{S}_1 \rangle + \langle \overline{P}_3 \overline{S}_3 \overline{S}_2 \overline{S}_1 \rangle + \dots + \langle \overline{P}_k \overline{S}_k \overline{S}_{k-1} \overline{S}_1 \rangle \quad (3)$$

where \overline{P}_i and \overline{S}_i in (3) represent the faulty primary and secondary links, respectively. Both of these faulty links are caused due to the occurrence of an event E at a discrete point in time within a network. It should be noted that we only consider the values of the most forwarding links that one may find within the primary path links from the generic equation (2).

One of our observations about the two phases of the proposed scheme is the life time of the primary path which we use to transmit the packets to the desired destination in the presence of the faulty links. In other words, in order to effectively implement the proposed scheme, we must determine the minimum value of the life time for primary path links. This calculation is essential, since the ration of determining the accurate valid primary links is critically dependent on the knowledge of accurate values of lifetime. The minimum life time of primary path links is simply chosen from one of the primary links that has a smallest value for the life time. In other words, if one of the i th primary routes has the smallest life time value, this will be chosen as a minimum life time value for the primary path links. This hypothesis can be changed into a simple expression:

$$X_R = \text{Min} | X_{p1}, X_{p2}, \dots, X_{pk} | \quad (4)$$

where X_R in (4) represents the minimum life time value for the collection of all values in the primary path links. The right hand side expression of (4) represents the life time of each individual primary route starting from X_{p1} to X_{pk} . These values are considered as a life time of the sub links in the primary path. Similar to (4), we can further extend our

mathematical model for computing the interval of time for the RD procedure:

$$T = \text{Max} | X_{s1}, X_{s2}, \dots, X_{sn} | \quad (5)$$

where T represents the intervals of time for the RD and X_{si} represents the life time of the i th secondary route.

Equation (5) gives an estimate of the time to be taken by the proposed scheme for the RD procedure. This value is evaluated from the maximum values of the collected time in the sub links of the secondary path. The right hand side expression of (5) represents the life time of each individual secondary route starting from X_{s1} to X_{sn} . For the sake of the simulation and the performance evaluation, we assume that the value of T will be measured in millisecond. Combining (4) with (5), we can compute the value of the alternative route discovery as follows:

$$T = \text{Min} \left\langle \begin{array}{l} \text{Max}(X_{p1}, X_{s1}), \text{Max}(X_{p2}, X_{s2}, X_{s1}) \\ \dots \text{Max}(X_{pk}, X_{sk}, X_{sk-1}, \dots, X_{s1}) \end{array} \right\rangle \quad (6)$$

Equation (6) gives the value of the alternative RD. This can be considered as the optimum value which is determined from all the available maximum values for both the primary and the secondary links. Using (6), we can compute the values for the RD metrics which is one of the subparts of the proposed scheme.

$$Z_i = \text{Max} \langle X_{pi}, X_s, X_{si-1}, \dots, X_{s1} \rangle \quad (7)$$

where Z_i represents the maximum life time among all available values for both primary and the secondary paths.

Recall (1), we can now derive an expression for the frequency of RD using equations (2) to (6).

$$f_T(t) = \sum_{i=1}^N \left(\lambda_i e^{-\lambda_i t} \prod_{k=1, k \neq i}^N (1 - e^{-\lambda_k t}) \right) \quad (8)$$

where the right hand side of (8) represents the frequency of RD.

Equation (7) also has a significant impact on the RD for the alternate path. Implementing the results of (7) on (8), we can derive a new expression for the frequency of the RD which take into account the maximum life time among all available values for both primary and the secondary paths. In addition, this implementation describes the PDF in Z_i with respect to the RD metrics.

$$f_{Zi}(t) = \sum_{j=1}^{i+1} \left\langle \left(\lambda_j(i) e^{-\lambda_j(i)t} j^{(i)} t \right) \prod_{k=1, k \neq j}^{i+1} (1 - e^{-\lambda_k(i)t}) \right\rangle \quad (9)$$

where $\lambda_j^{(i)} = ki/l \rightarrow$ for $j = 1, 2, \dots, i$ and for $i/l \rightarrow j=i+1$.

Equation (9) describes the summation of all the possible routes which can lead us to the desired destination. Equation (9) can be further extended for the following given expressions:

$$T = \min \left\langle \max(X_{p1}, X_{s1}), \max(X_{p2}, X_{s2}, X_{s1}) \right. \\ \left. \dots \max(X_{pk}, X_{sk}, X_{sk-1}, \dots, X_{s1}) \right\rangle$$

$$Z_i = \max(X_{pi}, X_{si}, X_{si-1}, \dots, X_{s1})$$

$$T = \min(Z_1, Z_2, Z_3, \dots, Z_k)$$

Based on the above three expressions, we can approximate the PDF of T for the frequency of RD as follows:

$$f_T(t) = \lim_{dt \rightarrow 0} p[t \leq T \leq t + dt] / dt \quad (10)$$

Equation (10) gives the value for the frequency of the RD in terms of a PDF function. Relating (8) and (9) with (10), we can derive the following mathematical expression

$$f_T(t) = \sum_{i=1}^k f_{Zi}(t) \prod_{j=1, j \neq i}^k p[z_j > z_i] \quad (11)$$

$$f_T(t) = \sum_{i=1}^k f_{Zi}(t) \prod_{j=1, j \neq i}^k (1 - F_{Zi}(t))$$

where, $F_{Zi(t)}$ in (11) was introduced from (7) to make Z_i as a function of PDF.

Equation (11) shows that we derived the expected expression which can be used to compute the interval between the rout discoveries. In other words, one could use (11) to determine the frequency of the alternate RD process. The same frequency value can be used to measure the efficiency of the network. In addition, the final results show that the use of the proposed reverse direction scheme with the derived mathematical model can effectively minimize the transmission delay especially in the presence of collisions (links error) or faulty links due to the malfunctioning.

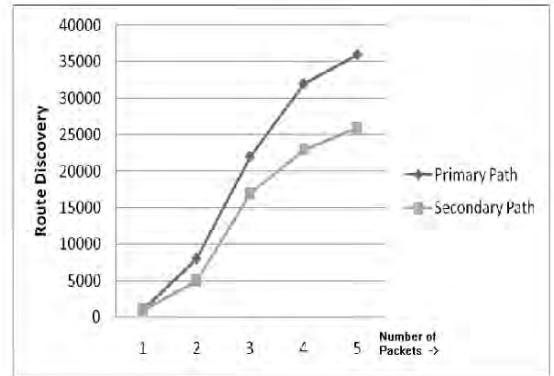


Fig.4. Number of nodes versus RD

III. SIMULATION RESULTS

We simulate our model based on the predicted data from the existing DSR model suggested in [1, 4]. For the sake of simulation and the performance evaluation, we consider two major metrics for RD and RM. These metrics are considered for the evaluation of the efficiency of a network.

For the sake of the first simulation (see Fig. 4), we characterize the behavior of the RD phase of the proposed scheme with respect to the number of nodes present in the network. The purpose of this experiment is to show the performance of the RD phase for discovering the alternate primary and the secondary path. During the simulation, we consider that as the number of nodes increases in the network, the more packets will be accumulated in the network that could affect the performance of the RD phase. It can be clearly evident in Fig. 4 that the RD phase of the proposed scheme performs better for the primary paths discoveries than for the secondary path. When we have small

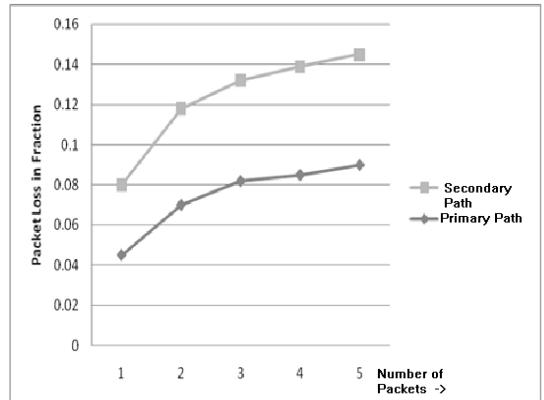


Fig.5. Packet loss in fractions versus number of nodes

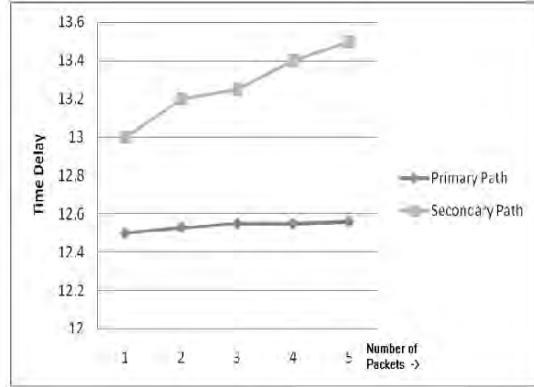


Fig. 6. Time delay versus number of nodes

number of nodes, it can be seen in Fig. 4 that the performance of the RD phase for both primary and secondary path discoveries is overlapping. However, as network grows in terms of the number of nodes, the performance differences between the primary and the secondary path is obvious.

Fig. 5 shows the packet losses (in the fraction value) with respect to the number of nodes during the transmission using both primary and the secondary paths. In addition, Fig. 6 represents a comparison between the time delay (represents in seconds) and the number of nodes. It can be seen in Fig. 6 that the time required to discover the primary paths using the RD phase is very low as compared to the time required to discover the secondary paths.

Based on the simulation results of Fig. 6, we can observe that the time delay for primary paths is not only small but also linear with respect to the number of nodes. In other words, when we increase the number of nodes in the network, more packets will be accumulated that make a linear increase in the time delay for discovering the secondary paths which is not really desirable as far as the optimum performance of the DSR protocol is concerned.

IV. CONCLUSION

In this paper, we presented a new scheme that improves the retransmission mechanism for the existing DSR protocol. In order to support our hypothesis, we provided a complete mathematical model that shows the formulation of the proposed scheme. In particular, we investigated the RD and the RM phases with respect to the proposed reverse direction scheme. We also showed that how effective the proposed scheme would be when we implement it with the reverse direction search for discovering the primary paths. Our analysis also suggested that the discovery of alternate primary paths from the current source of error significantly improves the network performance in terms of RD process, time delay, and the packet losses. Moreover, we have

experimentally verified that both the RD and the RM metrics perform well with the proposed scheme than the existing infrastructure of the DSR protocol. Our performance evaluation is also well supported by the simulation results presented in this paper.

REFERENCES

- [1] P. Papadimitratos and Z. Haas, "Secure Routing for Mobile Ad hoc Networks," In *Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio, TX, January 27-31, 2002.
- [2] J. Raju and J. Garcia-Luna-Aceves, "A comparison of on demand and table driven routing for ad-hoc wireless networks," In *Proc. IEEE International Conference on Communications (ICC 2000)*, June 2000, Volume 3, Issue 2000, pp. 1702 – 1706, 2000.
- [3] J. Raju and J. Garcia-Luna-Aceves, "Efficient On-Demand Routing Using Source-Tracing in Wireless Networks," In *Proc. IEEE Global Telecommunications (GLOBECOM 2000)*, Vol. 1, Issue 2000, pp. 577 – 581, November 2000.
- [4] B. Johnson, A. Maltz, and Y. Chun, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. (DSR)," *IETF INTERNET DRAFT*, 24 February 2003.
- [5] V. Park and M. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," *Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution (INFOCOM '97)*, pp.1405, 1997.

A New Analytical Model for Maximizing the Capacity and Minimizing the Transmission Delay for MANET

Syed S. Rizvi¹, Aasia Riasat², and Mustafa A. Khan³

Computer Science and Engineering Department, University of Bridgeport^{1,3}, Bridgeport CT, 06601

Department of Computer Science, Institute of Business Management², Karachi, Pakistan

{srizvi¹, mustafak³}@bridgeport.edu, aasia.riasat@cbm.edu.pk²

Abstract-The capacity of mobile ad hoc network (MANET) is typically determined by the size of network, routing protocol, mobility and the interactions that occur between the nodes. Moreover, these critical parameters cause the loss rate that has severed impact on the performance of the MANET. This situation even becomes worst when these critical parameters are chosen inappropriately. This paper presents an analytical model that incorporates most of the critical parameters that can influence the capacity of MANET. Based on the analytical model, an efficient 3-phase algorithm is designed to optimize the performance of MANET in terms of increased capacity and reduced transmission delay. The proposed 3-phase algorithm considers both delay-tolerant and delay-sensitive network traffics. In addition, the 3-phase algorithm can be used to approximate both the best and worst case capacities of MANET with the relaying and non-relaying nodes.

Keywords – Ad Hoc networks, capacity analysis, transmission delay, and bandwidth

I. INTRODUCTION

Much research has already been done for improving the performance of MANET [1, 2, 5]. The capacity of a fixed wireless network decreases as the number of nodes increases when all the nodes share a common wireless channel [1]. This scheme was shown to increase the capacity of the MANET in such a way that it remains constant as the total number of nodes increases in the system. More recently, [3] has proposed a two phase packet relaying technique. The main intention of this technique was to reduce the overall packet transmission delay. However, the delay experienced by packets under this strategy was shown to be large and it can be even infinite for a fixed number of nodes in the system, which has prompted more recent work presenting analysis of capacity and delay tradeoffs. However, the proposed 3-phase technique is highly efficient in such a way that it shows that the capacity of

MANET can be increased at the expense of comparatively small increased in the transmission delay.

According to the analysis of Gupta and Kumar [1], the capacity region of network is defined as $n(n-1)$ where n represents the number of nodes. Two types of capacities are typically measured: transport and throughput. The transport capacity is determined by multiplying bits and the distance per second whereas the throughput capacity is expressed simply by bits per second. In a MANET, the transport capacity is approximated as $O(\sqrt{n})$ bit-meter per second whereas the throughput capacity of each node is $O(1/\sqrt{n})$ bit per second. However, this analysis does not include the mobility of nodes. The proposed analytical model and 3-phase algorithm not only accounts the transport and throughput capacities of MANET but also considers the node mobility at one specific point. Our numerical and simulation analysis demonstrates that the capacity of MANET can be improved significantly if the critical parameters are set intelligently.

II. PROPOSED ANALYTICAL MODEL AND THE 3-PHASE ALGORITHM

Our proposed analytical model is based on the method proposed by Gupta and Kumar [1]. They considered a static model where all nodes are fixed and relaying is an allowable property of MANET. The node positions X_i are independent and identically-distributed in the open disk of a unit area. The destinations are chosen independently and the destination for each source node is chosen with respect to the node closest to a randomly chosen point on the disk. For such a static model, the upper and lower bounds on the asymptotically feasible throughput reaches to infinity for each pair of source and destination (S-D) [1]. However, the capacity of mobile nodes without relaying can also be computed [5]. This requires considering a model that consists of n nodes in an open disk of unit area where the radius can be approximated as $1/\sqrt{\pi}$.

Although, [3, 4] proved that the capacity of MANET is constant, but they did not determine the particular capacity at one certain point of time. In other words, the proposed algorithm considers the transmission time which involves one

¹Contact author: srizvi@bridgeport.edu,

particular pair of S-D. However, we use these 2 basic models to develop the proposed algorithm that considers both the delay time and the broadcasting between the nodes of MANET.

A. Proposed 3-Phase Algorithm

We use special scheduling policy [3], called as “ π ,” for our 3-phase transmission algorithm. This scheduling policy (π) selects S-D pairs randomly in each time slot t . Our transmission algorithm is divided into three phases. In the *first phase*, the transmission occurs only between the sender that has packets for transmission and the relay nodes as shown in Fig. 1. The relay nodes might have some part of packets which must be sent to the destination or between sender and destination if the nearest node of destination is sender node. In the *second phase*, these nodes move around in unit circle whose radius is $1/\sqrt{\pi}$. During the second phase, no transmission is carried out among mobile nodes until the relay nodes approach an appropriate destination node. Even though, this mobility of nodes may cause a delay time, this can not be influenced to the total throughput. Lastly, the processing of *third phases* begins when the location of mobile relay nodes is near the destination node as shown in Fig. 2. In such a case, the transmission can occur immediately between the relay and the destination nodes or between the S-D pair. It should be noted in Fig. 2 that the first and the last phases of the proposed algorithm are interleaved in a sense that the processing of first phase occurs in even time slots where as the processing of the last phase occurs in odd time slots.

B. Implementation of the Proposed 3-Phase Algorithm

In order to implement the proposed algorithm, we use scheduling model (π) that selects only one sender node which

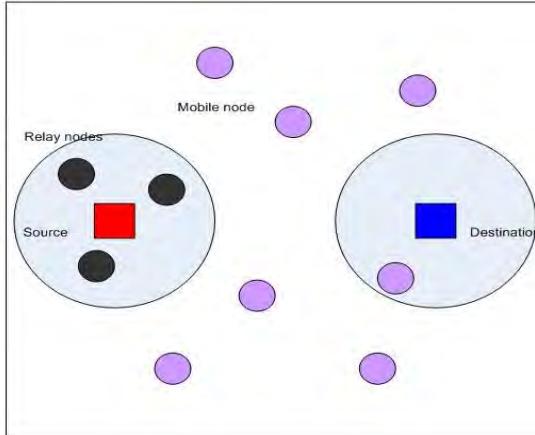


Fig. 1. Processing of the first phase. The biggest rectangle is *unit rectangle* which is 1m^2 . Small circle presents the distance at which nodes can communicate. This model has 12 mobile nodes and 3 relay nodes

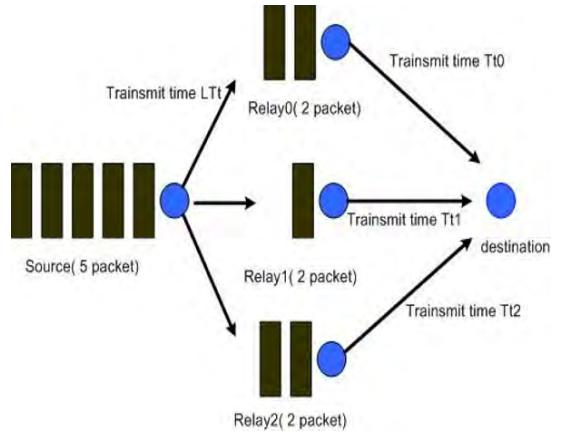


Fig. 2. Processing of the first and the third phase. The parameter L_p is set to 2, L_{Tt} is the transmission-time ≤ 2 packets, M is set to 3, P_0 is set to 2, P_1 is set to 1, P_2 is set to 2, and T_{t0} , T_{t1} , T_{t2} represents the required time to transmit 2, 1, 2 packets to the destination, respectively.

has 3 packets for transmission with one destination node within the unit circle which consists of n mobile nodes. Moreover, we assume that there are three mobile nodes which are located within the close proximity of the sender node. In other words, this second assumption implies that the transmissions can occur at distance of order of $1/\sqrt{n}$. In first phase, sender distributes each packet to 10 mobile nodes, so each mobile node (relay node) has a part of the sender's packets. In the second phase, these mobile nodes move around the unit circle. If some relay node(s) which has the part of the sender's packet enters within the close proximity of destination node, the transmission occurs immediately. Finally, in the third phase, the relay node(s) transmits the part of the sender's packet to the appropriate destination node. Both second and the third phases of the proposed algorithm are repeated until the destination receives the entire packets.

III. THE ANALYSIS OF BEST AND WORST CASE CAPACITIES

In this section, we present the analysis of the best and the worst case capacities for a MANET. Specifically, we show that how the proposed 3-phase algorithm can be implanted in order to compute the capacities for a MANET.

A. The Worst Case Capacity

For the worst cast capacity, it is assumed that the transmission occurs for the largest time. Also, we assume that P_i is the maximum number of packets that can be transmitted from the i th source node to a destination. The size of a

transmitted packet between each pair of S-D can not exceed to L_p . In the given scenario, each relay nodes may start transmission at different time. The packet transmission in MANET can be estimated as:

$$S - D \xrightarrow{\text{Transmission}} L_p + \sum_{i=0}^{M-1} P_i \leq 2L_p \quad \text{Property (1)}$$

where, M represents the number of relay nodes.

Moreover, if relay nodes transmission occurs at different times, then L_{Ti} represents the transmission time between the i th source and the other relay nodes. In addition, the source and the relay nodes are assumed to have the largest number of packets for transmission. Based on the above argument, the total transmission time can be approximated as follows:

$$\text{Transmission Time} = L_{Ti} + \sum_{i=0}^{M-1} T_{Ti} \quad \text{Property (2)}$$

Using (1) and (2), we can derive a closed form expression for estimating the worst case capacity (WC_{capacity}) such as:

$$WC_{\text{capacity}} \leq \left(2L_p / L_{Ti} + \sum_{i=0}^{M-1} L_{Ti} \right) \quad \text{Property (3)}$$

where the total delay time is set to 0

B. The Best Case Capacity

For the best case capacity, we consider the shortest transmission time between a pair of S-D. The shortest time is generated when the transmission starts simultaneously between the relay nodes and the destination node. This transmission time can be considered as a time in which the relay node has the largest packet size for transmission towards a destination. This time is the same as the transmission time between the source node and the relay node. This leads us to the following expression for the best case capacity: L_p/L_{Ti}

Finally, we can combine the result of worst and the best case capacities. When the characteristics of property (3) are true, the total transmission throughput reaches to $O(1)$ between node i and j at distance of order $1/\sqrt{n}$. We also assume that there is no direct transmission exists between the source and the destination system. Taking this into account, one can approximate the best and the worst case capacities such as:

$$\lim_{i \rightarrow \infty} \left(2L_p / L_{Ti} + \sum_{i=0}^{M-1} T_{Ti} \right) \leq \lambda(t) \leq (L_p / L_{Ti}) \quad \text{Property (4)}$$

where $\lambda(t)$ is the throughput with respect to the transmission time.

TABLE I THE RESULT OF RELAY MOBILE NETWORK WITHOUT REPRODUCTION				
NRN	Ttime (sec)	Delay (sec)	Throughput	
1	3	0.0112	3406232	14285.70
2	4	0.0096	5056653	16666.66
3	3	0.0112	3442331	14285.70
4	3	0.012	3515001	13333.32
5	5	0.0096	4160049	16666.66
6	8	0.0096	4758960	16666.66
7	6	0.012	5544597	13333.32
8	2	0.012	1378757	13333.32

NRN = THE NUMBER OF RELAY NODE, T_{TIME} = TRANSMISSION TIME, DELAY = DELAY TIME

C. Reducing Delay Time

The delay time is always generated with a certain probability with respect to a certain complexity such as of $O(1/n)$. In the given scenario, when the transmission occurs, relay nodes approach to appropriate destinations. The second phase of the proposed algorithm (see Fig. 2) can be effectively used to reduce the delay time by improving the probability (see Fig. 3 for delay reduction). We have shown that the second phase of the proposed algorithm improves this probability by asymmetrically distributing the packets that each relay node is supposed to transmit to other nodes. Based on the proposed approach, as the number of relay node increases that carry the identical packets, the probability of constructing the pairs of relay nodes and the destination nodes also increases. The improvement in the probability is in the order of $O(c/n)$, $c > 0$.

D. Numerical and Simulation Results

Before we discuss the simulation results, it is worth mentioning some of our key assumptions. We assume that the

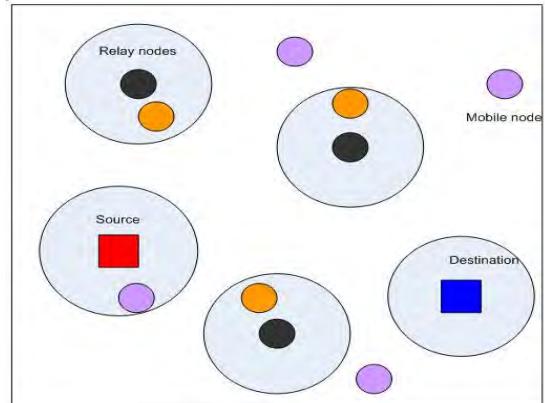


Fig. 3. This picture shows the improvement to reduce the overall delay time. The biggest rectangle is a *unit rectangle* ($1m^2$) where as the small circle represents the distance at which nodes can communicate. This model has 12 mobile nodes, 3 relay nodes and 3 reproduced relay nodes.

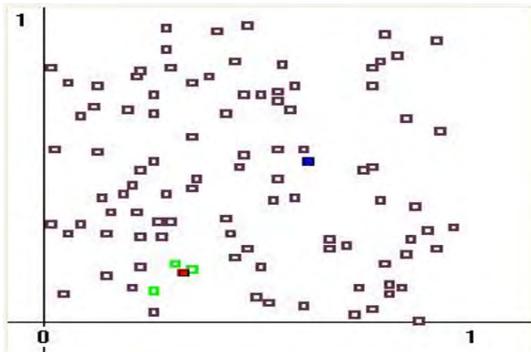


Fig. 4. This picture shows the location of mobile nodes in the simulation. The *unit rectangle* is 1m². The red, blue, and green nodes represent the source, destination, and the relay node, respectively. Simulation consists of 3 relay nodes and 100 regular nodes

location of a mobile node may change randomly as shown in Fig. 4. In addition, each node has enough buffer size with the maximum capacity of 80 kbps. We also assume that the packet size is typically 8 bits. For the sake of simulation, we consider a network that consists of 100 nodes where each node may transmit 10 packets. The simulation is run over a long period of time and the results are presented in Table I. It should be noted in Table I that the achievable throughput exists between the best and the worst case capacities. The proposed algorithm provides reduced delay time as shown in Table I.

IV. CONCLUSION

This paper presented an analytical model that uses special scheduling policy for the random selection of the S-D pairs. Based on the analytical model, we designed an efficient 3-phase algorithm that can be effectively used to analyze the capacities of MANET. The proposed algorithm considers the random selection of S-D pair which is essential in order to produce the correct approximation of best and worst case capacities. Our results have shown that the capacity of MANET can be improved by using the proposed algorithm. Also, the numerical results suggest that the transmission delay can be reduced even in the presence of node mobility.

REFERENCES

- [1] Piyush Gupta and P.Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, Vol. 46, pp. 388-404, 2000.
- [2] L. Jinyang, C. Blake, S. Douglas, D. Couto, I. Lee, and R. Morris, "Capacity of Ad Hoc Wireless Networks," *In the proceedings of the 7th ACM International Conference on Mobile*

- Computing and Networking*, pp. 61 – 69, Rome, Italy, July 2001.
- [3] M. Grossglauser and T. David, "Mobility increases the capacity of Ad-hoc wireless networks," *IEEE/ACM Transactions on Networking*, Vol.10, no. 4, pp. 477 – 486, 2002.
- [4] C. Schindelhauer, T. Lukovszki, S. Rührup, K. Volbert, "Worst case mobility in Ad Hoc networks," *Proceedings of the fifteenth annual ACM symposium on Parallel algorithms and architectures*, pp. 230 – 239, 2003.
- [5] C.-K. Toh, "Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Ad Hoc Networks," *IEEE Communications Magazine*, Vol. 39, no. 6, pp. 138 - 147 June 2001.
- [6] A.J. Goldsmith and S.B. Wicker, "Design challenge for energy constrained ad-hoc wireless networks," *IEEE Wireless Communication*, vol.4, pp.8–9, Aug. 2002.

Author Biographies



SYED S. RIZVI is a Ph.D. student of Computer Engineering at University of Bridgeport. He received a B.S. in Computer Engineering from Sir Syed University of Engineering and Technology and an M.S. in Computer Engineering from Old Dominion University in 2001 and 2005 respectively. In the past, he has done research on bioinformatics projects where he investigated the use of Linux based

cluster search engines for finding the desired proteins in input and outputs sequences from multiple databases. For last one year, his research focused primarily on the modeling and simulation of wide range parallel/distributed systems and the web based training applications. Syed Rizvi is the author of 15 scholarly publications in various areas. His current research focuses on the design, implementation and comparisons of algorithms in the areas of multiuser communications, multipath signals detection, multi-access interference estimation, computational complexity and combinatorial optimization of multiuser receivers, peer-to-peer networking, and reconfigurable coprocessor and FPGA based architectures.



AASIA RIASAT is an Associate Professor of Computer Science at Collage of Business Management (CBM) since May 2006. She received an M.S.C. in Computer Science from the University of Sindh, and an M.S in Computer Science from Old Dominion University in 2005. For last one year, she is working as one of the active members of the wireless and

mobile communications (WMC) lab research group of University of Bridgeport, Bridgeport CT. In WMC research group, she is mainly responsible for simulation design for all the research work. Aasia Riasat is the author or co-author of several scholarly publications in various areas. Her research interests include modeling and simulation, web-based visualization, virtual reality, data compression, and algorithms optimization.



MUSTAF A. KHAN is currently pursuing his M.S. in Computer Engineering from Computer Science and Engineering department of University of Bridgeport. Before coming to UB, he has worked for Pakistan Air force as a senior programmer on AS-400 machines for more than 5 years. His research interests include performance analysis of MANET, recourse optimization and management in wireless sensor networks, and multicast streaming over packet spwitching networks.

Faulty Links Optimization for Hypercube Networks via Stored and Forward One-Bit Round Robin Routing Algorithm

Syed S. Rizvi¹ and Adil Sheikh

Computer Science and Engineering Department
University of Bridgeport
Bridgeport, CT 06601
{srizvi, msheikh }@bridgeport.edu

Aasia Riasat

Department of Computer Science
Institute of Business Management
Karachi, Pakistan 78100
aasia.riasat@iobm.edu.pk

Abstract- Extensive research and studies have shown that the hypercube network is one of the most widely used techniques to build high performance parallel computers and it offers strong hierarchical structure with high symmetry properties. However, the performance of hypercube networks is mainly dependent on the link consistency between the nodes. Due to unexpected links failure and low connectivity, neither the hardware schemes nor point to point and multistage routing algorithms can be used without adding extra links. This paper presents a new stored and forward one-bit round robin routing algorithm that can efficiently send and receive messages between the nodes even in the presence of faulty links. In addition, we also examine and simulate the data throughput and hot spot properties of a hypercube network. Simulation results demonstrate that the proposed routing algorithm improves the overall performance of hypercube network by means of load-scalability that not only reduces the average waiting time per output queue but also increases the total data throughput even in the presence of faulty nodes.

Keywords— Faulty nodes, hypercube networks, load scalability.

I. INTRODUCTION

Advances in technology have dramatically increased the number of components typically needed to be simulated in a given design. One approach for providing improved simulation performance is the use of *parallel architectures*. A key component of parallel computer architecture is the interconnection network. This network enables the communication among different processors of the computer. Throughout the years, different interconnection networks have been used. One of the most popular and efficient networks is the hypercube network. This network has been used in different systems such as n-Cube, Intel IPSC etc.

With the continuous growth in network size, it is hard to find a large size network such as a hypercube network without the presence of faulty nodes and or links. It has been

shown that the performance of hypercube networks degrades as the number of faulty link increases in a large hypercube network [4]. When the number of faulty nodes increases in the system, the non-faulty reachable nodes of the network decrease proportionally. This, therefore, results performance degradation due to the lack of efficient routing algorithm that can provide full reachability to each non-faulty node of the network. This paper presents a new stored and forward one-bit round robin routing algorithm for hypercube networks which may consist of multiple nodes that can send random point-to-point messages to each other. The primary objective of this paper is to simulate the data throughput of a hypercube network as well as its performance in the presence of faults and hot spots. In addition, the simulation results of this paper allow one to examine the impact of different architectures on the overall performance of the hypercube networks. These different architectures include dimension of the hypercube networks, input parameter values such as the variation in total message generation rate per clock cycle, and the introduction of faulty links. We show that the performance of hypercube networks remain consistent even in the presence of multiple faulty nodes. Our analysis shows that the proposed algorithm maintains a consistent performance even in the presence of faulty nodes by making non-faulty nodes fully reachable.

The hypercube network has several attractive features. First, it has high connectivity between the various processors. In a P processor system, a message must traverse no more than $\log_2 P$ links before reaching its final destination and on average it may travel less than that distance [2]. Second, it is a multiple instructions multiple data (MIMD) machine, allowing the different nodes of a network to implement different component models [1]. Third, the architecture has good scaling properties. As the numbers of nodes grow in a hypercube network, the number of links required at each node increases logarithmically where as the required communication bandwidth increases linearly. Nodes in a hypercube network can also be viewed as a directed graph

¹Contact author: srizvi@bridgeport.edu.

where all interconnections between nodes occur in synchronous order. Each link may carry no more than one unit message in one step where each node during a step can send at most one message to each of its neighbors. Before going to present the performance and simulation model for hypercube networks, it is worth mentioning some of our key assumptions:

- The total number of nodes 'P' in the network is equal to 2^k where k represents the dimension of a hypercube.
- The total nodes P are identified with a unique node number in the range of $0 \dots 2^k - 1$.
- Every node in the hypercube network has k bi-directional links with the other nodes.
- Two nodes are said to be connected if and only if the binary their representations differ in exactly one bit order.
- The binary representation of a node in a hypercube network of dimension k has k bits (the exception is the singular case of hypercube with $k = 0$).

Fig. 1 is a graphical representation of hypercube network with a dimension of 1, 2, 4, and 8 nodes. A shortest path between any two nodes of a hypercube is represented as a sequence of nodes P_0, P_1, \dots, P_i where subscript i indicates the length of the path. In a hypercube network, multiple shortest paths can exist between any two nodes. For instance, if there are P total nodes exist and they are numbered from 0 to $P-1$ in such a way that addresses of connected nodes differ exactly by one bit in binary representation (see Fig. 2), then the hypercube network exhibits some desirable properties.

It can be evident in Fig. 2 that the routing in the cube is simplified to find any direct neighbor that reduces the number of bit differences between the address of the recipient and the address of the messenger. As an illustration, let P_0 and P_7 be the nodes in a k -dimensional hypercube network. The total number of bit positions at which these binary equivalents of P_0 and P_7 differ can be considered as the hamming distance H . In other words, the length of the shortest path between P_0 and P_7 is equal to the hamming distance H between them. For instance, in Fig. 2, in order to route a message from a node P_0 (000_2) to a node P_7 (111_2), the path through node P_4 (100_2) and P_6 (110_2) can be used as an optimal path since at each node along the path the bit differences with P_7 (111_2) are reduced by one.

The remainder of this paper is organized as follows.

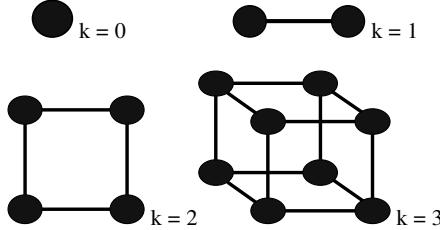
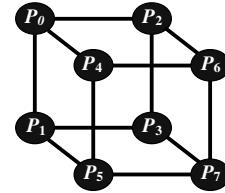


Fig.1. Hypercube interconnection networks for multiple dimensions



For example:
$P_0 = 0 = 000$ can go to P_1, P_2 , and
P_4 . This can also be represented
as:
$P_0 = 0 = 000$ $\rightarrow P_1 = 1 = 001$
$P_2 = 2 = 010$ \rightarrow
$P_4 = 4 = 100$ \rightarrow
<i>H. Distance</i> $\quad \quad \quad$ <i>One Bit</i>

Fig.2. Numbering scheme for three dimensional hypercube networks

Section II presents some of the well known routing algorithms used in hypercube networks for message routing. Section III presents the proposed stored and forward one-bit round robin algorithm. In Section IV, we examine and simulate the data throughput and hot spot properties to determine the overall performance of the proposed algorithm. Finally, Section V concludes the paper.

II. ROUTING ALGORITHMS FOR HYPERCUBE NETWORKS

Substantial efforts have been devoted to the study of message routing algorithms for hypercube networks. Routing algorithms for hypercube network are broadly classified into two categories: *oblivious* routing and *adaptive* routing. In an *oblivious* routing algorithm, the path of one message is unaffected by the presence of other messages in the network. On the other hand, in an *adaptive* routing algorithm, messages may be directed away from the congested parts of the network [3, 12]. Optimal routing for given paths on arbitrary networks has been studied extensively in the context of store-and-forward algorithms [7, 8]. Routing algorithms, in which packets do not strictly follow specific paths, are *matching routing* [9] and *hot-potato routing* [10, 11].

In randomized routing, a message is sent from a source to a destination in two stages [5, 6]. In the first stage, the message is sent from the source to a random intermediate node. In the second stage, the intermediate node forwards the received message to the intended destination. In each stage of randomized routing, the message is routed using the *bit-fixing* algorithm, which is also known as *dimension-order* and the *e-cube* routing algorithms. The randomized routing algorithms are fast and can solve any one-to-one packet routing problem on a P -node hypercube in the order of $O(\log P)$ packet steps [5]. One drawback to such algorithm, however, is that they all require in order of $O(\log^2 P)$ bit steps when implemented on real parallel machines such as

the Connection Machines. Since packets always contain at least in order of $\log(P)$ bits of addressing information, a typical packet step really consists of $O(\log P)$ bit steps [6].

In bit-fixing routing algorithm, dimensions are ordered in an arbitrary way and a message is always typically directed along the lowest dimension of the network in which its current position and its final destination differ [3]. A simple implementation of this algorithm is shown in Fig. 3. The following are the essential steps perform in bit-fixing algorithm.

The routing via bit-fixing algorithm can take exponential time. Consider a permutation on the n-cube where $n = 4$ and to route a packet from 0000 to 1111, the bit-fixing routing algorithm uses the following path: $0000 \rightarrow 1000 \rightarrow 1100 \rightarrow 1110 \rightarrow 1111$. It has been shown [5, 12] that this simple permutation causes the bit-fixing routing

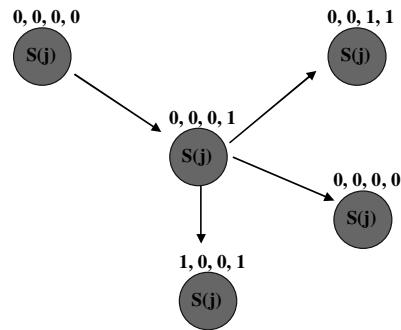


Fig.3. Example of bit-fixing routing algorithm

Formal Specification of the Proposed Store and Forward One-Bit Round Robin Routing Algorithm

- 1- Starts searching the nodes
Search Node_Address [Minimum] to Node_Address [Maximum]
- 2- Check the status of each visiting node
 - 2.1. [Set Node status]
 - Set Node Status == Sending or
 - Set Node Status == Receiving

[Repeat Step 2.2 or Step 2.3] While Node ≠ NULL
 - 2.2. [Check the Condition] If Node Status = Sending Then
 - Set Node Status == Creating a Message or
 - Set Node Status == Receiving a Message or
 - Set Node Status == Sending a Message or
 - Set Node Status == Idle

[End of Step 2.2]

[Go back to step-2] Advanced to Next Node
 - 2.3. [Check the Condition] If Status = Receiving Then
 - 2.3.1. Implement Round Robin Scheduling Algorithm
 - [Start Sequential Search for Node Status]
 - 2.3.1.1. If Node = Busy Then
 - 2.3.1.1.1. Advanced to Next Node
 - 2.3.1.1.2. Go back to Step 2.3.1
 - 2.3.1.2. If Node ≠ Busy Then
 - [Start Sequential Search for each outgoing link status]
 - 2.3.1.2.1. If Link = Busy Then
 - Advanced to Next Lin
 - 2.3.1.2.2. If Link ≠ Busy Then
 - [Get message from the free-node]
 - [Change the status of each node]
 - Set Sink Node ==BUSY
 - Set Destination Node = BUSY
 - 2.3.1.2.3. Advanced the Link
 - 2.3.1.2.4. Go back to Step 2.3.1

[End of Step 2.3(Round Robin Scheduling Algorithm for Message Reception)]

[Go back to Step 2] Advance to Next Node
 - 2.4. [End of Step-2]
[Go back to Step-1]
- 3- [End of Step-1]
[EXIT]

algorithm to take in order of $\Omega(2^{n/2})$ steps to route a message. From the performance point of view, the resultant computational complexity is not desirable.

III. PROPOSED STORED AND FORWARD ONE-BIT ROUND ROBIN ROUTING ALGORITHM

The proposed routing algorithm shows some good load-scalability characteristics among the hypercube nodes. One of the reasons for achieving high scalability is due to the use of round robin scheduling algorithm. Instead of separately using a scheduling algorithm on each output queue, we implement the round robin algorithm as a part of our proposed routing algorithm. By doing this, we greatly reduce the average waiting time of each output queue associated with each outgoing link. In other words, the proposed routing algorithm improves the overall performance of hypercube network by means of load-scalability that not only reduces the average waiting time per output queue but also increases the total data throughput even in the presence of faulty nodes. Our choice for using the round robin scheduling algorithm with the proposed routing algorithm is due to the fact that it is both simple and easy to implement as well as starvation-free. The advantages of the proposed routing algorithm such as the reduced average waiting time per output queue and consequently the improved data throughput can be evident in our simulation results.

A. Formal Specification of Proposed Routing Algorithm

The proposed routing algorithm starts by searching nodes in a hypercube network. The searching is performed in a sequential manner starting from the minimum value of the node-address to a maximum value. For instance, in a three dimensional hypercube networks, the proposed routing algorithm starts searching node addresses from *000* and goes in a sequential manner and ends to address *111*. The proposed routing algorithm continues searching nodes in a sequential manner until the node array becomes empty. Once it reaches to the end of the array, the algorithm starts over again and this cycle of searching goes on.

B. Implementation Of The Proposed Routing Algorithm

We assume that a node in a hypercube network can either generate a message or receive a message but not both during the same clock cycle. Fig. 4 shows the internal architecture of each node in a hypercube network that includes one processor *P*, one communication interface *C*, and four incoming and outgoing links. Each link in the node architecture has an output queue for outgoing messages. It should also be noted that there is no input queue for incoming messages as shown in Fig. 4. This assumption implies that each incoming message for a destination node simply goes into sink. We assume that a node can receive or send a message during a cycle. This implies that while *C* is getting a message from a different node through one of its links, it can not send a

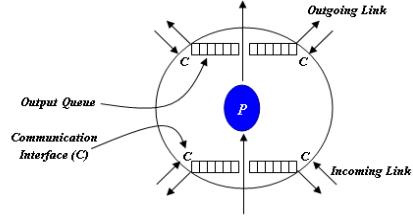


Fig. 4. Internal architecture of a node in a hypercube network

message out from an output queue from a link different than the one currently receiving a message as shown in Fig. 4. This assumption further leads us to the following two facts: An incoming message for a destination node can either directly go into an output queue or be absorbed by the processor. A message needs to wait at least one cycle before it can be sent once it is received. In other words, you cannot receive a message and send it out during the same cycle as if the node did not exist.

For the sake of simulation, we assume that a hypercube network can have at most 256 nodes at one time. In other words, for ease of understanding, our simulation supports at most 8 dimensional hypercube networks that can have at most 256 nodes. In addition, step 2.3 of the above algorithm shows the use of round robin scheduling algorithm for selecting communication link to receive messages. For instance, when a certain node is in the busy state (i.e., the current state of the node is either sending or receiving or idle), it can not receive messages from other nodes. Once the proposed routing algorithm gets a free-node, it implements round robin scheduling algorithm to check the status (Busy or Free) of each outgoing link attached to the output queue. These communication links are further attached to other nodes as shown in Fig. 5.

Once the round robin scheduling algorithm gets a non-busy link, it performs the following tasks. First, it checks the output queue of the attached node to see if there any message to read. If the output queue is empty, the round robin algorithm advances to the next communication link.

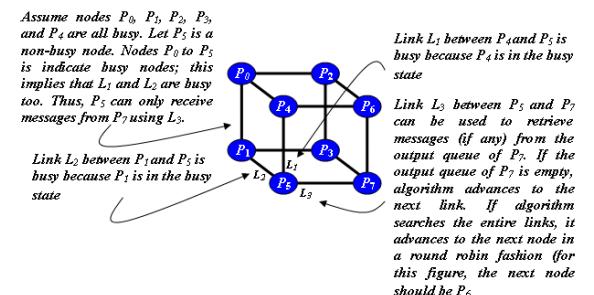


Fig. 5. Implementation of the proposed one-bit round robin routing algorithm

Secondly, if the output queue is not empty, the sinking node starts retrieving the message from the output queue of the attached destination node. Finally, the round robin algorithm changes the status of both sinking node and the communication link and set them as busy. It should be noted that the advancement of the round robin algorithm from the current link to the next communication link. If we do not advance to next link, the proposed routing algorithm does not achieve the load-scalability that results higher values of average waiting time in output queue. The higher values of average waiting time in output queue reduce the overall data throughput of hypercube networks.

IV. PERFORMANCE ANALYSIS AND SIMULATION RESULTS

We categorize our performance analysis of hypercube network in two parts. The first part describes the performance of hypercube network when all communication links are in operational mode. On the other hand, second part of performance analysis presents simulation results in the presence of broken links or faulty nodes.

A. Simulation Results Without Introducing Broken Link

For this section, we set the dimension of hypercube network to three and create 8 nodes. Furthermore, we run all simulations for 10000 cycles. In addition, the hot spot property is also set to zero.

Fig. 6 presents the total number of messages *created* and *received* with respect to different probabilities of message transmission. Probability of message transmission is a probability that a node creates a message per cycle. Fig. 6 represents total message creation reception without the presence of faulty link (i.e., the link-fault is set to zero). It can be seen in Fig. 6 that as we increase the probability of message creation, more messages will be created and randomly sent to other nodes of a hypercube network. On the other hand, Fig. 6 demonstrates the total number of messages

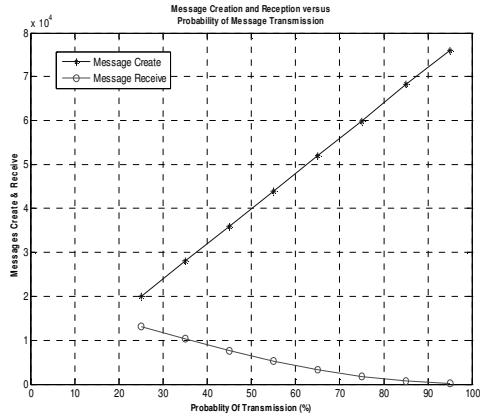


Fig.6. Message creation and reception versus probability of message transmission

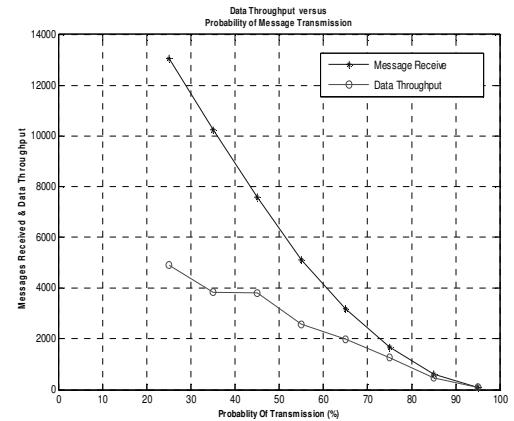


Fig.7. Data throughput versus probability of message transmission

received successfully by the network's nodes. As we create and send more messages, the hypercube network becomes congested which results poor message reception as shown in Fig. 6. This implies that the probability of message transmission is directly proportional to message creation where as it is inversely proportional to message reception.

Fig. 7 shows the data throughput with respect to probability of transmission. The data throughput is the product of utilization per node and the total messages received successfully. This is obvious that the reduction in the messages received per node results in the reduction of data throughput. It should be noted that the data throughput in Fig. 7 represents the number of messages received per node in total cycles (i.e., we set the design parameter (C_{Total}) 10000 cycles for all simulations we run). For instance, when we have 25% of probability, the total number of messages received is 13043 that generate approximately 4891 messages per node. This implies that each node processes approximately half message (0.489 messages) of information per clock cycle. It can be seen in Fig. 7 that the throughput reduces due to the reduction in the total messages received successfully.

B. Simulation Results In The Presence Of Faulty Link (FL)

For this section, we introduce a faulty link. As one can easily observe that the introduction of faulty link in hypercube network reduces both the message transmission and the reception. By carefully looking at the simulation results of Fig. 8, one can make a conclusion that broken links in hypercube network are more affected to message reception as compared to message transmission. With harmony to our expectations, the simulation results of Fig. 8 shows a nice reduction in both message transmission and reception.

Fig. 9 shows the simulation results for utilization per node and the data throughput in the presence of faulty links. It should be noted in Fig. 9 that an average utilization per node

in the presence of faulty link is the same as in the presence of no faulty link except at one place. This is due to the fact that the utilization per node heavily relies on the total number of messages generated and received. As we have mentioned in Fig. 8 that the presence of faulty link does not have any sever effects on message creation when compared to message reception. This implies that the message creation in the presence of faulty link dominates the total number of messages created and received per node and thus cancels out the effects of reduced message reception on the utilization.

This is one of the reasons that why utilization per node remains the same for both faulty and non-faulty link. On the other hand, the data throughput in the presence of faulty link has decreased slightly as shown in Fig. 9. It should be noted that the data throughput is a product of utilization per node and the total number of messages received successfully. Since the utilization is same for both faulty and non-faulty links, the reduction in the total number of received messages due to a faulty link causes a slight decrease in the data throughput. However, the overall data throughput performance is almost overlapping for most of the values of transmission probability as shown in Fig. 9.

V. CONCLUSION

In this paper, we have presented a simple stored and forward one-bit round robin routing algorithm for an efficient transmission and reception of messages between the nodes within the hypercube network. Our simulation results demonstrated that the proposed algorithm maintains a consistent performance even in the presence of faulty links. In addition, our experimental verifications suggest that the proposed routing algorithm improves the overall performance of hypercube network by means of load-scalability that not

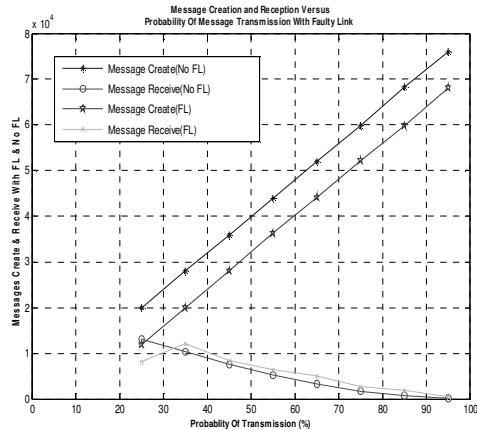


Fig.8. Message creation and reception versus probability of message transmission with faulty link (FL)

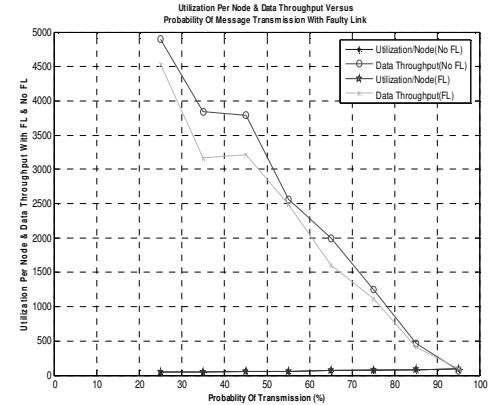


Fig.9. Utilization per node and data throughput versus probability of message transmission with faulty link (FL)

only reduces the average waiting time per output queue but also increases the total data throughput for both faulty and non-faulty links. Finally, the algorithm presented in this paper is obviously not only restricted to hypercube networks. Instead, the proposed algorithm can be implemented to any hierarchical networks structure such as mesh networks which is a generalization of hypercube network.

REFERENCES

- [1] K. Shin and P. Ramanathan, "Clock synchronization of a large multiprocessor system in the presence of malicious faults," *IEEE Trans. Computers*, vol. 36, Issue. 1, pp. 2-12, Jan. 1987.
- [2] D. Peleg and J. Ullman, "An optimal synchronizer for the hypercube," *Soc. Indust. Appl. Math.*, vol. 18, Issue. 4, pp. 740-747, Aug. 1989.
- [3] M. Harrington, "New method for synchronizing distributed systems in the presence of faults," *MSEE thesis, Dep. Elec. Eng., Univ. of Washington*, March. 1991.
- [4] M. Harrington and A. Somani, "Synchronizing hypercube networks in the presence of faults," *IEEE Trans. on Computers Archive*, vol. 43, Issue 10, pp. 1175 - 1183, 1994.
- [5] M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*, Cambridge University Press, January 31, 2005.
- [6] R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, Cambridge, UK, 2000.
- [7] T. Leighton, B. Maggs, A. Richa, "Fast algorithms for finding O (Congestion + Dilatation) packet routing schedules," *Combinatorica*, vol. 19, pp. 375-401, 1999.
- [8] F. Meyer and V. Åocking, "Shortest-path routing in arbitrary networks," *Journal of Algorithms*, vol. 31, pp. 105-131, 1999.
- [9] N. Alon, F. Chung, R. Graham, "Routing permutations on graphs via matching," *SIAM Journal on Discrete Mathematics*, vol. 7, pp. 513-530, 1994.
- [10] I. Ben-Aroya, D. Chinn, A. Schuster, "A lower bound for nearly minimal adaptive and hot potato algorithms," *Algorithmica*, vol. 21, pp. 347-376, 1998.
- [11] C. Busch, M. Herlihy, R. Wattenhofer, "Hard-potato routing," in *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pp. 278-285, 2000.
- [12] J. Kim and K. Shin, "Deadlock-free fault-tolerant routing in injured hypercube," *IEEE Trans. on Computers*, pp. 1078-1088, September 1993.

Improving the Data Rate in Wireless Mesh Networks Using Orthogonal Frequency Code Division (OFCD)

¹Jaiminkumar Gorasia, ¹Syed S. Rizvi, and ²Aasia Riasat

¹Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT-06604

²Department of Computer Science, Institute of Business Management, Karachi, Pakistan

¹{jgorasia, srizvi }@bridgeport.edu, ²aasia.riasat@iobm.edu.pk

Abstract:- In the present scenario, improvement in the data rate, scalability and throughput are some of the most time consuming issues in Wireless Mesh Networks (WMN). This paper discusses one of our proposed methods, i.e., improving data rate in Wireless Mesh Networks by redefining the mesh transceiver with the help of OFDM and CDMA called OFCD. The details are set down by dividing the transceiver into transmitter and receiver which incorporates OFDM and CDMA techniques.

Keywords - WMN, mesh topology, mesh routers, mesh clients, multihop, scalability and different layers of TCP/IP, OFDM, CDMA

I. INTRODUCTION

For more connectivity, mesh routers are equipped to provide connectivity between different networking technologies such as Wi-Fi, IEEE 802.11, mobile technology and wired Ethernet. In WMN, each client with same radio technology communicates via Ethernet links, for different clients communications are first made with their base station which has Ethernet connections to the mesh routers. Sometimes client nodes actually form network to perform routing and this kind of infrastructure is called client wireless mesh networks. Mesh clients can perform mesh functions with other mesh clients as well as accessing the network through routers yielding hybrid wireless mesh networks.

WMN's operation is similar to the way that packets are routed over the wired Ethernet i.e. data hops from one device to another until it reaches its destination. This is possible only when each node shares its dynamic routing algorithm with every single node to which it is connected. The routing algorithm implemented in each node takes the fastest route to its destination.

As it is mentioned before, WMN is the most recent network technology it attracts researchers to do some more development and improvement in it. As the part of

it this paper is focused on the improvement of the scalability and data rate [15]. There are some more research doing on better routing [13] [14]. There are only adaptive radios in mesh networks, a device in a mesh network will only connect with other devices if they are in a set range. If natural load balancing system has more devices in a network it will offer more bandwidth.

Since in WMN's there are no central servers each node (client) transmits data to as far as the next node. As a result of each node behaving like a repeater it forms an externally big network analogous to the internet. Now in today's scenario, hybrid WMN's have taken place of basic WMN's. The basic advantage of Hybrid WMN is that in the Hybrid MWN network can be accessible either through mesh routers or through mesh clients. It supports all different kinds of network technologies like wired Ethernet, mobile communication, Wi-Fi, Wi-MAX, IEEE 802.11 etc.

The access points form a wireless backbone, providing connectivity in places otherwise it is difficult to access through traditional wired infrastructure. The wireless communication between the access points can use different technologies such as IEEE 802.11a/b/g or IEEE 802.16 and different hardware (directional or Omni-directional antennas). The use of multi channels in wireless network leads to throughput and reduced delay. One class of such protocols divides the available channels in two classes, control and data channels. Control channels are used to exchange network control information, while data channels are used for data transfer [3] [4]. The use of multi transceiver allows a node to scan all available channels concurrently, hence solves many complex problems.

II. RELATED WORK

As it is mentioned before, this paper is focused on the improvement of scalability and throughput by some

modification of the mesh antenna. To redesign the mesh antenna, the combined technology of OFDM (Orthogonal Frequency Division Multiplexing) and CDMA (Code Division Multiple Access) is used.

OFDM is a multi carrier modulation in which multiple user symbol are transmitted simultaneously using different sub carrier [5]. Sub carriers used in OFDM have overlapping spectrum but their waveforms are orthogonal [6]. With the help of cyclic prefix longer time duration symbols are transmitted and these transmitted bits have a length longer than the length of impulse response of the channel [7]. By this way Inter Symbol Interference (ISI) is avoided which plays critical role in multipath delay spread. When the channel impulse response gets changed during an OFDM block, orthogonality of the sub channel is lost [7]. But still OFDM is much efficient for restricted wireless communication.

CDMA is a spread spectrum technique which uses no frequency channels or time slots. In CDMA, pseudo random noise (PN) code which is usually of large bandwidth is multiplied with a narrow band message. In CDMA all users use same frequency band and they are free to transmit simultaneously [9].

Using OFDM and CDMA symbols are transmitted on many carriers. With OFDM technique frequency selectivity in multipath fading channel is resolved [8]. The MC-CDMA i.e. Multi Carrier CDMA is a combination of OFDM and CDMA. It uses WALSH code (it is an orthogonal spreading code sequence) in frequency domain [9]. By this frequency, diversity is achieved. The WALSH code differentiates different users and can handle number of different users, even providing good BER (Bit Error Rate). Different spread input symbols are fed to the sub carriers, when OFDM and CDMA are combined [10]. In MC-CDMA, all data symbols are not transmitted on each sub carriers. But they are transmitted on some channels. Those few channels on which data symbols are transmitted are chosen after channel assignment. Thus a problem of flat fading is resolved as only some of the bits are lost. Each sub carrier is used by different users and these users are differentiated by WALSH code. Spreading technique is used in time domain. In MC-CDMA, with receiver using FFT and variable gain diversity combiner, signal can be easily recovered. Hence transmitting and receiving a signal can be easily solved [10].

III. PROPOSED TRANSMITTER AND RECEIVER MODEL

All system variables, along with their definition, are listed in Table I. Before we present the proposed models

TABLE. I
NOTATION USED IN ANALYSIS

Notation	Related Quantities
N	Number of channels
N	Number of nodes in unit area
T _f	Frame length
S _a	Number of contention slots
S _d	Number of data slots
T _a (interval length)	Contention duration
T _d (length of data interval)	Data duration

for transmitter and receiver, it is worth mentioning some of our key assumptions:

- There are n available channels, each has equal bandwidth.
- The access points can receive data on multiple channels simultaneously; this is a reasonable assumption since the access points can be more specialized higher end device compared to a simpler client that it serves.
- The channels are orthogonal and code division multiple access (CDMA) scheme is used, i.e. transmission on a channel do not interfere with transmission on any other channels. Here a channel may represent a code or a frequency band (OFDM-CDMA modulation technique).
- Each network node including the base station is equipped with multi radio, multi transceiver which is capable of performing in full duplex mode. Hence each node can either transmit or receive a signal on channel at any point of time. The nodes can however switch to different channels dynamically.
- The network is synchronized [11].

A. Static And Mobile Observer

For multi hop mesh network, we consider the hybrid architecture as it is the most widely deployed architecture. This architecture is characterized by the fact that mesh clients do not need direct connection to a mesh route, but can connect multi hop over mesh clients to a route. The advantages are improved connectivity and coverage. And the disadvantages are that mesh clients need more resources because they also need to have routing capability. Let's assume there are N sensor nodes distributed over an area A . Sensors are assumed to be independently and uniformly scattered over a region of interest [12]. n - Nodes are assumed to be distributed independently and uniformly over an area of πr^2 . Each

node can communicate with every other node within the radius r where,

$$\pi r^2 = (\ln n + c(n))/n$$

The networking is connected with unit probability if and only if $\lim_{n \rightarrow \infty} c(n) \rightarrow \infty$. From this, we can choose the

transmission range. After flooding the network is organized into a tree with the observer at its root. In the first step of flooding the observer first broadcasts a wakeup signal. All sensors within direct communication range hear this signal and reply to the observer, upon this observer registers them as first level nodes in the node tree and instructs them to repeat the process of broadcasting in a time shared manner to avoid collisions.

All the nodes encountered as a result of these new broadcasts and have not been encountered previously, are registered as second level nodes. Then the second level nodes broadcast and process repeat until all nodes have been registered. Whenever a node broadcasts wakeup signal, it also attaches its unique address and chain of nodes which leads to it, from the observer. Nodes that are wakened up by broadcast are designated as children of broadcasting node. These children obtain the chain of nodes leading from observer to them by concatenating the last link with the chain, leading to their parent. A node obtains a route to observer by reversing this chain.

The same reasoning suggests that a fewest-hop route should be optimal even in a mobile observer network. But since the observer does not stay at a fixed position, the fewest-hop route is time variant in nature, and so is the number of hops. Quite obviously, the best solution is to choose the route which consists of the fewest hops at any time. In other words, if $S = Ns_1, Ns_2, Ns_3, \dots$ is the set of all the nodes that come within direct communication range of the observer at any time, then the fewest-hop route to the observer is the shortest of the fewest-hop routes to any of the nodes in S joined with the link between the corresponding node in S and the observer.

Finding the shortest route in practice involves a procedure very similar to the flooding described in section 4.1.1, but with one difference. The 1st level nodes (those belonging to the set S just described) are discovered by moving the observer on its path while transmitting a wake-up signal to all nodes that are within range. These nodes are registered as 1st level nodes. The remaining process of flooding proceeds exactly as described in section 4.1.1. At the end of it, each node in the network knows its route to one of the nodes in S that communicate directly with the observer.

TABLE II
NOTATIONS USED IN PROPOSED TRANSMITTER AND RECEIVER MODEL.

Notation	Related Quantities
$x(k)$	Input from digital data source
x_1, \dots, x_N	Parallel data symbols
f_1, \dots, f_N	Carrier frequency
C_b	PRN codes
X_n	Symbol mixed with PRN codes
χ_k	Output of the mixer
Y_k	Output of IDFT block
$x(t)$	Analog received signal
$w(k)$	Non negative weight function
X_k	Output of DFT
$X(k)$	Output of mixer at receivers end
$n(t)$	White additive Gaussian noise
G	Guard time matrix

B. OFCD System Model

This is a hybrid combination of OFDM and CDMA spread spectrum modulation technique. All system variables, along with their definition, are listed in Table II.

Transmitter Model: As shown in Fig. 1, $x(k)$ is the discrete digital data which a transmitter will receive from digital data source where k represents discrete time. The serial to parallel converter will convert $x(k)$ into n number of parallel data symbols with a symbol rate of $1/T$. The parallel symbols are $x_1(k)$ to $x_n(k)$. QPSK block is used which will have the carrier frequency f_1 to f_n as its other inputs. The QPSK block will split the input bit stream into in-phase and quadrature phase components. The quadrature components and the in-phase components will be modulated with f_1 to f_n carrier frequencies. The output of QPSK block would be $x_n(k) + f_n$, which is then supplied to the mixer. At mixer, PRN code C_b will mix with the incoming signal $x_n(k) + f_n$. So, the output is

$$X_n = [x_n(k) + f_n].C_b$$

The Inverse Discrete Fourier Transform (IDFT) would be used for modulation and it is described as

$$Y_k = \sum_{n=0}^{N-1} X_n e^{-\frac{2\pi i k n}{N}}$$

where $k = 0, \dots, N-1$. The last symbol coming out of IDFT block is taken and added on the beginning of source code block to provide guard time which in fact will provide

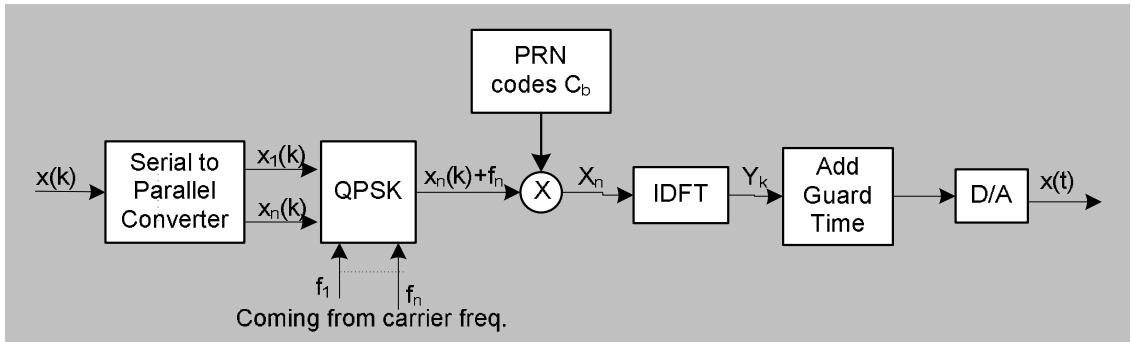


Fig. 1. Proposed Transmitter Model

orthogonality (Analogous of OFDM). If the last symbol coming out of IDFT block is X_n . Then,

$$\langle \chi_k, Y_k \rangle = \int_a^b \chi_k \cdot Y_k \cdot w(k) dk$$

Where $w(k)$ is the non negative weight function and χ_k and Y_k would be orthogonal if,

$$\int_a^b \chi_k \cdot Y_k \cdot w(k) dk = 0$$

As the input bit stream can be of infinite length, so for infinite integral

$$\int_{-\infty}^{\infty} \chi_k \cdot Y_k \cdot w(k) dk = |X_k|^2 = |X_n|^2$$

After digital to analog conversion, discrete digital signal would be converted into analog signal and then would be transmitted over the medium.

Receiver Model: In Fig. 2, $x(t)$ is the received signal which can be shown as:

$$x(t) = F^{-1}[X_k] + n(t)$$

where $n(t)$ is the noise which gets added during the transmission. The signal has been passed through the guard time removal block to remove the guard time G .

$$G = (0_{N \times l} \quad 1_{N \times N} \quad 0_{N \times N})$$

where G is a matrix of 0's and 1's. Receiver will perform Discrete Fourier Transform (DFT) to demodulate the signal. DFT can be represented as

$$X_k = \sum_{n=0}^{N-1} x_n \cdot e^{-\frac{2\pi i}{N} kn}$$

where $k = 0, \dots, N-1$. X_k is then fed to the mixer which will mix it with the PRN code C_b which is deterministic to the receiver. As we are deploying the CDMA's feature, the receiver should know the seeds of the PRN codes which were used at the transmitter. The output of mixer is represented by $X(k)$ and can be represented as

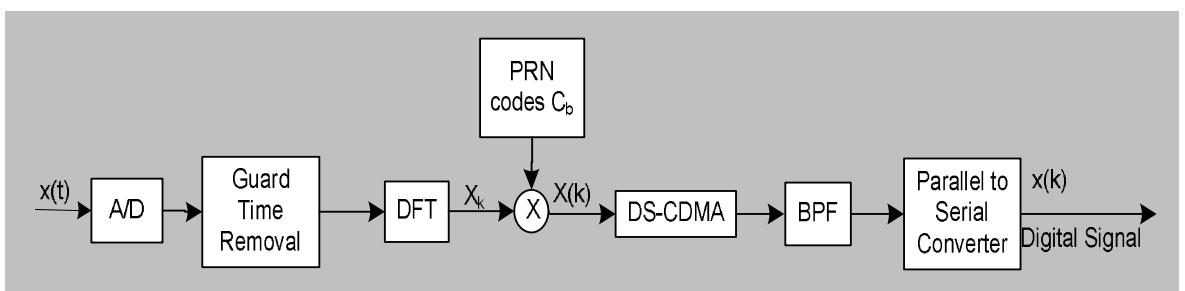


Fig. 2. Proposed Receiver Model

$$X(k) = C_b X_k$$

The Direct Sequence Spread Spectrum technique i.e. DS-CDMA is used to detect $X(k)$. DS-CDMA will simply perform the XOR operation between the PRN codes and the signal coming out of the mixer $X(k)$. The unique chip sequence is used by DS-CDMA depends on the number of seeds used by the transmitter. Band Pass Filter(BPF) will pass only a certain range of frequency by considering the maximum and minimum frequency components of the carrier frequency. If f_h is the highest frequency component and f_l is the smallest frequency component then $f_{BPF} = f_h - f_l$ and those detected signals will be passed which lie in the frequency range of f_h-f_l . With the parallel to serial converter original transmitted signal $x(k)$ will be recovered.

IV. CONCLUSION

In this paper, we have studied a multi radio multi channel Wireless Mesh Network (WMN) using OFCD which amalgamates the advantages of OFDM and CDMA. A transmitter and a receiver model are described with the help of useful mathematical expressions. This is a simple and a realistic technique and has good performance properties. In very noisy multipath channel the proposed hybrid scheme is expected to work efficiently and will give good Bit Error Rate (BER) value. We have also highlighted the potential of multi-radio wireless mesh networks, along with primary technical challenges that must be addressed for widespread deployment of such networks. Wireless mesh networks present a promising solution by extending network coverage based on mixture of above wireless technologies through multi-hop communications.

REFERENCES

- [1] F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey", Computer Networks (2005).
- [2] P. Kyasanur and N. Vaidya "Routing and interface assignment in multi channel multi interface wireless networks" Proc. Of IEEE WCNC 2005.
- [3] S.L. Wu and C.Y. Lin, "A New Multi Channel MAC Protocol" I-SPAN.
- [4] D.N.C. Tse and M. Grossglauser, "Mobility Increases the Capacity of Ad Hoc Networks" IEEE/ACM Trans. Net, vol. 10, no.4, Aug 2002.
- [5] O. Edfors, M. Sandell, J.-J. De Beek, D. Landström, F. Sjöberg, "An Introduction to Orthogonal Frequency-Division Multiplexing".
- [6] E. Lawrey, "The Suitability of OFDM as a Modulation Technique for Wireless Telecommunications, with a CDMA Comparison," MSc. thesis, James Cook University, Australia, October 1997.
- [7] A. Engelhart, H. Gryska, C. Sgraja, W.G. Teich, J. Lindner, "The Discrete-Time Channel Matrix Model for General OFDM Packet

Transmission Schemes" Proceedings of 1st International OFDM-Workshop Hamburg, 21-22 September 1999.

- [8] J. Proakis, "Digital Communications.New York: McGraw Hill", 3rd ed., 1995.
- [9] N. Yee, J.P.M.G. Linnartz, "Multi-carrier CDMA in an Indoor Wireless Radio Channel", UCB/ERL, 1994. U.C. Berkeley, UCB/ERL M94/6, Electronics Research Lab.
- [10] R. Van Nee, R. Prasad, "OFDM for Wireless Multimedia Communication", Boston London: Artech House Publishers, 2000.
- [11] Synchronization scheme reference IEEE working group "A Wireless LAN MAC and physical layer (PHY) Specification", Zhou D. and Lai T.H., A compatible and scalable clock synchronization protocol ICCP 2005.
- [12] P. Gupta and P. R. Kumar, Wireless Networking, 1998-99.
- [13] T. Keller, L. Hanzo, "Adaptive Multicarrier Modulation: A Convenient Framework for Time-Frequency Processing in Wireless Communication," IEEE, vol. 48, May 2000.
- [14] "Wireless Communications: Principles and Practice" 2nd edition, Theodore S. Rappaport, 2002.
- [15] Yi Li Lili Qiu Yin Zhang Ratul Mahajan "Effects of Interference on Wireless Mesh Networks: Pathologies and a Preliminary Solution"

Authors Biographies



SYED S. RIZVI is a Ph.D. student of Computer Engineering at University of Bridgeport. He received a B.S. in Computer Engineering from Sir Syed University of Engineering and Technology and an M.S. in Computer Engineering from Old Dominion University in 2001 and 2005 respectively. In the past, he has done research on bioinformatics projects

where he investigated the use of Linux based cluster search engines for finding the desired proteins in input and outputs sequences from multiple databases. For last one year, his research focused primarily on the modeling and simulation of wide range parallel/distributed systems and the web based training applications. Syed Rizvi is the author of 45 scholarly publications in various areas. His current research focuses on the design, implementation and comparisons of algorithms in the areas of multiuser communications, multipath signals detection, multi-access interference estimation, computational complexity and combinatorial optimization of multiuser receivers, peer-to-peer networking, and reconfigurable coprocessor and FPGA based architectures.



AASIA RIASAT is an Associate Professor of Computer Science at Collage of Business Management (CBM) since May 2006. She received an M.S.C. in Computer Science from the University of Sindh, and an M.S in Computer Science from Old Dominion University in 2005. For last one year, she is working as one of the active members of the wireless and mobile communications (WMC) lab research group of University of Bridgeport, Bridgeport CT. In WMC research

group, she is mainly responsible for simulation design for all the research work. Asia Riasat is the author or co-author of several scholarly publications in various areas. Her research interests include modeling and simulation, web-based visualization, virtual reality, data compression, and algorithms optimization.



JAIMINKUMAR GORASIA is a M.S. student of Electrical Engineering at University of Bridgeport. He received a B.S. in Electronics & Telecommunication Engineering from Nagpur University INDIA in 2006. In the B.S. he developed the Prepaid Electricity Billing system with the help of magnetized prepaid cards,

Card sensors, A/D converters, Microcontrollers, LCD display and transformers. He researched on the signal strength improvement on MTS and BTS in mobile communication. During his Masters he researched on the improvement of the High Level Architecture structure with the use of session initiation protocol. From last six month he is working on the project based on the packet sniffing and data security in computer network using LDEP protocol.

A Novel Encrypted Database Technique to Develop a Secure Application for an Academic Institution

¹Syed S. Rizvi, ²Aasia Riasat, ³Mustafa A. Khan and ⁴Khaled M. Elleithy

^{1,3,4}Computer Science & Engineering Department, University of Bridgeport, Bridgeport, CT

²Computer Science Department, Institute of Business Management, Karachi, Pakistan

srizvi@bridgeport.edu¹, aasia.riasat@iobm.edu.pk², mustafak@bridgeport.edu³, elleithy@bridgeport.edu⁴

Abstract— This paper presents the implementation of a secure application for an academic institution that offers numerous services to both students and the faculty. The primary focus of this paper is to provide a technical implementation of a new architecture for encrypting the database. The scope of this paper mainly includes but is not limited to symmetric and public-key cryptography, authentication, key management, and digital signatures. The final results of this paper demonstrate that what security features one should implement in order to achieve a highly secured application. This paper presents the implementation of a stand alone system that can be implemented on any legacy systems, and still operates effectively. In other words, it is self sufficient in terms of the data that it stores.

I. INTRODUCTION

Some of the major services that the intended application offers to both students and the faculty are as follows:

- The intended application is flexible in a sense that it gives ability to add/delete users, courses, students, and documents.
- Flexibility to change passwords. The secure application provides highly transparent environment to its users (i.e., the students and the faculty can use this application in a highly transparent manner). There should be minimal input from the user due to security features.
- One of the key features that the proposed application offers is the “forgotten passwords”. In other words, the secure application makes sure that if a user forgets his/her password, they should not completely lose their documents.
- In addition, the proposed application ensures that an administrator should not be able to decrypt the documents.
- Finally we design and develop this secure application by assuming that the communication is not secure at all.

Some of the security measures that we consider during the design and development of the targeted secure applications are as follows: Log all accesses activities to the server and provide features in the secure application to

search for unusual access patterns. If possible, put an upper limit on the number of document that a single user can access or we should have a warning mechanism in the application to ensure fairness. Our secure application should have a permission system to the document that determines if a user is permitted to access it. If the documents are read-only, add a software application called "Secure Viewer" that never stores the document to disk. A user should also have the capability to add a specialized crypto board on the server. This crypto card would be used to encrypt/decrypt files on the server.

One of the major objectives of the targeted secure application is to provide secure storage of the faculty documents as well as maintaining authorized access to the documents for the authorized users. In order to maintain this level of security, there is a need to design a strong and secured application that let the documents of the faculty being kept secret by implementing data Integrity and confidentiality as well as making the documents partially shared or available. Our design approach, therefore, implements a complete line of defensive authentication and authorization cryptographic standards to protect the data and to maintain its integrity while at the same time making it available for the authorized users. In particular, in order to design and implement such a secured application, the following are the minimum key security-elements that should be addressed by us in this paper: User authentication and Authorization [1, 2], ACL Management & Access Availability [3], Data encryption and decryption [4, 5], Data integrality, and Document Accountability [2]. Fig. 1 shows the implementation of the above five security components for both faculty as well as the student-users. Furthermore, the class diagram as shown in Fig. 2.

II. COMPONENTS OF THE PROPOSED ARCHITECTURE

A. User Authentication and Authorization

The secure application is certainly required to employ a strong mechanism to authenticate the users. The most frequently used strategy is asking for a user name and

¹Contact author: srizvi@bridgeport.edu,

password to authenticate the user. Some key points that we should consider in the design of authentication mechanism are: transmitting the password in clear (i.e., we may use SSL to protect the user privacy and to safe the application by being played in the hand of some intruder after he capture the network traffic and thus get the password). Also, it is required that the secure application provides secure storage of the user names and passwords along with

a method to manage them, including resetting or revoking the passwords or user accounts. Our another important concern during the preliminary design of secure application is whether to store the password in some hash format or storing it in the plain text format as the user entered. In order to keeps the user confidentiality intact and also letting the password to become non human understandable, hashing, therefore, becomes one of our design choices.

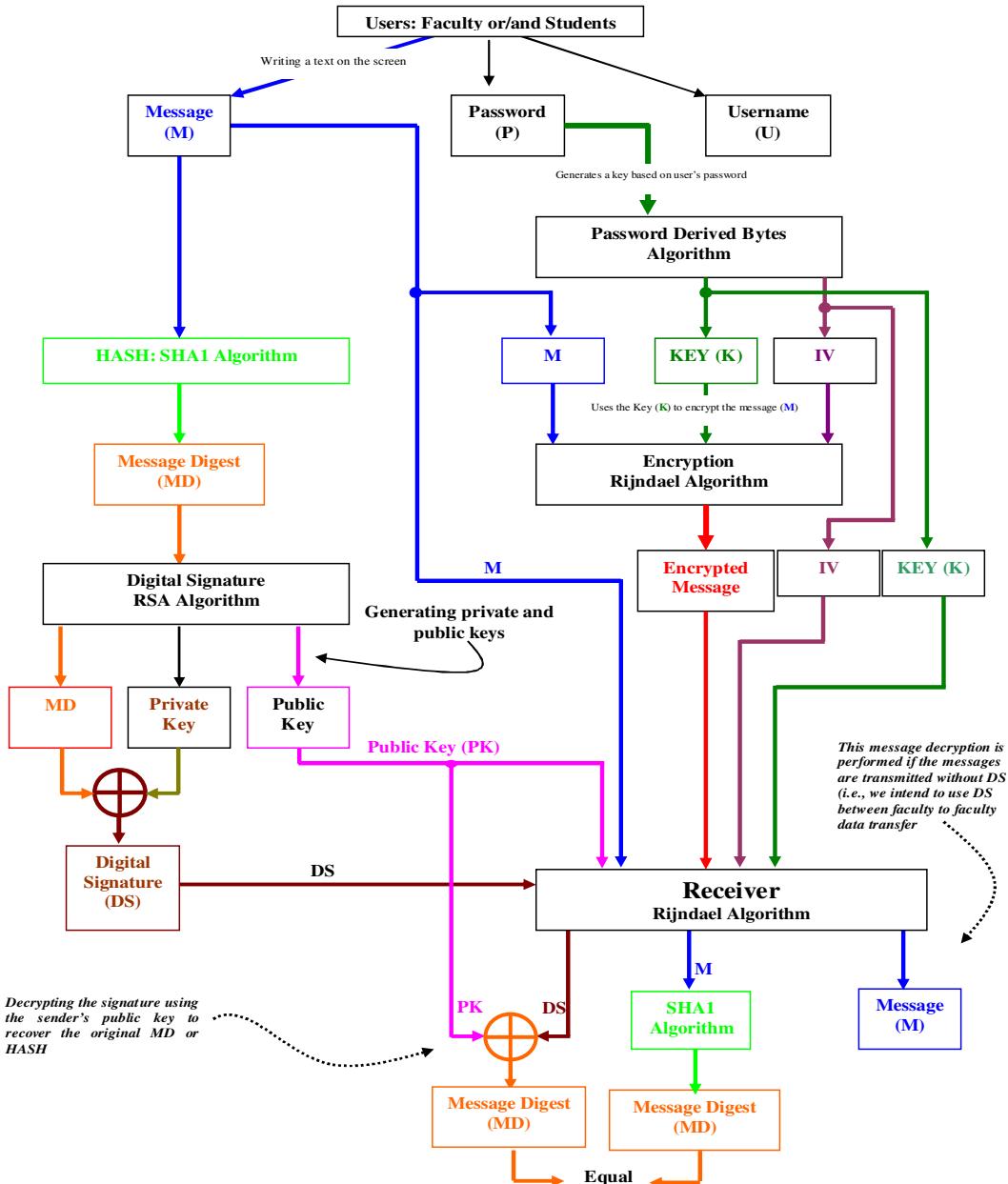


Fig. 1. Proposed Architecture for combining various security features for the intended application

B. ACL Management & Access Availability

One of the requirements of the secured application is making information always accessible to users who need it and who have sufficient permissions to access it. In order to achieve this task, the design of secure application should provide a robust mechanism to perform good management of document creation and access rights settings. Our secure application provides a number of features that, for example, allow owner to easily create and modify the documents, choose the encryption technique available in the secure application to store the document in encrypted format and most importantly setting the access control lists ACL. An owner can specify the objects and the accessibility domains associated.

C. Date Encryption and Decryption

The design of a secure application is not possible without the use of some encryption and decryption techniques. The secure application, therefore, should employ encryption and decryption technique for controlling the document integrity

and accessibility. The advantages of symmetric key cryptography make our design choice rather straightforward. However, since both parties need the same key for effective communication to occur, key distribution becomes an issue. For our secure application, the encryption will take place at the server where as the keys can be generated by the owner of the files entering some text. In addition, if file gets corrupted, the owner should be able to produce the same set of the keys if needed. The keys can be stored in encrypted format on the secured server, while just the server side application can access the file that contains the set of all keys that are used to encrypt the documents.

D. Data Integrity

Data integrity is one of the issues that we consider during the development phase of our secured application. The task is to make files secure by completely denying unauthorized access to the files while at the same time make sure that the files should be modified only by those (student or faculty) who are authorized to do so (If any) or can not be modified other than the owner of the document. We implement the

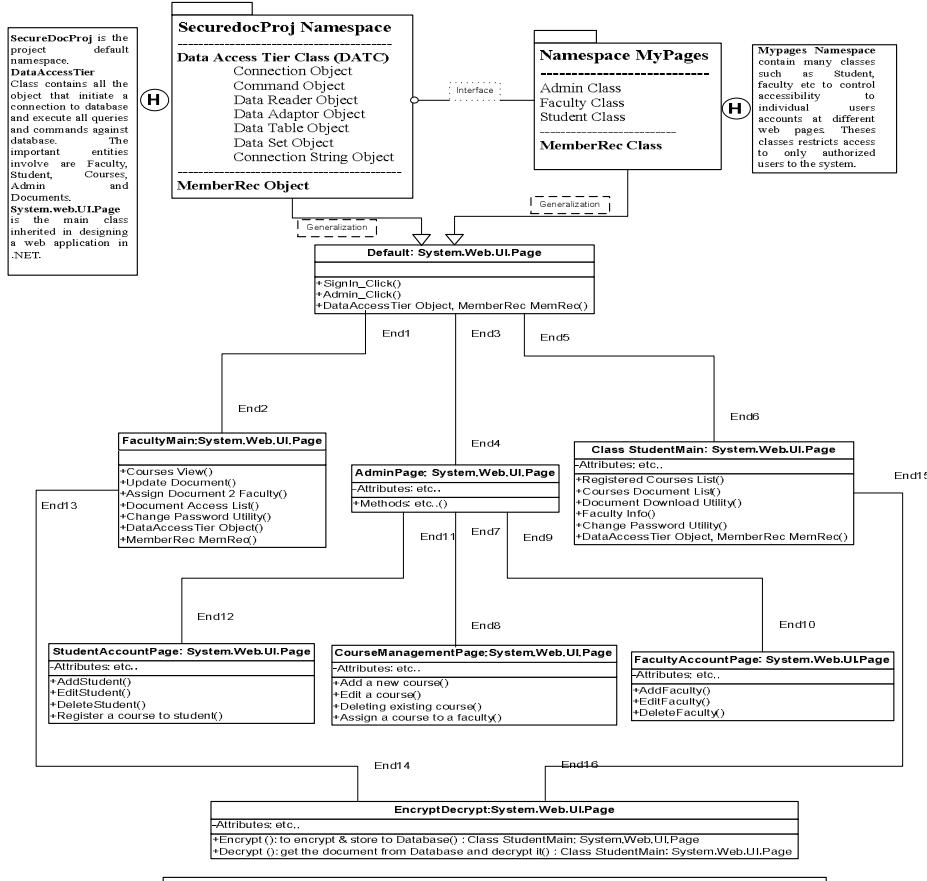


Figure 1. Class Diagram of a Secure Application for an Academic Institution

Fig. 2. Class diagram for the implemented project

concept of digital signatures that enable recipients to verify the integrity of an electronic document that is used. In our application, we ensure that the data integrity is maintained after implementing the digital signatures. One way of implementing this concept is the use of a one-way hash that creates a fixed-length hash value or message digest for a message of any length. With a hash attached to the original message, a user or owner can determine if the message was altered by re-computing the hash and comparing his or her answer to the attached hash.

III. IMPLEMENTATION ISSUES AND DESIGN CHOICES

In this section, we present our overall design structure for the targeted application. In addition, this section provides a comprehensive discussion on implantation issues and our design choices for implementing each security component we discussed above. The detailed flow diagram of the proposed project is shown in Fig. 3.

A. Project Design Phase

The Secure Document application is designed and developed to implement the security features that we have learned during this course of Network Security. This project was built using the .Net Framework and coded using C# as the base language. The main tools used in the project are: Visual Studio 2003 Development Environment, Asp .Net Framework, MS Access (Database) for storing projects entities and Documents, ADO.NET for database connectivity, Internet Information Server IIS 5.0 (web server), Secure Http (https). The database was designed in a way that it would suit the application flow and all the entities of the application. Next we describe each of them in some detail along with the over all database design. For the sake of simplicity, all the entities information are kept simple in database, although this information can be made comprehensive and complete in any real time implementation and as per the development requirements.

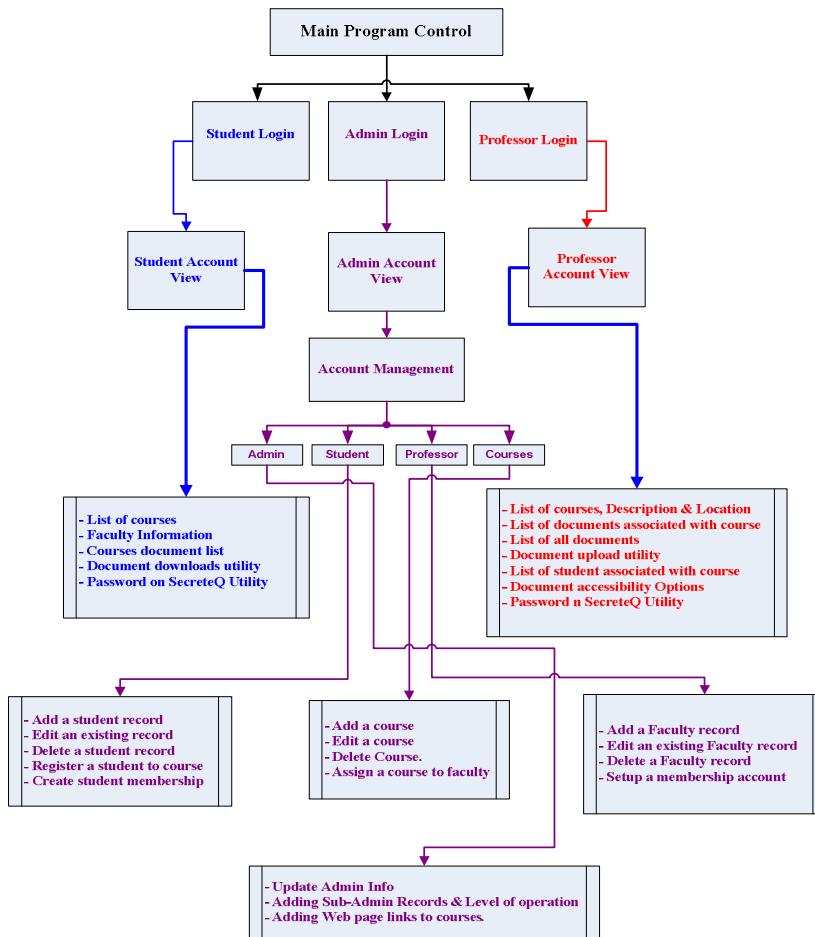


Fig. 3. Detailed Flow Diagram of Secure Application for an Academic Institution

B. Proposed Security Design

The proposed security design includes various security measures that are incorporated in the intended application.

1) Custom Base Class: In our project we have used ASP.NET Custom Base Class feature to secure access to all the project web pages, data and services available on them. For this purpose, we created custom base class called "My Pages" which is derived for System.Web.UI.Pages and consists of those classes that contain the code that put the security checks and take care of the process of authorization. All the web form's codes behind classes are derived from the Custom Base Class that provides the basic infrastructure for the web page's information access security. To implement this hierarchy, we implemented the .Net's most prominent feature: session management to maintain the user's identity at each step of the application. By using the custom based class implementation, we have avoided the URL spoofing in which a person who is not authorized to view the page contents or to access the resources offered by it can be able to access the page's contents.

2) Dynamic Key Generation and Management: In order to prevent the unauthorized access to the keys that are used to secure the documents upon storage, the keys for encryption and decryption are chosen entirely at run time. With this approach, we avoided to store them at any place which consequently avoided any security threats. The system will be a bit slow in the response but will save us the cost of being insecure. The keys are generated based on the session objects information of the person which is being signed at the time of the document upload and encryption request.

C. Basic Concepts Design and Flow Diagram

The basic concept includes the users, custom, validation and calendar controls. Validating the user inputs throughout the pages include telephone number and date

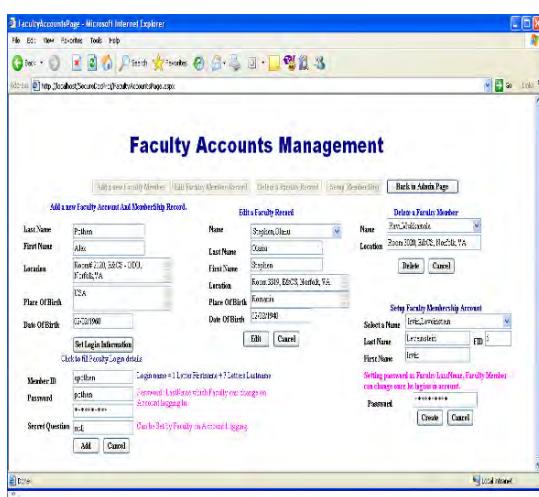
information. Updating the database based on the calendar when the user specify the date. The retrieved information from the database is displayed using data adapters, data sets, data grids and data list. The main tools used as a basic concept in .Net framework are: User Controls, Image Controls, Html File Control, Data List, Data Grid, Calendar Controls, Validation Controls, Regular Expressions, Data Readers, Data Adapters, and Data Sets. The data flow diagram is a high level representation of this project. It can be seen in Fig. 3 that the data flow from top to bottom where system administrator initiates and introduces students, courses, and faculty.

IV. SECURE DOCUMENT APPLICATION IMPLEMENTATION

In this section, we present a discussion on the technicalities we encountered during the development phase of this project. This includes implementation detail and interface choice. In this application, the flow of the application starts from the main (default) page where a person sign in and then based on its role or membership, he/she will be then directed to specific web pages and resources he can access. The main entities in this implementation include System Admin interface and Faculty and Student Interfaces as outlined below.

A. System Admin and Faculty Interface

The system admin interface contains the links to the pages where a system admin can perform course management, faculty & students accounts managements. In addition, a system admin can assign courses to faculty and can register students to specific courses. The links at the system admin interface include faculty accounts, admin accounts, student accounts, courses management interfaces. System administrator manages student's accounts by adding, modifying, deleting student record. He/she can setup their login accounts and can register them to the desired courses



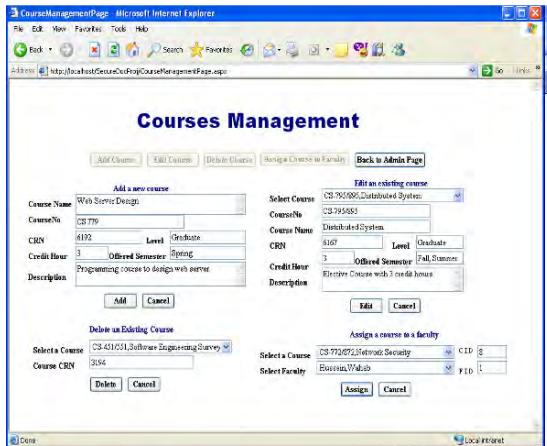


Fig. 6. System Admin Control Panel: Courses Management

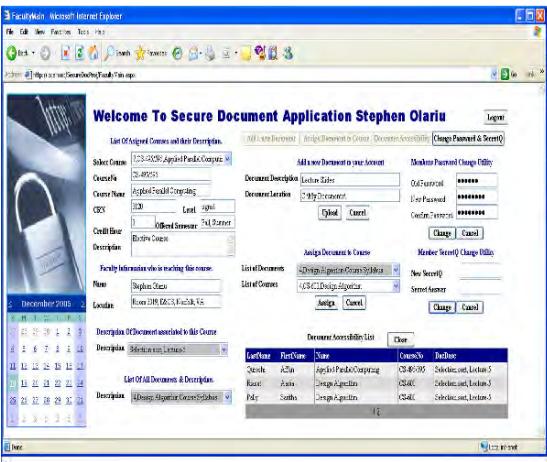


Fig. 7. Faculty Member Interface

offered by a certain semester. Figures 4, 5, and 6 show the different parts of the system administration.

When a faculty member logs in to the application, he/she is directed to a web page that provides the information and services that are only related to that faculty member. As one can see in Fig. 4, the faculty member has provided the information regarding the courses that are assigned to him and the documents (encrypted) that he has in his folder at the server. In addition when a course is selected, the page shows the documents that are related to that specific course. The list of students who have given the access to his (faculty member) documents are also shown here. The faculty member has given the option to change the accessibility permissions of the student by deleting the student record from the list for whom he doesn't want to allow the accessibility of the document. The documents are uploaded to the server in encrypted format and then stored into the data base as a BLOB. During the uploading and encryption, the secure Http Protocol is being used, so that the transfer of the documents takes place securely as shown in Fig. 7. In

addition, Fig. 6 can be used by a system administrator to manage the courses for both faculty and students.

B. Student Interface

When a student logs into the secure document application, he has shown the list of his registered courses and their complete description including faculty information (see Fig. 5). He can choose any of the documents that he want to access and can click the download button. The download button extract the document that are stored in the database in the BLOB form and then decrypt it on to the sever; finally the document is made available in the browser for the student. During the document transfer we again implemented secure Http protocol to securely transfer the document. The details are shown in Fig. 5. On the same page student can change his password or secret question and answer any time. Passwords and secret questions and answers are stored in the encrypted format in the database and hence.

V. CONCLUSION

In this paper, we presented a new design for providing comprehensive security for a secure application by combining many different security techniques using the .NET framework. The most prominent feature of the .NET is its full fleshed Cryptography-API that provides techniques of encryption and decryption while hiding all the technical details. This is one of the main reasons that we achieved the goal of completing this secure application. Secure HTTP communication provided by ASP.NET's API is also another most important and handy feature worth to mention here. Some of the tools used in the application include data access controls that avoid repetitive database programming, built in authentication features and security controls that enable automated management of user accounts and roles and simplified web deployment. The proposed project consists of different tools and techniques for building secure web applications with strong database accessibility and crypto graphic techniques. During the design phase, we learned and practiced many new techniques that we found very useful and interesting in the context of building a secure and powerful web application along with strong and real time database functionality.

REFERENCES

- [1] L. Moningi, "Authentication and Authorization in ASP.NET," September 09, 2003. Available at: <http://www.c-sharpcorner.com/mrsharp.asp>
- [2] D. Watkins, "An Overview of Security in the .NET Framework," Project 42, Sebastian Lange, Microsoft Corporation, January 2002.
- [3] J. Meier, A. Mackman, B. Wastell, P. Bansode, A. Wigley, K. Gopalan, "Security Practices: ASP.NET 2.0 Security Practices at a Glance," Microsoft Corporation, August 2005.
- [4] A. Yao, "How to generate and exchange secrets," *Proceedings IEEE 27th Symposium on Foundations of Computer Science (FOCS)*, pp. 162-167, 1986.
- [5] ISO/IEC 11770-2: 1996. "Key management - Part 2: Mechanisms using symmetric techniques," *International Organization for Standardization*, 1996.

A Mathematical Model for Reducing Handover Time at MAC Layer for Wireless Networks

Syed S. Rizvi¹, Aasia Riasat², Mohammad A. Sheikh³

Computer Science and Engineering Department, University of Bridgeport^{1,3}, Bridgeport, CT

Department of Computer Science, Institute of Business Management², Karachi, Pakistan

{srizvi¹, msheikh³}@bridgeport.edu, aasia.riasat@iobm.edu.pk²

Abstract—Extensive studies have been carried out for reducing the handover time of wireless network at medium access layer (MAC). However, none of them depicts the impact of reduced handover time on the overall performance of wireless networks. This paper presents the methodology that can be used to effectively reduce the handover time. Our proposed model incorporates many critical performance measurements to show the impact of reduced handover time on wireless networks. Our experiments verify that the active scanning can reduce the overall handover time at MAC layer if comparatively shorter beacon intervals are utilized for packet transmission.

Keywords— Handover time, medium access control, detection phase latency time, wireless networks.

I. INTRODUCTION

A Handoff occurs in IEEE 802.11b when a mobile station moves beyond the radio range of one access point (AP) and enters in another coverage area at the MAC layer. During the handoff, management frames are exchanged between the station (STA) and the AP. Consequently, there is a latency involved in the handoff process during which the STA is unable to send or receive traffic. On the other hand, our measurements are not only shown that the latencies are very high but also shown that they vary significantly for the same configuration of stations and AP. In this paper, we use *full scan handoff* to denote the original active handoff scheme of the wireless card which scans all channels consecutively in the discovery phase. Most improvements to the active scan handoff strive to scan fewer channels. This is called as *selective scan handoff*. The authors of [1] proposed a

MAC layer fast handoff. They use selective scan to record the scan results in the “AP cache” for future use. However, in the case of incorrect cached information, the handoff latency is the same as that of the full scan handoff. Recently, a fast scan handoff scheme is proposed [2]. Instead of broadcasting the probe request frame to all APs, the probe request frame is sent to a specific AP who will be the sole responder. However, this scheme needs to change both the wireless stations and the AP.

II. PROPOSED MATHEMATICAL MODEL FOR REDUCING THE HANDOVER TIME

This section presents a mathematical model that incorporates many critical performance measurements to show the impact of reduced handover time on wireless networks. The performance of the cells permits the use of the real time services when the MAC scheduler is modified [3]. However, our study focuses on the optimization of the second method. We have observed in our measurements that stations firstly assume collision and retransmit several times. If transmission remains unsuccessful, then radio fading is assumed and the link is probed by sending probe requests.

We present an argument that stations must start the search phase as soon as collision can be excluded as reason for failure. If the actual reason was a temporary signal fading, the selected AP’s search would likely be the current one and the handoff will not be executed. Thus, a key factor in our detection algorithm is the number of collisions that a frame can suffer before it is transmitted.

A. Proposed Mathematical Model for the Collision Detection and Avoidance

We use the probability distribution function (PDF) to approximate the number of collisions for both

¹Contact author: srizvi@bridgeport.edu,

saturated and non-saturated cases. The proposed probabilistic approach assumes that the STAs must start the search phase as soon as collision can be excluded as reason for failure. If the actual reason was a temporary signal fading, the selected AP after the search would likely be the current one and the handoff will not be executed. According to PDF, if we assume that a random variable X represents a collision per frame transmission, then X should lie within a certain range representing by R . We assume that the value of R belongs to an interval of two values representing as V_{MIN} and V_{MAX} . This argument leads us to the following mathematical expression:

$$X \in \{V_{MIN}, V_{MAX}\} \text{ where } R \xrightarrow{=} \{V_{MIN}, V_{MAX}\} \quad (1)$$

By further extending (1), we can approximate the probability that X lies in the ideal interval:

$$P(X) \in \{V_{MIN}, V_{MAX}\} = F|V_{MAX}| - F|V_{MIN}| \quad (2)$$

Where F represents the PDF and P is the probability that X lies within the defined interval for collision avoidance. Based on (1) and (2), one can produce the PDF for the collision avoidance as shown in (3):

$$R \rightarrow F_R(R) = P\{X \leq R\} \quad (3)$$

If we further assume that the system consists of K users, then (1) and (3) be used to approximate the probability of collision per frame transmission. In other words, by reversing the order of probabilities given in (1) and (3) with respect to the ideal range shown in (2), we can approximate the number of total collisions as follows.

$$P\{X \leq R\} = \sum_{j=0}^R (1-P)^j \square (1-P)^{R+1} \quad (4)$$

where the sign “ \square ” represents the estimated value and the term $(1-P)^{R+1}$ can be considered as a normalization term to ensure that the probability of each random backoff time follows a valid PDF.

The random backoff time will be discussed later in detail. In addition, R will be any real number representing the number of STAs ready to transmit the frames. The range of R is provided in (2). In order to derive a generic equation that includes both detection and avoidance, we can now combine our four equations that yield the following result:

$$P\{X \leq R\} = \sum_{j=0}^{P\{X \leq R\}} (1-P)^j \square (1-P)^{F_R(R)=P\{X \leq R\}+1} \quad (5)$$

Equation (5) consists of both the probability of detection and collision avoidance characteristics.

For the sake of simulation, we assume that there are n numbers of STAs that are transmitting a fixed packet size of typically 40 bytes using an ideal channel. Fig. 1 shows a regular case of packet transmission when only a limited number of users are transmitting at one time. In addition, for Fig. 1 we run our simulation multiple times for different values of n .

In order to address the worst case scenario, we consider n number of STAs with an additional assumption that all STAs have data to transmit all the time via an ideal channel (i.e., the standard IEEE 802.11 MAC [1]) as shown in Fig. 2. It should be noted in Fig. 2 that the probability of collision increases as we increase the probability of transmission per frame. However, the performance degradation was small compared to the increase in probability of packet transmission.

Fig. 1 shows that three consecutive collisions is a rare event, even in saturation as shown in Fig. 2. This implies that there is no need to explicitly probe the link. The same conditions that we used throughout our measurements, this time would be around 3 ms, which are approximately leads to 300.

In order to compute the minimum channel time, we follow the classical theory of Slotted Aloha protocol [4]. That is, each STA listens to the channel before the transmission of the frames. If the channel is busy, it defers the transmission with a certain probability. On the other hand, if the channel is free for a certain time (called DIFS, Distributed Inter Frame Space, in the standard [3]), then the STA can transmit the frames.

In addition, when the channel is busy, each node waits for a random amount of time and then periodically listen the channel to find possible DIFS. This random wait-time can be considered as a random backoff time that each node needs to experience during the high contention. Since each STA can only transmit during a certain slot, this random backoff time is, therefore, a multiple of slot times. In addition, we also assume that there is no propagation time and response generation time involve in the computation of minimum channel time. The above discussion leads us to the following mathematical expression:

$$\text{Min}_{(cr)} \geq (\text{DIFS}) + (\text{RB}_{Time} \times S_{Time}) \quad (6)$$

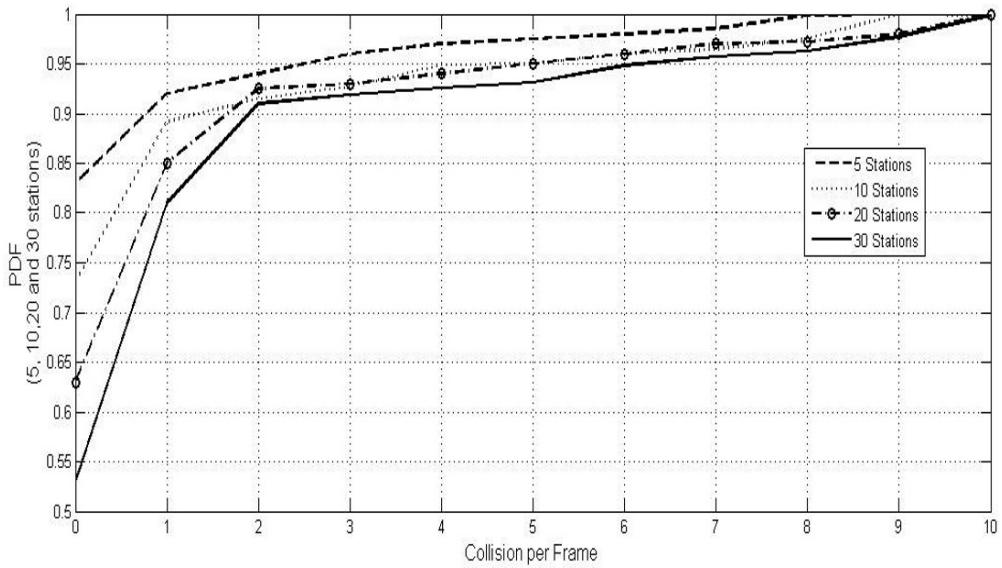


Fig.1. PDF versus number of collision per frame with ideal channel condition for a non-saturated condition

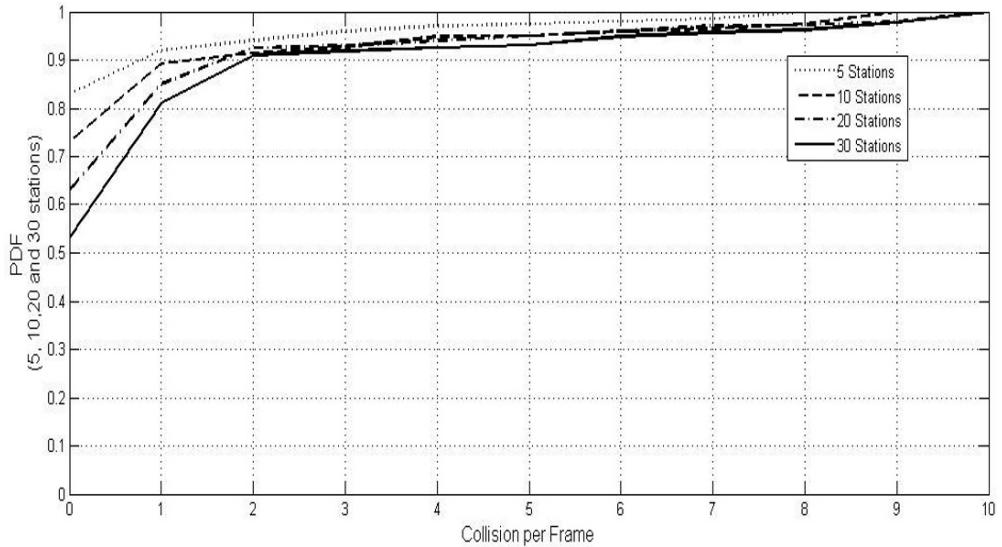


Fig.2. PDF versus number of collision per frame with ideal channel condition for a saturated condition

where $Min_{(ct)}$ refers to minimum channel time, DIFS, RB_{Time} represents *random backoff time*, and the parameter S_{Time} indicates the length of the slot.

We can approximate the ideal range of $Min_{(ct)}$ as follows: $AP_R \geq Min_{(ct)} \geq DIFS$

Next, we need to compute the values of *maximum channel time* which might work as the upper threshold value. Since 10 STAs per cell seem to be an adequate

number to achieve a good cell throughput [5], we have simulated the different beacon interval with OPNET to figure out the suitable max channel time. Based on our experiments, we conclude that the best value for *maximum channel time* is 10 milliseconds. The last step is to compute the *total search time*. According to the IEEE standard [1], each STA requires to scan all available channels during active scan. The available channels include both busy channels (*B*) and free channels (*F*). Also, the time to scan a busy channel is not necessarily the same as to scan a free channel. This, therefore, leads us to a simple mathematical expression for the total search time: $SE_{Time} = T_B(B) + T_F(F)$ where the left hand side of this expression represents the total search time, and T_B and T_F represents the time required to scan a busy and free channels, respectively.

The last step is to compute the *maximum channel time* and the total search time. The available channels include both busy channels (*B*) and free channels (*F*). The total search time will be based on the total time required to scan both busy and free channels. This leads to the following equation:

$$T_B = (2P_{(Delay)}) + (Max_{(CT)}) , T_F = (2P_{(Delay)}) + (Min_{(CT)}) \quad (7)$$

If we assume that we have an ideal minimum time for scanning free channels, then the following mathematical expressions must be true:

$$\begin{aligned} T_B &= (2P_{(Delay)}) + (Max_{(CT)}) \\ T_F &= (2P_{(Delay)}) + (DIFS) + (RB_{Time} \times S_{Time}) \end{aligned} \quad (8)$$

$$\begin{aligned} SE_{Time} &= [(2P_{(Delay)}) + (Max_{(CT)})(B)] \\ &+ [(2P_{(Delay)}) + (DIFS) + (RB_{Time} \times S_{Time})](F) \end{aligned} \quad (9)$$

The above *minimum channel time* and the *maximum channel time* provides the best searching result as compared to the current network cards provides. Specifically, we can use (9) to approximate the total scanning time involves in the search phase. Next section shows the effect of our proposed mathematical model in terms of load balancing, throughput, and transmission delay.

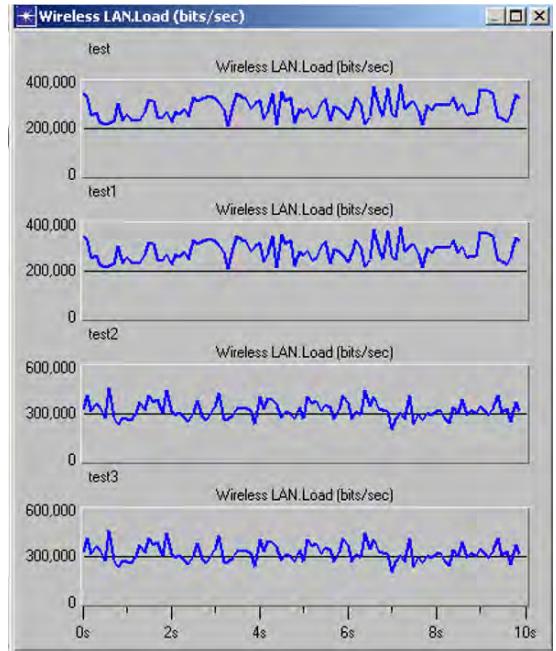


Fig.3. Network load with different values of beacon interval versus time

III. PERFORMANCE ANALYSIS OF THE PROPOSED MATHEMATICAL MODEL

The performance measures adopted in this paper are network load, throughput, and the media access delay. The system is modeled in OPNET for both lightly and heavily loaded networks. Fig. 3 is based on our mathematical derivation that simulates the *search-timer* for the *Min-Channel*. The result of this simulation should fall between 670ms and 1024ms. The lowest threshold value has been derived from standard industry and IEEE has given the constant factors [1]. The upper threshold value, however, is suggested based on the maximum latency involved in the given wireless network.

It can be evident in Fig. 3 that below 670ms there is no significant improvement. However, for such a short period of time (i.e., below 670ms), it would likely decrease the overall network efficiency. This is due to the fact that below 670ms, it is more likely that channels will be more quickly declared as empty channels where as the maximum latency time will gradually increase resulting in overall poor performance of the network. It should also be noted in Fig. 3 that as we increase the minimum threshold to 1024ms, this increases the overall network traffic.

Fig. 4 shows a comparison of throughput versus network traffic. It can be clearly seen in Fig. 4 that as

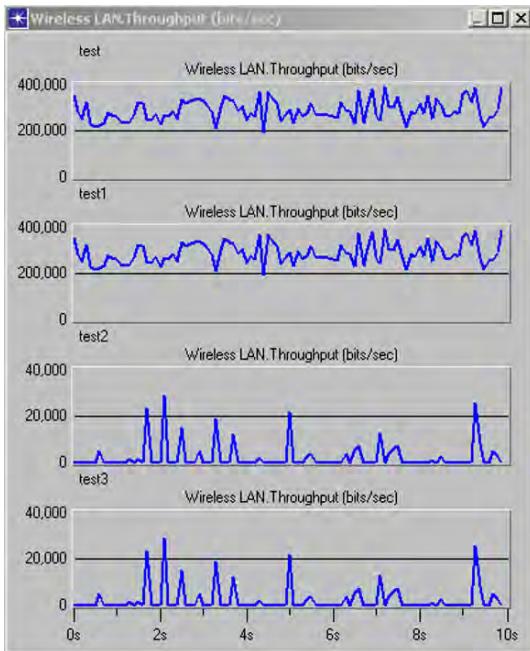


Fig.4. WLAN throughput versus probe request/response transmission time

we linearly increase the network traffic, the overall throughput of the system decreases. In other words, an increase in *minimum channel time* becomes one of the reasons for a decrease in overall network throughput. It should also be noted that the results of Fig. 4 is not only the experimental verification of the results of Fig. 3 but also provide some better and technical insight in the increase of throughput. In addition, the overall system throughput decreases sharply, however, it makes some spikes during the random intervals. It can be evident in Fig. 4 that the overall throughput increases significantly with respect to the varying network load represented in Fig. 3.

IV. CONCLUSION

In this paper, we have proposed a mathematical model that can be used to effectively reduce the handover time of WLAN at MAC layer. Specifically, we proposed a mathematical model for collision detection and avoidance as well as for search phase. Our simulation results verify that the utilization of probabilistic approach with the active scanning yields lower latency for each detection and search phases provided that if we utilize the appropriate values of some critical parameters such as the beacon interval, minimum and the maximum search times. Both simulation and numerical results of this paper

demonstrate that the reduced handover time at MAC layer provides better load balancing, high throughput, and minimum frame transmission delay.

REFERENCES

- [1] S. Shin, G. Forte, S. Rawat, and H. Schulzrinne, "Reducing MAC layer Handoff Latency in IEEE 802.11 wireless LANs," in *MOBIWAC '04: Proceedings of the second international workshop on Mobility management & wireless access protocols*, pp. 19–26, New York, NY, USA, 2004. ACM Press.
- [2] M. Jeong, F. Watanabe, and T. Kawahara, "Fast Active Scan for Measurement and Handoff," *Technical report, DoCoMo USA Labs, Contribution to IEEE 802*, May 2003.
- [3] G. Bianchi, "Performance analysis of the IEEE 802.11 Distributed Coordination Function," *Selected Areas in Communications, IEEE Journal*, Vol. 18, Issue 3, pp. 535 – 547, Mar 2000.
- [4] D. Geun and W. Sook, "Performance of an Exponential Backoff Scheme for Slotted-ALOHA protocol in local wireless Environment," *IEEE transactions on vehicular technology*, 1995, vol. 44, pp. 470-479, 1995.
- [5] S. Shin, G. Forte, S. Rawat, and H. Schulzrinne, "Reducing MAC layer Handoff Latency in IEEE 802.11 wireless LANs," in *MOBIWAC '04: Proceedings of the second international workshop on Mobility management & wireless access protocols*, pp. 19–26, New York, NY, USA, 2004. ACM Press.

Authors Biographies



SYED S. RIZVI is a Ph.D. student of Computer Engineering at University of Bridgeport. He received a B.S. in Computer Engineering from Sir Syed University of Engineering and Technology and an M.S. in Computer Engineering from Old Dominion University in 2001 and 2005 respectively. In the past, he has done research on bioinformatics projects where he investigated the use of Linux based cluster search engines for finding the desired proteins in input and outputs sequences from multiple databases. For last one year, his research focused primarily on the modeling and simulation of wide range parallel/distributed systems and the web based training applications. Syed Rizvi is the author of 45 scholarly publications in various areas. His current research focuses on the design, implementation and comparisons of algorithms in the areas of multiuser communications, multipath signals detection, multi-access interference estimation, computational complexity and combinatorial optimization of multiuser receivers, peer-to-peer networking, and reconfigurable coprocessor and FPGA based architectures.



AASIA RIASAT is an Assistant Professor of Computer Science at Institute of Business Management (IOBM) since May 2006. She received an M.S.C. in Computer Science from the University of

Sindh, and an M.S in Computer Science from Old Dominion University in 1999, and 2005, respectively. For last one year, she is working as one of the active members of the wireless and mobile communications (WMC) lab research group of University of Bridgeport, Bridgeport CT. In WMC research group, she is mainly responsible for simulation design for all the research work. Aasia Riasat is the author or co-author of more than 30 scholarly research papers in various areas. Her research interests include modeling and simulation for parallel and distributed systems, web-based visualization, virtual reality, data compression, and algorithms optimization.



MOHAMMAD A. SHEIKH is current pursuing his M.S. in Technology Management from University of Bridgeport, USA. Before coming to UB, he worked as a Quality Manager in a pharmaceutical company for more than 4 years. His research interests include hypercube networks, and QoS of wireless networks.

A Software Solution for Mobile Context Handoff in WLANs *

H. Gümüşkaya¹, M. V. Nural², S. Doğan²

¹ Department of Computer Engineering, Haliç University

Siracevizler Cad., No: 29, Bomonti-Şişli, İstanbul, Turkey

² Department of Computer Engineering, Fatih University

34500 Büyükçekmece, İstanbul, Turkey

Abstract. This paper presents a software solution for mobile context handoff in IEEE 802.11 Wireless Local Area Networks (WLANs) for a context-aware system in the campus area at Fatih University. This project provides a seamless mobility infrastructure to mobile applications that were developed as a part of SOWCAS (Service-Oriented Wireless Context-Aware System) project.

SOWCAS is a distributed pervasive system having a context-aware middleware server, proxy servers and mobile clients that support context-awareness and high adaptation to context changes for heterogeneous indoor and outdoor mobile applications. A handoff daemon named as Scriptex in Perl scripting language was developed. Scriptex provides a generic solution that is free from operating system and hardware implementations.

I. INTRODUCTION

Context-Aware Computing (CAC) refers to a general class of mobile systems that can sense their context of use, and adapt their behavior accordingly. CAC helps users interact better with their environment. Context may have different meanings and can be used to indicate who (identity), what (activity), status, where (location), when (time), nearby people, devices, lighting, noise level, network availability.

We have developed a context-aware system, Service-Oriented Wireless Context-Aware System (SOWCAS) for a university campus [1], [2]. Our primary focus in SOWCAS is to develop an indoor and outdoor context-aware system that benefits from the heterogeneity of wireless access technologies at a university campus. In SOWCAS, to collect and process context information we designed and deployed a distributed architecture composed of a central SOWCAS Server, Proxy PCs and mobile SOWCAS clients. The SOWCAS Proxy software runs on Proxy PCs located in classes, laboratories and some special locations in which students and professors are found frequently. The PCs are equipped with WLAN 802.11 network cards. These PCs and wireless access points (APs) located in buildings are used to locate and track the positions of mobile users in the university. SOWCAS locates and tracks the user having an IEEE 802.11 and GPS supported device at the Fatih University campus. It operates by processing received signal information from multiple WLAN APs and GPS data.

Besides indoor and outdoor location context information, we also keep other context information such as status, activity, weekly schedules, detailed personal information for students and faculty members in the central database at the SOWCAS Server.

An important issue for CAC or more generally pervasive computing is a mobile architecture. This mobile architecture can be provided by GSM like telecom networks or IEEE 802.11 like wireless data networks. In both networks, context-aware pervasive services need a seamless mobility to serve mobile clients without any distraction. These services need to be transparent for mobile users. To ensure transparency a handoff mechanism is required.

Our motivation in this project is to provide a seamless mobility infrastructure in IEEE 802.11 WLANs for context-aware pervasive applications which are developed together as a part of SOWCAS project [1] which is one of the projects of FCAPSYS *.

II. IEEE 802.11 HANDOFF MECHANISM AND PROBLEMS

The IEEE 802.11 specification allows two operating modes namely, the ad hoc and the infrastructure mode [3]. In the ad hoc mode, two or more wireless stations (STAs) recognize each other and establish a peer-to-peer communication without any existing infrastructure, whereas in the infrastructure mode there is a fixed entity called an access point (AP) that bridges all data between the mobile stations associated to it. An AP and associated mobile stations form a Basic Service Set (BSS). A collection of APs (within the same network) can extend a BSS into an Extended Service Set (ESS) as shown in Figure 1. Handoff is the mechanism that simply provides exchange of the currently connected AP with a better service provider AP without any loss of connection. In other words, a handoff occurs when a mobile station moves beyond the radio range of one AP, and enters another BSS. During the handoff, management frames are exchanged between the STA and the AP. Also the APs involved may exchange certain context information (credentials) specific to the station. Consequently, there is latency involved in the handoff process during the time in which the STA is unable to send or receive traffic.

*This work was supported by the Fatih University Research Fund (Grand No. P50050702, Frameworks for Context-Aware Pervasive Systems—FCAPSYS)

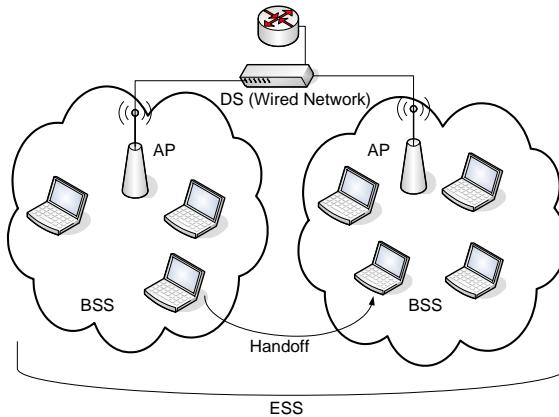


Figure 1. Extended Service Set (ESS) and Basic Service Set (BSS).

The IEEE 802.11 standard states that any mobile station associated with an AP, should “roam” to a different AP within the same ESS if the service quality (i.e. signal strength) has significantly dropped down. Many AP hardware companies did follow this standard, but in their own way. So there are some interoperability issues between different vendors. For example, when roaming to a new AP, old AP should transfer some credentials of the station to the new AP. Although IAPP (Inter Access Point Protocol) [4] is proposed for this operation, it is not followed by all vendors. Therefore most of the vendors implemented proprietary solutions for managing credentials.

If all APs in an ESS are from the same vendor, there is no problem for handoff. Otherwise a software solution may be needed to manage handoff since interoperability issues would violate the handoff procedure.

III. A SOFTWARE SOLUTION FOR HANDOFF

We developed a handoff daemon (named as *Scriptex*) in Perl scripting language for Linux computers. We tested Scriptex on the SuSe Linux 10.3. Scriptex communicates with a wireless network interface card via Wireless Tools for Linux [5] which is described below. The software architecture of handoff tools is shown in Figure 2.

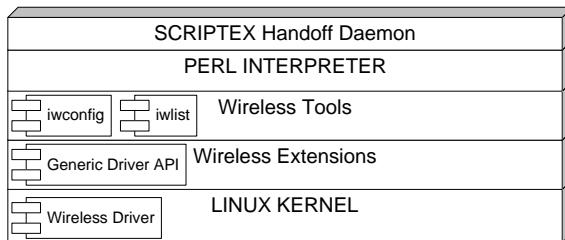


Figure 2. The software architecture of handoff tools.

The Linux Wireless Extensions and the Wireless Tools are open source projects sponsored by Hewlett Packard. The Wireless Extensions is a generic API allowing a driver to expose to the user space configuration and statistics specific to common WLANs. These tools can support all the variations of WLANs, regardless of their type (as long as the driver supports Wireless Extensions). Another advantage is that these parameters may be changed on the fly without restarting the driver (or Linux).

Perl is a general-purpose programming language originally developed for text manipulation and now used for a wide range of tasks including system administration, web development, network programming, GUI development, and more. The Perl language includes a specialized syntax for writing regular expressions, and the interpreter contains an engine for matching strings to regular expressions. Since we had to deal with text parsing and manipulation extensively in this project, Perl became the ultimate choice.

Scriptex is a daemon for triggering and managing handoff process. Handoff is managed in the application layer using some abstractions. By that way we challenge some application layer wireless problems that are normally very hard and costly if done in hardware in the data link layer. Since Scriptex is written in Perl, it can be used with virtually any Linux distribution. Scriptex provides a generic solution that is free from operating system and hardware implementations. It has two main functions, invoking Wireless Tools and parsing and interpreting produced text tokens.

IV. TEST SETUP, EXPERIMENTS AND ANALYSES

All our tests were performed in the basement floor of the Engineering Building at Fatih University. In this floor, there are 3 Cisco 1100 APs located especially for experimental use. These access points are located at the entrance of e-106, e-116, and e-109 classrooms and referred as AP1, AP2 and AP3 as shown in Figure 3. Before the tests were started, we created wireless signal coverage maps of our wireless network formed by AP1, AP2 and AP3.

WirelessMon [6] was used to create signal-strength maps of our test bed. WirelessMon is a software tool that allows users to monitor the status of wireless WiFi adapters and gather information about nearby wireless access points and hot spots in real time. WirelessMon can log the information it collects into a file, while also providing comprehensive graphing of signal levels, real time IP and 802.11 WiFi statistics. With WirelessMon we can verify that an 802.11 network configuration is correct or not. We can check signal levels from local WiFi network and nearby networks and create signal strength maps of an area. We can also observe wireless network coverages and ranges.

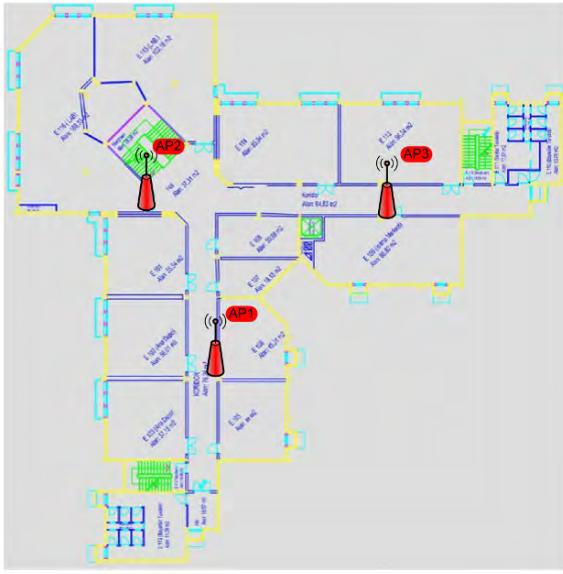


Figure 3. The test setup for handoff experiments.

WirelessMon has different views. The summary view gives a general idea for current networks. This view contains useful information about current connection and available access points. The radar like view shows the current signal level in a graphical way. This helps understanding of handoff regions.

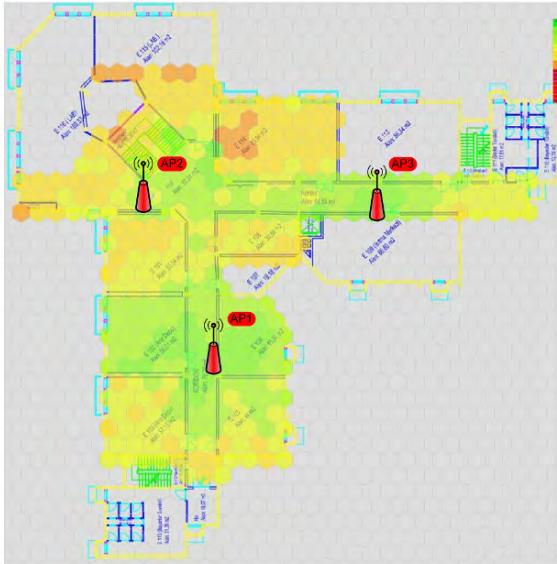


Figure 4. The wireless signal strength map in the test environment.

Another view is the map view. Using this view, we can create and edit signal strength maps. An example wireless signal strength map in the test environment is shown in Figure 4.

To create a signal-strength map we specify a building plan or a picture. After selecting the grid size and the AP's that we want to see, we start to walk grid by grid in the map. As we walk around the area, we click the grid we are in and WirelessMon automatically takes signal-strengths of selected AP's. Each signal strength map consists of a map and colored hexagon cells. Grey cells represent cells that have not been visited or have not been able to get signal. For any others, colors represent different signal-strengths of the correspondent cells.

In order to monitor wireless network packets of a handoff process, we need some extra effort. Triggering a handoff is an easy operation. A mobile station walking into a critical handoff region will trigger a handoff. However we cannot calculate handoff delays without a help of a wireless sniffer. Moreover we cannot understand details of a handoff if we don't look at the event logs of the AP's. For wireless sniffing, we used a separate mobile station (a notebook computer shown as HP1 in Figure 5) and CommView for WiFi [7] running on this computer. For monitoring the events of APs we used Syslog protocol [8] with the Kiwi Syslog Daemon Software [9]. The handoff monitoring environment in our test setup is given in Figure 5.

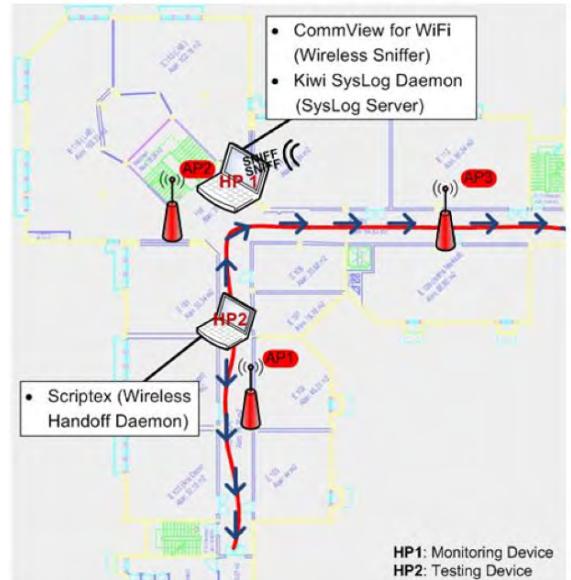


Figure 5. The test setup and handoff monitoring environment.

CommView for WiFi is a wireless network monitor and analyzer for 802.11 a/b/g/n networks. It captures every packet on the air to display important information such as the list of AP's and mobile stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc.

We only deal with three entities in the handoff experiments; mobile station (HP2), AP1 and AP3, so we have to filter out unnecessary packets from other stations. Moreover we need to ignore beacons since they are irrelevant and they produce huge amounts of unnecessary packets (an AP sends a beacon every 10-100ms). Also we don't want to see any data packets since we try to observe handoff in 802.11 management packets. Therefore filtering is inevitable.

Using CommView we can create rules for filtering packets. These rules are written with a proprietary language mainly containing Boolean algebra. By writing the following rules, we ensure that only management packets of type PROBE REQ, PROBE RESP, ASSOC, DISASSOC, AUTH and DEAUTH with the source and destination of HP2 are captured.

Monitoring the entire 802.11 spectrum (2412-2472 MHz / 13 Channels) is trivial. CommView can listen only one 802.11 channel at a time. If needed, multiple sniffers can be set on different mobile stations, but this is problematic. For setting up sniffers, we need more than one wireless interface (station). Also, we need time to be synchronized between sniffers distributed on different mobile stations in order to calculate handoff delays accurately. Time synchronization needs third-party solutions like NTP (Network Time Protocol) and is not so easy. Therefore we need to set both AP's to operate at the same channel although this conflicts with the 802.11 ESS principles. In our project we have set both AP1 and AP3 to operate at Channel 13 (2472 MHz). After choosing the channel and setting the filters, CommView is ready to capture packets.

Syslog is a standard for forwarding log messages in an IP network. The term *syslog* is often used for both the actual syslog protocol, as well as the application or library sending syslog messages. The syslog protocol is a client/server-type protocol. The syslog sender sends a small textual message (less than 1024 bytes) to the syslog receiver. Syslog messages can be sent via UDP and/or TCP.

Syslog is typically used for computer system management and security auditing. While it has a number of shortcomings, syslog is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository. Syslog is now standardized within the Syslog working group of the IETF.

Kiwi Syslog Daemon is a freeware Syslog Daemon for Windows. It receives logs, displays and forwards syslog messages from hosts such as routers, switches, UNIX hosts, access points and any other syslog enabled device.

V. TEST RESULTS

We took many different measurements using similar techniques given in [10] and calculated handoff delays for different setups. The typical delays for some setups are shown in Table 1 below.

TABLE I
CALCULATED HANDOFF DELAYS

Software	With Probe Delay(ms)	Without Probe Delay (ms)
WirelessMon/ Win XP	25,253	25,253
Native / Win XP	64,535	51,440
Native / Linux	163,347	8,798
Scriptex / Linux	437,095	9,953

In Table 1, the first field of the software column is the handoff manager while the second is the operating system on which the manager runs. For example, Native/Linux means handoff is performed by native Linux wireless drivers on Linux machine. There are two different results for each setup, one with the probe delay and the other is the one without probe delay. Actually these two results are obtained from the same experiment. However, in order to clearly see the effect of the probe delay, handoff delays were calculated both with and without probe delays and showed in the table.

The results are as we expected. Scriptex has the biggest handoff delay, since it is a software solution. The others have smaller delays as they perform handoff in hardware level. By looking at the table, we also see that most of the handoff delay is caused by active scanning (probe delays). If any active scanning is omitted, handoff delays will be less than 50 ms which is enough even for most of today's delay sensitive applications such as VoIP or multimedia streaming. This can be achieved through some trivial solutions like caching scan results. When we look at the table, we can say that WirelessMon uses this technique to avoid probe delays.

We have also observed that, handoff performance is much better on Linux systems than Windows systems. However, if probe delays are considered, Windows systems will have better delays.

In our tests, we have also observed that different setups follow different sequence of messages. In native Win XP and Scriptex, probe requests are sent after the Disassociation request is sent to the old AP. Moreover we may not even see this disassociation request in the Native Linux environment. In WirelessMon running on Win XP, we are not able to see probe requests and responses since it caches the scan results as we mentioned above. By looking at these results, we can clearly see that currently available hardware cannot interoperate with other hardware systems due to the different deployments. This leads us to our interoperable software solution Scriptex.

VI. CONCLUSION

This paper presented a software solution project Scriptex for handoff in WLANs for a context-aware system in the campus area at Fatih University. In this project, we developed and implemented a software solution for providing handoff infrastructure for mobile applications. We tested and compared Scriptex with the already deployed hardware solutions. Our efforts for this project were mainly focused on providing a stable infrastructure for the SOWCAS project so that we intensively tested our solution together with the current solutions. The test results showed that there is not a clear winner. In general, hardware solutions provided better delays while Scriptex provided interoperability. Therefore we have decided that both handoff solutions can be used interchangeably depending on the real-time operation needs of mobile applications. As a future work, Scriptex can be extended to use probe avoiding techniques to overcome large delays caused by active scanning.

This work has also shown that current 802.11 architecture is not suitable for most of the delay-sensitive applications like VoIP. It has been observed that there are interoperability problems with different access point and wireless network interface card vendors. But using a software solution, interoperability problems can be solved. Also with a software controlled solution, probe delays can be reduced with some trivial techniques. Using these techniques delays can be

reduced to acceptable rates which will lead to the possibility of using delay-sensitive applications.

REFERENCES

- [1] H. Gümüşkaya, M. V. Nural, "Service-Oriented Context-Awareness and Context-Aware Services", *Advances in Computer and Information Sciences and Engineering*, Springer, pp. 184 – 189, August 2008.
- [2] H. Gümüşkaya, A. V. Gürel, M. V. Nural, "Architectures for Small Mobile Communication Devices and Performance Analyses", *First IEEE International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2008)*, pp. 342 – 347, Ostrava, Czech Republic, 4-6 August 2008.
- [3] IEEE. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard 802.11, 1999.
- [4] IEEE. Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. IEEE Draft 802.1f/D3, January 2002.
- [5] The Linux Wireless Extension and the Wireless Tools, http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html.
- [6] WirelessMon, Wireless Monitoring Tool, PassMark Software Inc., <http://www.passmark.com/products/wirelessmonitor.htm>.
- [7] CommView for Wifi, Wireless Monitoring Software, <http://www.tamos.com/products/commwifi/>.
- [8] Syslog protocol, <http://en.wikipedia.org/Syslog>.
- [9] Kiwi Syslog Daemon, Syslog Monitoring Software <http://www.kiwisyslog.com>.
- [10] A. Mishra, M. Shin, W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process", *SIGCOMM Comput. Commun. Rev.*, Vol. 33, No: 2, pp. 93-102, 2003.

Robust Transmission of Video Stream over Fading Channels

Mao-Quan Li^{1,2}, Zheng-Quan Xu², Yan-Yan Xu²

¹School of Electronic Information, Wuhan University, Wuhan 430079, China

²State Key Laboratory of Information Engineering in Surveying, Mapping and Remote Sensing, Wuhan University, Wuhan 430079, China

E-MAIL: limaoquan@263.net, xuzq@whu.edu.cn, xuyy@whu.edu.cn

Abstract-Fading channels, such as mobile wireless channels, are characterized by long burst of packet loss. It usually results in several macroblock lines, a whole frame or even multiple successive frame loss that is difficult to be corrected by conventional error correcting techniques. This paper proposes a robust video coding scheme, which consists of three steps: 1) spatial decimation divides each frame into two similar fields which can be used to correct each other by spatial error concealment, 2) field-level Alternative Multi-hypothesis Motion Compensated Prediction (AMCP) makes the error from even top fields and odd bottom fields decrease and converge to zero quickly and automatically and 3) temporal interleaving is applied to disperse burst error to different frames which further enhances the error concealment capability to up to three successive lost frames. Simulation results show that the proposed scheme provides superior subjective and objective video quality than conventional schemes in long burst packet loss environment.

I. INTRODUCTION

Video transmission over fading channels is still a challenge to error resilient technologies. For example, mobile wireless channel is a typical fading channel which is characterized by long burst of packet loss because of multi-path fading, shadowing and noise and so on. In addition, the limited available bandwidth of mobile wireless channels, such as 3G wireless systems, restricts the frame size. Sometimes a frame is only divided into just 1 or 2 packets. Therefore, a loss of packet introduces the burst errors which are the loss of the several successive macroblocks (MBs), a whole frame or even multiple successive frames. For compressed video sequences, the burst errors not only impose significant quality degradation in the current decoded frame, but they are also propagated to succeeding frames due to the motion compensation (MC).

Error concealment (EC) technologies [1], [2] are usually used to minimize the visual degradation caused by transmission error. They can be divided into two categories: spatial error concealment (SEC) and temporal error concealment (TEC). In conventional SEC and TEC technologies, information of neighbor MBs, such as pixels and motion vectors, are employed to facilitate recovering of a lost MB. They can effectively deal with situations where only few sporadic MBs of a frame are lost. However, they become unusable or low efficient when burst packet loss occurs for the reason that there is no neighbor correct MB available.

Some research has been done to improve EC performance for burst packet loss, such as data partitioning [3], layered coding [4], unequal error protect (UEP) [3] and redundant picture [5], etc. Their EC performance depends highly on the main partition, enhancement layer, error protection data or redundancy data respectively. If they are lost, no EC gain can be obtained. Multiple Description Coding (MDC) [6] and Alternative Motion-Compensated Prediction (AMCP) [7], [8] are other two efficient technologies. In MDC, several independent code streams (descriptions) are transmitted separately. The quality of the reconstructed signal is acceptable with any one description and that incremental improvement is achievable with more descriptions at the destination. The coding efficiency is reduced in exchange for increase robustness to long burst errors. But it requires that at least one description is available at any time and it is helpless when a whole frame is lost. In AMCP, two-hypothesis (weighted MC from two reference frames) and one-hypothesis predictions are alternatively used frame by frame, if a two-hypothesis frame is lost, the error that propagates to the succeeding frames will decrease and converge to zero quickly and automatically by weighted MC. However, AMCP can only eliminate error in a two-hypothesis frame needless to say multiple successive frame loss.

In this paper, a new robust error concealment scheme is proposed to deal with loss caused by long burst packet loss. Input frames are divided into field-pairs by spatial decimation, so a pair of two fields can be used to recover each other. Two fields of a frame are motion compensated through interleaved AMCP, which makes error from one field of each frame can be eliminated by weighted MC. At last, temporal interleaving among co-located fields is applied to disperse burst error to different frames. It further enhances the error concealment capability to up to three successive lost frames.

II. ALTERNATIVE MOTION COMPENSATED PREDICTION (AMCP) [7]

In AMCP, a linear combination of multiple signals (hypothesis) is used to predict each macroblock in even frame. As shown in Fig. 1, each even frame is weighted predicted from its previous two frames; each odd frame, except for 1st frame, is predicted from its previous odd frame.

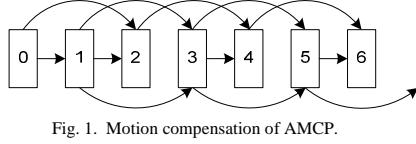


Fig. 1. Motion compensation of AMCP.

The frame $\psi(n)$ is predicted by

$$\psi(n) = \begin{cases} \tilde{\psi}(0), & n=1, \\ (1-h)\tilde{\psi}(n-1) + h\tilde{\psi}(n-2), & n=2k, \\ \tilde{\psi}(n-2), & n=2k+1. \end{cases} \quad (1)$$

where $k \geq 1$ and $h \in (0,1)$. $\tilde{\psi}(n-k)$ is a motion compensation prediction from the k^{th} previous reconstructed frame.

Consider the case of one frame loss. AMCP conceals the lost frame by copying the previous frame. Assume the lost frame is $\psi(l)$ and $e(k)$ is the difference between the reconstructed $(l+k)^{\text{th}}$ frame at the encoder and that at the decoder. Lost of an even or an odd frame will form different error propagation. If an even frame (except for 0th frame) is lost, the error propagation model is

$$\begin{aligned} e_e(2n) &= h^n e(0), & n \geq 1, \\ e_e(2n+1) &= 0, & n \geq 0. \end{aligned} \quad (2)$$

If an odd frame is lost, the error propagation model is

$$\begin{aligned} e_o(2n) &= e(0), & n \geq 1, \\ e_o(2n+1) &= (1-h^{n+1})e(0), & n \geq 0. \end{aligned} \quad (3)$$

So if an even (except for the 0th frame) frame is lost, the error value will decrease and converge to zero quickly; if an odd frame is lost, error will propagate to all the following frames. So AMCP is only suit for recovering error caused by a single even lost frame.

III. ERROR CONCEALMENT BASED ON SPATIAL DECIMATION (ECSD)

If each input picture is decimated by pixel lines into two similar fields by pixel lines and then they are merged together to form a new picture before encoding, the spatial adjacent pixel lines are not tend to be damaged simultaneously by transmission error, because they are scattered far away in the new picture. The strong similarity between two fields can be employed to facilitate EC. The decimation operation is shown in Fig. 2.

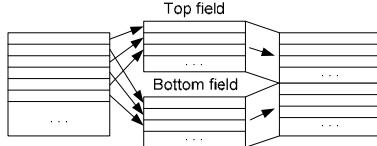


Fig. 2. Decimation operation.

After decoder, two fields of each decoded frame are interleaved back by pixel lines to reconstruct source picture. Fig. 3 shows the process of interleaving operation.

As shown in Fig. 4, a source frame is divided into some MB-pairs. Each MB-Pair consists of two co-located MBs in two fields which are decimated from a 16x32 district from the source frame, so they have very high correlation which can be employed to facilitate EC.

After decoding, if there is error, lost MBs are recovered as following steps.

Step 1. All MB-Pairs which has only one MB corrupted are processed firstly by SEC.

Each pixel line of a corrupted MB is recovered by vertical interpolation between its two spatial neighbor pixel lines in its co-located MB. Interpolation is made between two spatial neighbor pixel lines, it provides much better picture quality than conventional MB based SEC technologies.

The coding mode of this MB is replaced by that of its co-located MB.

Step 2. The top MBs of MB-Pairs which are totally lost are processed in raster scan order.

If at least one of its neighbor correct or concealed MBs is an intra MB, it is concealed by SEC method which is to recover each pixel line of the corrupted MB by vertical interpolation between its two spatial nearest correct or concealed pixel lines before and after it. This MB is marked with intra too. Otherwise, it is temporal concealed by a motion compensated error concealment algorithm [9]. As shown in Fig. 5, Zero-MV, MVs of neighbor blocks in the correct or concealed neighbor MBs and the MV from the co-located MB of last frame are all tried and the winning MV is the one which minimizes the side match distortion which is the average of sum of absolute Y sample value difference of the IN-block and neighboring OUT-block samples at the boundaries of the current block. This MB is marked with inter after concealment.

If current MB is at the border of a sub-picture, the neighbor MB which belongs to the other sub-picture is not considered in MV choosing and boundary matching calculation.

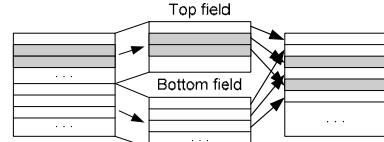


Fig. 3. Interleaving operation (Lost pixel lines are marked with gray color as an example).

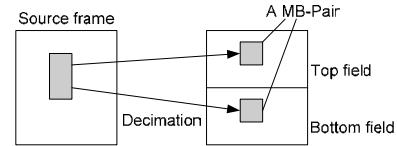


Fig. 4. A MB-Pair consists of two similar co-located MBs in two fields.

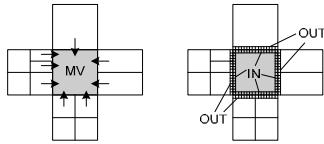


Fig. 5. MV selection and boundary matching.

Step 3. The bottom MBs of MB-Pairs which are totally lost are processed in raster scan order by SEC (Linear Interpolation) as described in step 1.

ECSD likes spatial sub-sampling MDC. But there is only one “description” in spatial decimation and no separately channels are required. It can only conceal MB loss within a frame.

IV. PROPOSED VIDEO CODING SCHEME

The frame index within a group of pictures (GOP) goes from 0. Only 0th frame is an Intra or IDR frame. Input frames are divided into field-pairs by spatial decimation firstly. Each field-pair has a top field and a bottom field. They are temporal predicted through different AMCP ($h=1/2$) as shown in Fig. 6. After decoding, field-pairs are interleaved back by pixel lines to reconstruct source picture as described in the section III. Reference fields of each field are described in Table I.

Before transmission, top fields and bottom fields are temporal interleaved independently as shown in Fig. 7. That is the even top fields exchange their positions with their succeeding odd top fields and odd bottom fields exchange their positions with their succeeding even bottom fields, so two fields of each frame are placed into different transmission frames. In other words, a transmitted frame is composed of two fields from different time.

AMCP, ECSD and temporal field interleaving are all contribute to the error concealment performance of the proposed scheme.

1. ECSD is employed to recover the error in a single frame. Two fields are also used to monitor each other to maintain picture quality in post processing.

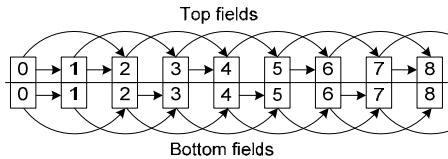


Fig. 6. Motion compensation is different between two fields of a frame in the proposed scheme.

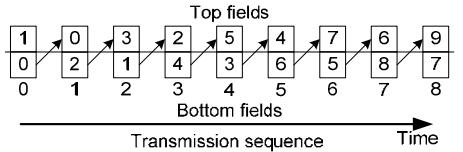


Fig. 7. A transmitted frame is composed of two fields from different source frames.

TABLE I
REFERENCE FIELDS OF EACH FIELD

Field type	Reference fields
1 st top field	0 th top field
Even top fields	Previous two top fields
Odd top fields	Previous odd top field
1 st bottom field	0 th bottom field
Even bottom fields	Previous even bottom field
Odd bottom fields	Previous two bottom fields

2. AMCP eliminates error propagation from half of the fields (even top fields and odd bottom fields).

If two successive source frames are all lost, Both ECSD and AMCP are useless. So temporal field interleaving is introduced to disperse lost fields.

3. Temporal field interleaving enhances the error recovering capability by placing two fields of a frame to different transmission frames to prevent two successive frame loss as possible.

Error recovery of the proposed scheme consists of two steps that are error concealment and post processing.

A. Error concealment

If one field in a frame is lost, it can be concealed by spatial or temporal methods by ECSD. If a whole frame is lost, it is concealed by copying from the last frame. Error from one field of the lost frame will decrease and converge to zero. Error from the other field will be monitored and alleviated in post processing.

Four typical cases of picture loss and error concealments are discussed here as shown in Fig. 8.

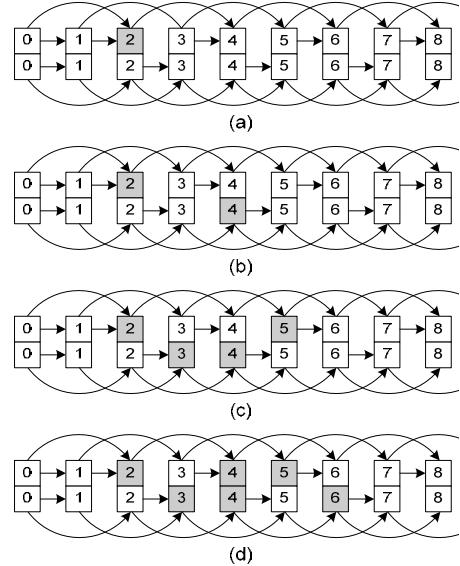


Fig. 8. Four typical cases of picture loss.
(a) top field of 3rd transmission frame is lost; (b) 3rd transmission frame is lost;
(c) 3rd and 4th transmission frames are lost; (d) 3rd to 5th transmission frames are lost.

Case 1. One field is lost.

Case 2. One whole transmitted frame is lost. Two fields are from two source frames.

Case 3. Two successive whole transmitted frames are lost. Four fields are scattered in four frames.

Case 4. Three successive whole transmitted frames are lost. Six fields are scattered in five frames. Only one whole source frame is loss.

In case 1 to 3, there is only one field loss in each error frame. The lost field can be concealed by ECSD. In case 4, a whole source frame is lost. It is concealed by directly copying from the last frame.

Error propagation behavior of each case is analyzed:

Case 1. The lost field is concealed by ECSD. If the lost field is an even top field or an odd bottom field, the propagated error will decrease and converge to zero. The error propagation is under the control of the post processing.

Case 2. The lost fields are concealed by ECSD. Two lost fields are all odd or even fields, so it can be guaranteed that error in one field group will converge to zero. The error propagation is also controlled by the post processing.

In case 3 and case 4, propagated error of two field groups will not be eliminated, by they could be alleviated by the post processing.

B. Post processing

Error in different fields results in different error propagation behavior. Sometimes there is a discrepancy between two fields in a frame. If they are not similar enough, there will be saw-tooth artifacts after interleaving.

In order to determine error of each field, new error propagation models are introduced. For top fields, the error propagation model is

$$\hat{e}_t(n) = \begin{cases} 0, & n=0, \\ \tilde{e}_t(0), & n=1, \\ [\tilde{e}_t(n-1) + \tilde{e}_t(n-2)]/2, & n=2k, \\ \tilde{e}_t(n-2), & n=2k+1. \end{cases} \quad (4)$$

For bottom fields, the error propagation model is

$$\hat{e}_b(n) = \begin{cases} 0 & n=0, \\ \tilde{e}_b(0), & n=1, \\ \tilde{e}_b(n-2), & n=2k, \\ [\tilde{e}_b(n-1) + \tilde{e}_b(n-2)]/2, & n=2k+1. \end{cases} \quad (5)$$

where $k \geq 1$, $\hat{e}_t(n)$ and $\hat{e}_b(n)$ are propagated error of the n^{th} top field and bottom field respectively. $\tilde{e}_t(n)$ and $\tilde{e}_b(n)$ are error after error concealment of the two fields

$$\tilde{e}(n) = \begin{cases} \hat{e}(n), & \text{no error,} \\ e_s, & \text{by ECSD,} \\ e_T, & \text{by frame copy.} \end{cases} \quad (6)$$

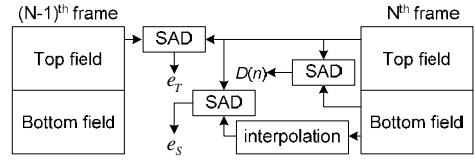


Fig. 9. Calculations of e_S , e_T and $D(n)$.

where e_S and e_T are estimated errors produced by ECSD and frame copy. Which is refreshed after each correct frame is decoded. As shown in Fig. 9, e_S is estimated by the sum of absolute differences (SAD) between the current top field and the interpolation between neighbor pixel lines of the bottom field; e_T estimated by the SAD between the current top field and the previous top field.

If there has been error in current GOP, then after each correct frame is decoded, the $D(n)$, SAD between two fields, is calculated as shown in Fig. 9. if $D(n)$ is more than a threshold H , the field with more $\tilde{e}(n)$ is reconstructed by the ECSD in order to reduce error propagation and saw-tooth artifacts after interleaving and $\tilde{e}(n)$ is replaced by e_S . H is initialized as

$$H = 2 \cdot SAD(T_0(0) - B_0(0)) \quad (7)$$

where $T_0(0)$ and $B_0(0)$ are the 0^{th} top field and the 0^{th} bottom fields of 0^{th} GOP.

Then in each GOP, before the first error frame, H is updated frame by frame as

$$H = \eta H + (1 - \eta) \cdot 2 \cdot SAD(T_m(n) - B_m(n)) \quad (8)$$

where η is 0.5, $T_m(n)$ and $B_m(n)$ are the n^{th} top field and the n^{th} bottom fields of m^{th} GOP.

V. EXPERIMENT

The proposed coding scheme is implemented in H.264 reference software JM12.4. To evaluate its performance, AMCP and the two description spatial sub-sampling MDC are tested as well. In MDC, error inside a frame is concealed by spatial interpolation. All picture loss in AMCP and the whole frame loss of the MDC are concealed by directly copy from the last frame.

100 frames of three CIF video sequences, Bus, Foreman and Stefan are tested under five typical cases which are: Case 1, error free, Case 2, the top half frame loss, Case 3, single whole frame loss, Case 4, two successive frame loss and Case 5, three successive frame loss. Each type of loss occurs three times from 20th, 50th and 80th transmitted frames respectively.

Only first frame is an I frame. Coding parameters are as follows: Frame rate is 15, Bitrate is set to 256kbps, Maximum QP is 40, only 16x16 inter-MB is adopted, each frame is composed of two slices, each slice has 198 successive MBs. Other parameters are copied from default baseline configuration file in JM12.4.

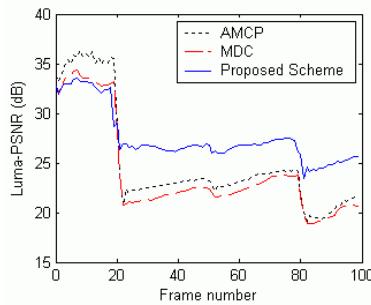


Fig. 10. Luma-PSNR of each frame by three schemes, when three successive frames ($20^{\text{th}}\text{-}22^{\text{nd}}$, $50^{\text{th}}\text{-}52^{\text{nd}}$ and $80^{\text{th}}\text{-}82^{\text{nd}}$ transmitted frames) are lost.

Luma-PSNRs of three video sequences under different cases by AMCP, MDC and proposed scheme are listed in Table II. Because of the temporal decimation, MDC and proposed scheme have lower coding efficiency than AMCP. However it can also be found that the proposed scheme has the least PSNR drop in every case compared to the other two schemes. It also achieves highest PSNRs in all cases when two or three successive frames are lost.

Take foreman sequence as an example. The Luma-PSNR of each frame when three successive frames are lost is compared in Fig. 10. We notice that after the first packet loss in the 20th frame, the Luma-PSNRs of the proposed scheme always surpass that of the other two schemes. Besides, the subjective perception quality of the proposed scheme is obviously much better than the other two schemes too. Two concealed frames (30^{th} and 85^{th} frames) coded by three schemes are listed in Fig. 11. Fig. 11(a) and 11(b) that are coded by AMCP and MDC have obvious distortion and annoying artifacts, and there is only little blur in Fig. 11(c) which is coded by the proposed scheme.

TABLE II
AVERAGE LUMA PSNRs (DB) OF VIDEO SEQUENCES CODED BY AMCP, MDC
AND THE PROPOSED SCHEME

Scheme	Case	Bus		Foreman		Stefan	
		PSNR	Drop	PSNR	Drop	PSNR	Drop
AMCP	1	28.63	-	35.89	-	30.22	-
	2	25.39	3.24	32.03	3.86	24.56	5.66
	3	23.15	5.48	31.31	4.58	24.25	5.97
	4	19.31	9.32	26.52	9.37	20.77	9.45
	5	18.45	10.18	25.06	10.83	20.02	10.20
MDC	1	25.59	-	33.35	-	26.00	-
	2	24.87	0.72	31.60	1.75	25.02	0.98
	3	19.42	6.17	28.66	4.69	21.88	4.12
	4	19.08	6.51	26.02	7.33	20.58	5.42
	5	18.07	7.52	24.06	9.29	19.85	6.15
Proposed	1	25.22	-	32.99	-	25.72	-
	2	24.72	0.50	31.70	1.29	25.06	0.66
	3	24.25	0.97	29.93	3.06	24.34	1.38
	4	23.76	1.46	28.36	4.63	23.61	2.11
	5	20.86	4.36	27.53	5.46	22.19	3.53



Fig. 11. Concealed frames (30^{th} and 85^{th} frames) of three schemes when three successive frames ($20^{\text{th}}\text{-}22^{\text{nd}}$, $50^{\text{th}}\text{-}52^{\text{nd}}$ and $80^{\text{th}}\text{-}82^{\text{nd}}$ transmitted frames) are lost.
(a) AMCP, (b) MDC, (c) Proposed scheme.

VI. CONCLUSIONS

In this paper, a robust video coding scheme is proposed to enhance error resilient capability against long burst of packet loss which is common in fading channels. Our research contributions are as follows:

1. Error concealment method based on spatial decimation is proposed. It is a robust error resilience technology in dealing with burst loss in a frame.
2. Field-level Alternative Multi-hypothesis Motion Compensated Prediction makes the error of one field of each frame decrease and converge to zero. It is also helpful for the error concealment of the other field.
3. Temporal interleaving disperses burst error to different frames which further enhances the error concealment capability for burst packet loss.

This coding scheme only requires little modification in video coding algorithms. As a result, it is suitable for all motion compensation based video coding codecs, such as H.26x and MPEG families.

ACKNOWLEDGMENT

This paper is supported by the National Basic Research Program of China (973 Program) (No. 2006CB303104).

REFERENCES

- [1] Y. Wang, S. Wenger, J.T. Wen, Katsaggelos, A. K., "Error resilient video coding techniques", *IEEE Signal Proc Magazine*, Vol 17, No. 4, pp. 61-82, July 2000.
- [2] Y. Wang, Q.F. Zhu, "Error control and concealment for video communication: a review", *Proceedings of the IEEE*, Vol 86, No.5, pp. 974-997, May 1998.
- [3] S. Xiao, C.K. Wu, J.C. Du, Yang, Y. D., "Reliable Transmission of H.264 Video over Wireless Network". *Int. Conf. On Advanced Information Networking and Applications (AINA-06)*, Vienna, Vol 2, pp. 844-848, April 2006.
- [4] T. de Souza-Daw, N.K. Chilamkurti, B. Soh, "An integration of H.264 based Error Concealment technique and the SPLIT layer protocol", *Int. Conf. On Networking, Morne*, pp. 109-114, April 2006.
- [5] C.B. Zhu, Y.K. Wang, H.Q. Li, "Adaptive Redundant Picture for Error Resilient Video Coding", *Int. Conf. on Image Processing (ICIP 2007)*, Atlanta, Vol 4, pp. 253-256, Sept. 2007.
- [6] Y. Wang, A. Reibman, S. Lin, "Multiple description coding for video delivery", *Proceedings of IEEE*, Vol.93, No. 1, pp. 57-70, Jan 2005.
- [7] M.Y. Ma, O.C. Aw, S.H.G. Chan, "A New Motion Compensation Approach for Error Resilient Video Coding", *Int. Conf. on Image Processing (ICIP 2005)*, Genoa, Vol 1, pp. 773-776, Sept. 2005.
- [8] S.N. Lin, Y. Wang, "Error resilience property of multihypothesis motion-compensated prediction", *Int. Conf. on Image Processing (ICIP 2002)*, New York, Vol 3, pp. 545-548, June 2002.
- [9] K.P. Lim, G. Sullivan, T. Wiegand, "Text Description of Joint Model Reference Encoding Methods and Decoding Concealment Methods", *ISO/IEC JTC1/SC29/WG11*, *JVT-R095*, Jan. 2006.

An Attack Classification Tool Based On Traffic Properties and Machine Learning

Victor Pasknel de Alencar Ribeiro^{1*} and Raimir Holanda Filho²

Universidade de Fortaleza, Brazil

¹pasknel@hotmail.com, ²raimir@unifor.br

Abstract—This work proposes an attack traffic identification based on traffic properties and machine learning. Attack identification is of great importance to many areas such as: intrusion detection, security, quality of service and the development of new hardware tools related to security. For the identification of each kind of attack, statistical discriminators were used based on their power of classification. The results obtained through this technique are presented in this work.

Index Terms—Attack Detection, Statistical Discriminators, Traffic Analysis.

I. INTRODUCTION

ATTACKS are a major source of risks for companies, so the detection and identification are activities that must occur quickly in order to treat them and prevent them.

Knowing that the identification of attacks, when they occur, is a difficult task, this paper presents a proposal for identifying and classifying attacks based on the analysis of traffic properties through the use of statistical discriminants and decision tree.

Networks are susceptible to various types of attacks (eg, UDP flood, dictionary attack, port scan) and each with its own characteristics [1], [2], [3]. The attacks considered in this work can be divided into three categories: denial of service, enumeration and password cracking.

To identify and separate attacks, we used the method of statistical discriminators where we elect one or more variables that can identify and isolate unique characteristics of an attack at the expense of others. These variables are called discriminators [4].

In this work the variables are selected by discriminant analysis of boxplot diagrams. The efficiency of each discriminator chosen is proven through the method of decision tree used for the classification of attacks.

Section 2 of this article presents some work on attack detection and the attacks used in this paper. In section 3 is demonstrated the generation of traces, as well as the network topology used. The methodology used for the classification of attacks is presented in Section 4. In section 5 are shown the final results and finally in section 6 are presented the main conclusions and future projects.

II. CLASSIFICATION OF ATTACKS

Traffic analysis is one area which has been the focus of attention for various researchers in recent years. The works of identifying attacks published demonstrate different methods for this task, among them are detection based on anomalies, behavior and statistical properties.

In [5] is presented a method to detect attacks based on traffic anomalies. This approach is based on the premise that attacks provoke a deflection on the normal behavior of a network. From these anomalies, this method is capable to identify both known attacks and new attacks.

Methods of identification based on behavior use learning algorithms with the aid of information about how the attacks behave [6]. A methodology for the classification of different classes of application traffic using statistical discriminators and clustering analysis is demonstrated in [7].

These previous works have been devoted to the detection of attack traffic; however this presents solutions to the classification of different types of attacks. This paper proposes the classification of attack traffic using the analysis of statistical properties of flows.

Flood attacks are aimed to send a large amount of data to a target, with the goal of overloading the victim, thereby preventing that requests made by legitimate clients are answered. This type of attack can be carried out using different protocols, among them the HTTP, SMTP and FTP [1].

A port scan attack refers to the technique of sequentially verify, through the requisition of a TCP connection or simple UDP datagrams, a number of ports on a machine that can be utilized in future attacks through possible security breaches under the same [8].

In this work are considered two types of attacks to crack passwords. The first (Dictionary attack) is aimed at breaking the passwords of an authentication mechanism using a predetermined set of words. The second (Brute Force), carries out the attack by merging letters and digits at random until it discovers the password [9].

III. GENERATING TRACES

For the realization of attacks and collection of packets, you must first create a scenario where the network can carry out these important tasks.

* This work is supported by CNPq

The whole process of generation, analysis and classification of the attacks was carried out through a controlled manner in a laboratory. Figure 1 show the environment used to generate all the attack traffic.

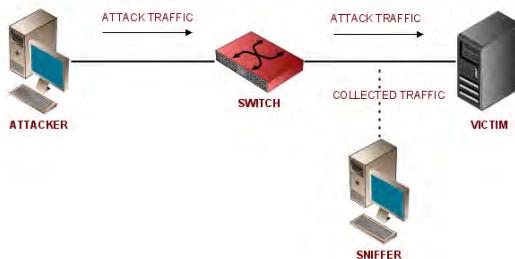


Fig. 1. Network Topology.

In this scenario were used three computers: the attacker, the victim and sniffer. The attacker has the role to send attack traffic, through services such as FTP, SMTP and HTTP, to a particular victim. For the realization of denial of service and port scan attacks the program used was DoS v5.5, while dictionary and brute force attacks were generated by the tools Hydra and Brutus respectively.

For the task of collecting packets is necessary to use a network protocol analyzer. This activity was realized using the Wireshark packet sniffer.

During the generation of traffic, sessions were held with a single attack, for better analysis of each type, and finally two sessions containing all attacks combined, which will be used to validate the classification method described in section 4.

This paper is based on the principle of data flows, which can be defined as a number of packets traveling between two devices through a common protocol and a specific pair of ports [4].

The packets collected from the network traffic were filtered by a program of our authorship, written in Perl. Our aim is to create flows of data based on information provided only by the headers of the packets obtained. The trace files are formed by TCP flows and store information such as: package size and TCP flags.

A manual classification of flows is performed during this stage of work. This task is to realize a manual identification for each type of attack examined. An identifying variable, which represents the flow of attack, is added in each trace file generated.

This activity will be required to verify the accuracy rate of the method of classification, as well as the values of false negatives and false positive during the stage of validation. A decision tree is created from a combination of various flows of attack collected. After the tree generation model, the identifying variables will be used to recognize each flow of attack on a leaf node of the tree.

IV. METHODOLOGY

The proposed methodology is the implementation of three phases: the standardization of traces, selection of discriminators and training.

A. Standardization of traces

All traces of attack used are formed by lines which each represents a flow of attack. Each flow contains information that will be explored by the discriminant candidates to be able to elect one or more for the classification of each trace of attack. The standardization occurs during the use of boxplot diagrams and the elimination of outliers.

Boxplot graphics are used in this study to analyze and compare data sets of different classes of attack. From these diagrams, we can see the data distribution and the presence of outliers.

The boxplot diagram demonstrates the median (50%), the first (25%) and third (75%) quartiles in the distribution of values that are being analyzed. The outliers are values that show more than a multiple of 1.5 and 3.0 of N values, above or below the percentage 75% and 25% respectively. N is the result of the difference between the first and third quartile.

The values of analyzed information which are above the 3.0 multiple, which can be below the first or above the third quartile, are considered deviations from behavior of the attack and the flow containing such information will be discarded. These are called extreme outliers.

The withdrawal of extreme outliers ensures the standardization of the behavior of all flows of traces of attack so that they can be analyzed and classified by discriminating each candidate.

B. Selection of discriminators

We consider the choice of discriminators to be used in the analysis of attacks as a major step towards the classification of them. We elected discriminant candidates to analyze the value of the variables discriminancia contained in each of the flows in the trace files. Thus the boxplot diagrams can be constructed and analyzed. The variables are presented in Table I.

TABLE I
DISCRIMINANT VARIABLES CANDIDATES

Discriminators
Total of packets from client to server
Total of packets from server to client
Total of packets
Total of bytes from client to server
Total of bytes from server to client
Total of bytes
Total of ACK packets from client to server
Total of ACK packets from server to client
Throughput of client to server
Throughput of server to client

While examining the boxplot diagrams with the values of the variables of all kinds of attacks, we seek to identify through that variable concerned, if there is a set of values

which are different from all others that are in the diagram. For the ranking of the six attacks that related work, were used the four best discriminators seen in Table II.

TABLE II
SELECTED DISCRIMINATORS

Discriminators
Total of bytes
Total of packets from server to client
Total of ACK packets from server to client
Total of bytes from client to server

Figure 2 shows the boxplot diagram of the variable “Total of Bytes”. This variable represents the sum of bytes sent between client and server and vice versa in each flow. This diagram shows that the values of brute force, port scan, SYN flood and SMTP flood can be separated between themselves. Dictionary Attack has some common values with FTP flood but it can be identified from other attacks.

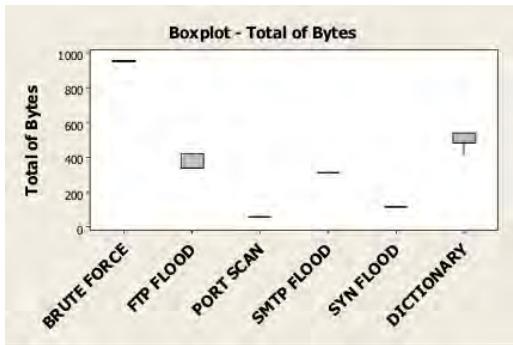


Fig. 2. Boxplot of the variable “Total of bytes”.

The boxplot of the variable “Total of Packets from server to client” is shown in Figure 3. Port scan, brute force and SYN flood do not show any common values, so they can be identified from each other. Dictionary attack and SMTP flood have overlapping values with FTP flood, but they can be separated from other flows.

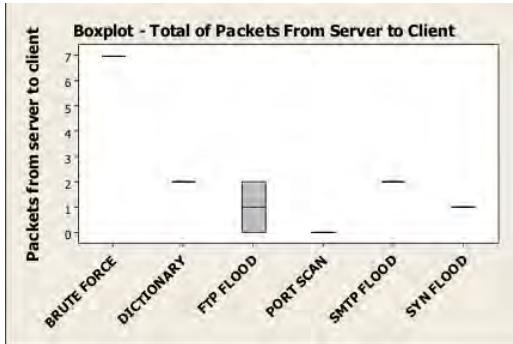


Fig. 3. Boxplot of the variable “Total of packets from server to client”.

Figure 4 demonstrates the boxplot diagram of the variable “Total of packets ACK from server to client”. This variable, as the previous one, can separate the values of brute force, SYN flood and port scan. SMTP flood and dictionary attack have common values with FTP flood, but they can be identified from other attacks.

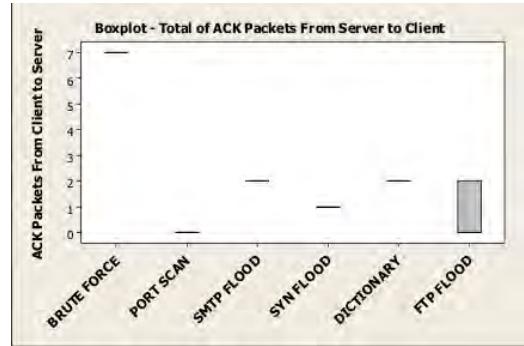


Fig. 4. Boxplot of the variable “Total of ACK packets from server to client”.

The boxplot diagram of variable “Total of bytes from client to server” can be seen in Figure 5. Port scan and SYN flood show overlapping values but these attacks can be separated from the other flows.

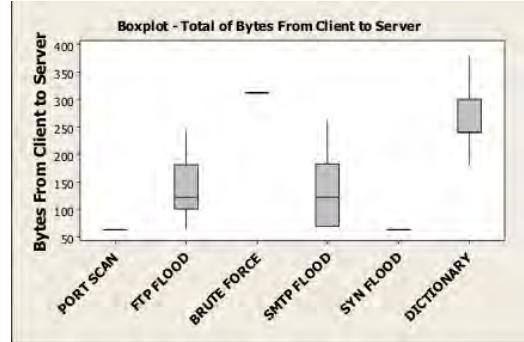


Fig. 5. Boxplot of the variable “Total of bytes from client to server”.

C. Training

Decision trees perform classification of data using pre-established input variables. This method uses the strategy of divide and conquer: a set of complex data is broken into smaller sets of data and the technique to break them into smaller sets is applied recursively [10].

In this study, all data collected are represented by numerical values and for this reason there is a need for the use of an algorithm of decision tree that is able to work with such values. The M5P [11] was selected as the learning algorithm. This method is used to work with both continuous and discrete values. Its efficiency is demonstrated in [12].

The first step towards the creation of a decision tree is to select the learning algorithm and from the value of entry

chosen, this algorithm creates a model tree where every leaf relates the values instantiated with the variable input chosen. This step is called the phase of training.

The discriminators selected (Table II) were used individually as input parameters to the M5P algorithm, therefore, generating 4 different decision trees. The other variables (Table I) are used in the definition of the production rules of the model tree. Among the 4 choices of trees generated, the variable "Total of Bytes" proved to be the best choice as the input parameter. The values of production rules used by the model tree are set by the M5P algorithm, based on the input variable in question.

Figure 6 shows the model tree created using the algorithm M5P. This decision tree was trained with the first group of data obtained from the collection of packets.

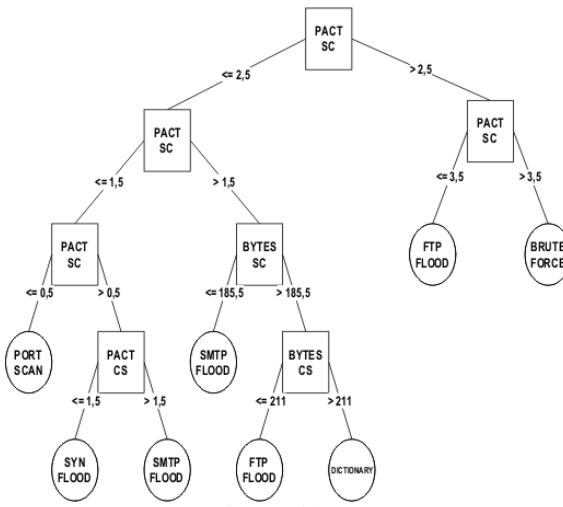


Fig. 6. Model Tree.

During the second step, the algorithm receives new flows of entry, but still using the model tree created during the training phase. In this step, we analyze the efficiency of the tree created using the discriminators selected in the previous section using new instances of data. This step is called the phase of validation.

V. RESULTS

After the training phase, the second group of flows, obtained during the collection of packets, was used for the validation of the model tree. The importance of the process of manual classification of flows is noted during the validation process. Though the use of the identifying variable, we can account the total quantity of each type of attack flow in the model tree. Table III shows the values of success rate, as well as the values of false positive and false negative obtained.

TABLE III
CLASSIFICATION OF ATTACKS

	Rate of Success	False Positive	False Negative
Port Scan	100%	-	-
SYN flood	91,9%	-	8,1%
FTP flood	99,2%	-	0,8%
Dictionary	98,2%	-	1,8%
Brute Force	98,2%	1,8%	-
SMTP flood	91,1%	8,9%	-

The rates of success vary from 91.1% to 100%. The port scan attack obtained 100% of classification. SMTP flood and brute force attack achieved 91.1% and 98.2% respectively for classification. The SYN flood acquired 91.9% of classification and the FTP flood received 99.2% of classification. The dictionary attack reached 98.2% of classification. The average rate of classification of the attacks stands at 96.4%.

The port scan attack was the only attack not to present values of false positive and false negative. The SYN flood had 8.1% of its flows classified as SMTP flood. FTP flood had 0.8% flows recognized as SMTP flood. Dictionary attack had 1.8% of flows classified as brute force.

Only two attacks had values of false positive. The brute force attack had 1.8% of flows from dictionary attack recognized as his, while SMTP flood gained 8.9% from a combination of flows from SYN flood and flood FTP.

VI. CONCLUSION

The technique of classification by statistical discriminators, aided by the use of decision trees, showed that it is possible to classify attacks with the use of few discriminators. This result was obtained with the analysis of discriminators, through boxplot diagrams and decision trees. We conclude that the attacks in this work can be classified by a small number of discriminant variables.

At the moment, our work uses an offline approach for the identification of attacks, reporting or not the occurrence of attacks. Currently, studies are being made to implement a real-time model of analysis.

While the proposed technique has been applied for 6 attacks, it presents totally extend to other attacks. We intend to add new attacks, seek new discriminators, validate using best-known data sets and simulate more realistic scenarios the environment of collection of flows to verify occurrence of changes in behavior and the variables in each attack.

REFERENCES

- [1] S. M. Specht, "Distributed Denial of Service: Taxonomies of attacks, tools and countermeasures", International conference on parallel and distributed computing systems, PP. 543-550, September 2004.
- [2] C. L Schuba, I. V. Krsul, M. G. Kuhn, "Analysis of Denial of Service Attack on TCP", IEEE Computer Society, Washington, DC, USA, 1997.
- [3] C. B. Lee, C. Roedel, E. Silenok, "Detection and Characterization of Port Scan Attacks", Department of Computer Science & Engineering University of California, San Diego.

- [4] A. W. Moore, D. Zuev, M. Crogan, "Discriminators for use in flow-based classification", In passive & Measurement workshop 2003 (PAM2005), August 2005.
- [5] P. Barford, J. Kline, D. Plonka, A. Ron, "A signal analysis of network traffic anomalies", Internet Measurement Workshop 2002.
- [6] Brutlag, J., "Aberrant behavior detection in timeseries for network monitoring", USENIX LISA 2000.
- [7] R. Holanda Filho, J. E. B. Maia, M. F. F. Carmo, , Paulino, G., "An Internet Traffic Classification Methodology based on Statistical Discriminators", In: IEEE/IFIP Network Operations & Management Symposium, 2008, Salvador, Bahia. Anais do NOMS 2008, 2008.
- [8] J. Kurose, K. Ross, Redes de computadores e a Internet: Uma abordagem top-down, Pearson Addison Wesley, 2006.
- [9] B. Pinkas, T. Sander, "Securing Passwords against dictionary attack", ACM conference on computer and communications security, pp. 161-170, 2002.
- [10] C. W. Kirkwood, "Decision Tree primer", Department of Supply Chain Management, Arizona State University Tempe, AZ 85287-4706.
- [11] Y. Wang, I. H. Witten, "Induction of model trees for predicting continuous classes", Poster papers of the 9th European Conference on Machine Learning, 1997.
- [12] T. Kalganova, "Towards the development of a Problem Solver for the Monitoring and Control of Instrumentation in a Grid Environment", School of Engineering and Design Brunel University, 2006.

Browser based Communications Integration using Representational State Transfer

Keith Griffin

Cisco

Galway, Ireland

kegriffi@cisco.com

Colin Flanagan

University of Limerick

Limerick, Ireland

colin.flanagan@ul.ie

Abstract— Web browser based real time communications applications such as instant messaging, call control and presence aware applications differ from traditional desktop based communications applications. Browser based applications typically rely on Hypertext Transfer Protocol (HTTP) as an application level communications protocol. Traditional desktop applications have used a variety of client/server protocols and techniques. Browser based applications offer many advantages but also introduce many constraints. This paper investigates the possible use of Representational State Transfer (REST) based architectures for real time communications integration systems. We look at REST in the context of an enterprise unified communication system using telephony and presence as representative features of a unified communications system. We contend that a REST based architecture offers benefits for thin clients in a unified communication environment.

Keywords: REST, Browser, Communications Integration, Telephony, Presence.

I. INTRODUCTION

Communication systems provide communication services which are presented to a user across multiple devices. Well known examples include:

- Phone systems, providing telephony (voice) services to fixed or mobile telephone devices.
- Instant messaging systems, providing instant messaging and presence services to desktop or mobile computing devices.

As the communication media capabilities of these systems increase so does the range and type of client devices capable of handling new communication media. Such devices include desktop computers, IP Phones and mobile devices. Some of these devices can be extremely capable and well resourced e.g. desktop PC's; others can be extremely limited in terms of computing power and

related resources e.g. handheld mobile devices. Integrating real time communication services into applications running in thin client web browser based environments is technically challenging. Real time communication integration clients often require locally deployed software components to manage messaging between the client and the communication server. The computing requirements of this software can often be beyond the resources available on some devices. One approach used on mobile devices that applies to a range of other devices is that of browser based thin client computing [1]. We suggest that an architecture for real time communications integration based on Representational State Transfer (REST) as an architectural style for networked systems can be used for thin client browser based communications applications. In this paper we describe communications integration systems including identification of a representative set of communication features, we describe REST and evaluate a REST based architecture for communication integration systems.

II. OVERVIEW OF COMMUNICATIONS INTEGRATION SYSTEMS

Communication integration systems are extremely varied. For the purpose of this paper the scope of the term communication system is restricted to enterprise communication systems [2]. An enterprise communication system is defined in this context as a system that serves the communication needs of users in multiple networked campus environments. Typically these systems serve less than hundreds of thousands of users unlike service provider solutions which serve public communication requirements and can scale to millions of users. As interfaces on a communications integration system abstract the underlying communication services on the network this paper will focus on a single campus implementation.

Modern enterprise communications systems offer communication over various media types including voice (telephony), video, instant messaging, web collaboration, document sharing and other features. Underlying network services such as presence and location are also core features of such systems. This is often referred to as Unified Communications. A high level diagram showing

some of the services and clients associated with such as system is shown in Fig. 1.

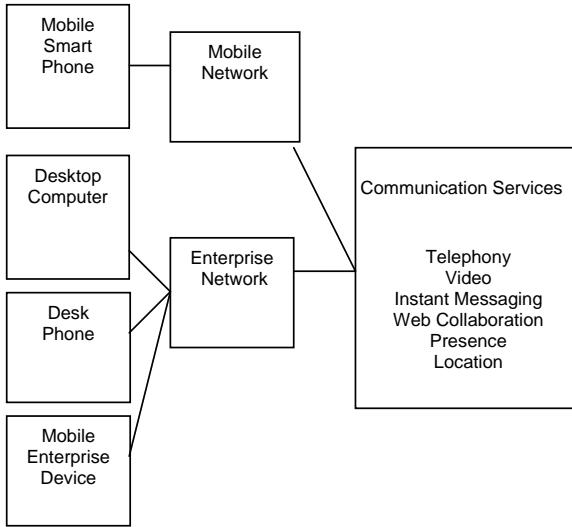


Fig. 1. Single campus unified communications solution architecture

For the purpose of this paper, telephony commands and events and presence manipulation mechanisms will be used as representative features of an enterprise communication system. Furthermore, interfaces representing abstractions of these services will be used to test the suitability of REST as an interface technology to these systems.

Telephony commands and events are fundamental to communication systems and voice telephony remains the most common form of communications in enterprise systems. Telephony commands and events are representative of an enterprise communications system as it requires bi-directional messaging of a real time nature with response times in the order of magnitude of hundreds of milliseconds typically required. Telephony represents a fundamental and legacy feature of an enterprise communication system.

In modern enterprise communication systems *presence* represents the availability for a user to communicate based on a number of relevant inputs. For example if a user is on a telephone call the users presence is typically set to busy by the system to advertise that the user is unavailable for communication. Presence related commands and events are representative of an enterprise communications system as it requires bi-directional messaging of a real time nature with sub second response times required. Presence also extends to all interested subscribers which can place further technical challenges on the system in terms of performance and scalability. Presence represents a

fundamental and new feature of an enterprise communication system.

A. Communications Features Considered

The following features were considered as part of a communication system as part of this study. It should be noted that before invoking such features it is assumed that an initiation sequence would take place between the communication application and communication system. This sequence would include registration and authentication of user, devices and application.

Telephony commands

- Makecall – Instruct the system to initiate a telephone call.
- Answercall - Instruct the system to answer a telephone call.
- Dropcall - Instruct the system to terminate a telephone call.
- Holdcall - Instruct the system to place a call on hold.
- Unholdcall - Instruct the system to retrieve a telephone call from hold.
- Conferencecall - Instruct the system to initiate a conference call.
- Transfercall - Instruct the system to initiate a call transfer.

Telephony events

- Call Initiated / Completed.
- Call Answered.
- Call Held.
- Call Retrieved.
- Conference Call Initiated / Completed.
- Transfer Call Initiated / Completed.

Presence Commands

- getPresence – retrieve presence state information for a user.
- setPresence – instruct the system to set a users presence state.

III. OVERVIEW OF REPRESENTATIONAL STATE TRANSFER

Representational State Transfer or REST is an architectural style for networked systems as described in Dr. Roy Fielding's Ph.D. dissertation [3]. It is not dependant upon any particular protocol. This means that it is possible to create a REST based system that is not built upon HTTP. However, most practical implementations of

REST are built on HTTP. REST is not a standard however it does prescribe the use of standards, including but not limited to:

- HTTP
- URL
- XML, HTML, GIF, JPEG... (representations of resources)
- TEXT/XML, TEXT/HTML, IMAGE/GIF, IMAGE/JPEG... (content types)

A. Design Principles of a REST based system

An important principle of REST is that of resources. A resource is a source of specific information which is named by a Uniform Resource Identifier (URI). Resources are manipulated by network components using a uniform interface e.g. HTTP. Resulting state changes for the resource are returned as representations e.g. an XML document. As REST interfaces are by definition highly connected via URI, deeply linked representations are typically used over wide or shallow representations. This means that a representation returns specifically the data that it represents but is tightly linked to related data that an application might be interested in. The following are the main design principles of a REST based system.

- Statelessness. Every request from client to server must contain all the information required to execute the request and must not rely on information known to the server.
- Uniform interface to support state transfer consisting of:
 - A constrained set of well defined operations e.g. the HTTP methods GET, PUT, POST, DELETE.
 - A constrained set of content types e.g. text/xml, image/jpeg.
- Client server pull interaction. Consuming clients pull representations.
- Uniquely Named Resources. A URI is used to

name the resources which comprise the system.

- Layered, interconnected resource representations: resource representations are interconnected using URLs enabling a client to progress through states.
- Cacheable responses to promote network efficiency.

B. Advantages and Disadvantages of a REST based Architecture

There are several advantages and disadvantages to REST based architectures. Indeed in Chapter 5 of the previously referenced doctoral dissertation from Dr Roy Fielding, many of these are described and discussed. What follows are some of the more commonly perceived advantages and disadvantages associated with REST.

REST Advantages

- Offers possibilities for thin client development as less client code is required.
- Does not require explicit resource discovery mechanism due to hyperlinking.
- Scalable architecture compared with those that require stateful servers.
- Caching promotes network efficiency and fast response times.
- Software versioning benefits including support of document type evolution such as HTML and XML without impacting backward or forward compatibility.
- Resource extensibility, allowing support for new content types without impacting existing and legacy content types.

REST Disadvantages

- HTTP as a uniform interface presents technical challenges for real time asynchronous events to a thin client or browser based application.
- Managing URI Namespace can be cumbersome

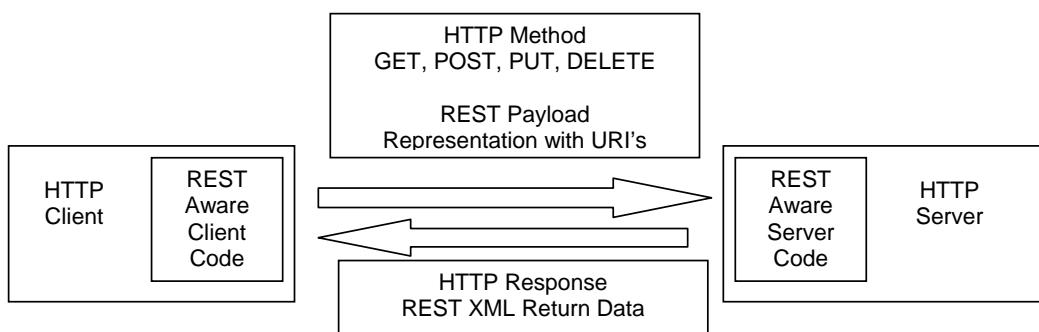


Fig. 2. REST based architecture for client – server communication

- Lacks supporting software tools
- Can impact network performance by encouraging more frequent client-server requests and responses.

C. REST Architecture

Fig. 2, shows an architecture for client – server communications based on REST. It can be seen that the uniform interface is presented by HTTP and the resource representations are shared over this interface. The REST aware client code shown is typically part of a web page that is loaded from a web server. JavaScript is commonly used as a client side language embedded in HTML to manipulate resources. Where data is returned it is parsed and acted upon by this client side code based on the logic of the application.

Later we will see how the interface is defined with operations in the uniform interface (HTTP) with resources represented as URI's. The architecture also shows how several underlying standards such as HTTP, URL, HTML and XML can be used to support a REST based architecture.

IV. ASYNCHRONOUS EVENT NOTIFICATIONS IN A BROWSER BASED APPLICATION

In real time communications integration systems, asynchronous events are a core and mandatory feature. Basic events like a presence state change from busy to available or lifting a telephone handset resulting in an offhook event being delivered to an application are fundamental to traditional desktop based communications integration applications. Browser based communications applications typically rely on HTTP as the protocol used to communicate with a web server. HTTP 1.0 [4] improved on previously defined versions of the protocol which provided for raw data transfer over the internet. Improvements included allowing messages to be of MIME like format containing meta information about the data being transferred. Amongst other things HTTP 1.0 did not sufficiently take into consideration persistent connections. However persistent connections are considered in HTTP 1.1 [5]. An asynchronous event effectively amounts to a response without a request. A mechanism is required which will allow the delivery of asynchronous events which occur in the communications integration system to browser based clients. However any such mechanism must respect the behavior of web based systems and not allow unsolicited events from the server to the client which could create a security vulnerability.

One way to handle asynchronous events would be to use a persistent polling mechanism but polling would impact both the performance and scalability of the system which are among the benefits that HTTP presents in the first place. One possible protocol to transport asynchronous messages with low latency between the communications integration system and the browser is the Bayeux protocol [6].

A. The Bayeux Protocol

Bayeux is a protocol used to transport messages between a web server and web browser using named channels. Messages can be delivered as follows:

- Client to server
- Server to client
- Client to client (via server)

Bayeux suggests that all requests originate from the client i.e. a server may not initiate a connection to a client unless a client has previously sent a request to a server. However asynchronous events intended for a given client are supported once a client has made a request to the server.

The transport for server to client event delivery can terminate the HTTP response after all messages are sent as in the case of a polling transport or use a streaming technique that allows multiple event messages to be sent in the same HTTP response. Two transport types are supported by Bayeux: Long-Polling and Callback-Polling. Connections between the client and server are negotiated with handshake messages that allow the content type, authentication, protocol version and other parameters to be agreed.

B. Bi-directional Asynchronous Events

In order to support bi-directional communications as required by communications integration systems, Bayeux clients use two connections to a server to allow client to server and server to client messaging occur simultaneously as shown in Fig 3. Bayeux offers a transport option called *long-polling* which attempts to hold open a request until there are related events to deliver to the client. The intent is to always have a pending request to deliver events as they occur. The reconnect and interval advice fields are used to maintain requests over time and address resource starvation and increased server load. In the worst case this behavior can degenerate to that of traditional polling but used efficiently it can minimize both latency in server to client message delivery and the network resources required for the connection.

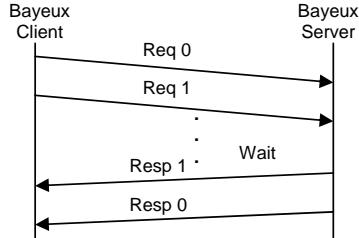


Fig. 3 Bi-directional Asynchronous Operation

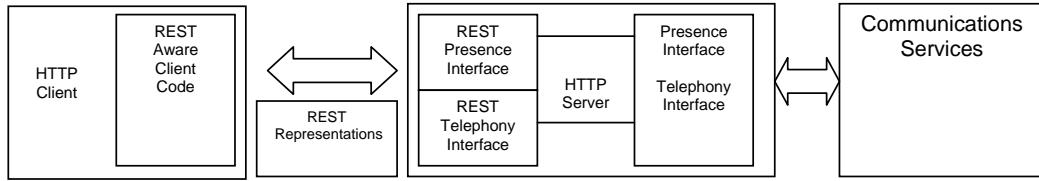


Fig.4. A Telephony and Presence architecture based on REST

V. REST BASED ARCHITECTURE FOR A COMMUNICATIONS INTEGRATION SYSTEM

Before looking at a REST based architecture it is important to consider the architecture of existing communication integration systems. Typically a client application is written against a defined interface. In the case of telephony, interfaces such as Microsoft Telephony API (TAPI) or Sun's Java Telephony API (JTAPI) are commonly used [7]. The client application typically consists of software which resides on a desktop computer and invokes the telephony interface from a telephony server using a remote invocation mechanism such as RPC or RMI.

By defining resources on the server and creating URI representations of these resources, a REST based architecture allows the client to run without requiring software to reside on the desktop. REST aware client code can be downloaded and run as part of a web based application running within a browser based thin client. An example of this would be JavaScript code that is loaded in a browser with a web page as part of a communications application. An architecture supporting this is shown in Fig. 4.

A. Defining the Interface

As described in section III, Design principles of a REST based system, the uniform interface used is HTTP with representations as named URI. What follows are some examples of a sample interface for getting and setting a users presence state which would be used by an application to advertise or modify a users availability to communicate. Similar interfaces can be created for the telephony features previously mentioned however for the sake of brevity only the presence interface is shown here in Fig. 5 - 7. Note how the interface follows some the basic rules of REST:

- Stateless: requests from client to server contain all information required to execute the request.
- Uniform interface: uses a constrained set of defined operations (HTTP methods).
- Uniquely named resources: URI's are used to name resources which comprise the system.

```
PUT systemusers/user/presence HTTP/1.1
<?xml version="1.0"?>
<presence>{state}</presence>
```

Fig. 5. A sample REST request to set a users presence

```
GET systemusers/user/presence HTTP/1.1
```

Fig. 6. A sample REST request to get a users presence

```
HTTP/1.1 200 OK
<?xml version="1.0" ?>
<presenceList>
  <user userURI="{uri}" presenceState="{state}"/>
  ...
</presenceList>
```

Fig. 7. A sample REST response containing users presence

The sample response shown in Fig.7 is sent in response to a request to GET the users presence state. However in the case that the user's presence is subsequently modified the previously referenced Bayeux protocol can be used to inform the consumer of the interface of the state change in an asynchronous operation.

B. Sample Presence Application

Using the interface defined in the previous section it is possible for a thin client, browser based application to request information relating to the availability of a colleague to communicate. The presence information is displayed on a web page which may run in a browser on the user's desktop computer, PDA or other device [8]. In fact, using this interface it could be displayed on all devices simultaneously. To display a user's presence information the client side of the application uses JavaScript to invoke a HTTP GET for the URI associated with that user's presence. The returned XML from the communications integration system denotes the current state and can be rendered in the browser based application accordingly. Using long-polling the application can choose to keep the request open for subsequent presence updates, allowing asynchronous presence events coming from the server to be received, interpreted and rendered in the browser based application. Based on this presence information, using a similarly defined telephony interface the user may use the browser based application to initiate a

telephony based communication with the colleague if his or her presence is set to an available state. It should be noted that other services in the system may manipulate the presence state for a user. Examples of such services include busy or available calendar operations and telephony state. It is a combination of such user and system driven events that make asynchronous event notification to the browser an important factor in browser based presence clients.

VI. EVALUATION

The loosely coupled nature of REST makes it suitable for creating interfaces that abstract the underlying communication system. Combined with the uniform interface of HTTP as an almost universally adopted message transport makes REST a suitable, lightweight technology for browser based thin client unified communications applications.

From a deployment and administrative perspective the fact that the well known port for HTTP is generally open on enterprise firewalls makes it an acceptable interface technology. Furthermore a REST based architecture offers potential for performance and scalability benefits over existing architectures. The deeply linked nature of REST allows client software to request only the resource that is required while having the flexibility to link to further resources in the systems. This can result in increased network traffic but again, due to the near universal adoption of HTTP most networks are tuned for this type of traffic.

For synchronous operations such as setting a presence state or placing a telephone call, creating an interface abstraction using REST is relatively straightforward:

- Resources are identified.
- Resources are named with URI's.
- Server and client side representations are designed.

However in real time enterprise communication systems asynchronous events are a core feature. A simple example of an asynchronous event is an inbound telephone call or a user's presence being changed based on some event. As a REST based system typically relies on HTTP as the underlying transport this presents a challenge for a REST based communications integration architecture. An asynchronous event amounts to a response without a request. The Bayeux protocol offers a mechanism to support asynchronous events from the web server on a communications integration system to a browser based client using a long-polling event mechanism.

VII. CONCLUSION

As an architectural style REST offers many benefits for communication integration systems but also presents

several challenges, the most significant of which appears to be returning asynchronous event notifications to browser based applications. This is one of many limitations associated with HTTP as the protocol most commonly used in REST based architectures [9]. The combination of REST using HTTP for its uniform interface with the Bayeux protocol for asynchronous events appears to be a suitable architecture for browser based communication clients as defined in this paper.

VIII. FUTURE WORK

Future work includes an investigation into the performance of the Bayeux long polling mechanism in the context of unified communications systems. This will be based on the Dojo Foundation's Cometd implementation of the Bayeux Protocol [10].

ACKNOWLEDGMENTS

The first author has worked with several people on a variety of REST based projects and would like to acknowledge them, in particular Rick Dunlap for an introduction to REST as an architectural style and an ongoing education on the topic.

REFERENCES

- [1] Albert M. Lai, Jason Nieh, Bhagyashree Bohra, Vijayarka Nandikonda, Abhishek P. Surana, Suchita Varshneya (2004). "Improving web browsing performance on wireless pdas using thin-client computing". Proceedings of the 13th international conference on World Wide Web, ACM.
- [2] Cisco Systems (2008). Unified Communications Technology Overview. http://www.cisco.com/en/US/products/sw/voicesw/products_category_technologies_overview.html
- [3] Dr. Roy Fielding (2000). Published doctoral dissertation, Architectural Styles and the Design of Network-based Software Architectures, University of California. <http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm>
- [4] Berners-Lee, T., Fielding, R. and H. Frystyk, "Hypertext Transfer Protocol -- HTTP/1.0", RFC 1945, May 1996.
- [5] Fielding, Gettys, Mogul, Frystyk, Masinter, Leach, Berners-Lee (1999). HTTP – Hypertext Transport Protocol, W3C RFC2616. <ftp://ftp.isi.edu/in-notes/rfc2616.txt>
- [6] Alex Russell, Greg Wilkins, David Davis, Mark Nesbitt, "Bayeux Protocol Draft 1.0", The Dojo foundation 2007. <http://svn.cometd.com/trunk/bayeux/bayeux.html>
- [7] Sun Microsystems (2008). Java Telephony API (JTAPI), <http://java.sun.com/products/jtapi/>
- [8] Beltran V, Paradells J (2008). Middleware-based solution to offer mobile presence service, Proceedings of the 1st international conference on MOBILE Wireless MiddleWARE, Operating Systems, and Applications. ACM International Conference Proceeding Series; Vol. 278
- [9] Roy T Fielding, Richard N. Naylor, Principled design of the modern Web architecture (2002), ACM Transactions on Internet Technology (TOIT)
- [10] Dojo Foundation (2008), <http://cometdproject.dojotoolkit.org/>

Security Aspects of Internet based Voting

Md. Abdul Based

Department of Telematics, NTNU, Norway

based@item.ntnu.no

Abstract-An Internet voting is an electronic voting system that uses electronic ballots to allow voters to transmit their vote to election officials over the Internet. Electronic voting has become a significant research topic in the new century. Many countries use electronic voting devices, but there are still many flaws due to attacks present in the network system or the devices themselves. The aim of a secure voting system over Internet is to provide security attributes to the voting process like authentication and identification of voter, ballot encryption and signing, encrypted ballot transmission over Internet, privacy of the voter, anonymous ballot decryption, and counting of ballots, all in a secure way. A central server model for Internet voting is presented in this paper. With the concept of Public Key Cryptography (PKC), this model satisfies identification and authentication of the voter, confidentiality of the vote, integrity and anonymity of the ballot/vote. The objective of this paper is to present these privacy and security issues for the voter and the vote itself.

I. INTRODUCTION

Trusted election process and outcome are fundamental to democratic societies. Government leaders must be elected in a proper way so that people can trust them. Computer Scientists have found that paper-based voting devices have some serious flaws which leave space for corruption and irregularities in the election process. This problem accelerates the attention of many people [1-3] and has pushed them to improve the voting opportunities and election process. One possible way of solution could be multiparty network-based voting, aiming to give better chances to reduce election problems and irregularities especially in the countries where voting is a prominent issue.

In this paper, background of Internet voting is briefly described in section II. Section III describes a central server model for Internet voting, whereas section IV shows the security aspects of this model. Section V presents some of the related works, and the paper concludes with section VI, where the summary and future plans are discussed.

II. BACKGROUND

There is not much software available that can be purchased or downloaded for use to run the voting system electronically, though, some systems are developed and used [4, 5] for Non Government Organizations (NGO). There are many countries that have already introduced partially electronic voting in their areas. For example, the United Kingdom in 2002 and 2003 [6], the Dutch government in 2004 [7], the French government offered the possibility for French citizens living in USA to vote online. The first country that introduced Internet voting is Estonia for elections in March 2007 [8, 9]. The Norwegian Ministry of Local Government and Regional Development issued a comprehensive report on the challenges and opportunities of electronic voting [10].

III. A CENTRAL SERVER MODEL FOR INTERNET VOTING

Some models of electronic voting [11-14] have already been proposed. A central server model for Internet voting is shown in Fig. 1. This model assumes that the list of voter is prepared, the list of candidate is prepared, and the government has issued smartcards which contain fingerprint of voter. The smartcard also contains the private key of the voter, and the public key of the server. The server has the public key of all voters and its own private key. This model also assumes that key management is performed with proper monitoring of independent third party like United Nations Organization (UNO). That is, government generates private and public key of the server. The public part of the key (public key of the server) should be saved in voters' smartcard. It is important to mention here about the Certificate Authority (CA). The CA is a third party organization that guarantees that the public key which is saved in the voters' smartcard belongs to the government. The trusted third party can be the UNO that can guarantee for that. The certificates are very important in Internet voting because when the voter encrypts the ballot the voter should be ensured that the ballot is encrypted with the original public key of the server. If we encrypt the ballot with the wrong public key, when the ballot will be accepted at the server side the decryption of that ballot will not make any sense.

The first step of this model for Internet voting is the voter identification and authentication. To make it sure that no unauthorized voter will be allowed to vote, the voter identifies himself/herself by using smartcard enabled with fingerprint, and smartcard authentication with server is done by using digital signature.

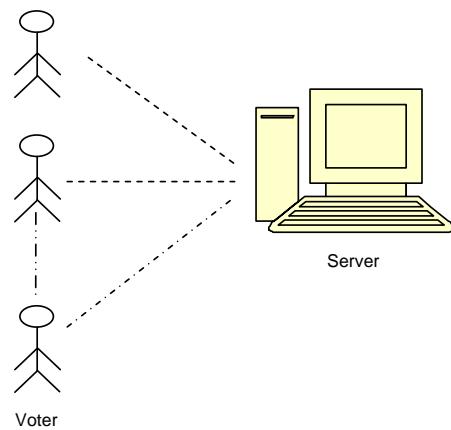


Fig. 1: A central server model for Internet voting.

Then ballot encryption is performed in 128 byte encoding, because 128 byte encoding has shown that is still unbreakable. After the ballot is encrypted at the client side (with the public key of the server) the vote is sent to the server using the Internet. The longer the key space (the range of possible values of the key) the more difficult it is to break the key in a brute-force attack. In a brute-force attack, the attackers apply all combinations of a key to the algorithm until they succeed in deciphering the message. Using the mathematical formula for finding the number of combinations required to release the key, for 128 bit encryption key, $2^{128} = 3.402823669209 * 10^{38}$ calculations are necessary. This number is very large and requires a lot of computation and many years calculation. Even the attacker in the future will be capable to find the key, this will not be important because the voting process would have been finished by that time.

IV. SECURITY ASPECTS OF INTERNET VOTING

This section describes the security aspects of the central server model for Internet voting (presented in the previous section) that satisfies authentication of voter, confidentiality and integrity of the vote with Public Key Cryptography (PKC), and anonymity by server separation. The biometric smartcards security is one of the most highly accepted technologies which require the least user effort and knowledge. Unlike Personal Identification Number (PIN) identification which in information security world is understood as “something that you know”, the introduction of fingerprint scanner brought a new security layer called “something that you are”. The combination of smartcard and biometric technologies not only offer increased security and user convenience but also offers a high degree of user control over personal data. Today many applications use smartcards including phone cards, health insurance cards, pay TV, banking and payment applications, and GSM (Global System for Mobile) communications. Fig. 2 shows the voter authentication by using smartcard enabled with fingerprint (biometric identification), and Fig. 3 shows smartcard authentication with server by using digital signature. After the

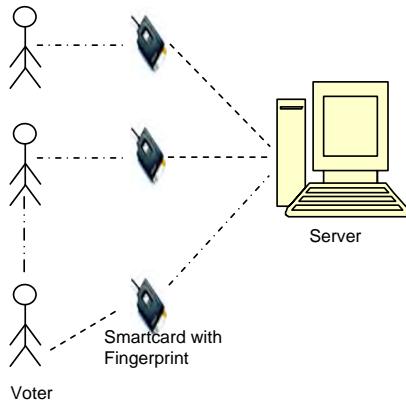


Fig. 2: Voter identification by using smartcard enabled with fingerprint (biometric identification).

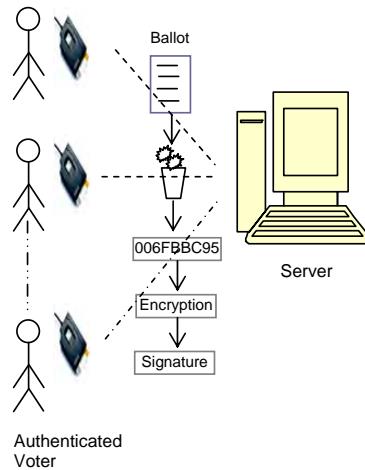


Fig. 3: Smartcard authentication with server by using digital signature (ballot signing).

voter enters the smartcard into the smartcard reader, the voter has to put the finger in the fingerprint-scan sensor. As it is shown in Fig. 4, fingerprint-scan sensor can be contained in the smartcard reader or in mouse. The smartcard reader matches the scanned fingerprint with the stored templates in the smartcard, if they are the same the voting web page is opened, if not the voter has no access to the web page for voting. Then the voter signs the ballot using his/her own private key and encrypts the ballot using the public key of the server.

This model of Internet voting provides confidentiality with the concept of PKC. Since only the server has its own private key, when the voter will encrypt the ballot using the public key of the server stored in the smartcard of the voter, no one can decrypt this encrypted ballot. This scenario is depicted in Fig. 5. With the concept of PKC, this model also achieves integrity of ballot through message authentication [shown in Fig. 6] by means of digital signature (since the voter will sign the ballot using the private key of the voter and encrypt the ballot using the public key of the server). It is mentioned earlier that this key pair (private key of the voter and public key of the server) will be stored in the smartcard of the voter.



Fig. 4: Biometric smartcards (with fingerprint reader).

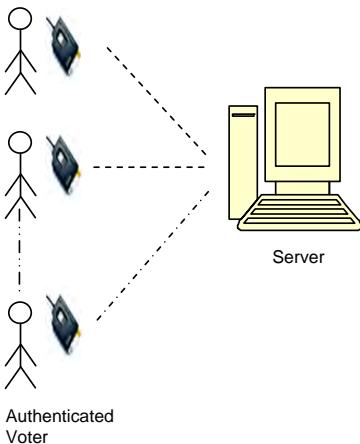


Fig. 5: Confidentiality with PKC since only server has the private key; no one can decrypt the encrypted ballot.

Anonymity is very important in the voting system. By anonymity we mean that no one in the voting process will be able to know for whom the voter has voted. If we use two servers and separate them by a firewall in such a way that there will be no communication between the voter and the second server (server2 in Fig. 7), we achieve anonymity property from this model. The concept is, the voter will sign and encrypt the ballot, and will send it to server1. Server1 will verify the signature and will forward the encrypted ballot to server2. An important point to mention here is that, server1 is not decrypting the ballot, it is just verifying the signature of the voter, since it has public key of the voter. Thus, by separating server this model provides anonymity of ballot.

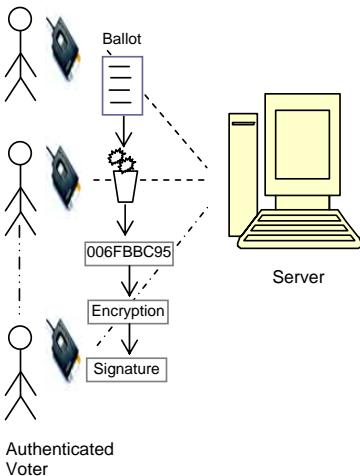


Fig. 6: Integrity of ballot comes through message authentication which is achieved by means of digital signature.

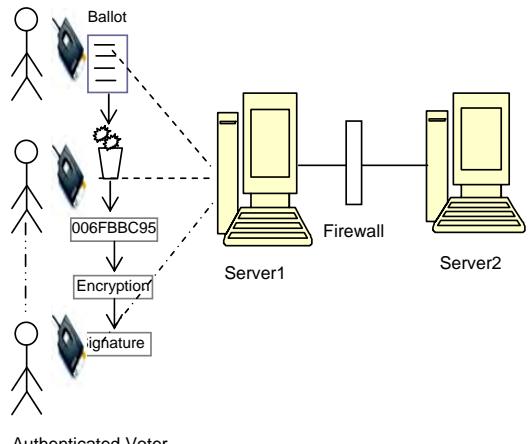


Fig. 7: Anonymity can be achieved by server separation.

V. RELATED WORK

There is a flourishing literature on electronic voting recently last five years. A few of the published papers are mentioned here. David Chaum, Jeron van de Graaf, Peter Y. A. Ryan, Poorvi L. Vora, presented a voting system [15] which allows voters to be sure that whatever they see in the booth will be included correctly in the outcome. They presented a rigorous and understandable model of requirements for election systems, state formally the properties of the system, and prove them. Jens-Matthias Bohli, Jorn Muller-Quade, and Stefan Rohrich, presented a new verifiable and coercion-free voting scheme Bingo Voting [16], based on a trusted number generator to prevent electoral fraud and avoid coercion and vote buying. Jeroen van de Graaf presented a variation [17] of the Pret-a-Voter voting protocol that keeps the same ballot layout but borrows and slightly modifies the underlying cryptographic primitives from Punchscan, which is based on bit commitments. They use unconditionally hiding bit commitments to obtain unconditional privacy.

In addition, some research work has been carried out on homomorphic elections [11], mixnet-based voting scheme providing receipt-freeness [12], and electronic voting to support decision-making in local government [18].

VI. CONCLUSION AND FUTURE WORK

Internet voting is a challenging area in terms of security features. With the implementation of the Internet voting system that is discussed in this paper many countries will overcome the problems exist in traditional paper-based election systems and will have successful voting system. The security and faith of people will be increased. All people will be able to vote no matter how old they are since they won't have to walk and go far from their home, that is, people will be able to vote anywhere at home or office. This system will allow voters to cast their vote quickly and will allow citizens with disabilities to cast their ballots. In addition, the system will provide flexibility and mobility.

Security of Internet voting is a very wide area. There may have some other security aspects of Internet voting (verifiability, soundness, fairness, unreuseability), that were left due to shortage of time. The model does not address the availability issue. The model authenticates the voter only, but there is no server authentication. The mechanisms proposed in the model (smartcard with biometric identification) are time-consuming and expensive. The voting system could be inconvenient to the general voters who have no/less technical background.

In this paper, the analysis is based on theoretical descriptions. Better analysis, simulations, and experiments should be done in the future. Many open issues and research work can be done to validate this voting system. After implementation of this system, performance verification will be another necessary work. So, with many facilities and some of the limitations, the proposed Internet voting system will increase the public participation in the election process through encouraging citizens to exercise their right to vote on common matters and public concerns.

ACKNOWLEDGMENT

I would like to thank Professor Stig Frode Mjølsnes and Anton Stolbunov, Department of Telematics, Norwegian University of Science and Technology (NTNU), Norway for their support and fruitful discussions. I am also thankful to Luan Ibraimi, Information and Communication System Security, Department of Computer and System Sciences, Royal Institute of Technology (KTH), Stockholm, Sweden.

REFERENCES

- [1] T. Tjøstheim, T. Peacock, and P.Y. A. Ryan, ‘‘A case study in system-based analysis: The Threeballot voting system and Pret a voter’’, VoComp, 2007.
- [2] T. Tjøstheim, T. Peacock, and P.Y. A. Ryan, ‘‘A model for system-based analysis of voting systems’’, Fifteenth International Workshop on Security Protocols, 2007.
- [3] T. Tjøstheim and G. Røslund, ‘‘Remote electronic voting using verifiable chain encryption’’, Frontiers in Electronic Elections, 2006.
- [4] Web: <http://www.gnu.org/software/free/#TOCintroduction>, January 20, 2007.
- [5] Web: <http://www.adderpit.com/~sjaveed/coding/votebot.html>, January 20, 2007.
- [6] Web: <http://www.electoralcommission.org.uk/elections/pilotsmay2006.cfm>, February 05, 2007.
- [7] Web: <http://www.sos.cs.ru.nl/research/society/voting/>, February 05, 2007.
- [8] Web: <http://www.foruminternet.org/telechargement/documents/reco-evote-en-20030926.pdf>, February 10, 2007.
- [9] European University Institute, Robert Schuman center for Advanced Studies, Report for the Council of Europe: ‘‘Internet Voting in the March 2007 Parliamentary Elections in Estonia’’, July 31, 2007.
- [10] Norwegian Ministry of Local Government and regional Development, ‘‘Report: Electronic voting- challenges and opportunities’’, February, 2006.
- [11] Alessandro Acquisti, ‘‘Receipt-free homomorphic elections and write-in ballots’’, Cryptology ePrint Archive, Report 2004/105, <http://eprint.iacr.org/>.
- [12] Riza Aditya, Byoungcheon Lee, Colin Boyd, and Ed Dawson, ‘‘An efficient mixnet-based voting scheme providing receipt-freeness’’, In Sokratis K. Katsikas, Javier Lopez, and Gunther Pernul, editors, TrustBus, volume 3184 of Lecture Notes in Computer Science, pages 152-161. Springer, 2004.
- [13] Tatsuaki Okamoto, ‘‘Receipt-free electronic voting schemes for large scale elections’’. In Bruce Christianson, Bruno Crispo, T. Mark A. Lomas, and Michael Roe, editors, Security Protocols Workshop, volume 1361 of Lecture Notes in Computer Science, pages 25-35. Springer 1997.
- [14] Berry Schoenmakers, ‘‘A simple publicly verifiable secret sharing scheme and its application to electronic voting’’. In Michael J. Wiener, editor, CRYPTO, volume 1666 of Lecture Notes in Computer Science, pages 148-164. Springer, 1999.
- [15] David Chaum, Jeron van de Graaf, Peter Y. A. Ryan, Poorvi L. Vora, ‘‘High Integrity Elections’’. Cryptology ePrint Archive, Report 2007/270, <http://eprint.iacr.org/>.
- [16] Jens-Matthias Bohli, Jörn Müller-Quade, and Stefan Rohrich, ‘‘Bingo Voting: Secure and coercion-free voting using a trusted random number generator’’. Cryptology ePrint Archive, Report 2007/162, <http://eprint.iacr.org/>.
- [17] Jeroen van de Graaf, Universidade Federal de Minas Gerais, ‘‘Merging Pret-a-Voter and PunchScan’’. Cryptology ePrint Archive, Report 2007/269, <http://eprint.iacr.org/>.
- [18] C. Bouras, N. Katris, V. Triantafillou, ‘‘An electronic voting service to support decision-making in local government’’, Telematics and Informatics 20 (2003) 255-274, February 12, 2003.

Middleware-based distributed heterogeneous simulation

Cecil Bruce-Boye¹, Dmitry A. Kazakov², Helge Colmorgen³, Rüdiger zum Beck⁴, Jehan Z. Hassan⁵
and Harald Wojtkowiak⁶

Abstract— In this paper we discuss an implementation of distributed heterogeneous simulation applications. The LabMap middleware is used as a vehicle for distribution and synchronization between simulating components. We present a simulation setup using two popular simulation tools: MATLAB/Simulink and LabVIEW. We show the feasibility and advantages of deployment of a middleware as an abstraction layer for simulation applications, in particular a smooth transition from simulation to hardware-in-the-loop setups and back.

Index Terms— Middleware, Software bus, LabMap, Simulation, MatLab/SIMULINK, LabVIEW

I. INTRODUCTION

Modern simulation applications are very complex and tend to consume a lot of resources. A lot of these applications are mutually incompatible with each other. The complexity of the simulation software requires reusing the existing simulation models without the need to translate them into another simulation language additionally even without gluing them into one model under the same tool.

Another problem of simulation applications is a transition to the real-time test environment, especially when some parts of the simulation are to be replaced by the real hardware. Due to different platforms, several time bases have to be synchronized.

A distributed middleware appears an ideal tool, on one hand, to distribute parts of simulation across multiple computing entities and on the other to abstract the differences between the simulation components and the hardware, when it comes to hardware-in-the-loop systems.

With the unified middleware layer the simulation components can be designed in the most appropriate modeling language as well as in a universal purpose programming language.

In our earlier works [1, 2, 4] we showed how a middleware can be used for distribution of hardware-in-the-loop applications. Two novel characteristics distinguish this setup from our last ones. The first one is that the simulation runs heterogeneously; we are using two different simulation tools on different computers. The second is that the parts of a distributed application run in real time and thus necessarily stay synchronized to each other as long as they satisfy the real-time constraint. The middleware takes care of clock synchronization and data distribution.

A distributed simulation application is not synchronized this way, because the clocks used in its parts are independent, showing simulated time. There is no common reference clock. This problem of synchronization is the central issue for a distributed simulation we address in this paper.

II. SYNCHRONIZATION MECHANISMS OF THE MIDDLEWARE

The middleware LabMap provides a variety of synchronization mechanisms considered for a distributed application. All these mechanisms are bound to the states of a variable, which is the atomic object the middleware deals with. So LabMap can be considered as a message oriented middleware described in [10, 11].

A. Waiting for I/O completion

The application may enter time-limited waiting for completion of I/O involving a variable. This type of synchronization can be used with any hardware. For a distributed application the major interest naturally represents a networking hardware. A part of the application running on one host may request or send a variable to another part on another host and then block until the I/O completes. This is a one way synchronization which can be used only on the remote side. The counterpart should use another synchronization mechanism.

B. Waiting for value change

The application may enter time-limited waiting while the value of a variable is being changed. This method is very often used for monitoring system state variables. This type of synchronization between distributed parts of the application can only be used when the shared variable guarantees to change its value. A toggling bit can be used to ensure that. The synchronization is two way, if both sides write the variable. Yet it might be difficult to deploy this mechanism in a simulation language.

¹ Cecil Bruce-Boye, University of Applied Sciences Lübeck, 3 Stephensonstrasse Luebeck, 23562 Germany

² Dmitry A. Kazakov, cbb software GmbH, 1 Charlottenstrasse Luebeck, 23560 Germany

³ Helge Colmorgen, cbb Software GmbH, Rebenring 33, 38106 Braunschweig

⁴ Rüdiger zum Beck, cbb software GmbH, 1 Charlottenstrasse Luebeck, 23560 Germany

⁵ Jehan Z. Hassan, cbb Software GmbH, Rebenring 33, 38106 Braunschweig

⁶ Harald Wojtkowiak, cbb Software GmbH, Rebenring 33, 38106 Braunschweig

C. Blackboard

The application may trace all changes of a variable. For instance an application would like to trace a signal waveform for visualizing. A usual approach for catching value changes involves some kind of notification mechanism between the source of the value and the application. Such point-to-point bias is hard to implement without overstraining the system resources and a danger of running out of resources when an application ends abnormally. The software bus uses an alternative approach. All value changes are written onto the blackboard and remain there for a certain time. Any application may inspect the blackboard contents in order to trace the changes of desired variables.

D. Computable registers

Computable registers are represented in the middleware LabMap as a virtual hardware. The computable registers interface makes calculation of registers from other register values possible. It appears useful for distributed simulation applications, especially for synchronization purpose, because the language of computed registers has its own operations to evaluate the data consistency. These can be used for triggering synchronized parts of the distributed simulation. The operator \sim over two arguments yields 1 when both operands reach a non-zero value. It functions as follows: If both arguments are zero, the result is also zero. If one of the arguments becomes non-zero, the operation remembers that fact, but the result remains zero. The operator triggers only when the two arguments are both zero. Its result becomes 1, and a new cycle begins. Together with the register update operator $\%$, this operation can be used to eliminate race condition. The expression

$$\%2810 \sim \%2820 \sim \%2830$$

yields 1 only when all three variables are updated. The updates may happen asynchronously, i.e. first 2810, then 2830 and 2820 at last. This can be used as a trigger condition for a simulation part.

III. INTERFACING SIMULATION SOFTWARE

In order to keep the simulation consistent, the simulation time of all units must run synchronous. In this work we assume that the simulation time is discrete and incremented by a constant time interval. We do not consider the cases when distributed simulations change the time constants, for example in some adaptive process, or when they have different time constants. Although this issue can be mastered by the means of computable middleware registers described above. Therefore on the fly spline interpolation operations integrated in the middleware can be considered in such cases.

The synchronization of the simulation time is achieved by blocking the simulation until a triggering event occurs. This means that the variables needed for the next simulation step are updated.

Usually simulations are mutually dependent, because the controlling loops stretch across the network, so that the same

simulation is a producer and a consumer of data. Therefore a straightforward blocking until inputs change would create a deadlock. The solution in the event of change can also be triggered externally.

The triggering event in LabMap is implemented as a variable which can be changed. The simulation software interface has two triggering events: one at the beginning of the simulation step and another at its end. The step is blocked until the first event. At the end of the step, when all relevant outputs are written, the second event is triggered. The LabMap variables corresponding to the events are connected over the network.

Because LabMap has the architecture of a bus, the same step-end triggering signal can be distributed to many subscribers, i.e. routed to many step-start events. Triggering is implemented as toggling the corresponding LabMap variable between 0 and 1.

IV. THE SYSTEM SETUP

For illustration purposes we created a distributed simulation of a control system described in [3]. A state-feedback-controller with a Luenberger observer [5, 9] is used to control speed of a DC Motor. The input to the motor model is voltage in volts and output is speed in revolution/minute. The controller and observer gains are calculated with the help of Ackermann's formula. The pre-filter is also calculated to eliminate steady-state-error. Since we used a different DC Motor from the one

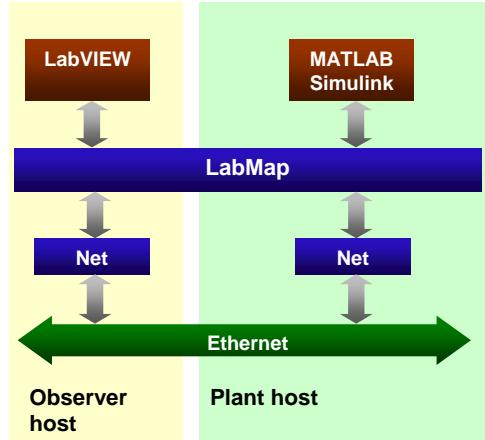


FIG.1 Distributed heterogeneous simulation

used in [3], new controller and observer gains as well as motor model parameters were calculated.

The closed loop control system model is divided into two sub-models. One model is comprised of subsystems in the forward path of closed loop system i.e. pre-filter, plant (motor model), gains etc. This model is implemented in MATLAB/Simulink [6]. The other model simulates the subsystems in feedback path of closed loop system i.e. observer and state-feedback controller. This model is implemented in LabVIEW [7]. These models run on two separate network hosts. The communication between two

models is carried out with the help of LabMap and its interfaces to MATLAB/Simulink and LabVIEW.

In the second step, the motor model in MATLAB/Simulink is replaced by a real DC Motor. The Simulink model is modified by removing the model and connecting the corresponding inputs and outputs to the motor over LabMap. In this case both models run in real time controlling the motor. We perform this second step in order to verify our simulation results.

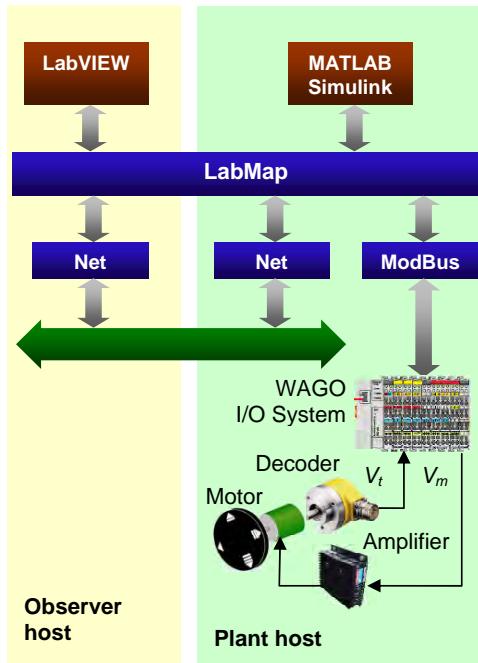


FIG.2 Real-time verification

V. INTERFACING MATLAB/SIMULINK

The MATLAB/Simulink interface is established through a library of MATLAB s-functions, which encapsulates the standard LabMap programming interface, written with the c programming language. Fig. 3 shows an example of such a s-function for the LabMap interface. The "direction" indicates whether MATLAB should send or retrieve data from LabMap. For synchronization purposes "External Trigger" and "Completion Trigger" can be activated. It uses the value change synchronization mechanism (Chapter II). Therefore two handles "External Trigger Name" and "Completion Trigger Name" should be named. The external trigger is an input and its value will be set by 3rd party software (for instance LabVIEW). A changing value of this trigger indicates that MATLAB can now start its own calculations. After it has finished and the values were updated in LabMap, the completion trigger will change its value, and shows so, that MATLAB has finished its calculations for this step.

In case of connection or transmission errors, several kinds of behavior are possible. In this case, the whole simulation will

be aborted, indicated by the value "abort" for the parameter "By Timeout". Alternatively a warning can be given. The timings for the error conditions can be set by the parameters "External Trigger Timeout" and "Completion Trigger Timeout". The complete parameter configuration can be assigned to one or more LabMap handles listened in the "HandleArray".

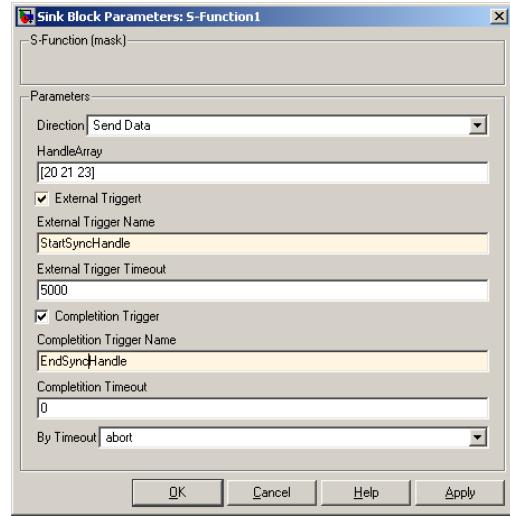


FIG.3 Parameters of the MatLab/SIMULINK interface

VI. INTERFACING LABVIEW

The interface to LabVIEW is comparable to the one for MATLAB/Simulink. It also provides customized blocks for accessing process variables from the LabMap middleware in a synchronized manner.

VII. SIMULATION

For the test system we chose a Luenberger state observer controller with following parameters, calculated by this MATLAB script:

```
%calculation of state space controller and
%luenberger observer
%the system identification was carried out
%by the system identification
%software tool box IDCON
num = [1. 9618e-004] %result f from system
identification
den = [1 37. 7028 69. 9862] %frequency domain
Ac=[0 1; -den(3) -den(2)]; %state spaces description
bc=[0; num];
Cc=[1 0]; %measurement factor
cm=km*Cc;
p=[-10 -20];
gc=(acker(Ac', Cc', p))'; %pole placement observer
%state observer
prc = [-2 -2. 5]; %pole placement
controller
rc=acker(Ac, bc, prc); %state controller
vc=inv(cm*inv(bc*rc-Ac)*bc); %state space description of motor model;
```

state space description of motor model:

$Ac = [0 \ 1.0000 \ -69.9862 \ -37.7028]$
 $bc = [0; 19618]$
 $Cc = [1 \ 0];$

prefilter and measurement factor:
 $vc = 0.0714$
 $km = 0.0036$

state observer and controller gains:
 $gc = [-7.7028; 420.4309]$
 $rc = [-0.0033; -0.0017]$

gc and rc are calculated by the Ackermann formula. Motor model parameters were identified with the software toolbox IDICON.

Fig. 4 represents an observer implemented in LabVIEW. The observer simulation runs on a separate computer. It communicates with the controlled system running on another host. The observer model has two synchronization blocks, which provide triggering signals from and to plant host (simulated in MATLAB/Simulink) via LabMap. Triggering the signal indicates that data is available. LabVIEW model then completes an iteration of the control loop. After the calculations have been completed the send block notifies MATLAB/Simulink and sends the data over the middleware.

The controlled system simulation is implemented in MATLAB/Simulink as shown in fig. 5. The simulation includes the motor model.

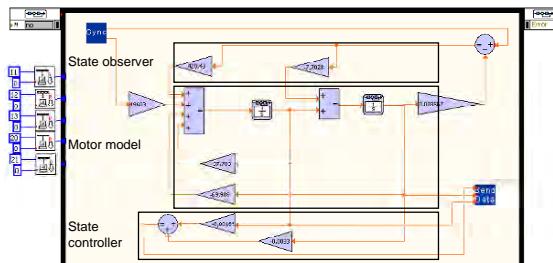


FIG.4 Simulated observer and state-feedback-controller. LabVIEW

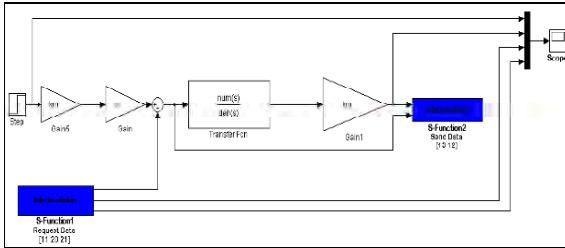


FIG.5 Simulated controlled system. MatLab/SIMULINK

In fig. 6 the following signals of the step response are plotted; set value and output value of the system, system state variables – motor velocity (state value 1) and motor acceleration (state value 2). The values of state variables are calculated by observer running on LabVIEW. It can be

observed from fig. 6 that the motor velocity calculated by observer and actual motor velocity has the same response.

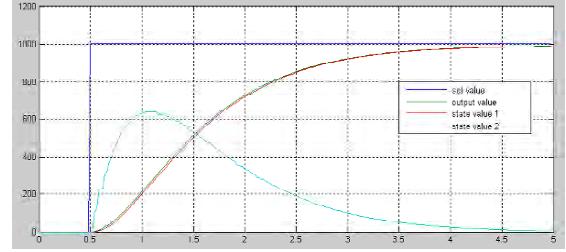


FIG.6 Simulated system response

In simulation mode the quality of data distribution services of the middleware play no significant role, because there is no real-time constraint. For the cases when the controller is to be transferred onto a target platform distributed via the middleware, the quality of service should satisfy certain constraints. In the given case using LabMap as a middleware does not deteriorate the stability of the implemented controller. The quality of data distribution services of LabMap was explored in [2]. It was shown that the latency lies between 250µs without a stress load and 1ms with such load. Because the fixed simulation time step is set to 10ms, the latency and jitter inflicted by the middleware data distribution layer should have no effect on the stability of the controller in real time.

VIII. HARDWARE-IN-THE-LOOP

In order to verify the simulation we replaced the motor model simulation block with a real motor. The observer part shown in fig 4 does not require any modification, if the system would run in real time. Necessary synchronization to real time is performed by the LabMap middleware.

In the controlled system we replaced the block simulating the motor with the blocks of LabMap communicating with the real motor over the WAGO I/O modules [8]. The modified controlled system is shown in fig 7.

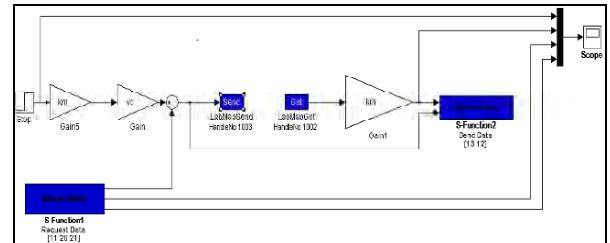


FIG.7 Controlled system modified for real motor. MatLab/SIMULINK

The system step response is shown in fig 8. It can be observed that the simulated system and system with real DC Motor produce identical transient responses.

These results verify the reliability of real-time synchronization mechanism presented in this work using LabMap.

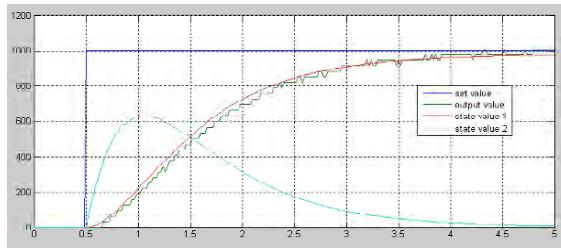


FIG.8 Response with a real DC motor

IX. CONCLUSION

The synchronization mechanisms provided by the middleware LabMap are suitable for distributed heterogeneous simulations. The middleware interface to wide spread modeling tools supports a generic synchronization of the simulation time. The designer has a choice to use it with a concrete synchronization mechanism.

The simulation model can be smoothly transformed into a hardware-in-the-loop system.

The middleware abstraction layer allows construction of heterogeneous simulations using a variety of modeling tools. The models designed in different simulation languages or tools can be reused without the need to integrate them in a unified model in one simulation language or tool. Parts of the models can be designed in general purpose languages as well.

REFERENCES

- [1] C. Bruce-Boye and D. Kazakov, "Distributed data acquisition and control via software bus," Proceedings CSMITA'04, pp. 153–156, Sep 2004.
- [2] C. Bruce-Boye, D. Kazakov, Quality of Uni- and Multicast Services in a Middleware, LabMap Study Case," Conference CIS³E 06 (International Joint Conference on Computer, Information and System, Science and Engineering") 2006, IEEE, 4-14 December 2006
- [3] C. Bruce-Boye, D. Kazakov; Rüdiger zum Beck, "An approach to distributed remote control based on middleware technology, MATLAB/Simulink-LabMap/LabNet framework", Conference CIS³E (International Joint Conference on Computer, Information and System, Science and Engineering") 2005, IEEE, 10-20 December 2005.
- [4] C. Bruce-Boye, D. Kazakov, "Distributed data acquisition and control via software bus", International Industrial Ethernet Development High Level Forum 2004 (IEHF 2004) in Peking, Automation Panorama No. 5
- [5] D Luenberger, "An introduction to observers", IEEE Trans. Automatic Control, AC-16 1971
- [6] Ashish Tewari, "Modern Control Design with MATLAB and Simulink" John Wiley and Sons, Inc. 2002.
- [7] "LabVIEW Simulation Module User Manual", National Instruments, April 2004.
- [8] <http://www.wago.com>
- [9] C. Dorf, R. Bishop, „Modern Control Systems (9th Edition)", Science Press and Pearson Education North Asia Ltd. 2002, ISBN 7-03-010133-2
- [10] D. Bakken, "Middleware", Washington State University
- [11] G. Coulous, J. Dollimore, T. Kindberg, "Distributed systems. Concepts and design", Addison-Wesley, fourth edition 2005, ISBN-10: 0-321-26354-5.

Analysis of the flooding search algorithm with OPNET

Arkadiusz Biernacki

Abstract—In this work we consider the popular OPNET simulator as a tool for performance evaluation of algorithms operating in peer-to-peer (P2P) networks. We created simple framework and used it to analyse the flooding search algorithm which is a popular technique for searching files in an unstructured P2P network. We investigated the influence of the number of replicas and time to live (TTL) of search queries on the algorithm performance. Preparing the simulation we did not reported the problems which are commonly encountered in P2P dedicated simulators although the size of simulated network was limited.

Index Terms—Computer networks, Computer performance, Overlay networks, P2P networks

I. INTRODUCTION

A large number of peer-to-peer (P2P) systems based on overlay networks have been developed in recent years. Simultaneously with the evolution of P2P systems a number of P2P overlay simulators have been developed, among them are: P2PSim, PeerSim, NeuroGrid and PlanetSim. Most of these simulators were created by various research groups for use by the P2P academic community. In spite of the simulators diversity most of them lack some important features required from this kind of software [1]. Usually the documentation is poorly written or parts of the software functionality remain undocumented. Some of the simulators, such as PlanetSim, have no means to collect statistics and those that do provide often very limited sets of variables which are available for an end user. Sometimes user wishing to change the variables for which data can be captured, will have to modify the code as required. Lack of clarity in the properties of experiments makes reproducibility of results and analysis and comparison between algorithms problematic. The full survey of P2P simulators and their suitability for simulations may be found i.e. in [1][2].

In this paper we examine suitability of OPNET, which is well known commercial discrete event simulator, as a tool for performance evaluation of P2P overlay networks. The main contribution of the paper is creation of simple framework for a simulation of unstructured P2P networks in the OPNET environment. We show practical usage of the framework analyzing the flooding search algorithm used in this type of networks.

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

II. THEORETICAL BACKGROUND

A. P2P overlay networks

A Peer-to-Peer (P2P) file sharing system is built as an overlay on the existing Internet infrastructure. It provides a file sharing service to a highly transient population of users (peers). Early systems, such as Napster, used a central server to store indices of participating peers. This centralized design concerns of performance bottleneck and single point of failure. To avoid such possibility, instead of maintaining a huge index in a centralized system, a decentralized system distributes all searching and locating loads across all the participating peers. Though the decentralized approach concerns the overloading and reliability issues, and it is thought to build a scalable P2P system, its success is considerably dependent on an efficient mechanism to broadcast queries (messages, packets) across a large population of peers. Reaching out to a large scope of peers is a fundamental procedure in an unstructured P2P network.

In our work we consider purely unstructured network where each peer stores a local collection of objects. Nodes generate search queries and send them through the network. Peers and objects are assumed to have unique identifiers, with object IDs used to specify the query target. Search algorithms can not in any way dictate object placement and replication in the system. They are also not allowed to alter the topology of the P2P overlay. Nodes that are directly linked in the overlay are neighbours. A node is always aware of the existence and identity of its neighbours.

To improve the search and whole system performance, the object may be replicated on certain number of hosts.

B. Flooding algorithm

The popular technique for searching files in an unstructured network is the flooding algorithm. In the algorithm each node acts as both a transmitter and a receiver and each node tries to forward every search query to every one of its neighbours except the source node. Each search query has an unique number. A query received by a peer that has the same number as the one received previously will be discarded in order to avoid redundancy. Flooding is performed in a hop by hop fashion counted by time-to-live (TTL) counter for each query. A query starts off with its initial TTL set to specified value, which is decremented by one when it travels between two nodes. A query comes to its end either when it becomes a redundant

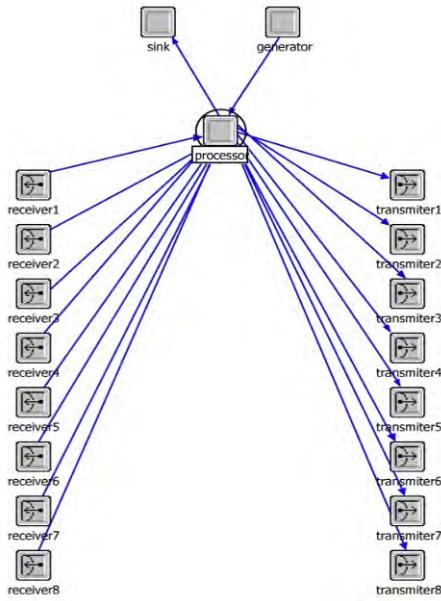


Fig. 1. Architecture of a single network node

query, when its TTL is decreased to 0 or when the data it is looking for is found. The flooding algorithm is not too efficient, because queries are generally broadcast indiscriminately in a whole neighbourhood using lot of network resources. As a result its search efficiency decays as the search time increases since the number of query messages increases with the size of visited peers. Consequently the algorithm faces the scalability problem when the query time increases. To mitigate those drawbacks there have been created numerous others flavours of the flooding algorithm, i.e. [3][4]. Despite the aforementioned drawbacks the algorithm advantage is that it demands very little management overhead, adapts well to the transient activity of P2P clients and takes advantage of the spontaneous replication of popular content. The flooding algorithm is used i.e. in popular Gnutella system [5]. General review of other search algorithm can be found among other in [6].

C. Performance metrics

To measure search performance we took metrics commonly used in the papers concerning this topic [7][8].

A search query is successful if it discovers at least one replica of the requested object. The ratio of successful to total searches made is called the *success rate*.

A single search can result in multiple discoveries (hits), which are replicas of the same object stored at distinct nodes. Number of discoveries per single search query is called the *hits per query*.

Average number of hops needed for successful search is called the *average hops number*. It is information about delay in finding an object as measured in number of hops. We did not model the actual network latency here, but rather just

measured the abstract number of hops that a successful search message travelled before it replied to the originator. A global TTL parameter represents the maximum hop-distance a query can reach before it gets discarded.

Overhead of an algorithm is measured in average number of packets which the P2P network has to process per single search query. All the packets generated during a single search are called the *forwarded packets*.

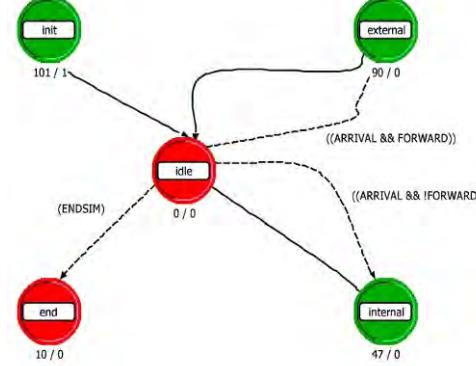


Fig. 2. State machine diagram of node's processor

III. EXPERIMENT

A. Assumptions

We created an overlay peer-to-peer network consisting of 1000 nodes, the links distribution was a random variable with the uniform distribution ranging between 2 and 8. In network nodes we placed 500 distinct objects. The above assumptions were simplified; in the real the topology of P2P network like Gnutella is a two-stage power-law graph [5]. The number of nodes used in the simulation is also smaller by at least an order of magnitude compared to the real network.

Each object was assigned a unique natural number. Replication of the objects was a parameter of the simulation and for our experiment we used a set consisting of five values: 2, 8, 32, 128 and 512. When replication parameter is set to n it means there are n instances of every object in the network. We used uniform strategy, replicating everything equally between nodes. Each node contained similar number of object which may be estimated by the following formula:

$$SObjCount = TObjCount \cdot RP / TNodeCount$$

where: $SObjCount$ is number of objects in a single node, $TObjCount$ is total number of objects, RP replication parameter and $TNodeCount$ is total number of nodes.

In order to get better simulation performance and to simplify simulation design we did not take into account protocols stack (TCP/IP). Simulation was based only on passing search queries between networks nodes which was sufficient in the case of the flooding algorithm. The search query (packet) has 4 fields: ID, source address, searched object ID and TTL. The first two fields were not explicitly used in the communication

(we did not send any acknowledgement packets concerning successful search queries), however they were used for statistical purposes.

In our experiment we tried to answer the following questions:

- What percent of search queries ended up with success in function of objects replication, TTL of search packets?
- How many packets were found in a single query?
- In the case of successful query what was its search time measured in search query hops?
- How many packets were generated by a single search query?

B. Simulation architecture

The architecture of a single network node is presented on figure 1. It consisted of a packet generator, a packets sink, transmitters and receivers through which connections were made with others nodes. Search queries were generated according to the Poisson distribution by ten of the nodes. Packets which their TTL reached 0 were forwarded to the *sink* module and destroyed. A node was connected with other nodes through bidirectional links associated to the pairs of transmitters and receivers modules. The main logic was included in the processor module based on a state machine diagram – figure 2. The *init* state in the diagram was responsible for initialization of statistic and other node parameters. Incoming packets were serviced by the *internal* or *external* states depending on whether they were newly generated or they were coming from other nodes.

IV. SIMULATION RESULTS

We gathered the experiment results on two levels – global and local. The global level concerned the averaged aggregated network statistic while on the local level we were able to examine single node behaviour. We collected four statistics from the metrics mentioned in section II C.

On the figure 3 we presented success rate per single query. As expected there is a direct relation between TTL and the success rate of a search query. The choice of proper TTL value is important in case of small number of replications, the larger the number of replicas the lower the value of TTL which is sufficient to find an object.

The hits per single query are presented on figure 4. The higher is the number of the replication the higher is the hits value except situation where the replication parameter is 512 and TTL is 8 or TTL is 6. This abnormality may be explained as the following: in the case of high number of replications the success rate is very close to one (figure 3) and the flood of packets is quickly attenuated. Search queries did not have enough time to replicate themselves because they quickly ended up as successful queries and were perished.

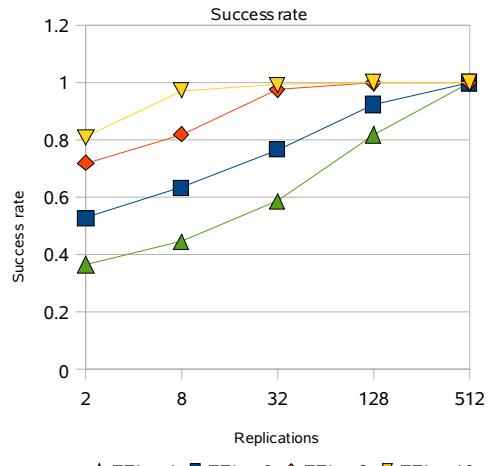


Fig. 3. Success rate per single query

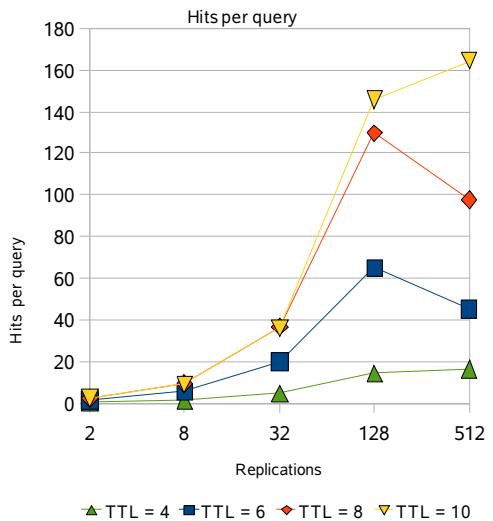


Fig. 4. Successful hits per single query

Average hops number is presented on figure 5. Except case were replications was 512 hops number are close to TTL. Such results indicate that most of the searched objects were placed relatively far from the node which invoked the search.

On the figure 6 we presented number of forwarded packets per query. The umber of forwarded packet is directly proportional to TTL and inversely proportional to the objects replications number.

The statistics related to the *success rate*, *hits per query*, *average hops number* and *forwarded packets* gathered at the global level were also gathered at the local level. Although it is possible to gather the local statistic for every node, such strategy would have slowed down the simulation speed, therefore we gathered them for only three selected nodes. The results

were presented on figure 7 and are with agreement with the global statistics.

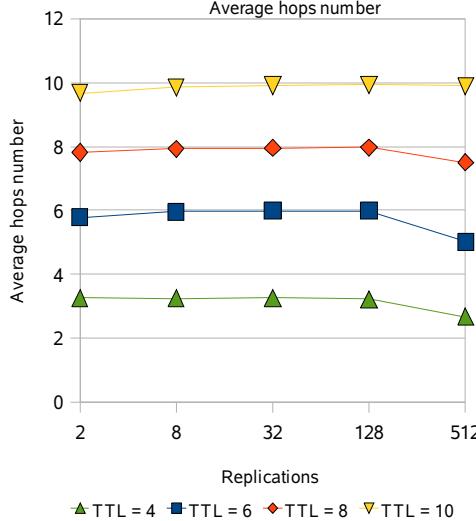


Fig. 5. Average hops number per successful query

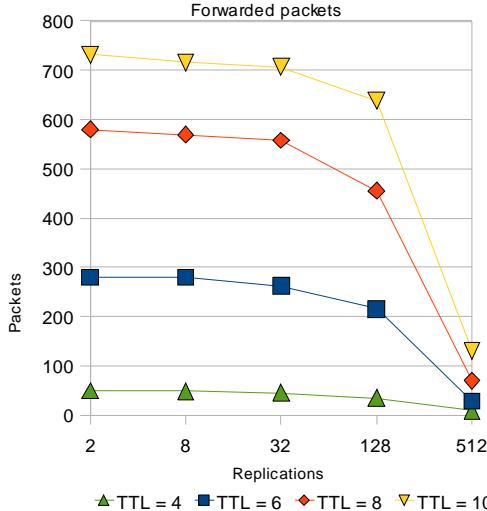


Fig. 6. Number of forwarded packets per single query

V. CONCLUSIONS

In this work we presented analysis of flooding search algorithm, popularly used in P2P networks, using the OPNET simulator. Performing the simulation we did not reported the problems which are commonly encountered in P2P dedicated simulators. The architecture of the simulation seemed to be clear, modularized and easily scalable. Although we reported some others issues, amongst them is restricted number of nodes in the network. Tries with simulation of network con-

sisting of more than 5000 nodes lasted much longer and sometimes OPNET stopped responding at all.

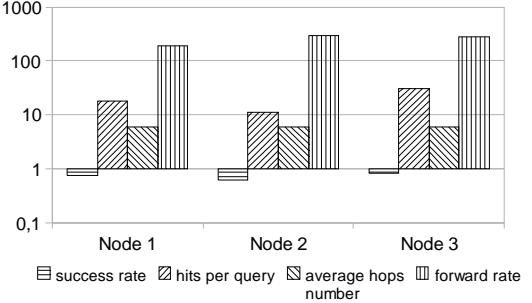


Fig. 7. Local statistic for single nodes

Despite these drawbacks we may state that the OPNET environment is suitable for a “first-look” performance evaluation of P2P algorithms. The environment may be helpful i.e. for a first assessment of the algorithm: if the results of quick analysis in the OPNET are promising than it may be simulated in a dedicated P2P simulator.

Further works will concentrate on the adoption of our framework to a simulation of more realistic models. We plan to import P2P network power-law graph topology and evaluate performance of the simulation which contains larger number of nodes. These steps should lead to analysis of more advanced search algorithms and proposals of new ones.

REFERENCES

- [1] S. Naicken et al., “A Survey of Peer-to-Peer Network Simulators,” *Proceedings of The Seventh Annual Postgraduate Symposium, Liverpool, UK, 2006.*
- [2] S. Naicken et al., “Towards yet another peer-to-peer simulator.” *Proc. Fourth International Working Conference Performance Modelling and Evaluation of Heterogeneous Networks (HET-NETS’ 06), September, 2006.*
- [3] S. Jiang, L. Guo, i X. Zhang, “LightFlood: An Efficient Flooding Scheme for File Search in Unstructured Peer-to-Peer Systems,” 2003, s. 627-635.
- [4] N. Bisnik i A. Abouzeid, “Modeling and Analysis of Random Walk Search Algorithms in P2P Networks,” IEEE Computer Society Washington, DC, USA, 2005, s. 95-103.
- [5] M. Ripeanu, I. Foster, i A. Iamnitchi, “Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design,” *Arxiv preprint cs.DC/0209028*, 2002.
- [6] J. Risson i T. Moors, “Survey of research towards robust peer-to-peer networks: Search methods,” *Computer Networks*, vol. 50, 2006, s. 3485-3521.
- [7] D. Tsoumakos i N. Roussopoulos, “A comparison of peer-to-peer search methods,” *Proceedings of the Sixth International Workshop on the Web and Databases*, 2003.
- [8] Q. Lv et al., “Search and replication in unstructured peer-to-peer networks,” *Proceedings of the 16th international conference on Supercomputing*, ACM New York, NY, USA, 2002, s. 84-95.

Efficient Self-Localization and Data Gathering Architecture for Wireless Sensor Networks

Milan Simek¹, Dan Komosny¹, Radim Burget¹, Ricardo Silva², Jorge Silva²

simek,komosny,burgetrm@feec.vutbr.cz
rnsilva@student.dei.uc.pt,sasilva@dei.uc.ptt

¹Department of Telecommunications, Brno University of Technology, Czech Republic
members of “Multicast and IPTV Research Group” <http://iptv-server.com>

²Department of Informatics Engineering, University of Coimbra, Portugal

Abstract—Plenty of proposed architectures for effective data gathering in WSN rely on the smart location awareness sensors and optimize just the data gathering processes. However, application of the several protocols to completely ensure the proper and effective function of the WSN load the entire energy-constrained sensor network. Hence, the designing of the complex protocol for the localization and the effective data gathering seems to be the suitable solution. Our complex architecture for WSN is partly based on the Tree Transmission Protocol that we have recently proposed for the effective fast data gathering in the IP networks with the great number of users.

I. INTRODUCTION

With the emerging application feasibilities of the wireless sensor networks (WSNs), several efficient algorithms and protocols proposed for the IP networks could be applied with some modifications into these energy and bandwidth restricted micro sensor networks. With the growing number of Internet users, the recent research in IP networks is devoted to the effective communications in the large-scale IP networks. Suitable example could be the issue of the IPTV applications with the huge numbers of receivers taking advantage of the RTP/RTCP protocol. In accordance with the RTP/RTCP specification[6], the receivers send in the periodic interval report messages to inform the IPTV server about the quality of the multimedia content receiving. In this report, the information about the delay, jitter or packet loss is transferred. It is obvious, that sending side needs to receive this information with the shortest delay to react at the unexpectedly complaints in the network. In accordance with the specification[6], the feedback report interval is linearly dependent on

the number of receivers. Therefore, with the growing number of receivers in the given session, the report interval reaches the unusable values. To settle this issue, several approaches optimizing time delay of the receiver's reports were proposed. The TTP protocol was recently proposed to outperform the mentioned issues and its performance is investigated further. In the WSNs, we battle with the similar issue. Since the WSNs are composed of the high number of narrow sensor nodes, the optimization of the energy-intensive data reporting process becomes the manner that need to be effectively solved. For the future, there is a considerable effort to merge the quite different networks such as the IP and WSN networks and that is why, the several protocols for IP networks could be successfully applied to the WSN environment. Hence, we consider applying the efficient TTP protocol for hierarchical data aggregation in IP networks to the WSN environment, where it can serve for the energy-efficient data gathering from the large-scale sensor networks. The rest of paper is organized in the following manner. Chapter II describes and evaluates the performance of the proposed TTP protocol. In the chapter III, we describe our energy-effective localization algorithm and data gathering model that uses the basic of the TTP model, whereas the chapter IV evaluates the radio energy model of WSN. The chapter V brings the conclusion and the future work.

II. TREE TRANSMISSION PROTOCOL – TTP

To outperform the issues mentioned above, we have developed a new protocol referred as TTP (Tree Transmission Protocol)[2][3] ensuring the creation and management of the effective hierarchical structure for large-scale IP sessions. TTP allows the transmission of great data volume in the short times through the relatively narrow links. It utilizes the centralized approach

togetherwith the summarization mechanism to gather a data from the large number of nodes. If the number of nodes exceeds the certain threshold, the summarization is performed in more aggregation levels. However, to completely apply our protocol, several new components need to be engaged to the given network. Basically, the end nodes (rcv) need to find out its geographic position (coordinates) to determinate to which summarization node send data. Application running at the end node uses the GNP (Global Network Positioning)[4]and Vivaldi[5]algorithm to estimate the correct geographic position of the given node. The position ranging is performed by means of the Landmarks (LM) whose position is well-known to all nodes. The RTT (Round Trip Time) counted by means of the ICMP messages was determinate as the basic metric for the position estimation. When the location process is done, all end nodes send own geographic coordinators to the FTM (Feedback Target Manager) that computes the optimal hierarchy of the summarization nodes FTs (Feedback Targets). The form and capacity of this hierarchy structure illustrated in Fig. 1. is based on the session conditions announced by the sender (S). The root of the whole structure situated in level 0 is the Root Feedback Target (RFT), common FT node that communicates directly with the S. This S could be represented by the IPTV server in case of the IPTV session. The S requirements include the demanded bandwidth for the given multicast session and the assumed number of clients interested in the session. We have used the formula (1) to compute the number of necessary levels $H_{FT}(n)$ for the specific number of end nodes. The results are denoted in Fig.2. Parameter n stands for the number of nodes. The S requirements include the demanded bandwidth for the given multicast session and the assumed number of clients interested in the session. Obviously, $H_{FT}(n) = 1$ for the number of receivers less N_5 parameter that stands for the number of receivers for which, the feedback interval does not exceed the 5 secs threshold defined according to RTP/RTCP standard.

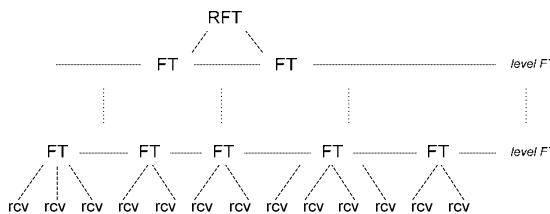


Fig.1 Hierarchy structure of TTP

In accordance with the formula (2), we are able to determinate the number of the FTs for the each level of

the HA tree. Here, the n parameter stands for the number of leaves in the next lower layer.

$$H_{FT}(n) = \begin{cases} 1 : n \leq N_5 \\ 1 + H_{FT}(n/N_5) : n > N_5 \end{cases} [-] \quad (1)$$

$$L_{FT}(n) = [n/N_5] [-] \quad (2)$$

From the formula (1) and (2), we calculate the total number of FTs for the whole session, see formula (3).

$$N_{FT}(n) = \begin{cases} 1 : n \leq 0 \\ L_{FT}(n) + N_{FT}(n/N_5) : n > 0 \end{cases} [-] \quad (3)$$

The results from the Matlab simulation were obtained for the following network conditions:

Session bandwidth	4 Mbps
Report interval	5 sec
Size of report message	480 b
Size of aggregated message	8000 b
Number of end nodes	10^6

As one can see in Fig.2, there could be just only one HA level for the network scale of 1000 end nodes. When this number grows up, the creation of the multilevel tree is necessity. For the session with the 1 million end nodes, the HA tree needs to be organized into the three levels e.g. FTM maintains the set of FTs and forms them to the hierarchical tree structure. Thus the FTs can transmit information from a huge number of receivers to a single node (RFT) in very short time when compared with RTP/RTCP standard. FTM also monitors the number of nodes and when needed, it updates the hierarchical tree structure. As the algorithm is proposed to use a constant bandwidth, when a few receivers are reconnected, e.g. on start of the session, it could lead to send the reports too often. Therefore a good idea is limit the lower bound by 5s. This constant is also used in RTP/RTCP standard

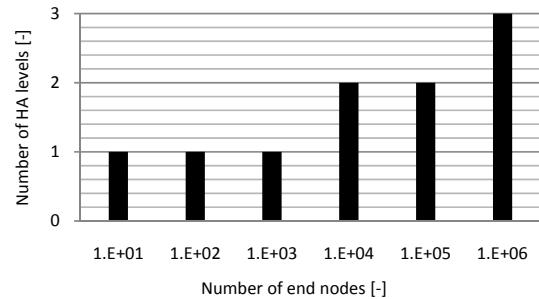


Fig.2 Dependency of the number of HA levels on the number of the end nodes

To use the TTP protocol for the efficient data gathering from the large-scalesessionsone need to know, where to properly place the reference points LMs. To settle this issue, we have implemented the “Global Network Position”[1]JAVA application simulating the GNP and Vivaldi algorithms (mentioned above) for the determination of the optimal LMsplacement. We have performed the simulation of our approach in the Matlab, where we have investigated the dependency of the time-interval reportson the number of the HA tree levels. Furthermore, we have compared the obtained results with the DT (Direct Transmission) approach, where all nodes send reports via the unicast channel directly to the S. This DT approach is used in nowadays IPTV sessions e.g.thesimulation conditions were kept same as in the first investigation.

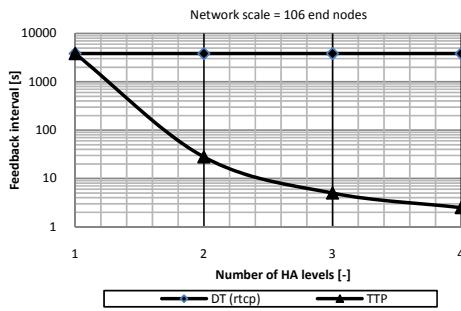


Fig.3Optimization of the feedback report time with the growing number of the HA levels. And comparison with the common DT approach.

For the DT approach, the number of the HA levels does not affect the final feedback interval, since the reports are transmitted via unicast directly to the S. This interval was calculated accordingtoRTP/RTCP specificationin[6]. Hence the feedbackinterval remainsconstant at the value of 3834 sec. To ensure the certain quality of IPTV session, this feedback interval is absolutely deficient.Next, we haveevaluatedthearchitecturefor the efficient data gathering based on the TTP model.In the results from theTTPstructure illustrated inFig.3, the feedback interval at the rcv level is decreased under the 5sec threshold at the cost of the FTs number increasing in the higher level. One can observe, that the 4-level structure of the TTP_{OPT} is able to reduce the feedback interval at the value of 2,5 sec.Thus, this approach absolutely outperforms the feedback intervals calculated by the DT model of data gathering used in the nowadays large-scale IP sessions.TTP protocol is more complex and itscomprehensivedescription is out of this paper scope. For more information see[1],[2],[3].

III.ARCHITECTURE FOR WSN

We have proved that TTP works well for efficient data gathering in the environment of the large-scaleIP sessions. But, it is obvious that this protocol designed for the IP networks cannot be implemented to the WSN environment without the crucial modifications.Hence, we have to retransform the feedback delay optimization of TTP to the energy-efficiency optimization manner of the TTP/WSN to prolong the sensor network lifetime.

The computing and communications capabilities of the IP networks are many times powerful than the facilities of the restricted wireless sensor networks. In WSN, we have to battle with the restriction in terms of the energy supplies, the narrow bandwidth and the constrained computing processes. To go ahead, the main conditions of the WSN environment need to be defined. We consider a homogeneous network where all nodes have the same communication and computing capabilities together with the same level of the energy reserve. At this point we turn aside from the described TTP network structure, where the aggregation FT nodes are more powerful than the end nodes.

III.I LOCALIZATIONARCHITECTURE

In the TTP protocol, all nodes locate own geographic position by means of the triangulation algorithms by the focusing at the LMs reference points. Most of therecently proposedprotocols suppose the location awareness sensor nodes in scale of thousands or millions. However, these expectations are rather out of the reality. GPS equipped nodes are quite expensive (do not fulfill sensor’s narrow and low-cost assumption) and their considerable energy consumption is also a big drawback. Hence, these GPS equipped nodes are not suitable to deploy in the large-scale low-cost WSNs. Our approach, it is to investigate the WSNs in the scale of up to 1000 nodes that will use the GNP[4]and Vivaldi[5]algorithms to determinate own position in the sensor field regarding the decreasingofthe energy-load of the entire network. As we described above, to find out own position the end nodes in TTP measure the RTT parameter toward the LMs. In WSN, the similar approach could be used.The RSSI (Receive Signal Strength Indication) and LQI (Link Quality Indicator) could be used as the metric for the localization process.We assume the random deployment of sensor nodes with the certain prediction of nodes position. From this assumption, we are able to pose in the concrete location the definite number (3 minimally) of reference nodes referred as AnchorSensors(AS) with the known geographic coordinates.In case that all nodes in sensor field calculate own position by means of these three ASs, the energy supplies of the AS’s ambient nodes is depleted very fast. Since the far-away nodes use theintermediatenodes as the

routers to reach the given ASs and thus they deplete theirs energy supplies.

We have proposed the localization architecture, completely illustrated in Fig.5a. Simultaneously with the sensor nodes deploying in the sensor field (in random way), the three GPS equipped ASs are placed in the certain optimal positions inside of the sensor field (a_{s1} , a_{s2} , a_{s3} nodes in Fig.5a). Theirs radio range is restricted to reach only ambient nodes. ASs nodes broadcast the synchronization message to determinate the set of nodes that can reach all ASs and thus to calculate own positions. To describe the localization architecture, certain formal terms needs to be defined. Let's have the set of sensor nodes $S = \{s_1, s_2, \dots, s_n\}$ with the R_s radio range and the set of the anchor sensors AS $= \{as_1, as_2, \dots, as_n\}$ with R_{as} radio range whereas the $R_s \neq R_{as}$ and $R_s < R_{as}$. We have used the basic assumption that each has the sufficient R_s to reach the direct neighbor nodes via the one hop transmission (see Fig.5a) and thus to save the energy of tiny sensors, since the energy-cost of the transmission process depends on the transmission distance as we describe in chapter IV.

Furthermore, we define the AS_p set of nodes that can directly reach minimally three $as \in AS$. We can define the AS_p set as follows:

$$AS_p = S_{R_{as}x1} \cap S_{R_{as}x2} \cap S_{R_{as}x3} \quad (4)$$

$$S_{R_{as}x} = \{s \in S : d < R_{as}\}$$

In the statement (4), the $S_{R_{as}x}$ stands for the set of nodes that are covered with the radio signal of the given as_x with the R_{as} radio range and d parameter denotes the distance of s_x from the given as_x . Fig.4 illustrates the AS_p determination in detail.

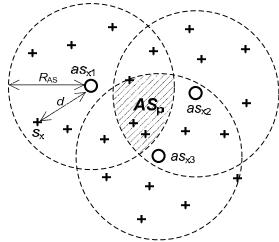


Fig.4 AS_p set definition.

Each $s \in S$ is able to calculate own coordinates if $givens \in AS_p$. When the given sensors determinate own coordinates, they are subsequently used for the rest of the sensor field as the anchor nodes (Fig.5b). By means of this approach, the far-away sensors do not need to communicate with the remote anchor sensors, but they

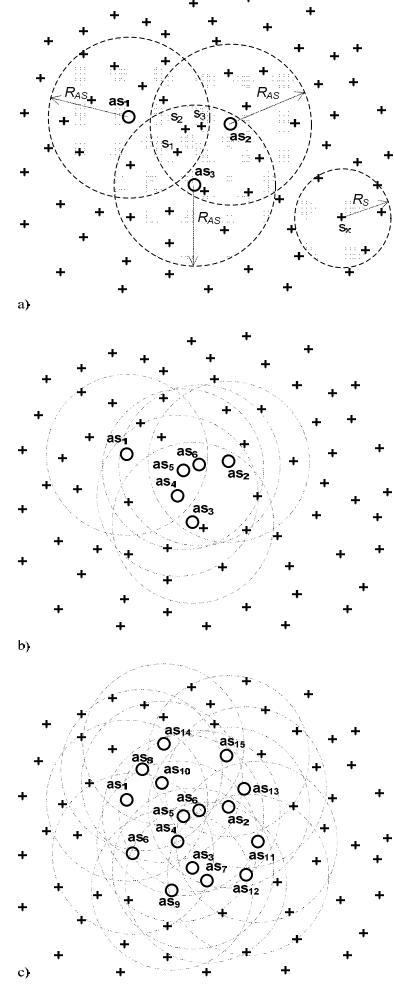


Fig.5 Localization architecture a) In the sensor filed, the three GPS anchor sensors as_1, as_2, as_3 are placed, b) s_1, s_2, s_3 sensors are covered with the as_1, as_2, as_3 thus they became the anchor sensors and extend the radio range of all anchor sensors, c) almost 70% of sensor field is covered with the radio signal of the anchor sensors.

wait for s nodes that will placed in theirs radio range (see Fig.5c) and thus can save energy for the further monitoring and aggregating processes. In Fig.6 we illustrate the proposed algorithm for the localization architecture described above.

III.II DATA AGGREGATION

Since the aggregation process consumes the considerable amount of energy, the function of the aggregation nodes referred in WSNs as the CHs (Clusterheads) needs to be rotated among all nodes. This rotation process is

necessary for spreading out the energy-load of the aggregation process and thus to retain the same energy-level of all nodes in the sensor field. Furthermore, as we show later in the chapter IV, the communication in WSN is the fundamental energy consumer.

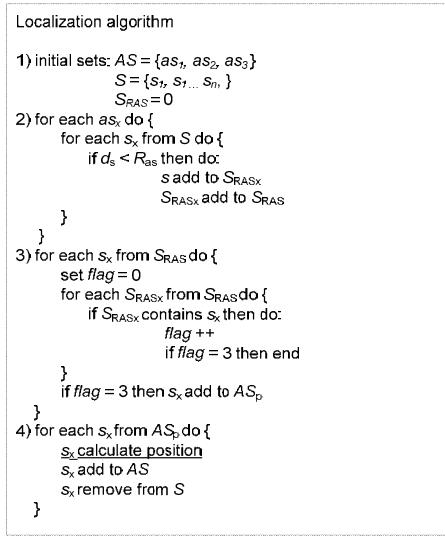


Fig.6 Localization algorithm divided to four parts.

From this reason, the number of transmission during the initial network configuration and data collecting process need to be kept as low as possible. Hence, the TTPs centralized approach must to be retransformed to the distributed manner to reduce the communication with the base station (BS) that controls the structure of the created HA tree and thus to prolong the network lifetime. BS maintains the form of HA tree, but we try to force sensor nodes to be self-organized as much as possible. For example, when the sensor field will be expanded with a new set of nodes by the human intervention, this set needs to join itself to the existing HA tree with the minimum BS cooperation. The dynamic form and structure of the WSN and TTP tree is the common behavior for the both environment and thus the proposed algorithms for TTP tree could be partly used in the WSN case. However, the often changes in the number of sensor nodes are not expected. In future, we suppose to investigate the energy consumption of this approach via the ns2 simulations and the real measurement in the BENSlaboratory (Brno - Experimental Network of Sensors), experimental sensor network containing 100 sensor nodes Crossbow MicaZ[7]. As well as in the TTP architecture where the FTM is able to communicate with the all nodes of the session, for our WSN architecture, we consider the asymmetric communication where the BS is capable to

communicate directly (by one-hop) with all nodes in the sensor field whereas the nodes are capable to reach the BS via the multihop transmission. This situation is denoted in Fig.7.

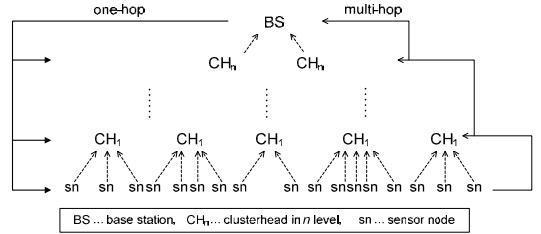


Fig.7 Hierarchical structure for TTP-WSN extension. Base station communicates directly with all nodes in sensor field whereas the sensor nodes use the multihop communication to reach the Base station.

Since the sensor network is divided into the several clusters where for each cluster one specific node acts as the clusterhead, for the far-away clusterheads is energy-uneconomical to transmit aggregated data directly to the BS. Hence, we consider using of the multihop communication for the CHs or as well as in the TTP model, to form the multilevel hierarchical tree where data will be aggregated in the multilevel hierarchy of CHs (see Fig.7). During our investigation and designing of new WSN architecture, we would like to combine the basics of the TTP and LEACH[8]algorithms. Nevertheless, in contrast of the LEACH we assume to form the fix clusters being constructed just once at the beginning of first data gathering process, such as the LEACH-F[9]. In the case of the WSN expansions with another set of sensor nodes, then the clustering process will be performed again. The new nodes announce to the BS that performs the re-clustering process. Far-away CHs will use the other CHs for the multihop transmitting of aggregated data to the BS. This approach was firstly used in LEACH-M[10].

IV. INVESTIGATION OF RADIO ENERGY MODEL

To investigate the energy-efficiency of the proposed WSN architecture, it is necessary first of all to evaluate the energy-cost of the fundamental communication processes such as the transmission and receiving processes of the sensor nodes. To fulfill these requirements, we have described the energetic mathematical model and consequently performed the real measurements with the MicaZ motes[7]. For the description of the mathematical model, the first order radio model from[8] was used. This model is illustrated in Fig.8. To transmit the message with the size of kbits, it is necessary to consider the energy consumption of the transmitter and receiver circuits'

activation E_{elec} , as well as the energy cost of transmit amplifier E_{amp} to reach the acceptable E_b/N_0 [8].

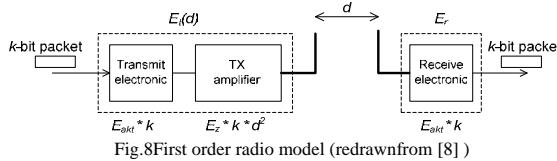


Fig.8First order radio model (redrawnfrom [8])

During the transmission it is necessary to assume the energy loss r^2 due to the channel propagation. Thus to transmit k bit message to the distanced, the radio interface consumes amount of the energy calculated according to formula(5).

$$\begin{aligned} E_{TX}(k, d) &= E_{TX-elec}(k) + E_{TX-amp}(k, d) \\ &= E_{elec} * k + E_{amp} * k * d^2 \end{aligned} \quad (5)$$

In the next paragraph, the energy consumption of the communication processes in the real wireless sensor network is investigated. We have performed the real investigation at the experimental WSN network, where the real cost of the transmission process was evaluated. We have used the different size of messages being transmitted via the IEEE 802.15.4 and IPv6 protocol that is supported in the Tiny OS-2.x of MicaZ sensors. Two AA batteries from Varta(2 x 1,5V) were used as the power supply. This kind of the supply was not changed during of all evaluations. From the results illustrated in Fig.9, one can see that there is almost no difference between the consumption over the IEEE 802.15.4 and IPv6 protocol.

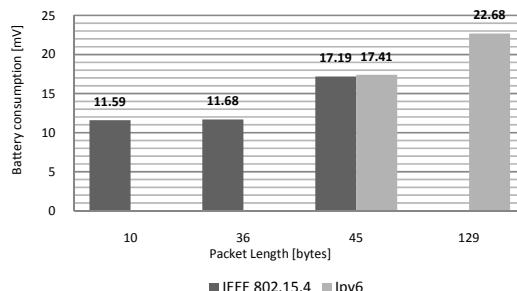


Fig.9Energy consumption per hour/bytes

Knowing that in one hour $3600/5 = 720$ messages were sent, we can present the results listed in Tab.1.

Tab.1Energy consumed for different message size and calculated consumption per bit for IEEE 802.15.4 and IPv6

Protocol	IEEE 802.15.4			IPv6	
Message size [bytes]	10	36	45	45	129
Volts/message	16,09	16,22	24,29	24,18	31,5

[μ V]				
Volts/bit [μ V]		0.09		0.03

V. CONCLUSION AND FUTURE WORK

In this paper, we have investigated the efficiency of the Tree Transmission Protocol for the effective data gathering in the time manner that could be successfully used in the IP networks with the IPTV service e.g. We have proved, that TTP protocol is able to outperform the present RTP/RTCP standard used for the IPTV applications. Since the TTP protocol obtains the successful results, we have proposed WSN architecture for the localization and effective data gathering that is partly based on TTP structure. The simulation and further optimization of the proposed architecture is the challenge for the future work. In chapter IV, the fundamental radio energy model was defined together with the real measurement of the transmission energy-cost in the sensor network to obtain the reliable values for the future investigation. However, these values need to be transferred in the energy terms described in Joules. Mentioned will be investigated in the future as well.

ACKNOWLEDGMENTS

This work was supported by Academy of Sciences of the Czech Republic - project 1ET301710508.

REFERENCES

- [1] R. Burget: "Global Network Position", <http://www.ipv-server.com>
- [2] D. Komosny, R. Burget, V. Novotny Tree Transmission Protocol for Feedback Distribution in IPTV Systems". In Proceedings of the Seventh IASTED International Conference on Communication Systems and Networks.Palma de Mallorca, Spain: International Association of Science and Technology for Development, 2008. s. 1-7. ISBN: 978-0-88986-758-1.
- [3] D.Komosny, V.Novotny,Feedback Distribution in Specific Source Multicast using Tree Transmission Protocol, Sixth International Conference on Networking (ICN'07).
- [4] T. S. E. Ng and H. Zhang, Predicting Internet network distance with coordinates-based approaches, in Proceedings of the IEEE INFOCOM, New York, NY, June 2002.
- [5] F. Dabek, R. Cox, F. Kaashoek, and R. Morris, Vivaldi: A decentralized network coordinate system, in Proceedings of the ACM SIGCOMM, Portland, OR, August 2004
- [6] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson.: RTP: A Transport Protocol for Real-Time Applications, Request for Comments 3550, Internet Engineering Task Force, 2003
- [7] Crossbow, Wireless Sensor Networks, MicaZ 2,4 GHz, Crossbow Technology Inc., 2007, online:<http://www.xbow.com>
- [8] , and H. Balakrishnan."Energy-Efficient Communication Protocols for Wireless Microsensor Networks". In Proceedings of Hawaiian International Conference on Systems Science, January 2000.
- [9] W. B. Heinzelman et al., "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions on Wireless Communications Volume 1, No. 4, Oct 2002, pp.660 - 670.
- [10] V. Mhatre, C. Rosenberg, „Homogeneous vs heterogeneous clustered sensor networks : A comparative study”, IEEE International Conference on Communications, Paris , FRANCE,June 2004. ISBN 0-7803-8533-0

Two Cross-Coupled H_∞ Filters for Fading Channel Estimation in OFDM Systems

Ali Jamoos¹, Ahmad Abdo¹, Hanna Abdel Nour¹ and Eric Grivel²

¹Department of Electronics Engineering, Al-Quds University, Jerusalem, Palestine

²Equipe Signal & Image, UMR CNRS 5218 IMS – Dpt. LAPS, Université Bordeaux 1, 33405 Talence Cedex, France
email: ali@eng.alquds.edu, aabdo@eng.alquds.edu, habdalnour@eng.alquds.edu, eric.grivel@laps.ims-bordeaux.fr

ABSTRACT

In this paper, our purpose is to estimate time-varying Rayleigh fading channels in Orthogonal Frequency Division Multiplexing (OFDM) mobile systems. When the fading channel is approximated by an AutoRegressive (AR) process, the direct estimation of the model parameters from the noisy observations available at the receiver may yield biased values. To avoid this drawback, the joint estimation of both the channel and its AR parameters must be addressed. Existing solutions to this dual estimation issue require Kalman filtering. This kind of filtering is optimal in the H_2 sense provided that the underlying state-space model is accurate. Moreover, the initial state, the driving process and the measurement noise must be independent, white and Gaussian. However, in real cases, these assumptions may no longer be satisfied. To relax them, we propose to consider a structure based on two cross-coupled H_∞ filters. This method makes it possible to provide robust estimation of the fading channel and its AR parameters.

1. INTRODUCTION

Orthogonal Frequency Division Multiplexing (OFDM) is an effective modulation technique that can achieve high data rates by the simultaneous transmission over orthogonal carriers [1]. This scheme makes it possible to convert the severe wide-band frequency-selective fading channel into many narrow-band frequency non-selective flat fading sub-channels, which are free from Inter-Symbol Interference (ISI). Given its various advantages, OFDM has been adopted in several wide-band digital communication systems such as Digital Audio and Video Broadcasting (DAB/DVB), Asynchronous Digital Subscriber Lines (ADSL), IEEE 802.11 a/g Wireless Local Area Networks (WLAN) and the Worldwide Interoperability for Microwave Access (WiMAX).

In OFDM systems, due to user mobility, each carrier is subject to Doppler shifts, resulting in time-varying fading. Thus, the estimation of the time-varying fading process over each carrier is essential to achieve coherent symbol detection at the receiver [2]. The time-varying Rayleigh fading channels are usually modelled as zero-mean wide-sense stationary circular complex Gaussian processes with band-limited Doppler power spectrum according to the Jakes model [3]. This kind of channel statistics are useful to select a model for the channel and to derive a parametric approach based on an optimal filtering for channel estima-

tion. Thus, in [5] and [7], AR modelling combined with Kalman filtering is considered. Nevertheless, the AR model parameters are unknown and, hence, must be estimated.

Some authors, e.g. [5], have expressed the AR parameters by first fitting a low-order AR process autocorrelation function to the theoretical Jakes one and then solving the resulting Yule-Walker (YW) equations. However, this requires the preliminary estimation of the maximum Doppler frequency, which is not necessarily a trivial task [6]. As an alternative, the AR parameters can be estimated from the noisy observations available at the receiver. Among the existing methods, the AR parameters can be estimated from estimates of the channel covariance function by means of a standard YW estimator in [7]. However, this method results in biased AR parameter estimates due to the additional noise.

To avoid this drawback, one can look at other approaches initially proposed in other fields than wireless communications. Thus, the Expectation-Maximization (EM) algorithm which often implies a Kalman smoothing can be used [8]. Nevertheless, since it operates repeatedly on a batch of data, it results in large storage requirements and high computational cost. When dealing with the dual estimation issue, i.e. the joint estimations of the process and its AR parameters from noisy observations, the corresponding state-space representation is non linear. In that case “local methods” such as the Extended Kalman Filter (EKF) or “global methods” such as the Unscented Kalman Filter (UKF) could be considered, but they require the noise covariance matrices. As an alternative, two Kalman filters can be cross-coupled to solve the joint estimation issue as proposed by Labarre *et al.* in [9]. This approach can be seen as a recursive instrumental variable technique and hence provides consistent estimates of the AR parameters. Its relevance has been hence studied in [10] and [11] to estimate Multi-Carrier Direct-Sequence Code Division Multiple Access (MC-DS-CDMA) and OFDM fading channels, respectively.

Using Kalman filtering is of interest, but several assumptions must be fulfilled. Indeed, Kalman filtering is optimal in the H_2 sense providing that the underlying state-space model is accurate. Moreover, the initial state, the driving process and the measurement noise must be independent, white and Gaussian. However, these assumptions do not always hold in practical cases, especially when dealing with OFDM systems, due to the following uncertainties and approximations:

- Firstly, the AR model does not fit exactly the fading process, especially when considering low-order AR models.

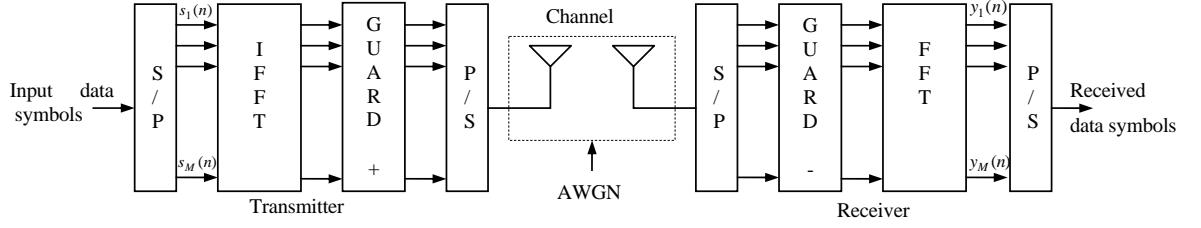


Figure 1 - OFDM System.

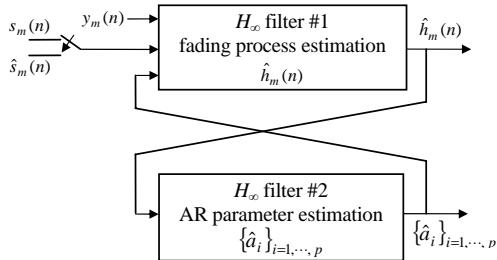
- Secondly, the noise variances in the state space representation and the AR parameters are usually unknown and, hence, must be estimated.

Therefore, H_∞ estimation techniques, initially developed in the framework of control [12], can be considered.

The estimation criterion is to minimize the worst possible effects of the noise disturbances (i.e., the initial state, the driving process and the measurement noise) on the estimation error. Furthermore, this criterion requires no *a priori* constraints about the noises, except that they have bounded energies. In that sense and according to [12], H_∞ filtering is more robust against the noise disturbances and modelling approximations than Kalman filtering.

In the framework of OFDM wireless systems (see Figure 1), Cai *et al.* [13] have proposed a channel estimation scheme based on two serially-connected H_∞ filters. The first one is used for AR parameter estimation and the second one for fading process estimation. Nevertheless, the AR parameter estimates are biased since they are estimated directly from the noisy data. This might result in poor estimation of the fading process.

In this paper, we propose to take advantage of the two cross-coupled H_∞ filters, initially developed in the framework of speech enhancement [14], for the joint estimation of time-varying OFDM fading channels and their corresponding AR parameters. See Figure 2. This method has the advantage of yielding unbiased estimation of the AR parameters. It also outperforms the approach proposed in [13].

Figure 2 – Two cross-coupled H_∞ filters for the joint estimation of the fading process and its AR parameters along the m^{th} carrier.

The remainder of the paper is organized as follows. The OFDM system model is recalled in section 2. The fading channels estimation based on two cross-coupled H_∞ filters is introduced in section 3. Simulation results are reported in section 4. Conclusion remarks are drawn in section 5.

2. OFDM SYSTEM MODEL

In this section, let us consider a standard OFDM system as depicted in Figure 1.

The input serial data stream is firstly converted into parallel data blocks. An Inverse Fast Fourier Transform (IFFT) is then performed on each block and a guard interval is added to avoid the Inter-Symbol Interference (ISI). The transmitted OFDM signal is assumed to go through a rapidly time-varying Rayleigh fading channel. At the receiver, the guard interval is removed and a FFT is then performed on each received OFDM symbol. Thus, with proper selection of the guard interval and perfect carrier synchronization, we assume that the received signal sample over the m^{th} carrier for the n^{th} OFDM symbol can be written in the following manner [13]:

$$y_m(n) = h_m(n)s_m(n) + v_m(n), \quad m = 1, 2, \dots, M \quad (1)$$

where M is the total number of carriers, $s_m(n)$ is the m^{th} data symbol of the n^{th} OFDM symbol which is drawn from a Quadrature Phase Shift Keying (QPSK) constellation $\{1, -1, j, -j\}$ independently for different m and n , and $v_m(n)$ is a zero-mean complex Additive White Gaussian Noise (AWGN) process with variance σ_v^2 . In addition, the fading process over the m^{th} carrier $h_m(n) = \beta_m(n)e^{j\theta_m(n)}$ is assumed to be a zero-mean complex Gaussian process with uniformly distributed phase $\theta_m(n)$ on $[0, 2\pi)$ and a Rayleigh distributed envelop $\beta_m(n)$. The variances of the processes $\{h_m(n)\}_{m=1, \dots, M}$ are all assumed equal to σ_h^2 .

The stochastic characteristics of the m^{th} carrier fading process $h_m(n)$ depend on the maximum Doppler frequency:

$$f_d = v f_c / c \quad (2)$$

where v is the mobile speed, f_c is the central carrier frequency and c is the light speed.

According to [3], the theoretical Power Spectral Density (PSD) associated with either the in-phase or quadrature portion of the fading process $h_m(n)$ is band-limited and U-shaped. Moreover, it exhibits two peaks at $\pm f_d$ as follows:

$$\Psi_{hh}(f) = \begin{cases} \frac{1}{\pi f_d \sqrt{1-(f/f_d)^2}}, & |f| \leq f_d \\ 0, & \text{else where} \end{cases} \quad (3)$$

Its corresponding normalized discrete-time Autocorrelation Function (ACF) hence satisfies:

$$R_{hh}(n) = J_0(2\pi f_d T_s |n|) \quad (4)$$

where $J_0(\cdot)$ is the zero-order Bessel function of the first kind, T_s is the symbol period, and $f_d T_s$ is the Doppler rate.

3. H_∞ FILTERING FOR CHANNEL ESTIMATION

3.1 AR Modelling of Rayleigh Fading Channels

To exploit the statistical properties of the fading channel given by its PSD (3) and ACF (4), the fading process over the m^{th} carrier is often approximated by a p^{th} order AR process, denoted by AR(p) and defined as follows [4]:

$$h_m(n) = -\sum_{i=1}^p a_i h_m(n-i) + w_m(n) \quad (5)$$

where $\{a_i\}_{i=1,\dots,p}$ are the AR parameters and $w_m(n)$ denotes the zero-mean complex white Gaussian driving process with equal variance σ_w^2 over all carriers.

Using low-order AR model for the channel is debatable. On the one hand, some authors (e.g., [5] [7]) suggested using AR(1) or AR(2) process, because these models are simple and can be easily used for channel estimator. On the other hand, from a theoretical point of view, a deterministic model should be used for the channel due to the band-limited nature of its PSD according to Kolmogoroff-Szégo formula [15]:

$$\sigma_w^2 = \exp\left(\frac{1}{2\pi} \int_{-\pi}^{\pi} \ln(\Psi_{hh}(\omega)) d\omega\right) \quad (6)$$

where $\Psi_{hh}(\omega)$ denotes the PSD of the AR process that fits the Jakes spectrum. Other solutions have been also proposed in [4], where high-order AR processes (e.g. $p \geq 50$) are used to simulate the channel. For this purpose, Baddour *et al.* modify the properties of the channel to make its PSD log-integrable by considering the sum of the theoretical fading process and a zero-mean white process whose variance ε is very small (e.g., $\varepsilon = 10^{-7}$ for $f_d T_s = 0.01$). Then, the AR parameters are estimated with the YW equations based on the modified ACF:

$$R_{hh}^{\text{mod}}(n) = J_0(2\pi f_d T_s |n|) + \varepsilon \delta(n) \quad (7)$$

Taking into account the above discussion, we propose to use an AR model whose order is high enough for the channel. Figure 3 shows the ACF of the Jakes model and that of the fitted AR process whose order is 1, 2, 5 and 20.

In the following, as $R_{hh}(n)$ is usually unknown, we propose to jointly estimate the fading process $h_m(n)$ and its AR parameters $\{a_i\}_{i=1,\dots,p}$.

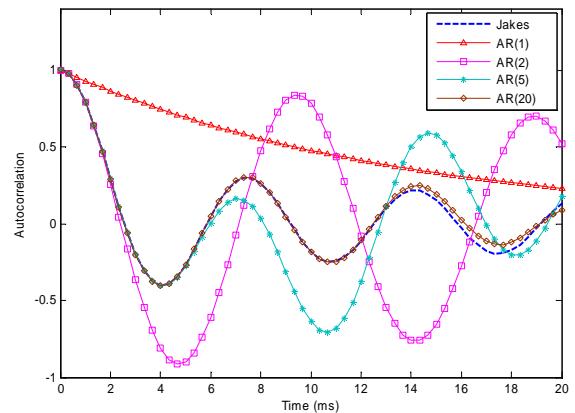


Figure 3 - Autocorrelation function of the Jakes model and that of the fitted AR (p) process with $p=1, 2, 5$, and 20. $f_d T_s = 0.05$.

3.2 Estimation of the Fading Processes

To estimate the fading process $h_m(n)$ along the m^{th} carrier, and for the sake of simplicity and clarity of presentation, the carrier subscript is dropped let us define the state vector as follows:

$$\mathbf{h}(n) = [h(n) \ h(n-1) \ \dots \ h(n-p+1)]^T \quad (8)$$

Then, equation (5) can be written in the following state space form:

$$\dot{\mathbf{h}}(n) = \Phi \mathbf{h}(n-1) + \mathbf{g} w(n) \quad (9)$$

where

$$\Phi = \begin{bmatrix} -a_1 & -a_2 & \dots & -a_p \\ 1 & 0 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 1 & 0 \end{bmatrix} \text{ and } \mathbf{g} = [1 \ 0 \ \dots \ 0]^T \quad (10)$$

In addition, given (1) and (8), one has:

$$\mathbf{y}(n) = \mathbf{s}^T(n) \mathbf{h}(n) + v(n) \quad (11)$$

$$\text{where } \mathbf{s}(n) = [s(n) \ 0 \ \dots \ 0]^T.$$

Hence, equations (9) and (11) define the state space representation dedicated to the one-carrier fading channel system (1) and (5). Unlike Kalman filtering, the H_∞ filtering not only deals with the estimation of the state vector $\mathbf{h}(n)$, but also makes it possible to focus on the estimation of a specific linear combination of the state vector components, as follows:

$$\mathbf{z}(n) = \mathbf{l} \mathbf{h}(n) \quad (12)$$

where \mathbf{l} is a $1 \times p$ linear transformation operator. Here, as we aim at estimating the fading process $h(n)$, this operator is selected to be $\mathbf{l} = \mathbf{g}^T = [1 \ 0 \ \dots \ 0]$.

Given the state space representation of the fading channel system (9), (11) and (12), the H_∞ filtering can provide the estimation of the fading process $\hat{\mathbf{h}}(n) = \hat{\mathbf{l}} \hat{\mathbf{h}}(n)$ by minimizing the H_∞ norm of the transfer operator that maps the noises $w(n)$, $v(n)$ and the initial state error $\mathbf{e}_0 = \mathbf{h}(0) - \hat{\mathbf{h}}(0)$ to the

estimation error $e(n) = h(n) - \hat{h}(n)$, as follows:

$$J_{\infty} = \sup_{w(n), v(n), \mathbf{h}(0)} J$$

where

$$J = \frac{\sum_{n=0}^{N-1} |e(n)|^2}{\mathbf{e}_0^H \mathbf{P}_0^{-1} \mathbf{e}_0 + \sum_{n=0}^{N-1} (Q_w^{-1} |w(n)|^2 + R_v^{-1} |v(n)|^2)} \quad (14)$$

with N the number of available data samples. In addition, \mathbf{P}_0 , $Q_w > 0$ and $R_v > 0$ are weighting parameters that are tuned by the designer to achieve performance requirements. However, as a closed-form solution to the above optimal H_{∞} estimation problem does not always exist, the following suboptimal design strategy is usually considered:

$$J_{\infty} < \gamma^2 \quad (15)$$

where $\gamma > 0$ is a prescribed level of disturbance attenuation. Following the method presented in [16], there exists an H_{∞} channel estimator $\hat{h}(n)$ for a given $\gamma > 0$ if there exists a stabilizing symmetric positive definite solution $\mathbf{P}(n)$ to the following Riccati-type equation:

$$\mathbf{P}(n+1) = \Phi \mathbf{P}(n) \mathbf{C}^{-1}(n) \Phi^H + \mathbf{g} Q_w \mathbf{g}^T, \quad \mathbf{P}(0) = \mathbf{P}_0 \quad (16)$$

where:

$$\mathbf{C}(n) = \mathbf{I}_p - \gamma \mathbf{l}^T \mathbf{l} \mathbf{P}(n) + \mathbf{b}(n) R_v^{-1} \mathbf{b}^T(n) \mathbf{P}(n) \quad (17)$$

This leads to the following constraint:

$$\mathbf{P}(n) \mathbf{C}^{-1}(n) > 0 \quad (18)$$

If the condition (18) is fulfilled, the H_{∞} channel estimator exists and is given by:

$$\hat{h}(n) = \mathbf{l} \hat{\mathbf{h}}(n) \quad (19)$$

$$\hat{\mathbf{h}}(n) = \Phi \hat{\mathbf{h}}(n-1) + \mathbf{K}(n) \alpha(n), \quad \hat{\mathbf{h}}(0) = \mathbf{0} \quad (20)$$

where the so-called innovation process $\alpha(n)$ and the H_{∞} estimator gain $\mathbf{K}(n)$ are respectively given by:

$$\alpha(n) = y(n) - \mathbf{b}^T(n) \Phi \hat{\mathbf{h}}(n-1) \quad (21)$$

and

$$\mathbf{K}(n) = \mathbf{P}(n) \mathbf{C}^{-1}(n) \mathbf{b}(n) R_v^{-1} \quad (22)$$

It should be noted that the H_{∞} channel estimator (16)-(22) has similar observer structure as the Kalman one. However, due to (17), the H_{∞} channel estimator has a computational cost slightly higher than Kalman's one. Indeed, if the weighting parameters Q_w , R_v and \mathbf{P}_0 are respectively chosen to be σ_w^2 , σ_v^2 and the initial error covariance matrix of $\mathbf{h}(0)$ then as $\gamma \rightarrow \infty$ the H_{∞} estimator reduces to the Kalman one.

3.3 Estimation of the AR Parameters

In this subsection, we propose to estimate the AR parameters $\{a_i\}_{i=1,\dots,p}$ from the estimated fading process $\hat{h}(n)$. For this purpose, equation (19) and (20) are firstly combined to express $\hat{h}(n)$ as a function of the AR parameters:

$$\begin{aligned} \hat{h}(n) &= \mathbf{l} \Phi \hat{\mathbf{h}}(n-1) + \mathbf{l} \mathbf{K}(n) \alpha(n) \\ &= \hat{\mathbf{h}}^T(n-1) \mathbf{a}(n) + u(n) \end{aligned} \quad (23)$$

where $\mathbf{a}(n) = [-a_1 \ -a_2 \ \cdots \ -a_p]^T$ is a vector of the AR parameters and the “noise” process $u(n) = \mathbf{l} \mathbf{K}(n) \alpha(n)$.

When the channel is assumed stationary, the AR parameters are time-invariant and satisfy the following relationship:

$$\mathbf{a}(n) = \mathbf{a}(n-1) \quad (24)$$

Equations (23) and (24) hence define a state space representation for the estimation of the AR parameters. A second H_{∞} filter can then be used to recursively estimate $\mathbf{a}(n)$.

3.4 Operation of the channel estimator

During the so-called training mode, the first H_{∞} filter in Figure 2 uses the training sequence $s_m(n)$, the observation $y_m(n)$ and the latest estimated AR parameters $\{\hat{a}_i\}_{i=1,\dots,p}$ to estimate the fading process $h_m(n)$; while the second H_{∞} filter uses the estimated fading process $\hat{h}_m(n)$ to update the AR parameters. At the end of the training period, the receiver stores the estimated AR parameters and uses them in conjunction with the observation $y_m(n)$ and the decision $\hat{s}_m(n)$ to predict $h_m(n+1)$ in a decision directed manner. At that stage, the received signal in (1) is multiplied by the conjugate of the channel estimate to compensate for the phase offset introduced by the fading channel, and the data symbols are recovered by coherent detection.

4. SIMULATION RESULTS

4.1 Simulation Protocol

In this section, we carry out a comparative simulation study on the estimation of OFDM fading channels between several methods:

1. the proposed two cross-coupled H_{∞} filters,
2. the two cross-coupled Kalman filters [9][10],
3. the two serially-connected H_{∞} filters [13],
4. the standard LMS and RLS channel estimators.

We consider an OFDM system with QPSK modulation, 52 carriers, and a central carrier frequency of 1900 MHz. The transmitted frame size over each carrier is assumed to be 256 symbols. The fading processes $\{h_m(n)\}_{m=1,\dots,M}$ are generated according to the Jakes model with 16 distinct oscillators and Doppler rate $f_d T_s = 0.0916$. They are normalized to have a unit variance, i.e. $\sigma_h^2 = 1$. The average Signal-to-Noise Ratio (SNR) per carrier is defined by:

$$\text{SNR} = 10 \log_{10} (\sigma_h^2 / \sigma_w^2) = 10 \log_{10} (1 / \sigma_w^2) \quad (25)$$

4.2 Results and Comments

Figure 4 and Figure 5 illustrate the Bit Error Rate (BER) performance of the OFDM system with the various channel estimators when considering different order AR models.

According to Figure 4, the proposed two cross-coupled H_{∞} filter based estimator yields lower BER performance than

the two cross-coupled Kalman filter based one when considering AR(1) model. Hence, the proposed two cross-coupled H_∞ filter based estimator is more robust to modeling approximation than the Kalman based one. The two approaches provide approximately the same BER when the AR model order is greater than one. Nevertheless, the proposed approach has the advantage of relaxing the Gaussian and whiteness assumptions required by Kalman filtering. An AR(20) model is a priori preferable as it provides better approximation of the Jakes channel and yields lower BER than the low-order AR models. Nevertheless, to reduce the computational cost $O(p^3)$ of the estimation algorithm, an AR(5) is recommended.

Given Figure 5, the proposed two cross-coupled H_∞ filter based estimator results in lower BER performance than the two serially-connected H_∞ filter based one when considering AR(2) and AR(5). This is due to the fact that the later approach yields biased AR parameter estimates which have a bad influence on the estimation of the fading process.

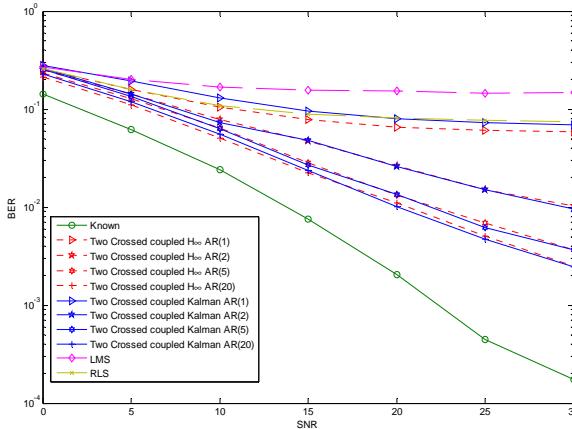


Figure 4 - BER versus SNR of the OFDM system with the cross-coupled Kalman and H_∞ filter based channel estimators, and with different AR model order.

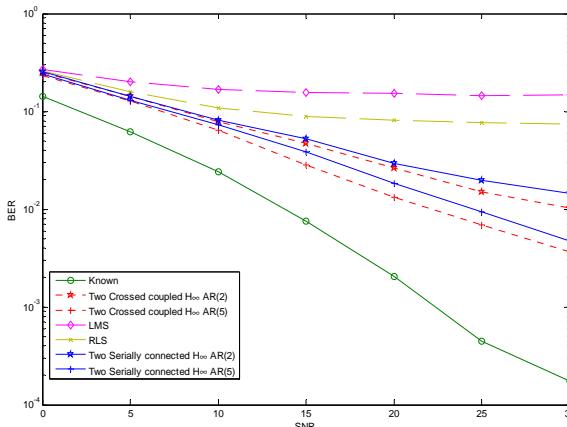


Figure 5 - BER versus SNR of the OFDM system with the cross-coupled and serially-connected H_∞ filter based channel estimators when considering AR(2) and AR(5) models.

5. CONCLUSION

This paper investigates the estimation of rapidly time-varying OFDM fading channels based on H_∞ filtering. A structure consisting of two cross-coupled H_∞ filters is proposed for the joint estimation of the fading process and its corresponding AR parameters over each carrier. The simulation results showed that the proposed approach out performs the one based on two serially-connected H_∞ filters.

REFERENCES

- [1] Z. Wang and G. B. Giannakis, "Wireless multicarrier communications, where Fourier meets Shannon," *IEEE Signal Process. Magazine*, vol. 17, pp. 29-48, May 2000.
- [2] M. K. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *IEEE Communications Surveys*, vol. 9, no. 2, pp. 18-48, 2nd Quarter 2007.
- [3] W. C. Jakes, *Microwave Mobile Communications*. New York: Wiley, 1974.
- [4] K. E. Baddour and N. C. Beaulieu, "Autoregressive modeling for fading channel simulation," *IEEE Trans. On Wireless Commun.*, vol. 4, pp. 1650-1662, July 2005.
- [5] W. Chen and R. Zhang, "Estimation of time and frequency selective channels in OFDM systems: a Kalman filter structure," in *Proc. IEEE GLOBECOM'04*, pp.800-803, Nov. 2004.
- [6] C. Tepedelenlioglu, A. Abdi, G. B. Giannakis and M. Kaveh, "Estimation of Doppler spread and signal strength in mobile communications with applications to handoff and adaptive transmission," *Wireless Commun. Mobile Comput.*, vol. 1, pp. 221-242, Jun 2001.
- [7] M. Tsatsanis, G. B. Giannakis and G. Zhou, "Estimation and equalization of fading channels with random coefficients," *Signal Process.*, vol.53, pp. 211-229, Sep. 1996.
- [8] M. Deriche, "AR parameter estimation from noisy data using the EM algorithm," in *Proc. of the IEEE-ICASSP*, Adelaide, Apr 1994, pp. 69-72.
- [9] D. Labarre, E. Grivel, Y. Berthoumieu, E. Todini and M. Najim, "Consistent estimation of autoregressive parameters from noisy observations based on two interacting Kalman filters," *Signal Process.*, vol. 86, pp. 2863-2876, Oct 2006.
- [10] A. Jamoos, D. Labarre, E. Grivel and M. Najim, "Two cross coupled Kalman filters for joint estimation of MC-DS-CDMA fading channels and their corresponding autoregressive parameters," in *Proc. EUSIPCO'05*, Antalya, 4-8 Sep. 2005.
- [11] A. Jamoos, A. Abdo and Hanna Abdel Nour, "Estimation of OFDM Time-Varying Fading Channels Based on Two-Cross-Coupled Kalman Filters," in *Proc. CISSE 07*, University of Bridgeport, 3 – 12 December, 2007.
- [12] B. Hassibi, A. H. Sayed, and T. Kailath *Indefinite quadratic estimation and control: a unified approach to an H_2 and H_∞ theories*. Philadelphia, PA: SIAM, 1999.
- [13] J. Cai, X. Shen, and J. W. Mark, "Robust channel estimation for OFDM wireless communication systems - an H_∞ approach," *IEEE Trans. On Wireless Commun.*, vol. 3, no. 6, pp. 2060 - 2071, Nov. 2004.
- [14] D. Labarre, E. Grivel, M. Najim, "Dual H_∞ algorithms for signal processing, application to speech enhancement," *IEEE Trans. on Signal Processing*, vol. 55, no. 11, pp. 5195-5208, Nov. 2007.
- [15] A. Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Processes*. McGraw-Hill, 2002.
- [16] X. Shen and L. Deng, "Game theory approach to discrete H_∞ filter design," *IEEE Trans. On Signal Processing*, vol. 45, no. 4, pp. 1092-1095, Apr 1997.

An Architecture for Wireless Intrusion Detection Systems Using Artificial Neural Networks

Ricardo Luis da Rocha Ataide & Zair Abdelouahab

Federal University of Maranhão, CCET/DEEE

Av. Dos portugueses, Campus do Bacanga, São Luis – MA 65080-040

ricardo.ataide@eletronorte.gov.br, zair@dee.ufma.br

Abstract- The majority existing wireless intrusion detection systems identifies intrusive behaviors are based on the exploration of known vulnerabilities called signatures of attacks. With this mechanism, only known vulnerabilities are detected which leads to bringing the necessity of new techniques to add in the system. This work considers an architecture for intrusion detection in wireless network based on anomaly. The system is capable to adapt itself to a profile of a new community of users, as well as recognizing attackswith different characteristics than those already known by the system, by considering changes from normal behavior. The system uses artificial neural networks in the processes of detecting intrusions and taking countermeasures. A prototype is implemented and submitted to some simulations and tests, with three different types of attacks of Denial of Service (DoS).

I. INTRODUCTION

Wireless networks IEEE 802.11, also known as Wi-Fi or wireless, are a standard connectivity for local networks. A combination of factors such as free *expectro*, efficient canal codification and relatively cheap interface hardware is making extremely popular these type of networks in recent years [3].

Even though the advantages of wireless networks are great, they brought a set of new security threats whose treatment cannot be carried out through traditional countermeasures, applicable to traditional wired networks [22]. The nature of wireless environments has become sufficiently vulnerable to attacks because of the physical characteristics of radio enlace. The dissemination of wireless waves is not restricted to physical cables and thus it is easy to determine the existence of wireless network and make a connection. With this, individuals that mere listen to radio waves without authorization, called eavesdroppers, can locate wireless networks by making a sweeping with an SSID (Service Set Identifier), as well as determining if a cryptography is being used or not. Another possibility is a creation of DoS attacks (Denial of Service), since a network can simply be flooded with a static noise that can cause its complete interruption.

An IDS (Intrusion Detection System) is an efficient tool used to determine if an unauthorized user is trying to gain access, or has already obtained access, or even though has compromised the computer network [11]. A conventional IDS concentrates its focus in the highest layer of protocols of the model OSI (Open Systems Interconnection). On the other hand, an IDS for wireless networks (WIDS) concentrates its

efforts in the identification of problems within layers 1 and 2 of OSI model [17].

The majority of existing WIDS presented Section II identifies intrusive behaviors by exploring well known vulnerabilities called signatures of attacks. They analyze the activity of the system by observing events that are similar to a predetermined standard that describes a known intrusion. With this mechanism, only known vulnerabilities are detected; however, for other types of vulnerabilities it is necessary to introduce new techniques to detect threats.

For this purpose, WIDS (Wireless Intrusion Detection System) are required to identify as well intrusion based on behavior change of users. A normal behavior of a user must be established based on historical data which is collected on a long period of time. A system can be adapted to a profile of a new community of users, as well as it is possible to recognize attacks that were not been registered previously. This is achieved based only on the change to a normal behavior of this new community.

This paper has the objective to present a model of an intrusion detection system for wireless network (IEEE 802.11 standard), an implementation of this model and show the results of simulations and tests. The system uses a detection based on anomaly and artificial neural networks. A neural network is a massively parallel and distributed processors that consists of simple processing units which store knowledge based on experience for posterior use [10]. Neural networks are used because of their efficiency and capacity of generalization.

This rest of the paper is organized as follows. Section 2 describes the main systems and existing architectures for intrusion detection on wireless environment. In Section III, we propose an architecture for intrusion detection on wireless networks. In Section IV, we describe the implementation of our system as well as the simulations and tests.

II. EXISTING ARCHITECTURES AND SYSTEMS

In [19], an architecture for WIDS is proposed and consists of the following components: agent, sensor, console of management and tools of report. The architecture is based on intelligent agents with some capacities of auto learning, cooperation, autonomy and power of decision. These agents are integrated with clients in the network and can perform

some tasks such as data collection and filtering , and cooperate with neighboring agents, thus constituting a module of cooperative detection. In this form, the response to attacks can be local or global. The architecture also can be associated with techniques of authentication and cryptography considered by the IEEE 802.11i and 802.1X, for a greater guarantee of security. Furthermore, new attacks can be detected thanks to the power of auto-learning, that uses techniques of Artificial Intelligence, Neural Networks and Fuzzy Logic.

In [22], a distributed and collaborative architecture is presented for wireless intrusion detection. In this architecture, each mobile node possesses an agent IDS that is monitoring local activities of users, system and communication. Each agent actively participates in the detection and takes actions to intrusions. The agents are responsible for detecting intrusion signals independently, and may collaborate with its neighboring for wide detection. The conceptual model of each IDS agent is constituted of a sensor and four modules. Each module represents a light mobile agent with certain functionalities, where some of these modules are present in all mobile hosts and others are distributed only in one selected group of mobile hosts.

In [6] ,a system called multi-agent MMDS (Multi-level Monitoring and Detection System) is presented. The system does in real time monitoring, analysis, detection and generation of responses to the intrusion attempts. MIMS uses a Fuzzy module based on rules for different types of attacks. MIMS uses anomaly detection for ad-hoc and infra-structured wireless networks. The behavior modeling is elastic, that is, it adapts to normal fluctuations of use in function of the time. The system provides a hierachic framework of security agents; where each security node consists of four types of agents: management, monitor, decision and action. The activities of these agents are coordinated by the management agent during the perception process, communication and generation of responses.

In [14], an implementation prototype of an intrusion detection and active response system for wireless network is presented. The system consists of various wireless devices spread on all the network and are connected to a central server a an organization. Since the devices are managed by a central server, it is possible to determine through a triangulation process the approximate position of the attack or the AP given the intensity of the signal received in each device. A central server can also correlate the wireless authentication with the authentication in other security systems such as RADIUS (Remote Authentication Dial-In User Service). An architecture is implemented with a modification in the access point USRobotics USR2450, installing a new operational system Linux with extra functionalities of access point. The system actively reacts to intrusions attempts using DoS attacks against the intruder using badly-formed pictures or through the use of honey pots (decoys).

In [21], an architecture for a wireless intrusion detection system with adaptive responses for confidence of alarms, frequency of attacks, evaluation of risks and estimate costs of

response is presented. In this architecture, each node uses an IDS agent to monitor local activity and to give response to intrusions. Knowing that local activities do not provide with sufficient data to determine the type of attacks, all agent must be capable of communicating safely form and acting collectively when an activity is under suspicion. A prototype is developed by creating a tool to detect attacks and to send frames of responses 802.11. The well known MiTM attack is used as a case study.

In [13], an architecture for monitoring wireless networks is described. The architecture has a similar vulnerability Evaluation topology of traditional intrusion detection systems and it is called WIDE (Wireless Intrusion Detection Extensions). WIDE consists of three main components: sensor, master analyzer, and alerts adapter. Each sensor is configured to send data to the master analyzer in a safe form for analysis. The master analyzer can reside in the proper sensor to conserve band width, or can reside another central localization to provide correlation between multiple sensors. In both the cases, the master is configured with a certain number of modules of attacks. These modules are independent programs which can be loaded individually in master analyses space of execution to process and generate alerts. For example, the detection module of DoS attacks uses statistical methods on the signal intensity and levels of noise to determine when potential attacks are occurring.

AirDefense [1] is a wireless intrusion and prevention system and consists of sensors distributed in the network, with an interface to a console of a management tool. The system detects non authorized APs and potential vulnerabilities. AirDefense offers other functions such as tracking of faults and auditory.

AirMagnet [2] is a commercial tool of monitoring and diagnosis of networks for Windows and Pocket PC that run on laptops and handhelds. AirMagnet detects non-authorized access points and clients and DoS attacks by flooding. The software requires that one technician moves around the network to detect possible security threats. It can also be used by an intruder, but this use is little probable because of its high cost.

Surveyor [9] is a tool similar to AirMagnet for monitoring and analyzing wireless networks 802.11 and runs on Windows 2000 and XP.

AirSnare [7] is a program for Windows that functions as an intrusion detection system detecting not-authorized DHCP solicitations or MAC addresses trying to connect itself with an access point. The response to an intrusion consists sending an alert message or an email to the administrator, recording the entire session, or writing a message to the intruder informing him that he is being monitored. The system is compatible with the Ethereal in order to offer resources of analysis and tracking.

Wireless-Snort [15] is projected as an open-source WIDS to combine with the environment Snort 2.x which is an IDS for wired networks. It allows the creation of customized rules

based in the structure of wireless packages for detecting non authorized access points, wardrivers and ad-hoc networks.

Red-M [20] has developed a wireless IDS for monitoring services in Wi-Fi and Bluetooth, identifying security weaknesses in systems that can become them vulnerable to attacks. Equipment of sensors are installed in all the covering area to monitor and prevent non authorized access of intruders or activity of supplicates APs. These equipments are controlled in a centralized form, and send information and alerts to a server of intrusion detection. Moreover, the module of countermeasures can interrupt and isolate devices of intruders that are trying to infiltrate in the network.

III. THE PROPOSED ARCHITECTURE

The proposed architecture uses a detection strategy based on anomaly for analysis, searching to identify intrusive behaviors by observing a change from normal behavior of network users. After detecting an intrusion, countermeasures are carried out in real time. This is possible thanks to the neural network which is implemented as a part of the system for determining the diagnosis of the wireless network and thus taking the countermeasures in an efficient way. The model allows taking countermeasures in a passive or active form. Countermeasures carried out in an active form are more effective in the occurrence of attacks against the integrity of the system, such as attacks of DoS. The proposed architecture is organized in modules, and shown in Figure 1.

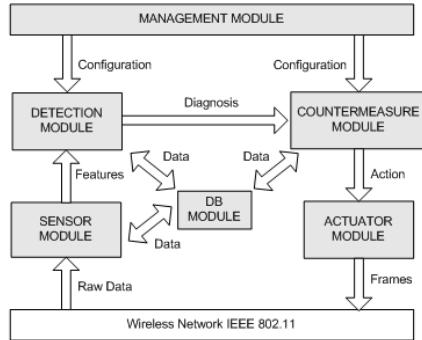


Figure 1: General Architecture of WIDS

The Sensor module is responsible for capturing all wireless network traffic. This module does a pre-formation on the captured data and sends them to a WIDS server. The data is grouped according to two criterias: by interval of 2s and by emitting source conform illustrated in Figure 2. An analysis carried through an interval of 2 seconds makes it possible to detect any alteration in the behavior in network instantaneously [3]. This interval must be flexible allowing the alteration on this part by the administrator of the system, in order to test the reaction of WIDS under different conditions. On the other hand, an analysis carried through emitting sources makes it

possible to identify the responsible for any anomalous behavior. Once the frames are grouped according to these features, the largest measures are totalized for each group and used as parameters for the determination and diagnosis of the network in one interval of time.

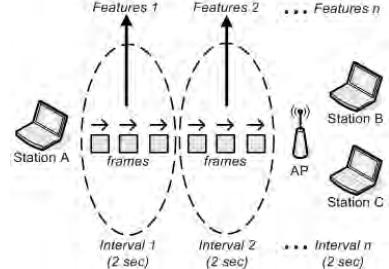


Figure 2: Mechanisms of Grouping frames

The detection module is responsible for receiving the information sent by the sensor module to carry through an analysis on these information, in order to try to identify intrusive activities occurring in the monitored network. The process of detection of intrusions is carried through the use of artificial neural networks. In case an intrusive activity is detected, the information is immediately sent to the module of Countermeasures.

The Countermeasures module is responsible for deciding which countermeasures must be taken in order to react in real time to any intrusion occurring in the monitored network.

These countermeasures are mapped in actions that are sent to the actuator module. The process of taking countermeasures is also carried through the use of artificial neural networks.

The module actuator is responsible for executing the actions determined by the Countermeasures module to react to the intrusion occurring within the network. The execution of these actions is in many cases by injecting traffic actively in the network.

The management module is responsible for devising a graphical interface for the operation and the management of WIDS. It also allows configuration and update elements of WIDS, graphical monitoring and analysis of the network and generation of reports.

The data base module is responsible for managing a repository of information registered by the sensors and the WIDS server. Moreover, this module has a basic role in adapting WIDS to a new environment providing entry information for training neural networks.

The system functioning is basically done in two phases: training and simulation. In the training phase, the system adapts itself to a new community of users, which generally presents a peculiar standard use of the wireless network. This is necessary so that the system can detect sufficiently any coherent form of change from the normal behavior of communication in the network and keeping low a rate of false

positives. The system adaptation is done by doing training with artificial neural networks that are part of the central process of detecting intruders and taking countermeasures. In the simulation phase, the system realizes a capture of traffic in the monitored network as well as the detecting intrusions, taking countermeasures and registering all necessary information in the data base for posterior analysis and reports.

IV. SOLUTION PROTOTYPE

The prototype of the solution is divided in three stages:

- Implementation of the Sensor module;
- Generation of the data for training and test Neural Network;
- Implementation of the detection module

A. Implementation of the Sensor Module

In the implementation of the Sensor Module, we have used the API (Application Program Interface) Jpcap [4] which runs on the API Libpcap [8]. The Libpcap is an independent interface system for capturing packets in the user level. It provides a portable framework for monitoring network low level under Linux systems, BSD and derivates of Unix. The Jpcap is an API for the application development for capturing packets in Java. In the hardware level, we have used an Adapter D-link DWL-G520 PCI Wireless 2,4 GHz AirPlus Xtreme G, installed in a PC with the operational system Linux Fedora and a driver MadWifi. The driver supports operation modes: station, access point, ad-hoc and monitor. The monitor mode known as promiscuous mode is used by the sensor module since it allows that the network interface captures all packets that pass through the network even those that are not destined to itself.

Figure 3 presents the diagram of classes of the Sensor Module.

The class FrameWifi defines the objects that represent the frames captured in the wireless network. Examples of this class attributes are the version, the type and the subtype of the frame, defined in the IEEE standard 802.11b. The class Station defines the objects that groups the largest measures for each station in one time interval. Examples of largest measures are: the number of pictures RTS (Request to Send) sent per station or the total duration of the communications in the network involving the station.

The classes FrameWifi and Station are associated to the class SensorRadio where it is located the main function of the sensor program. The SensorRadio class possesses three vectors which stores the captured data of the network, as well as the pre-processing that is carried through on these data.

The SensorRadio class possesses as one of its components SensorRadioGUI class that inherits the JFrame class of the package javax.swing, and defines the attributes and methods of graphical interface object of the sensor. The attributes have items of the main menu and the area of text where information of the captured traffic is shown. The methods are of configuration of the graphical interface, exhibition of a text in

the screen, screen cleaning, initiation of the mechanism of capturing packets and exhibition of largest measures totalized for each station.

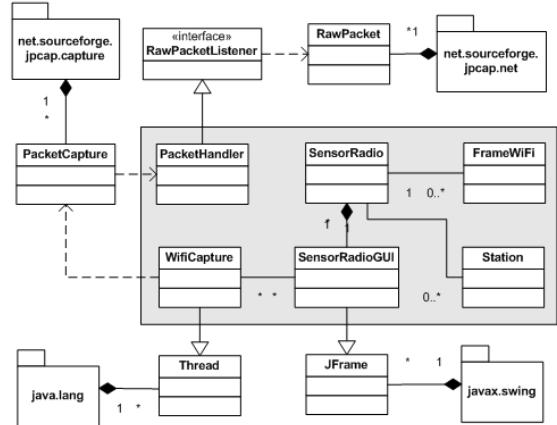


Figure 3: Class Diagram of Sensor Module

When set in motion the mechanism of capturing packets through the graphical interface, it is created and placed in execution an object of the class WiFiCapture. Knowing that this class inherits of the class Thread of the package java.lang, its objects executes concurrently in the processor, thus leaving graphical interface free to receive commands from the user, such as an order of interruption of capturing.

Internally, the class WiFiCapture makes use of the PacketCapture of the package net.sourceforge.jpcap.capture which is the class kernel of the packets capture of the package library Jpcap. It provides a high level interface for capturing packets through an encapsulation of Libpcap library.

To capture packets, an object of the class PacketCapture must register an object of the class PacketHandler which is a class that implements the RawPacketListener interface. The PacketHandler class implements the method rawPacketArrived (), through which it receives an object from the class RawPacket of the net.sourceforge.jpcap.net package which is a package for capturing raw data. This method is responsible for analyzing the received raw data in order to extract the fields of each frame and to mount corresponding the FrameWifi object.

B. Data Generation for training and testing Neural Networks

The data for training and testing neural networks are composed of normal and attack registries. Normal registries are generated through the capture of traffic of a real wireless network in which it is possible to guarantee that during the period of capture all the traffic is within the habitual standard of use of the network. This guarantee is given through a continuous monitoring of all stations accessing the wireless network by executing the Kismet [12].

The capturing environment is composed from 3 PCs, 3 notebooks, 1 palmtop and 1 AP. All of components have an

interface to access the access point. Traffic capture has lasted 1 hour approximately (between 19:00 hrs to 20:00 hrs), and has resulted in generating 21.000 (twenty one thousands) registries of network measures. During the capture period, all client stations have carried through diverse activities such as accessing Web pages, downloading of archives and presentation of internet videos.

Each registry stored in the file is composed of a set of measures referring to traffic characteristics of the emitting station within an interval 2 seconds of time in the network conform to figure 2. The attack registries are generated through traffic capture of packets in the network where three types of Denial of Service (DoS) attacks are used: Virtual Carrier Sense, Association Flood and De-authentication.

An attack of type Virtual Carrier Sense committed by an aggressor can inform a filed with a long duration making in this manner that other stations cannot get access to the canal [3]. The maximum value for NAV is 32767, or approximately 32 milliseconds in networks 802.11b. Thus, in principle, the aggressor only needs to transmit 30 times per second approximately to obstruct access to the canal. Repeating the attack several times, the aggressor can cause a degradation network performance resulting in an attack of denial of service.

The association flood attack is executed through sending multiple solicitations of authentication and association for the access point with only one source MAC address [5]. When a station is associated with an access point, this one liberates an AID (Associate Identification) for the station in a range of 1 to 2007. This value is used to communicate energy management information for the station when the same in state "power save". The access point is incapable to differentiate the authentication solicitations generated by an aggressor from those created by legitimate clients in the network. In this manner, the access is forced to process each solicitation. Eventually, the access point is going to deplete its AIDS and thus is going to be forced to dissociate stations in order to use AIDS already allocated. In practice, some access points restart after some minutes of flooding. However, this attack is sufficiently efficient to knock down a network segments or even though the entire network.

The De-Authentication attack is carried out through sending a message of authentication framework 802.11 standard that allows that clients and access points request explicitly de-authentication. Unfortunately, this message is not authenticated and does not use any type of cryptography. Consequently, the aggressor can counterfeit it, trying to play the role of the access point or client and thus can redirect any transmission to other parts. When this occurs, the access point or client can leave the state of authenticated and thus rejects all the following packets until the authentication is reestablished [3]. With a persistent repetition of this attack, a client cannot transmit nor to receive data indefinitely.

C. Implementation of Detection Module

In the Detection module prototype, we have used the MATLAB Toolbox [16] which has powerful set of tools for the project, implementation, visualization and simulation of neural networks.

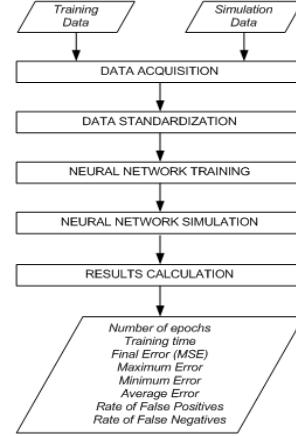


Figure 4: Class Diagram of the Sensor Module

The simulations is carried out using a computer with an AMD Athlon 64 3700+ (2,2 GHz) processor, an Asus A8V-E motherboard, 1GB memory running Microsoft Windows XP SP2. The program operates with the following stages: data acquisition, data standarzation, neural network training, neural network simulation and results calculation conform as illustrated in Figure 4.

The neural network is a multilayer of perceptrons with twenty entry units, seven neurons in the first hidden layer, five neurons in the second hidden layer and a neuron in the exit layer. The general architecture of the neural network is illustrated in Figure 5. The algorithm used for training the neural network uses the second order method of Levenberg-Marquardt (LM) implemented in MATLAB.

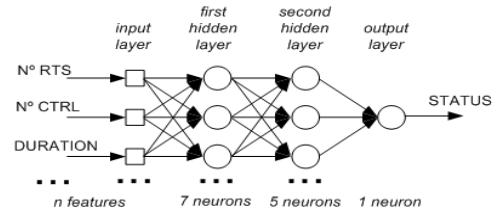


Figure 5: Neural network Architecture

The main indices calculated by the program are: number of times spent for training, time of training, MSE (Mean Square Error), maximum error, average error, minimum error, false positive rate and false negative rate.

V. SIMULATIONS AND RESULTS

Simulations are carried out in the prototype to verify the effectiveness of the neural network that is used in our solution for detecting intrusions. Such simulations have concentrated on the power of neural network generalization in order to guarantee that the system detects attacks despite the presence of different characteristics than those already known by the system. To best analyze the capacity of interpolation and extrapolation of the neural network, simulations are divided in 5 stages: interpolation, lower extrapolation, top extrapolation, general extrapolation and generalization, conform to Figure 6. In this figure, each line represents a set of available values to be divided between the sets of training and test the neural network. Stage 5 has presented a big degree of difficulty for generalizing the neural network, since in this stage the neural network is tested with values of the extremities and the center, represented for the white boxes, The training archive is composed of 10000 normal registries and 4000 attack registries of virtual carrier sense, association flood and de-authentication totaling 14000 registers. The test archive is composed of 4000 normal registries and 1600 attack registries of virtual carrier sense, association flood and def-authentication totaling 5600 registries.

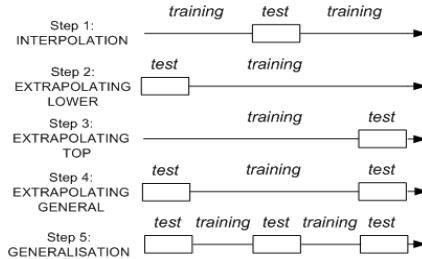


Figure 6: Simulation stages

The results obtained for a sequence of training and simulation are promising. The largest test error obtained is of 9.8902% and this which corresponds to the largest rate of false positives. The largest rate of false negatives is 5.0963%. The results average errors rate is 0.093% and the largest of the minimum errors is 8.4204e-004%. These results are very good compared to the results of similar research, in the area of intrusion detection applying techniques of artificial neural network.

VI. CONCLUSION

This work has presented an architecture for intrusion detection for wireless networks based on anomalies. The architecture employs neural networks in the processes for intrusion detection as well as for taking countermeasures in real time. To demonstrate the effectiveness of the proposed architecture, an implementation prototype is devised for the sensor device and the mechanisms of detection as well some simulations have been presented.

Conform to the results obtained, the rate of maximum error is below 9.9% for all the testes of attack combinations. The rates are compatibles with the rates of errors found in two intrusion detection systems of intruders for TCP/IP [18]. However, if we compare the rates of errors found in wireless intrusion detection system [23], the rate of our work has evidenced a gain of 5%.

ACKNOWLEDGMENT

Financial support of FAPEMA is gratefully acknowledged.

REFERENCES

- [1] AirDefense. Enterprise class wireless intrusion prevention systems: Requirements and figure of merit. Available at <http://www.airdefense.net/whitepapers/>. Access on November 2007.
- [2] AirMagnet. Manual do usuário - airagnet laptop wireless lan analyzer user guide. Available at <http://www.airmagnet.com/>. Access Jul 2008.
- [3] J. Bellardo and S. Savage. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. Proceedings of the USENIX Security Symposium, August 2003.
- [4] P. Charles. Jpcap. Available at <http://sourceforge.net/projects/jpcap/>.
- [5] K. Curran and E. Smyth. Demonstrating the Wired Equivalent Privacy (WEP) Weaknesses Inherent in Wi-Fi Networks. Information Systems Security, 15(4):17–38, Set/Oct 2006.
- [6] D. Dasgupta, J. Gómez, F. González, M. Kaniganti, K. Yallapu, and R. Yarramsetti. MMDS: Multilevel Monitoring and Detection System. Proceedings of the 15th Annual Computer Security Incident Handling Conference.
- [7] J. L. DeBoer and T. Bruinsma. Airsnare. Available at <http://home.comcast.net/jay.deboer/airsnare/>. Access Dec 2007.
- [8] B. Fenner, G. Harris, and M. Richardson. Libpcap. Available at <http://sourceforge.net/projects/libpcap/>. Access Dec 2007.
- [9] Finisar. Surveyor wireless. Access Jul 2007. Available at <http://investor.finisar.com/ReleaseDetail.cfm?ReleaseID=89597>.
- [10] S. Haykin. Redes Neurais: Princípios e Prática. Bookman, Porto Alegre, 2 edition, 2001.
- [11] T. Karygiannis and L. Owens. Wireless network security. Technical Report NIST 800-48, National Institute of Standards and Technology, USA, November 2002. Available at <http://csrc.nist.gov/publications/nistpubs/800-94/SP800-48.pdf>.
- [12] Kismet. Kismet wireless. Available at <http://www.kismetwireless.net>.
- [13] R. A. Lackey, J. and J. Goddard. Wireless intrusion detection. Technical report, IBM Global Services, 2003.
- [14] Y. Lim, T. Schmoyer, J. Levine, and H. L. Owen. Wireless Intrusion Detection and Response. Proceedings of the 2003 IEEE Workshop on Information Assurance, March 2003.
- [15] A. Lockhart. Snort-wireless project. Available at <http://www.snortwireless.org/>. Access Nov 2007.
- [16] MATLAB. The mathworks - MATLAB and simulink for technical computing. Available at <http://www.mathworks.com/products/matlab/>.
- [17] G. G. Meade. Guidelines for the development and evaluation of IEEE 802.11 intrusion detection systems (IDS)), Technical report, NSA Num 1332-005R-2005. 2005
- [18] M. Moradi and M. Zulkernine. A Neural Network Based System for Intrusion Detection and Classification of Attacks. Proceedings of 2004 IEEE International Conference on Advances in Intelligent Systems Theory and Applications, page 6, November 2004.
- [19] D. Pleskonjic. Wireless Intrusion Detection Systems (WIDS). 19th Annual Computer Security Applications Conference, December 2003.
- [20] Red-M. Taking control of wireless. Available at <http://www.red-m.com/>.
- [21] T. R. Schmoyer, Y. X. Lim, and H. L. Owen. Wireless Intrusion Detection and Response: A case study using the classic man-in-the-middle attack. IEEE Wireless Communications and Networking Conference, March 2004.
- [22] H. Yang, L. Xie, and J. Sun. Intrusion Detection Solution to WLANs. IEEE 6th CAS Symp. On Emerging Technologies: Mobile and Wireless Comm., June 2004.
- [23] L. Yanheng, D. Tian, and B. Li. A wireless intrusion detection method based on dynamic growing neural network. 1st International Multi-Symposium on Computer and Computational Sciences, 2006.

A highly parallel scheduling model for IT change management

Denilson Cursino Oliveira, Raimir Holanda Filho

University of Fortaleza- UNIFOR

denoliveira@edu.unifor.br, raimir@unifor.br

Abstract – The IT governance is defined as a set of rules, activities and processes that fits with the IT company strategy, ensuring the return provide by IT in terms of services and maintainability of the organization. The change management shows as a sensible point inside of the IT governance and the main one activity of change management is to build the better scheduling, being the scheduling definition the main activity. This scheduling definition consists of the allocation of changes to each change window. The current literature argues about sequential implementation of the changes allocated into each change windows, but not a sequential and parallel implementation. In this paper we optimize the scheduling presenting a model of parallel implementation of changes, resulting in an higher number of changes in each window and consequently reducing the time to implement all changes.

I. INTRODUCTION

The IT governance is no more a refined way to match the IT processes, activities and business objectives, it became Law. To formalize with governance process, were established management frameworks recognized and applied in the world, like ITIL and COBIT. Many points, like best practices of change management, are detailed and measured by these two frameworks.

The IT information library (ITIL) [2] consists of a set of best practices that determine how the IT infrastructure of a company is organized. The library ITIL is an IT service management framework that promotes an efficient management of IT changes in order to minimize any impact upon IT services.

Control Objectives for Information and related Technology (COBIT, [1]) promotes a management and control of information with use of measures, performance indicators and maturity models. Cobit includes many processes that describe good practices. We describe how we use the process p05 (manage the IT investment) of COBIT to determine the set of changes do be done.

The solutions proposed in this paper are in accordance with the principles of Business-Driven IT Management (BDIM) [3]. BDIM has brought the use of metrics over the IT governance, establishing detailed planning, mapping quantitatively the IT governance and business performance. BDIM promotes a stricter control, allowing previous ratings on the shares held on IT, measuring risks, costs and return of investment.

On this paper, we propose a contribution to resolve an issue not yet discussed in the current state-of-the-art: do a parallel implementation of changes of a change window.

II. RELATED WORK AND MOTIVATION

The term BDIM was used for first time in [5] and in [4] where the terms were thoroughly reviewed, showing that application of the concepts, processes and metrics of BDIM is a powerful tool to promote better decision-making, return of investments and minimizing the impact that IT changes imposes on business. In [4] are presented an optimization of scheduling of IT changes, showing mathematical concepts to determine the loss before change implementation, cost of changes implementation over a set of changes attached to a change window over a sequential implementation of this set of changes.

All claims and improvements attributed to the studies of BDIM offers a primacy in IT management, enabling an automated response over the IT changes and the real impact. These studies follow two premises: The first one is to reduce the impact of IT changes; the second is to improve the goals of business.

Our model comes to optimize the establishment of change scheduling allocated to a change window. We will present the opportunity to have a highly parallel implementation of a set of changes assigned to a change window. The two main expected objectives are: increase the amount of changes attributed to each change window and consequently decrease the amount of change windows to implement this set of changes.

III. THE PROPOSED MODEL

In this section we will describe all steps to find changes to be implemented and how our model builds the scheduling to be allocated in the window.

A. Determining the set of changes

The main object of work is to determine the set of changes to be implemented in a certain infrastructure and to establish the best scheduling for these changes, we need to follow some steps.

The model presented in this paper follows the good processes and activities included in ITIL, COBIT and the

current state-of-the-art of BDIM. The previous steps to determine the set of changes are represented in figure.1.

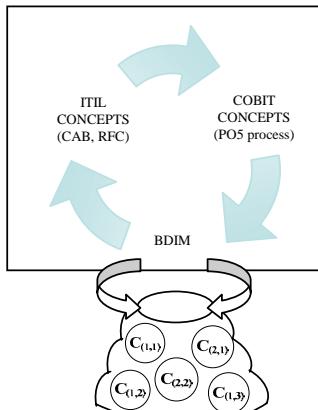


Figure 1. Steps to find the set of changes

The good practices of ITIL such as Change Advisory Board (CAB) [2], Requests for Changes (RFC) help to direct all information to be raised about which changes to be made.

The CAB is a group of people that advises the change manager in the assessment, prioritization and scheduling of Changes. This board is usually compounded of representatives from all areas like change manager, IT service provider, business directors and third parties such as suppliers. Meeting should be held with all these stakeholders above to develop a RFC document.

The Request For Change (RFC) is a document that includes details of the proposed change, and may be recorded on paper or electronically. This document includes a proposal of which set changes could be done, cost of each change, effect of implementation and not implementation of each change, return of investments and a estimating a date to begin.

The good practices of COBIT come to formalize all information that will form the RFC document. One of the processes of COBIT is PO5 (manage the IT investments). The PO5 has the main objective of work with stakeholders to identify and control the total costs and benefits within the context of the IT strategic, tactical plans and initiate back-out-plan where needed.

The metrics established by BDIM [4] helps to find answers to the questions made by the five activities of PO5 COBIT process. These activities formalize creation of a financial management framework, prioritization of changes, cost management and benefit managements. The formalization of the partnership brought by the activities of PO5 and BDIM help to create the RFC document.

The relationship between the practices of ITIL and COBIT and the answers provided by BDIM metrics for

the questions of these practices are executed until have a set of changes accepted by stakeholders.

B. Scheduling of change in change window

In this section we detail the steps to be followed until the allocation of a scheduling of changes in a Change window.

The first step is to build the change dependency definition. Like we can find in RFC document, each change is formed by a set of characteristics and detailed in RFC document as the cost to drop the service, cost of implementation and not implementation, date to begin, etc. The change dependency is one characteristic to be analyzed just after of establishment of the set of change. In our work we present the concepts of direct and indirect dependency for the changes of set of changes. We represent each change by $C_{i,j}$ and the set of changes by $SC=\{C_{i,j}, C_{i+1,j+1}, \dots, C_{i+n,j+m}\}$. The determination of direct and indirect dependency must be done by IT staff members.

The second step will define the change windows allocation. This step takes care of find change windows out of one or more client. The time of this change window is negotiated with client, considering a time that have less impact for business objectives. If one or more changes affect more than one client, should be finding change windows considering these clients.

The last step takes care about the change scheduling. In this step, we already have a set of changes, with all change dependencies and change windows defined to build the possible scheduling, ever with objective to have less business impact.

C. Formalizing the model

In this topic we formalize all steps and rules for applying our model. Initially we need keep in mind that we have the set of changes do be done represented by $SC=\{C_{i,j}, C_{i+1,j+1}, \dots, C_{i+n,j+m}\}$ and we need to choose some of these changes to create the best scheduling. These scheduling are allocated in one of windows previously established represented by $W=\{w_1, w_2, \dots, w_n\}$. Each scheduling have a total time ΔS formed by the sum of implementation time of each change that are part of it, where allocated to a window W_n with a time Δw , we must have ($\Delta S \leq \Delta w$).

Now we can begin to present the steps of our model, dividing them in concepts about direct and indirect change dependences, rules to build an array of changes and rules of allocation of changes on array.

1) Concepts about indirect and direct dependences

We need of formal concepts to determining when a change will have one or more direct dependence and/or indirect dependence, they are:

- Direct dependence: All set of change $C = \{C_{(i,j)}, \dots, C_{(i-1,j-1)}, C_{(i,j)}\}$, where the value i , where ($\forall i \in C_{(i,j)} \in C$) is equal and the growing order values of j represented by $J=\{1, 2, 3, \dots, m\}$, which $C_{(i,j)}$ depends on $C_{(i,(j-1))}$. For illustrate, If we have three changes to be implemented $SC=\{C_{(1,1)}, C_{(1,2)}, C_{(1,3)}\}$. We have the change $C_{(1,2)}$ depends on $C_{(1,1)}$, $C_{(1,3)}$ depends on $C_{(1,2)}$ and by equivalence ($C_{(1,2)}$, $C_{(1,3)}$) depends on $C_{(1,1)}$.

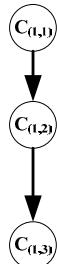


Figure 2. Representation of direct dependences

- Indirect dependence: Defined by all set of changes represented by $ID=\{C_{(i,j)}, \dots, C_{(i,j)}\}$, where $i=\{1, 2, 3, \dots, n\}$ and $j=\{1, 2, 3, \dots, m\}$ carries a dependence on $C_{(i,j)}$, where $((\forall i \in C_{(i,j)}) \neq (\forall i \in C_{(i,j)} \in ID))$. We can give an example: If we have a Set of changes line figure 4, we will have $ID=\{C_{(2,2)}\}$, where just $C_{(2,2)}$ carries an indirect dependence on $C_{(1,2)}$.

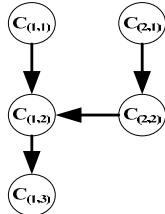


Figure 3. Representation of indirect dependences

If ID have more than one $C_{(i,j)}$ with the same value of i , we represent this changes by $R=\{C_{(i,j)}, \dots, C_{(i,j)}\}$, where R is growing by values of j , we only to consider the indirect dependence of $(C_{(i,j)} \in R)$ with bigger value of j . The figure 4 illustrates this case, where just to consider the indirect dependence of $C_{(2,3)}$ over $C_{(1,2)}$.

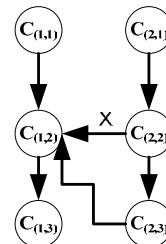


Figure 4. Indirect dependences with same value of i .

2) Rules to build an array of changes

Our model uses an array to allocate the set of changes. It will become easy to apply and to understand the model. We have two rules to formalize this step, they are:

- 1st rule: All $C_{(i,j)}$ are allocated in a array, which $I=\{1, 2, 3, 4, \dots, n\}$ represent the columns and $J=\{1, 2, 3, 4, \dots, m\}$ represent the lines.

The representation of i to columns comes to facilitate the learning, since we can allocate all the changes with direct dependence by columns.

- 2nd rule: The changes are allocated in a position respectively equal the values $(i, j) \in C_{(i,j)}$, where $C_{(i,j)}$ haven't indirect dependency. If any change have an indirect dependence, must follow the rules of allocation of changes with indirect dependence on array described in next step.

3) Rules of allocation of changes with indirect dependence on array

The allocation of changes on array follow the rules described in item B until find anyone with an indirect dependence. In this moment we use the rules shown below.

- 1st rule: Considering an set of changes $T=\{C_{(i,j)}, C_{(i,j)}, \dots, C_{(i,j)}\}$, where $i=\{1, 2, 3, \dots, n\}$ and $j=\{1, 2, 3, \dots, m\}$ each one have one or more indirect dependences, the application of second rule must follow obligatorily the increasing ordinance of the values of j , where $((j \in C_{(i,j)}) \in T)$.

- 2nd rule: All changes $C_{(i,j)}$ that have one or more indirect dependences represented by $K=\{C_{(i,j)}, C_{(i,j)}, \dots, C_{(i,j)}\}$, where $i=\{1, 2, 3, \dots, n\}$ and $j=\{1, 2, 3, \dots, m\}$, get the values of $j \in K$, forming a growing set $U=\{j_1, j_2, j_3, \dots, j_m\}$, where $\forall j$ the value $(j_m > j_{m-1})$, the change $C_{(i,j)} \rightarrow C_{(i,(j_m+1))}$, and will be allocated in a position of the array respectively equal the values $(i, j) \in C_{(i,(j_m+1))}$. To have the application of this rule, we must to respect the concept of indirect dependence and have $((j \in C_{(i,j)}) \leq (\forall j \in k))$.

After application of second rule, we take the difference between values j , where $D=((j \in C_{(i,(j_m+1))}) - C_{(i,j)})$.

3rd rule: After application of second rule on $C_{(i,j)}$ and it carries a direct dependency over a set of changes $V=\{C_{(i,j+1)}, C_{(i,j+2)}, C_{(i,j+3)}, \dots, C_{(i,j+m)}\}$, we adds the value of variable D to each $j \in V$. The application of this rule must be done immediately after second rule.

We will use the example of figure 5 to explain the interaction of these three described rules. Here we have a change $C_{(1,2)}$ that have an indirect dependence $T=\{C_{(2,2)}\}$, and following the rules of the model we get the values of $J \in T$ represented by $U=\{2\}$. Now we catch the bigger value of U to get $C_{(1,2)} \rightarrow C_{(1,2+1)}$. The new position of $C_{(1,2)}$ will be $C_{(1,3)}$.

Automatically we need to apply the 3rd rule. We check that $C_{(1,2)}$, which assumed a new position $C_{(1,3)}$, after application of 2nd rule, brings direct dependency. We get the value of variable D, which will be $D=(3-2)$. Now we can determine new position of the dependent change of $C_{(1,2)}$. The position of $C_{(1,3)}$, will be $C_{(1,3+D)}$, where $D=1$ we have $C_{(1,3)} \rightarrow C_{(1,4)}$.

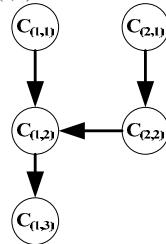


Figure 5. Representation of indirect dependences

After the application of the rules in the set of changes shown in figure 5, we can determine the final array of changes, represented in table 1.

Table 1. Array of changes

		I	
		1	2
J	1	$C_{(1,1)}$	$C_{(2,1)}$
	2		$C_{(2,2)}$
	3	$C_{(1,3)}$	
	4	$C_{(1,4)}$	

The Rules of our model are applied in a cyclical form, until hasn't motive to apply them. Is an essential point out that all indirect dependences are persistent because we can have one indirect dependence at any point of the cyclical application out of the frame rules and, in other point, these same indirect dependence is framing. Give us the chance to show one example: In figure 6 we have an change $C_{(2,3)}$ depends on $C_{(1,2)}$ but is not in frame to application of rules but after rules application over dependence of $C_{(2,3)}$ in $C_{(1,2)}$, where $C_{(1,2)} \rightarrow C_{(1,3)}$, we could apply the rules over dependence of $C_{(1,3)}$ over $C_{(2,2)}$. This example shows the evidence about the indirect

dependence persistence between the cyclical rules application.

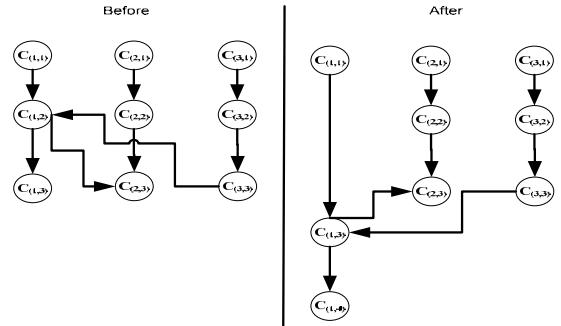


Figure 6. Representation of one cycle of rules

4) Rules of implementation of changes

Here we present the final object of our model, that will by an array of changes where we have all set of changes to be implemented. We define which sequence the set of array will be implemented with three rules shown below:

1st rule: The application of a set of changes $SC=\{C_{(i,j)}, C_{(i+1,j+1)}, \dots, C_{(i+n,j+n)}\}$ will follow the growing order of the values of J.

2nd rule: All changes with the same value i must to be implemented in a sequential mode.

3rd rule: All changes with the same value J could be implemented in a parallel mode.

Now our model is formalized and we are able to allocate each change to an available change window. We assume that cyclical application of our model are applied, the window time is sufficient to carry out all set of changes, the implementation time will be of 1 hour to each change and the set of changes will be the same of table 2. With these premises we will get a change window of figure 7.

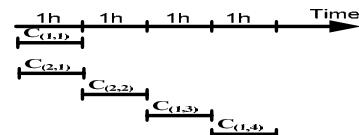


Figure 7.Implementation of change of a change window

IV. VALIDATION

This section have the objective of present a real problem to apply our model and determine how he contributes if compared with sequential application of changes in a change windows which is covered by the current state of the art.

Our scenario happens in a Forum of Justice, where need to implement change of your infrastructure of routers, switches and structure cable. In this, we already

have determined the set of change, the change dependences and the changes windows. To turn the validation more comprehensible, we going to admit 1 hour to implementation time of each change. A Set of changes are represented in figure 8 below.

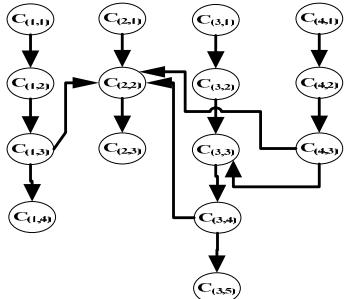


Figure 8. Set of changes to be implemented

As a demonstration, we will show the application of our model over the set of changes shown in figure 8 through a cyclical rules application.

1st cycle: applying the first rule of allocation of changes with indirect dependences on array, we have some changes with two indirect dependence represented by $T=\{C_{(2,2)}, C_{(3,3)}\}$, we will apply the second and third rule in change $C_{(2,2)}$.

Applying the second rule in $C_{(2,2)}$ depends on $K=\{C_{(1,3)}, C_{(4,3)}, C_{(3,4)}\}$, we get the ordered values of $(j \in K)$ represented by $U=\{3,4\}$, we will have $C_{(2,2)} \rightarrow C_{(2,5)}$.

Applying the third rule, the change $C_{(2,2)}$ carries direct dependency over $V=\{C_{(2,3)}\}$, we adds the value of $D=5-2$ to each value of $(j \in V)$. The result is $C_{(2,3)} \rightarrow C_{(2,6)}$.

After the application of the second rule and, if necessary of the third rule, we close the first cycle of application. The final result is shown in figure 9.

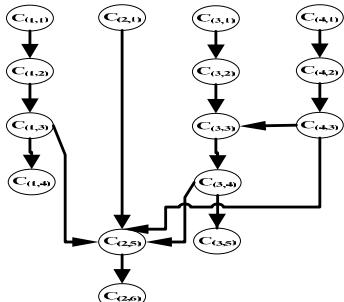


Figure 9. Set of changes after first cycle

2nd cycle: applying the first rule in this second cycle, the changes with indirect dependence are $T=\{C_{(2,5)}, C_{(3,3)}\}$, we will apply the second and third rule in change $C_{(3,3)}$.

Beginning the applying of the second rule in $C_{(3,2)}$ depends on $K=\{C_{(4,3)}\}$, we get the ordered values of $(j \in K)$ represented by $U=\{3\}$, we will have $C_{(3,3)} \rightarrow C_{(3,4)}$.

Applying the third rule, the change $C_{(3,3)}$ carries direct dependency over $V=\{C_{(3,4)}, C_{(3,5)}\}$, we adds the value of $D=4-3$ to each value of $(j \in V)$. The result is to this two changes is $C_{(3,4)} \rightarrow C_{(3,5)}$ and $C_{(3,5)} \rightarrow C_{(3,6)}$

To ends this cycle, after the application of the second rule and, if necessary of the third rule, we close the second cycle of application. The final result is shown in figure 10.

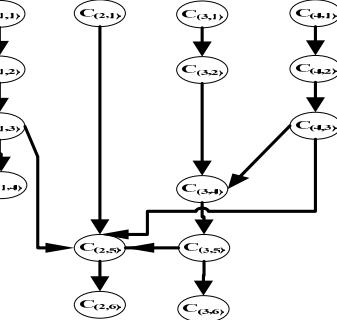


Figure 10. Set of changes after second cycle

3rd cycle: applying the first rule of allocation of changes with indirect dependences on array in this third cycle, the changes with indirect dependence are $T=\{C_{(3,4)}, C_{(2,5)}\}$. Normally the application will be in $C_{(3,4)}$ but we not apply the second rule because $((j \in C_{(3,4)}) \leq (\forall j \in k))$ is false, where $k=\{C_{(4,3)}\}$. In this case, apply the second and third rule in change $C_{(2,5)}$.

Applying the second rule in $C_{(2,5)}$, and using the argument of implementation of the second rule, where $((j \in C_{(2,5)}) \leq (\forall j \in k))$ must be true, we have just one element, where $k=\{C_{(3,5)}\}$, get the ordered values of $(j \in K)$ represented by $U=\{5\}$, we will have $C_{(2,5)} \rightarrow C_{(2,6)}$.

Applying the third rule, the change $C_{(2,5)}$ carries direct dependency over $V=\{C_{(2,6)}\}$, we adds the value of $D=4-3$ to each value of $(j \in V)$. The result is $C_{(2,6)} \rightarrow C_{(2,7)}$.

After the application of the second rule and, if necessary of the third rule, we close the third cycle of application. The final result is shown in figure 11.

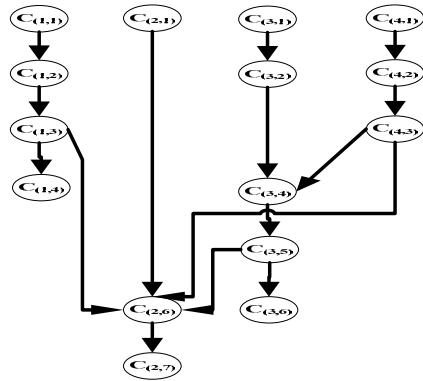


Figure 11. Set of changes after third cycle

After of this third, we haven't anyone more application of cycle of rules because all indirect dependence turn the sentence ($(j \in C_{(i, j)}) \leq (\forall j \in k)$) false. In this moment the changes are allocated on array following the rules of allocation of changes with indirect dependence on array, the result is shown in table 2.

Table 2. Array of changes

		I			
		1	2	3	4
J	1	C_{(1,1)}	C_{(2,1)}	C_{(3,1)}	C_{(4,1)}
	2	C_{(1,2)}		C_{(3,2)}	C_{(4,2)}
	3	C_{(1,3)}			C_{(4,3)}
	4	C_{(1,4)}		C_{(3,4)}	
	5			C_{(3,5)}	
	6		C_{(2,6)}	C_{(3,6)}	
	7		C_{(2,7)}		

Following the rules of implementation of changes we have an implementation of a change windows with the possibility implementation of change in sequential and concurrently form. The result is show in figure 12.

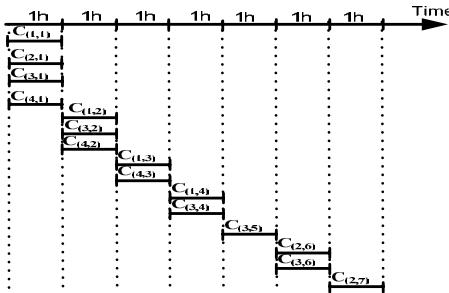


Figure 12. Change windows

Through the use of our model, the implementation of this set of changes will be able to be carried out in seven hours. If this same set of changes was implemented only in the sequential form, the necessary time would be fifteen hours. Our model offers an economy of time and a possible reduction of the quantity of change windows.

V. CONCLUSION AND FUTURE WORK

Our model was defined to work with the changes dependences of a set of changes to build a parallel implementation. It reduce the time of a set of changes across implementation of a parallel model that optimized the scheduling allocated to each window and it turn possible the reduction of the number of change windows.

Our future work will check an autonomic allocation of this set of changes in different change window to optimize the total time of each change window.

REFERENCES

- [1] IT Governance Institute, " COBIT 4.1rd Edition, 2006, www.isaca.org/cobit.
- [2] IT Infrastructure Library (ITIL 3.0), www.itil-officialsite.com.
- [3] Sauvé, J., Moura, A., Sampaio, M., Jornada, J. and Radziuk, E., "An Introductory Overview and Survey of Business-Driven IT Management", in Proceedings of the 1st IEEE / IFIP International Workshop On Business-Driven IT Management, in conjunction with NOMS 2006, Vancouver, Canada, pp. 1-10.
- [4] Rebouças, R., Sauvé J., Moura A., Bartolini C., Trastour D., "A Decision Support Tool for Optimizing Scheduling of IT Changes", 10th IFIP/IEEE Symp. On Integrated Mgmt, 2007.
- [5] Machiraju, V., Bartolini, C. and Casati, F., "Technologies for Business-Driven IT Management", in "Extending Web Services Technologies: the Use of Multi-Agent Approaches", edited by Cavedon, L., Maamar, Z., Martin, D. and Benatallah, B., Kluwer Academic, 2005, pp.1-28.
- [6] Sauvé, J. P., Marques, Filipe Teixeira, Moura, José Antão Beltrão, Sampaio, Marcus Costa, Jornada, João, Radziuk, Eduardo Optimal Design of E-Commerce Site Infrastructure from a Business Perspective In: Hawaii International Conference on System Sciences, 2006, Waikoloa, Hawaii. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). Washington DC: IEEE Computer Society, 2006. v.8. p.178.3 - 178.3
- [7] Bartolini, C., Sauvé, J. and Sahai, A. (eds.), "Information Technology Management from a Business Perspective. Proceedings of the 1st IEEE / IFIP International Workshop on Business-Driven IT Management (collocated with NOMS 2006), Vancouver, Canada, April 2006
- [8] Abrahão, B., Almeida, V., and Almeida, J., "A Self-Adaptive SLA-Driven Capacity Management Model for Utility Computing", Elsevier Service, 2005.
- [9] Aib, I., Sallé, M., Bartolini, C. and Boulmakoul, A., "A Business Driven Management Framework for Utility Computing Environments", HP Labs Bristol Tech. Report, 2004-171.
- [10] B. Abrahão, V. Almeida, and J. Almeida, "Self-adaptive SLA-driven capacity management for internet services," in 17th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management,DSOM 2006, 2006.
- [11] Brown, A.B., Keller, A., Hellerstein, J.L., "A model of configuration complexity and its application to a change management system", in: Integrated Network Management, 2005. IM 2005, pp. 631- 644.

Design and Implementation of a Multi-sensor Mobile Platform

Ayssam Elkady

School of Engineering

University of Bridgeport

Email: aelkady@bridgeport.edu

Tarek Sobh

School of Engineering

University of Bridgeport

Email: sobh@bridgeport.edu

I. ABSTRACT

In the last several years, mobile manipulators have been increasingly utilized and developed from a theoretical viewpoint as well as for practical applications in space, underwater, construction, and service environments. Our mobile manipulator RISCbot, is comprised of a manipulator arm mounted on a motorized mobile base wheelchair. The work presented in this chapter explores the use of multi-sensor for combining measurements from ultrasonic and infrared sensors for mobile manipulator navigation and obstacle avoidance. Furthermore, we deal with the problem of controlling of a mobile manipulator via sensor fusion in order to reduce the uncertainty in localization and obstacle avoidance. Sensor fusion is used by combining and integrating data gathered from sensory information provided by ultrasonic and infrared sensors to enhance the quality of information provided to RISCbot.

II. INTRODUCTION

A mobile manipulator is a manipulator mounted on a mobile platform with no support from the ground. A mobile manipulator offers a dual advantage of mobility offered by the platform and dexterity offered by the manipulator. For instance, the mobile platform extends the workspace of the manipulator. We are developing and constructing a mobile manipulation platform called RISCbot . The prototype of the RISCbot is shown in figure 1.

Sensor fusion has been an active area of research in the field of computer vision and mobile robotics. Sensor fusion can be defined as a method for conveniently combining and integrating data derived from sensory information provided by various and disparate sensors, in order to obtain the best estimate for a dynamic system's states and produce a more reliable description of the environment than any sensor individually. Sensor fusion algorithms are useful in low-cost mobile robot applications, where acceptable performance and reliability is desired, given a limited set of inexpensive sensors such as ultrasonic and infrared sensors. Depending on the modalities of the sensors, sensor fusion can be categorized into two classes (as described in [1]), sensor fusion using complementary sensors and sensor fusion using competing sensors. Complementary sensors consist of sensors with different modalities, such as a combination of a laser sensor and a digital camera. In contrast to complementary sensors,

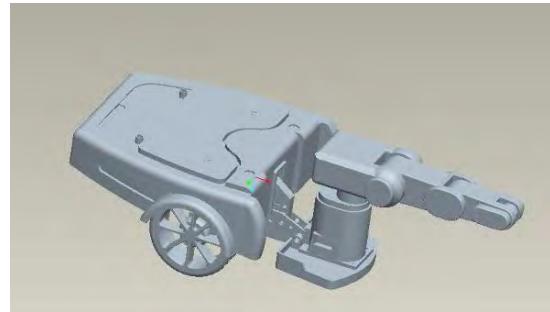


Fig. 1. A prototype of the RISCbot.

competing sensors are composed of sensors suit which have the same modality, such as two digital cameras which provide photographic images of the same building from two different viewpoints.

Sensor fusion has some critical problems such as the synchronization of sensors. Different sensors have different resolutions and frame rates so the sensors need to be synchronized before their results can be merged by fusing the data from multiple sensors and presenting the result in a way that enables autonomous robot to perceive the current situation quickly. Sensor fusion is commonly used to reduce uncertainty in localization, obstacle avoidance, and map building. In this paper, we discuss sensor fusion for navigation and obstacle avoidance, describe our mobile manipulation platform , and present our results.

III. DESIGN SPECIFICATIONS

A. Data Acquisition

In our project, we used a data acquisition module called *Data Translation DT9814* which is a low cost USB data acquisition module that offers 24 analog input channels, 2 analog outputs channels, and one 32-bit counter timer to accommodate most applications. Furthermore, it provides a resolution of 12 bits for both the analog input and analog output subsystems, and input throughput up to 50 kHz. The analog signal range is from -10 Volt to 10 Volt. This module also provides the following features: (as described in [14])

- One 32-bit counter/timer channel.
- Internal and external A/D clock sources.

- Internal and external A/D trigger sources.
- No external power supply required.
- It supports a 32-location channel-gain list. You can cycle through the channel-gain list using continuous scan mode or triggered scan mode.
- It can be connected directly to the USB ports of a computer.

B. Sensors

There are various sensor types used for measuring distances to the nearest obstacle around the robot for navigation purposes such as ultrasonic and infrared sensors. The sensors can be classified as proprioceptive/exteroceptive and passive/active [4]. Proprioceptive sensors measure values internal to the robot such as motor speed, wheel load, and battery voltage. Exteroceptive sensors acquire information from the robot environment such as distance measurements. Passive sensors measure ambient environmental energy entering the sensor; such as temperature sensors, and microphones. Active sensors emit energy into the environment, then measure the environmental reaction.

There are two important concepts to understand when analyzing any sensor; sensitivity and range. A sensing device reacts to varying levels of some physical stimulus by outputting a characteristic voltage (or current, frequency, etc.). Sensitivity is a measure of the degree to which the output signal changes as the measured quantity changes. Let's call the sensor output r and the measured physical quantity z . The sensitivity S can be computed from equation 1.

$$\frac{\Delta r}{r} = S \frac{\Delta z}{z} \quad (1)$$

Where Δz is a small change in the measured quantity and Δr is related to a small change in the sensor response.

1) *Sonar Sensor:* A sonar sensor measures the time of flight of a sonar pulse to travel to the object in front of this sensor and the time to be received again. Given the speed of the sound, one can compute the distance to the object.

The distance d to the nearest object within the sonar cone can be computed from equation 2. Where t is the elapsed time between the emission of the sonar signal and the reception of its echo and C is the speed of the sonar signal in the medium (the speed of the sound (m/s) in dry air is given approximately by equation 3 where T_c is the Celsius temperature)

$$d = \frac{Ct}{2} \quad (2)$$

$$C \approx 331.4 + 0.6 \times T_c \quad (3)$$

There are some uncertainties associated with readings from sonar sensors. The uncertainties are due to:

- The exact position of the detected object is unknown because the computed distance d in equation 2 could be anywhere within the sonar cone.
- Specular reflections problem occurs when the sonar beam hits a smooth surface at a shallow angle and is therefore not reflected back to the robot.

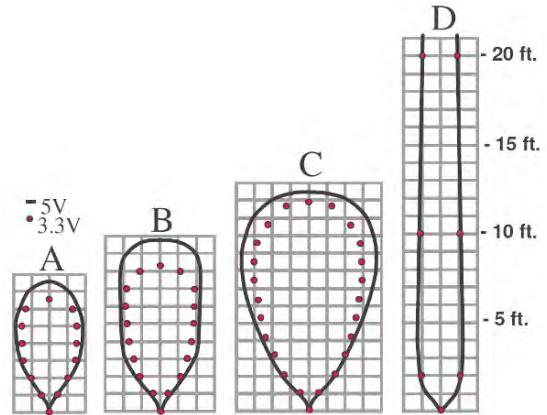


Fig. 2. Beam characteristics (As described in [2]).

- Crosstalk can occur when an array of sonar sensors is used.

We used the *LV – MaxSonar® – EZ0™* ultrasonic sensors. As described in [2], they can detect objects from 0-inches to 254 inches (6.45 meters) and provides sonar range information from 6-inches out to 254-inches with 1-inch resolution. Objects from 0-inches to 6-inches range as 6-inches. They are low cost sonar ranger actually consisting of two parts: an emitter, which produces a 42kHz sound wave; and a detector, which detects 42kHz sound waves and sends an electrical signal back to the microcontroller. Readings can occur up to every 50 ms, (20-Hz rate) and designed for indoor environments. The advantage of using ultrasonic sensors is that they can detect obstacles with high confidence especially when the object is well defined (i.e., located perpendicular to the sonar axis and has good ultrasonic reflectivity). As described in [2], the sample results for measured beam patterns are shown in figure 2 on a 12-inch grid. The detection pattern is shown for;

- 0.25-inch diameter dowel, note the narrow beam for close small objects.
- 1-inch diameter dowel.
- 3.25-inch diameter rod, note the long controlled detection pattern.
- 11-inch wide board moved left to right with the board parallel to the front sensor face and the sensor stationary. This shows the sensor's range capability.

2) *Infrared Proximity Sensor:* Infrared sensors operate by emitting an infrared light, and detecting any reflection off surfaces in front of the robot. If the reflected infrared is detected, it means that an object is detected. On the other hand, if the reflected infrared is absent, it does not mean that there is no object in front of the infrared sensor because certain darkly colored objects are invisible to infrared signal. Therefore, infrared sensors are not absolutely safe to use alone in obstacle avoidance applications and they can not be used for range measurements. We have used an infrared proximity

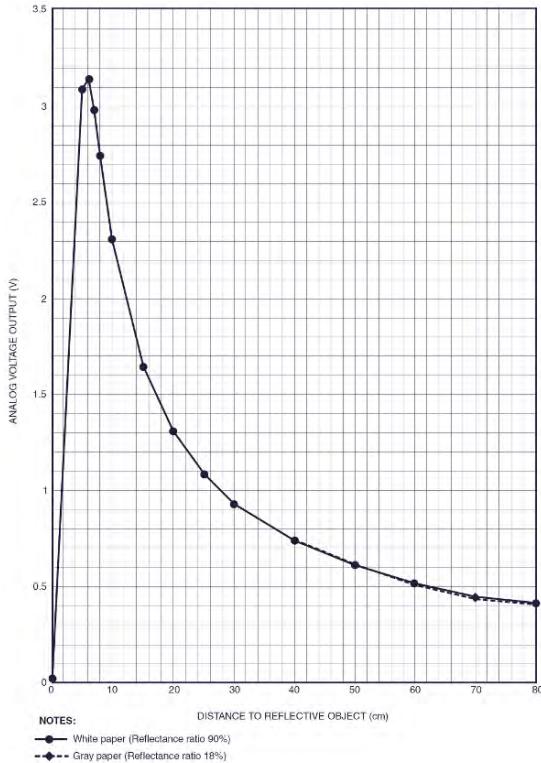


Fig. 3. Analog output vs. distance to reflective object (As described in [7]).

sensor - Sharp GP20A21YK. As described in [7], this sensor has an analog output that varies from 3.1V at 10 cm to 0.4V at 80 cm as shown in figure 3. The analog sensor simply returns a voltage level in relation to the measured distance. As shown in figure 3, it is clear that the sensor does not return a value linear or proportional to the actual distance because the intensity of the infrared signal is inversely proportional to the square of the distance. Therefore, the infrared signal falls rapidly as the distance increases.

C. Jazzy 1122 Wheelchair

As described in [3], the jazzy wheelchair has two main assemblies: the seat and the power base as described in figure 4. Typically, the seating assembly includes the armrests, seatback, and controller. The power base assembly includes two drive wheels, two anti-tip wheels, two rear caster wheels, and a body shroud. In our project, we remove the armrests and seatback as shown in figure 5.

The specifications of the Jazzy 1122 wheelchair are described in table 1. The jazzy 1122 wheelchair also provides the following features: (as described in [3])

- 1) Active-Trac Suspension: The wheelchair is equipped with Active-Trac Suspension (ATS) to be able to traverse different types of terrain and obstacles while maintaining

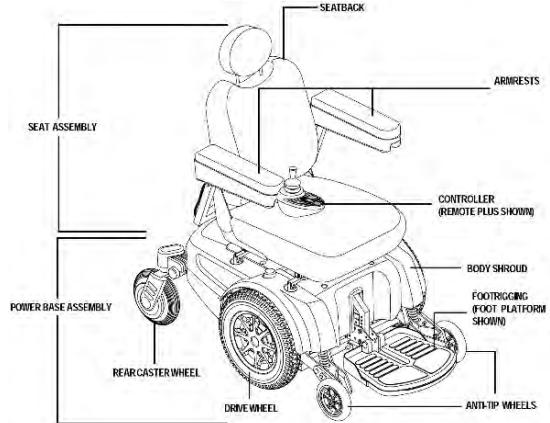


Fig. 4. The Jazzy 1122 (As described in [3]).



Fig. 5. The RISCbot base.

smooth operation. With ATS, the front anti-tip wheels work in conjunction with the motor suspension to maneuver over obstacles. As the front anti-tip wheels come in contact with an obstacle, the front anti-tip wheel assembly is drawn upward. At the same time, the motors are forced downward. This allows the motors to push the wheelchair over an obstacle.

- 2) Rear Suspension: The wheelchair is equipped with a rear suspension system to work in conjunction with the ATS and is designed to maintain a smooth ride when driving over rough terrain and up and down curbs.

IV. NAVIGATION AND OBSTACLE AVOIDANCE

A prerequisite task for the autonomous mobile robot is the ability to detect and avoid obstacles given real-time sensor readings. Obstacle avoidance is a crucial issue in robot's navigation. Given partial knowledge about its environment and a goal position or a series of positions, navigation encompasses

TABLE I
SPECIFICATIONS OF THE JAZZY 1122 WHEELCHAIR [3].

Suspension:	ATS and rear suspension
Drive Wheels:	14 in., pneumatic, center-mounted
Caster Wheels:	8 in., solid, rear-articulating
Anti-tip Wheels:	6 in., solid, front-mounted
Maximum Speed:	Up to 6 mph
Brakes:	Intelligent Braking, electronic regenerative, disc park brake
Drivetrain:	Two motor, mid-wheel
Batteries:	Two 12-volt, Group 24 batteries
Component Weights:	Base: 129 lbs. Seat: 40 lbs. (standard seat). Batteries: 53.5 lbs.

the ability of the robot to act based on its knowledge and sensor values so as to reach its goal positions as efficiently and as reliably as possible. The obstacle may be defined as any object that appears along the mobile robot's. The techniques used in the detection of obstacles may vary according to the nature of the obstacle. The resulting robot motion is a function of both the robot's sensor readings and its goal position. The obstacle avoidance application focus on changing the robot's trajectory as informed by sensors during robot motion. The obstacle avoidance algorithms that are commonly used can be summarized as the following: (as described in [4])

- **The bug algorithm:** The basic idea is to follow the easiest common sense approach of moving directly towards the goal, unless an obstacle is found. If an obstacle is found, the obstacle is contoured until motion to goal is again possible. In [4], two approaches are described; Bug1 and Bug2. In Bug1 Algorithm, the robot fully circles the object first, then departs from the point with the shortest distance toward the goal. This approach is very inefficient but it guarantees that the robot will reach any reachable goal. In Bug2, the robot will follow the object's contour but it will depart immediately when it is able to move directly toward the goal.
- **Tangent Bug:** As described in [8], tangent bug algorithm is a variation of the bug algorithm. The robot can move more efficiently toward the goal also go along shortcuts when contouring obstacles and switch back to goal seeking earlier. In many simple environments, tangent bug approaches globally optimal paths.
- **Artificial Potential Fields:** The artificial potential fields (APF) is proposed by Khatib in [9]. The robot is considered as a moving particle in a potential field generated by the goal and by the obstacles that are presented in the environment. In APF method, the robot immersed in the potential field is subject to the action of a force that drives it to the goal. This approach uses repulsive potential fields around the obstacles (and forbidden regions) to force the robot away and an attractive potential field around goal to attract the robot. A potential field can be viewed as an energy field and so its gradient, at each point, is a force. Consequently, the robot experiences a generalized force equal to the negative of the total

potential gradient. This force drives the robot towards its goal while keeping it away from the obstacles (it is the action of a repulsive force that is the gradient of the repulsive potential generated by the obstacles). However, There is a major problem with the APF approach because the local minima can trap the robot before reaching its goal. One of the powerful techniques for avoidance of local minima is the simulated annealing approach which has been applied to local and global path planning as described in [13]

• **Vector Field Histogram:** Borenstein and Koren developed the vector field histogram (VFH) [10]. Borenstein and Ulrich extended the VFH algorithm to yield VFH* [11] and VFH⁺ [12]. As described in [4], the instantaneous behavior of the mobile robot in the bug algorithms is a function of only its most recent sensor readings which may lead to undesirable problems in cases where the robot's instantaneous sensor readings do not provide enough information for robust obstacle avoidance. The VFH algorithm is computationally efficient, very robust and insensitive to misreading. The VFH algorithm allows continuous and fast motion of the mobile robot without stopping for obstacles.

The VFH algorithm [10] permits the detection of unknown obstacles and avoids collisions while simultaneously steering the mobile robot toward the target. This algorithm uses a two-dimensional cartesian histogram grid to represent a local map of the environment around the robot which is updated continuously with the sampled data from range sensors. The VFH algorithm generates a polar histogram to represent the relation between the angle at which the obstacle was found and the probability that there really is an obstacle in that direction based on the occupancy grids cell values. From this histogram, a steering direction is calculated. The polar histogram is the most significant distinction between the virtual force field (VFF) and the VFH method as it allows a spatial interpretation (called polar obstacle density) of the robot's instantaneous environment. In the VFH⁺ algorithm [12], the basic robot kinematics limitations are used to compute the robot possible trajectories using arcs or straight lines. The VFH* algorithm [11] proposes look-ahead verification. The method investigates each possible direction provided by the VFH⁺ approach, checking their consequences concerning the robot future positions. The experimental results [11] shows that this look-ahead verification can successfully deal with problematic situations that the original VFH and VFH⁺ can not handle and the resulting trajectory is fast and smooth.

Given a map and a goal location, path planning involves identifying a trajectory that will bring the robot from the initial location to reach the goal location. During execution, the robot must react to unforeseen events such as the obstacles in such a way to still reach the goal. For some purposes, such as obstacle avoidance, constrained workspace, and time-

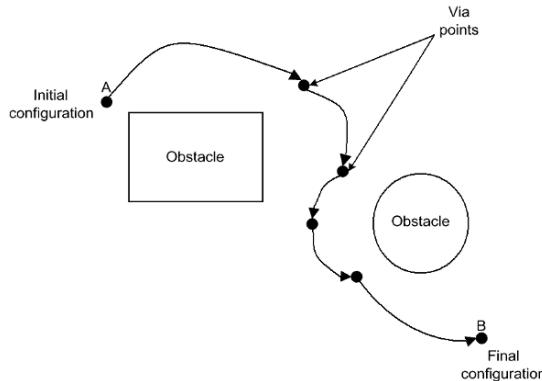


Fig. 6. Via points to plan motion around obstacles.

critical applications, the path of the end-effector can be further constrained by the addition of via points intermediate to the initial and final configurations as illustrated in figure 6. Additional constraints on the velocity or acceleration between via points can be handled in the trajectory planning.

The implementation of the path-planning system requires that the continuous environmental model is transformed into a discrete map suitable for the chosen path-planning algorithm. The three general strategies: (as described in [4])

- 1) **Road map:** This approach identifies a set of routes within the free space in a network of 1D curves or lines. In this approach, the path planning is used to connect the start position with the target position of the mobile platform by looking for a series of routes from the initial position to the goal position.
- 2) **Cell decomposition:** This approach distinguishes between the free areas and the areas that are occupied by objects [4].
- 3) **Potential field:** As described in the previous section, this approach considers the robot as a moving particle in a potential field generated by the goal and by the obstacles that are presented in the environment.

In the navigation problem, the requirement is to know the positions of the mobile robot and a map of the environment (or an estimated map). The related problem is when both the position of the mobile robot and the map are not known. In this scenario, the robot starts in an unknown location in an unknown environment and proceeds to gradually build the map of the existing environment. In this case, the position of the robot and the map estimation are highly correlated. This problem is known as *Simultaneous Localization and Map Building* (SLAM) ([5] and [6]). SLAM is the process of concurrently building a feature based map of the environment and using this map to get an estimation of the location of the mobile platform.

V. IMPLEMENTATION AND RESULTS

We are developing and constructing the mobile manipulator platform called RISCbot (the prototype of the RISCbot is shown in figure 1). The RISCbot mobile manipulator has been designed to support our research in algorithms and control for autonomous mobile manipulator. The objective is to build a hardware platform with redundant kinematic degrees of freedom, a comprehensive sensor suite, and significant end-effector capabilities for manipulation. The RISCbot platform differs from any related robotic platforms because its mobile platform is a wheelchair base. Thus, the RISCbot has the advantages of the wheelchair such as high payload, high speed motor package (the top speed of the wheelchair is 6 mph), Active-Trac and rear caster suspension for outstanding outdoor performance, and adjustable front anti-tips to meet terrain challenges.

In order to use the wheelchair as a mobile platform, a reverse engineering process has been used to understand the communication between the joystick of the wheelchair and the motor controller. This process was done by intercepting the continuous stream of voltages generated by the joystick after opening the joystick module and reading the signals within joystick wires that are sent to the signals to the wheelchair controller.

We used different types of sensors so that the RISCbot can perceive its environment with better accuracy. Our robot hosts an array of 13 *LV-MaxSonar®-EZ0™* ultrasonic sensors. The ultrasonic sensors are suitable for obstacle avoidance applications but their wide beams are unable to distinguish features within the beam angle, making sonars a poor choice of sensor for fine feature extraction within indoor environments. This resolution problem is magnified for objects further away from the robot (i.e., objects appearing at the wide end of the beam). Lastly, our robot is also equipped with an array of 11 Sharp GP20A21YK infrared proximity sensors below the sonar ring. The sonar and infrared sensors were mounted together so that their beams are oriented in the same direction. The configuration of sonar and infrared sensors is shown in figure 7. These sensors allow the RISCbot to obtain a set of observations to provide these observations to the controller and higher decision making mechanisms. The controller acts upon this set of observations to cause the robot to turn in the correct direction. The Integration of these modules together constitutes an intelligent mobile robot.

A main drawback of the infrared sensors is that they can only accurately measure obstacle distances within a range of 0.1m to 0.8 m. Another drawback of these sensors is that they are susceptible to inaccuracies due to outdoor light interference as well as an obstacle's color or reflectivity characteristics which can be seriously affected by windows and metallic surfaces.

Note that since our sonar and infrared sensors are in fixed positions, our experiments concentrated on performing data fusion on data obtained from a particular fixed height in the environment. In this project, sonar and infrared sensors

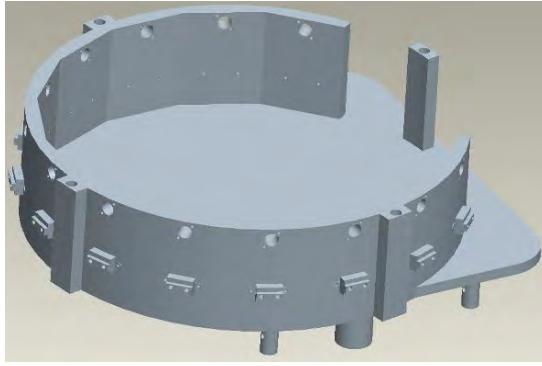


Fig. 7. A closeup view of the sonar and infrared sensors array.

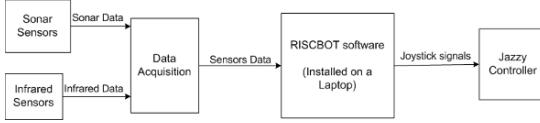


Fig. 8. The components of the RISCbot system.

are used together in a complementary fashion, where the advantages of one compensate for the disadvantages of the other.

As shown in figure 8, the RISCbot software which is written in Visual C# and runs on a laptop reads the values of all sensors at a rate of 10 HZ gathered in the data acquisition. The RISCbot software maps the sensory inputs to a series of actions which is used to achieve the required task. Based on the used algorithm, the RISCbot software responses to the sensor data by generating stream of voltages corresponding to the joystick signals to the wheelchair controller. These voltages control the direction and the speed of the wheelchair to cause the RISCbot to turn in the desired direction.

The experimental result indicates that the RISCbot can detect any unknown obstacle and avoid collisions while simultaneously steering from the initial position toward the target position.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, the mobile manipulation platform RISCbot has been presented. The RISCbot platform differs from any other robotic platform because its mobile platform is a wheelchair base. Thus, the RISCbot has the advantages of the wheelchair. Furthermore, the RISCbot consists of a comprehensive sensor suite, and significant end-effector capabilities for manipulation. In addition, we have used infrared and sonar sensors to monitor if any type of obstruction is in the path of the robot. This research aspires to find online real-time collision-free trajectories for mobile manipulation platforms in an unknown static or dynamic environment containing some obstacles, between a start and a goal configurations.

Path planning for mobile robots is one of the key issues in robotics research that helps a mobile robot find a collision-free path from the beginning to the target position in the presence of obstacles. Furthermore, it deals with the uncertainties in sensor data.

The objective for this project is to implement an autonomous mobile manipulator via Sensor Fusion. There are great benefits in using an autonomous mobile manipulator in dangerous, inaccessible and toxic environments.

In our anticipated future work, there will be an ongoing effort for the development of multiple mobile manipulation systems and platforms which interact with each other to perform more complex tasks exhibiting intelligent behaviors utilizing the proposed manipulability measure.

REFERENCES

- [1] A. Yilmaz, "Sensor Fusion in Computer Vision", Urban Remote Sensing Joint Event, 2007.
- [2] LV-MaxSonar-EZ0TM Data Sheet, www.maxbotix.com, Copyright 2005 - 2007.
- [3] "Jazzy 1122 the owner's manual", www.pridemobility.com, Pride Mobility Products Corp, 2006 .
- [4] Roland Siegwart and Illah R. Nourbakhsh, "Introduction to Autonomous Mobile Robots", Intelligent Robotics and Autonomous Agents series. The MIT Press, ISBN 0-262-19502-X, 2004.
- [5] M.W.M.G. Dissanayake, P.Newman, S. Clark, H.F. Durrant-Whyte, and M. Csorba, "A solution to the simultaneous localization and map building (SLAM)problem", IEEE Transactions on Robotics and Automation, Volume 17, Issue 3, Jun 2001, Page(s):229 - 241, 2001.
- [6] J.E. Guivant, E.M. Nebot "Optimization of the simultaneous localization and map-buildingalgorithm for real-time implementation", IEEE Transactions on Robotics and Automation, Volume 17, Issue 3, Jun 2001, Page(s):242 - 257.
- [7] SparkFun Electronics, www.sparkfun.com.
- [8] I. Kamon, E. Rivlin and E. Rimon, "A New Range-Sensor Based Globally Convergent Navigation Algorithm for Mobile Robots", In Proceedings of the IEEE International Conference on Robotics and Automation, Minneapolis, 1996.
- [9] O. Khatib, "Real-time obstacle avoidance for manipulators and mobile robots", International Journal of Robotics Research, vol. 5, no. 1, pp. 9098., 1986.
- [10] J. Borenstein and Y. Koren, "The Vector Field Histogram Fast Obstacle Avoidance for Mobile Robots", IEEE Journal of Robotics and Automation, 7, 278 - 288, 1991.
- [11] I. Ulrich and J. Borenstein, "VFH*: Local Obstacle Avoidance with Look-Ahead Verification", In Proceedings of the IEEE International Conference on Robotics and Automation, San Francisco, 2000.
- [12] I. Ulrich and J. Borenstein, "VFH+: Reliable Obstacle Avoidance for Fast Mobile Robots", In Proceedings of the International Conference on Robotics and Automation (ICRA98), Leuven, Belgium, 1998.
- [13] Min Gyu Park, Jae Hyun Jeon and Min Cheol Lee, "Obstacle avoidance for mobile robots using artificial potentialfield approach with simulated annealing", Industrial Electronics, 2001 (ISIE 2001). IEEE International Symposium on Volume 3, Issue , 2001 Page(s):1530 - 1535 vol.3
- [14] DT9814 user's manual, www.datatranslation.com, Ninth Edition, July, 2007.

Methods based on fuzzy sets to solve problems of Safe Ship control

Mostefa Mohamed-Seghir

Gdynia Maritime University
Poland

Abstract – In this article author describes three methods based on fuzzy set theory to determinate safe ship trajectories in the collision situation in fuzzy environment: branch and bound method, dynamic programming method and method based on genetic algorithms. Optimal safe ship trajectory in collision situation is presented as multistage decision-making in a fuzzy environment. The Collision Avoidance Regulations, the maneuverability parameters of the ship and the navigator's subjective assessment in making a decision are taken under consideration in the process model.

1. INTRODUCTION

Ship safe control is one of more important problems in the marine navigation. The problem of collision avoidance has thus become an urgent issue, therefore it is necessary to describe the process of collision avoidance more accurately.

To assure safety ship navigation is one of most important problems in the marine navigation. It is difficult to make correct decision in a collision situation because the largesse, velocity and the number of the ships which are taking a part in the maritime transport. A contemporary tendency in the domain of ship control, concern automation process of choosing optimal manoeuvre or optimal safety trajectory bases on the information from the anticollision system.

In proposed paper it is discussed the solution of base task of the determining ship's optimal course (ship's position), in every stage of ship trajectory, based on process kinematics model. It is assumed that the motion of encounter targets is straight-line and uniform.

Because of process fuzziness, cased from the subjectivity characterising the direct role of officer-navigator in a decision-making in the process also ambiguously describing safe distance of approach and safe time to make avoidance collision maneuver, it is assumed that an optimal safe trajectory in collision situation as multistage decision-making in fuzzy environment.

In this paper, collision avoidance with many targets in open sea is treated as a problem of optimal control using the fuzzy set theory. Optimal safe ship trajectory in collision situation is presented as multistage decision-making in a fuzzy environment.

The Collision Avoidance Regulations, the maneuverability parameters of the ship and the navigator's subjective

assessment in making a decision are taken under consideration in the process model.

2. A MULTISTAGE DECISION MAKING IN FUZZY ENVIRONMENT

In order to describe the safe ship trajectory, a motion of a ship returning by rudder in deep water is in work, but they are slightly useful the synthesis of safe ship trajectory. to evaluate the dynamic properties of the ship we use the parameters of the transfer function or the advance time and maximal angle speed $\psi_m - \omega_m$ [2,5].

With a negligence of speed decrease on the course maneuver, the ship's kinematics real motion, with giving consideration to dynamic properties, becomes:

$$x(t) = x(t-1) + \left(t_w + \frac{1}{\omega} \operatorname{tg} \frac{\left| \psi^* - \psi \right|}{2} \right) (V \sin \psi) + V t \sin \psi^* \quad (1)$$

$$y(t) = y(t-1) + \left(t_w + \frac{1}{\omega} \operatorname{tg} \frac{\left| \psi^* - \psi \right|}{2} \right) (V \cos \psi) + V t \cos \psi^* \quad (2)$$

Where:

x, y - the coordinates ship position,
 ψ, ψ^* - ship course before and after maneuver,
 V - speed of the ship.

Model of safe ship trajectory can be represented by the state equation:

$$f(\mathbf{X}, \mathbf{S}) \rightarrow \mathbf{X}_{t+1} \quad (3)$$

$$\mathbf{X}(t+1) = f(\mathbf{X}(t), \mathbf{S}(t)), \quad t = 1, 2, \dots, N \quad (4)$$

where:

$\mathbf{X}(t+1), \mathbf{X}(t) \in \mathbf{X} = \{a_0, a_1, \dots, a_{p-1}, a_p, a_{p+1}, \dots, a_n\}$ - set of real ship position coordinates

$\mathbf{S}(t) \in \mathbf{S} = \{c_0, c_1, \dots, c_m\}$ - control set

The process comes to an end when a ship attains back points (final points) called the final states $[1, 2] \mathbf{W} \subset \mathbf{X}$

$$\mathbf{W} = \{ a_{p+1}, a_{p+2}, \dots, a_n \} \quad (5)$$

The set of final states must satisfy this condition

$$S_{opt}, \mu_R \leq \mu_{Rsafe}, \quad (6)$$

where:

$S_{opt} = (\psi_{opt}, V_{opt})$ - optimal control,

μ_R - membership function of fuzzy set collision risk

This membership function of fuzzy set collision risk can be presented in the form [2, 3, 4]:

$$Z \subseteq XxX, \quad (7)$$

$$\mu_R: XxX \rightarrow [0,1] \in \mathbf{R} \quad (8)$$

$$\mu_R(k,j) = \frac{1}{\exp(\lambda_{RD}(k,j)D_{DCPj}^2 + \lambda_{RT}(k,j)T_{CPAj}^2)} \quad (9)$$

Similar, the membership function of fuzzy set of goal can be written in the form:

$$G \subseteq XxS, \quad (10)$$

$$\mu_G: XxU \rightarrow [0,1] \in \mathbf{R} \quad (11)$$

$$\mu_G(k,j) = 1 - \frac{1}{\exp(\lambda_d(k,j)D_{DCPj}^2)} \quad (12)$$

Now, it must be defined a membership function of fuzzy set constraints as constraints of maneuver at each step:

$$C \subseteq XxS, \quad (13)$$

$$\mu_C: XxU \rightarrow [0,1] \in \mathbf{R}, \quad (14)$$

$$\mu_C(k) = \frac{1}{\exp(\lambda_c(k)(Vcos\psi(k) - Vcos\psi(k-l))t_k^2)} \quad (15)$$

The fuzzy set decision is determined as the fuzzy set $D \subseteq XxS$, it's a result of an operation "*" of the fuzzy set of goal and fuzzy set of constraints:

$$D = G * C, \quad (16)$$

$$\mu_D(..) = \mu_C(..) * \mu_G(..) \quad (17)$$

To resolve this task authors submits, three following methods.

3. BRANCH A BOUND METHOD

A fuzzy decision is a result of a certain compromise between these sets G (fuzzy set of goals) and C (fuzzy set of constraints), if the trajectory is called sequence states attained, then membership function of fuzzy set decision define as

$$\mu_D(S_0, S_1, \dots, S_{N-1}, | X_0) = \mu_C(S_0) * \mu_G(X_1) * \mu_C(S_1) * \mu_G(X_2) * \dots * \mu_C(S_{N-1}) * \mu_G(X_N) \quad (18)$$

To maximise a membership function of fuzzy set decision, at using minimum type, we obtain the optimal decision [1]

$$\mu_D(S_0^*, S_1^*, \dots, S_{N-1}^*, | X_0) = \bigvee_{S_0, S_1, \dots, S_{N-1}} (\mu_C^0(S_0/X_0) \wedge \mu_G^1(S_1/X_1) \wedge \dots \wedge \mu_C^{N-1}(S_{N-1}) \wedge \mu_G^N(X_N)) \quad (19)$$

The decision process can be conveniently represented in the form of a decision tree, the root of the tree is the initial state x_0 . We start from x_0 , and looking for the optimal decision, after that to put it to control S_0 and we pass to state x_1 . We determine again the optimal decision S_0 and we pass to the next state, until we attain the final state. In this manner we obtain sequence of states which present a ship's optimal safe trajectory [4].

$$\left\{ \begin{array}{l} \eta_0 = \mu_C(S_0) \wedge \mu_G(X_1) \\ \eta_1 = \mu_C(S_0) \wedge \mu_G(X_0) \wedge \mu_C(S_1) \wedge \mu_G(X_2) = \\ = \eta_0 \wedge (\mu_C(S_1) \wedge \mu_G(X_2)) \\ \dots \\ \eta_k = \mu_C(S_0) \wedge \mu_G(X_1) \wedge (\mu_C(S_1) \wedge \mu_G(X_2)) \wedge \\ \wedge (\mu_C(S_k) \wedge \mu_G(X_{k+1})) = \\ = \eta_{k-1} \wedge (\mu_C(S_k) \wedge \mu_G(X_{k+1})) \\ \dots \\ \eta_{N-1} = (\mu_C(S_0) \wedge \mu_G(X_1)) \wedge (\mu_C(S_1) \wedge \mu_G(X_2)) \wedge \\ \wedge (\mu_C(S_{N-1}) \wedge \mu_G(X_N)) = \\ = \eta_{N-2} \wedge (\mu_C(S_{N-1}) \wedge \mu_G(X_N)) \end{array} \right. \quad (20)$$

If range controls a mount $S_0, S_1, \dots, S_k, k < N-1$, it for each $L > k, L < N-1$ it gets

$$\eta_k \geq \eta_L \quad (21)$$

From this inequality emerge, that each value η_L can not be greater than value η_k in other case at use of operation minimum „ \wedge “. This way, it is possible to ascertain progressing, that inequality gets:

$$\eta_k \geq \eta_N = \mu_D(S_0, S_1, \dots, S_{N-1}, | X_0) \quad (22)$$

To suppose, that it obtain k control stage and certain state of process state, now it must be choose optimal state from states achieved earlier.

To continue this procedure until we obtain final state, the process ends and we get optimal safe ship's trajectory in collision situation.

4. DYNAMIC PROGRAMMING METHOD

In case of represent this method, it is necessary to express the task in following form [1,2]

$$\mu_D(S_0^*, S_1^*, \dots, S_{N-1}^* | X_0) = \bigvee_{S_0, S_1, \dots, S_{N-1}} (\mu_C^0(S_0) \wedge \mu_G^1(X_1) \wedge \dots \wedge \mu_C^1(S_1) \wedge \mu_G^2(X_2) \wedge \dots \wedge \mu_C^{N-1}(S_{N-1}) \wedge \mu_G^N(f(X_{N-1}, S_{N-1}))) \quad (23)$$

Structure of this equation makes possible applying dynamic programming. Namely the last two parts on the right side,

$$\mu_C^{N-1}(S_{N-1}) \wedge \mu_G^N(f(X_{N-1}, S_{N-1})) \quad (24)$$

depend only on control S_{N-1} , and they do not depend on other controls.

Maximizing range control S_0, \dots, S_{N-1} , can be divided on two phrases:

- Maximizing S_0, \dots, S_{N-2} ,
- Maximizing S_{N-1} .

$$\begin{aligned} \mu_D(S_0^*, S_1^*, \dots, S_{N-1}^* | X_0) &= \bigvee_{S_0, S_1, \dots, S_{N-1}} \\ &(\mu_C^0(S_0) \wedge \mu_G^1(X_1) \wedge \mu_C^1(S_1) \wedge \\ &\mu_G^2(X_2) \wedge \dots \wedge \mu_C^{N-2}(S_{N-2}) \wedge \mu_G^{N-1}(X_{N-1}) \wedge \\ &\bigvee_{S_{N-1}} (\mu_C^{N-1}(S_{N-1}) \wedge \mu_G^N(f(X_{N-1}, S_{N-1}))) \end{aligned} \quad (25)$$

In case of next part for N-2 depends only on control S_{N-2} , therefore equation can be described as

$$\begin{aligned} \mu_D(S_0^*, S_1^*, \dots, S_{N-1}^* | X_0) &= \bigvee_{S_0, S_1, \dots, S_{N-3}} \\ &(\mu_C^0(S_0) \wedge \mu_G^1(X_1) \wedge \mu_C^1(S_1) \wedge \mu_G^2(X_2) \wedge \dots \wedge \mu_C^{N-3}(S_{N-3}) \wedge \\ &\wedge \mu_G^{N-2}(X_{N-2}) \wedge \bigvee_{S_{N-1}} (\mu_C^{N-2}(S_{N-2}) \wedge \mu_G^{N-1}(X_{N-1}) \\ &\wedge \bigvee_{S_{N-1}} (\mu_C^{N-1}(S_{N-1}) \wedge \mu_G^N(f(X_{N-1}, S_{N-1}))) \end{aligned} \quad (26)$$

This reverse iteration, which reflects essence of dynamic programming, can be repeated for other stages, which follows to consecutive scheme of recurrent equations of dynamic programming

$$\left\{ \begin{array}{l} \mu_G^{N-i}(X_{N-i}) = \bigvee_{S_{N-i}} (\mu_C^{N-i}(S_{N-i}) \wedge \mu_G^{N-i+1}(X_{N-i+1})) \\ X_{N-i+1} = f(X_{N-i}, S_{N-i}) \end{array} \right. \quad (27)$$

Wanted optimal range of controls S_0, \dots, S_{N-1} is expressed by ordered maximal values of controls S_{N-i} , $i=1, \dots, N$.

For every maximizing value, received S_{N-i}^* as function of state X_{N-i} , obviously if looking on left side of first equation in equations (27).

Optimal solution for this task exists if there is at least one range control S_0, \dots, S_{N-1} , for which $\mu_D(S_0, S_1, \dots, S_{N-1} | X_0) > 0$.

5. METHOD BASED ON GENETIC ALGORITHMS

Mentioned task can be solved also with using the genetic algorithms [1].

Genetic algorithms base elements are:

Problem is represented by range controls S_0, \dots, S_{N-1} ; function of goal is fuzzy decision

$$\mu_D(S_0, S_1, \dots, S_{N-1} | X_0) = \mu_C(S_0) * \mu_G(X_1) * \mu_C(S_1) * \mu_G(X_2) * \mu_C(S_{N-1}) * \mu_G(X_N) \quad (28)$$

Using

-standard random selection from following population

-standard crossing and mutation

-standard stopping condition, as number of iteration or correction lower than certain threshold

Supposing that:

- a) controls are defined as even real numbers in interval $[0, 1]$, c_1, \dots, c_m ,
- a) states are also defined as even real numbers in interval $[0, 1]$, a_1, \dots, a_n .

In the following way it is possible to present structure of genetic algorithm:

BEGIN

$t := 0$;

- it establish $P(t)$ (initial population) consists of random generated ranges of controls (from fate generated real numbers from interval $[0, 1]$);

- for every S_0, \dots, S_{N-1} in every range In population $P(t)$, it find achieved X_{t+1} from equation of switching states $X_{t+1} = f(X_t, S_t)$, and apply goal function $\mu_D(S_0, S_1, \dots, S_{N-1} | X_0)$, for every range $P(t)$;

WHILE $t < \text{maximal iteration number}$ **DO**

BEGIN

$t := t + 1$;

- attribute probabilities to every range in $P(t-1)$ for value of goal function proportional;

- random generate new population $P(t)$;

- it perform the crossing an mutation on ranges in $P(t)$; calculate of goal function for every range in $P(t)$.

END;

It depend of iteration number we obtain a final results (optimal safe ship's trajectory in collision situation).

5. SIMULATION

In this part of paper author presents one example. The result of simulation of the collision situation in passing with one target with application this following methods:

- branch and bound method,
- dynamic programming method,
- method based on genetic algorithms (figure 1).

Table 1: Data of navigation situation in case of passing with 1 motion target.

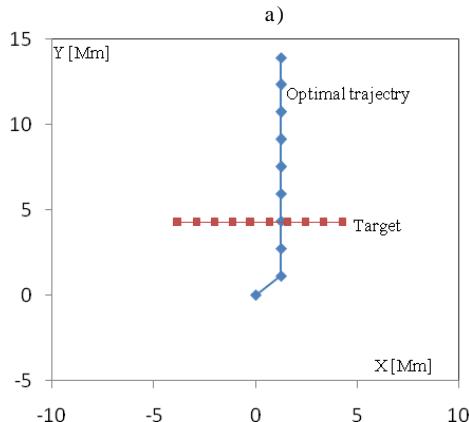
Target	N_t [degree]	D_t [Mm]	V_t [Kn]	ψ_t [degree]
1	45	6	14	270
Owen ship			16	0

Where: N_t - bearing,

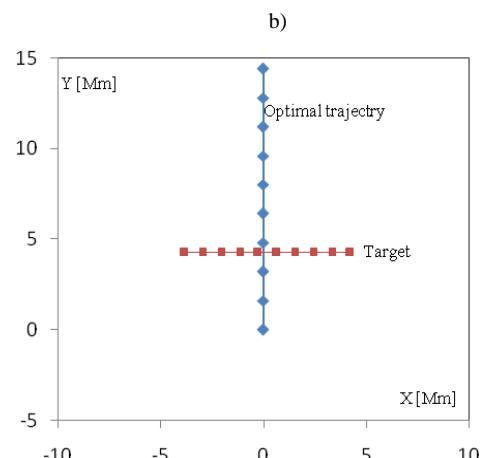
D_t - distance,

V_t - velocity,

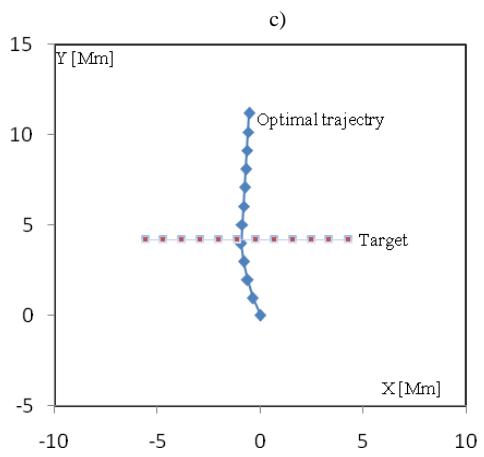
ψ_t - ship's head,



a)



b)



c)

Figure 1: The result of simulation of the collision situation in passing with 1 motion targets:
a) branch and bound method
b) dynamic programming method,
c)method based on genetic algorithms.

6. COCLUSION

In this paper it presented three methods based on fuzzy set theory to solve task of optimal safe ship trajectory in collision situation, according to the international Rules of the Road at Sea, can be conduct to multistage decision-making in fuzzy environment.

The present paper showed that proposed concepts of application of fuzzy set theory is a promising way to solve the considered task and design novel anticollision system in the future.

The fuzzy set theory can be applied in many domain, and can provide better solutions than in models of conventional mathematical apparatus.

7. REFERENCES

- [1] Kacprzyk J., „Wieloetapowe sterowanie rozmyte”, WNT, Warszawa 2001.
- [2] Lisowski J., Mohamed-Seghir M., „The Safe Ship Control with Minimum Risk of Collision”, Wit Press Comp. Mech. Publ., Boston 1998.
- [3] Mohamed-Seghir M, The safe ship control with application of fuzzy set theory, Scientific Journal WSM Gdynia, Gdynia 2006, № 55, pp. 96-105.
- [4] Mohamed-Seghir M, „Optymalna bezpieczna Trajektoria statku w Rozmitym Otoczeniu”, XIII Międzynarodowa Konferencja Naukowo-Techniczna, Gdynia 2002.
- [5] Mohamed-Seghir M, „application of fuzzy set theory to determinate optima safety trajectory of the ship In a collision situation”, Modelling, Measurement and control, AMSE Press. 1995, Vol. 12, № 1, pp.49-54.

Network Topology Impact on Influence Spreading

Sasho Gramatikov, Dimitar Trajanov, Ljupco Kocarev, Aksenti Grnarov

Dept. of Computer Sciences

Faculty of Electrical Engineering and Information Technology

University Ss. Cyril and Methodious Skopje

Skopje, R. Macedonia

{saso.gramatikov, mite, lkocarev, grnarov}@feit.ukim.edu.mk

Abstract — Networks composed of large number of nodes interacting in structured ways such as power grids, communication networks, social networks or market networks are critical part of the world's infrastructure. Many times minor changes of the state in some of the nodes can spread rapidly and cause major effects in the network, so understanding the behavior of the complex network due to changes of the state is of a great interest. In this paper we present influence spreading in networks driven by the influence model. We also show how the topology and connectivity of a network affect the spread of influence.

Keywords — influence, complex networks, standard deviation.

I. INTRODUCTION

Networks containing large number of nodes connected in a specific way are common topic of research, because inner changes caused by some events make the network a dynamic system with certain behavior specific to network topology and variety of parameters of the network. The nature of the network dynamic is versatile and what is nowadays most commonly studied is spreading of failures of nodes, spreading of information, influence, or spreading of computer and natural viruses. Once an event is introduced in the network, nodes react to it, possibly changing their state, and according to their influence level in the network, they try to spread their current state to the nodes they are connected to.

For example, let us take failure of a router as an event in internet network. The event causes increased rerouted traffic in the neighbor routers, causing possible changes in their state. After the failure, each node determines its current state according to the influence it gets from the neighbor nodes. However, the state of each router does not only depend on the offered traffic from the neighbors, it also depends on the possibility of hardware failures or power loss. Similar example are social networks. When an idea is lunched, people make decision whether to accept the idea or not. Since in social network people are connected with weighted links defined according to influence power of each individual, every person gets certain amount of influence from the people it is connected to. Thus, both the attitudes of the environment and the attitude of each individual in a network are important for making certain decision. Clearly, nodes which have high power of influence are not very likely to change their own decision under influence of weak nodes, which on the other side, are susceptible to easy changes due to outer influence.

No matter what is chosen to be an event in the network,

there are several possible models of spreading the change in the networks. In [1] two basic diffusion models for spreading influence are used: linear threshold model and independent cascade model, offering algorithms for maximizing the spread. [2] is presenting the spread of computer viruses in a computer network. In [3] the worldwide web is used as a complex network for spreading ideas in the blogosphere. The concept of spreading in complex networks is even popular in the field of marketing by promotion of new products and spreading their popularity to the consumers [4]-[6].

The concept that we would like to introduce in this paper is spreading the influence in a network using the influence model defined in [9]. In this model, nodes are presented with Markov chain. The state of each chain (node) not only depends on the state of its neighbors, but depends on its own current state. We consider networks with nodes that can have two different states.

The goal of this paper is to determine the system state regarding the average number of failed/influenced nodes, as well as its standard deviation for a different configuration of the local Markov chain, different network topologies and different weight calculation algorithms.

In the following text, we first give (section II) a short description of the general influence model and propose structure of local Markov chains for a heterogeneous network where sites are can be interpreted as network routers or individuals in social networks. Afterwards in section III we give different algorithms for calculating the weight of links in such networks. Since we want to analyze the behavior of different real network topologies, in section IV we give a brief overview of the most common topologies of complex network. Results of the behavior analysis of different complex networks, obtained by simulations are presented in section V. Eventually the conclusions of the work in this paper are given in section VI.

II. INFLUENCE MODEL

The influence model is suggested in [9] as a model of random, dynamical interactions on networks. We refer the reader to [9] for a full account of the model and its properties; here we give a brief description of the model.

In the influence model the network is observed at two levels: the network level and the local level. At network level each node is treated as one active entry and is called site. Each site can be in different state, defined at the local level. Looking at local level, each site is presented by a

local Markov chain. Each node of the Markov chain is called state and represents the state of the site.

The quantitative measure of the influence that each node has on the neighbors, is defined at the network level with the directed graph $\Gamma(D')$ with nodes from 1 to n. D is $n \times n$ stochastic matrix called network influence matrix, containing information about the nodes interconnectivity. The entry d_{ij} has a non zero value only if node i is connected to node j . The magnitude of d_{ij} defines the amount of influence node i exerts on node j . In order to get a network where the influence that each node receives from its neighboring nodes equals one, the graph is defined through the transposed form of D .

On the local level each node is represented with another directed graph $\Gamma(A)$. A is again stochastic matrix with size $m \times m$, called local-state transition matrix, where m is the number of different states that a node can take. The graph defines a Markov chain, where each entry a_{ij} is the transition probability from state i to state j .

At any discrete moment k , the node i has status defined with the vector $s_i[k] = [0...010...0]'$. This vector has only one 1 at position equal to the status of the node. The status of the network, expressed with one vector will be:

$$S[k] = [s_1[k] s_2[k] \dots s_n[k]]' \quad (1)$$

The probability that node i will have certain status in time k is defined with the vector $p_i[k] = [p_i(0) p_i(1) \dots p_i(m)]'$ where $p_i(m)$ is the probability that the Markov chain of node i is in state m . The status probability of the whole network, expressed with one vector will be:

$$P[k] = [p_1[k] p_2[k] \dots p_n[k]]' \quad (2)$$

The evolution of the state at every next time step $k+1$ is related to the probability of the current time step and defined with the equations:

$$S'[k+1] = \text{MultiRealize}(P'[k+1]) \quad (3)$$

$$P'[k+1] = S'[k]H \quad (4)$$

The *MultiRealize* operation is equivalent to n independent flipping of a coin. Each outcome of the flipping determines the state of a node.

H is influence matrix defined as *Kronecker* product of the network matrix D' and the transition matrices of each local chain A_{ij}

$$H = D' \otimes \{A_{ij}\} = \begin{bmatrix} d_{11}A_{11} & \dots & d_{n1}A_{n1} \\ & \ddots & \\ d_{1n}A_{1n} & \dots & d_{nn}A_{nn} \end{bmatrix} \quad (5)$$

H is not a stochastic matrix because its row sum is not one, but it still has some properties of stochastic matrix: it is nonnegative and has 1 as a dominant eigenvalue [9]. A_{ij} represents a transition matrix of a Markov chain and can

be any matrix which satisfies the condition $A_{ij}1_{m_i} = 1_{m_i}$, where m is the number of states of the local Markov chain. Each submatrix $d_{ij}A_{ij}$ of H contains the influence that every single state of node i exerts on node j . That influence can be decomposed in two parts. The first part A_{ij} represents the dynamics of states which influence the state of node j , whereas the second part d_{ij} is a connection specific value which determines the amount of that dynamics that will be used for deciding the state of node i .

According to the value of A_{ij} , the influence model can be homogenous or heterogeneous. In the homogeneous model each node has the same structure of local Markov chain and therefore $A_{ij} = A$. In the heterogeneous model, nodes have different structure of the local Markov chain.

In reality networks are heterogeneous and have local Markov chains which are different for every single node. For example, from a functional aspect of view, in the internet network routers have local Markov chains with two states, on or off. The transition probabilities of each router are different and depend on many factors like, traffic load, maintenance, environmental factors etc. It is the same case in the social networks: individuals have different probabilities of changing their own attitude under no influence. In order to make a model where nodes will not have randomly distributed local Markov chains, we define the structure of A_i by a simple rule: the importance of a node. The main idea comes from the fact that in practice, well connected nodes are of great importance, and therefore are better protected and maintained rather than nodes that are connected with just a few neighbors. Nevertheless, there is a possibility that even those nodes fail because well connected nodes are subdued to a larger demand of service by the neighbor nodes. Therefore better connected nodes are assigned smaller probabilities for failure rather than weakly connected nodes.

For these types of networks, each node i has the same dynamics of influence towards every node it is connected to, and therefore we assume that the local Markov chain for a single node has the same structure in the influence matrix H i.e. $A_{ij} = A_i, \forall j \in \{1, \dots, n\}$. Although A_i can be of any size, we consider that each node is a two-state Markov chain, with transition matrix A_i .

Let A_i is defined as follows:

$$A_i = \begin{bmatrix} 1-p_i & p_i \\ q_i & 1-q_i \end{bmatrix} \quad (6)$$

where $1-p_i$ is the probability that once in normal state, node i will remain normal, while p_i is the probability of failure. Seemingly, $1-q_i$ is the probability that a failed node will remain failed, while q_i is the probability that the node will be repaired. Let p_{\min} and p_{\max} are the minimum and maximum values that can be assigned to any p_i in the network. Let $d(i)$ is the degree of node i and d_{\min} and d_{\max} are the minimum and maximum degree of the network. The probability p_i is defined as:

$$p_i = p_{\max} - \frac{p_{\max} - p_{\min}}{d_{\max} - d_{\min}} (d(i) - d_{\min}) \quad (7)$$

According to (7) each node gets portion of failure probability inversely proportional to the degree. As far as the probability q is concerned, we assume that it has the same value for every node. That means that every failed node is recovered with the same probability.

III. WEIGHT CALCULATION TECHNIQUES

The amount of influence that a link possesses depends on many factors. In the following text we present four different techniques for weight calculation, which take into consideration different aspects of network topology.

A. Equal weight distribution algorithm

The simplest solution for assigning weights to incoming links of a node in a network is to take a model where each neighbor of a node implies the same amount of influence. Thus, the influence that node A imposes on node B decreases as the number of incoming links of B increases. Except the influence from the neighbor nodes, each node has the ability of self-influence of a same amount as the influence from other nodes. This results with adding a self-loop in the network graph. Assuming that the total influence a node can get from the neighbors and from itself is:

$$\sum_{i \in V} d_{ij} = 1 \quad (8)$$

and assuming that the j is connected to m neighboring nodes, then the weight of each link that leads to the node of interest will be

$$d_{ij} = \frac{1}{m+1} \quad (9)$$

This solution does not give the best results in practice, because the influence each node has on others depends on the number of nodes it is connected to. If we take a simple example in computer networks consisting of few stations generating high traffic flow towards the router they are connected to, joining of another station with very little traffic flow towards the router equally reduces their influence. This means that in real networks of any type, not all the nodes have the same importance and influence to the nodes they are connected to.

B. Node betweenness algorithm

In order to get a model closer to the real networks, we assign weights to the links according to the importance of the nodes. For that reason we use the betweenness from the theory of graphs [7], as parameter for the weight calculation algorithm.

Betweenness is a measure of the importance of a node in a network, and is calculated as the fraction of shortest paths between node pairs that pass through the node. Betweenness is, in some sense, a measure of the influence a node has over the flow of information through the network. Let G is a graph given with set of nodes V and

set of edges E . Let s and t are two nodes of the graph. σ_{st} is the number of paths that pass from s to t . Let $\sigma_{st}(v)$ is the number of shortest paths that pass through the node v . The central betweenness of node v is:

$$C(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \quad (3)$$

For example, let us consider a simple network shown with the directed graph on Fig. 1.

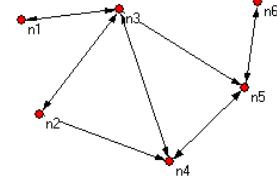


Fig. 1. Simple network

Fig.2 shows importance of each node according to the number of shortest paths that pass thorough it.

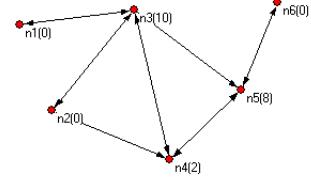


Fig. 2. Simple network with assigned node betweenness

Once we have the betweenness of each node, we aim to assign weight to incoming links according to the value of node betweenness of their originating nodes. Let P_i is a subset of nodes from V that have outgoing links directed to node i . Let $C(i)$ is the betweenness of node i . We assign weight to each incoming link proportional to the originating node betweenness. We first sum the betweenness of all nodes that belong to the set P_i , including the betweenness of node i , and then divide the betweenness of each node by the sum. Each link that originates from node $j \in P_i$ is assigned magnitude which is fraction of the total incoming influence, proportional to the fraction of its betweenness in the total sum of betweenness. Taking in consideration that the incoming influence of each node equals 1 (8), the expression for determining the weight of the influence that j has on node i will be calculated as

$$d_{ji} = \frac{C(i)}{C(i) + \sum_{k \in P_j} C(k)} \quad (10)$$

C. Edge betweenness algorithm

Just like node betweenness denotes the importance of the nodes, the edge betweenness, in the similar way assigns values to links according to their importance. It is calculated as a number of shortest paths that pass through the edge. Let $\delta_{st}(e)$ is the number of shortest paths from s

to t that pass through the edge e and δ_{st} is the total number of paths from s to t . The edge betweenness of edge e is:

$$C(e) = \sum_{s \neq t \in V} \frac{\delta_{st}(e)}{\delta_{st}} \quad (11)$$

The weight that is assigned to links leading to a certain node is calculated from the edge betweenness divided by the sum of all incoming links, thus providing that the sum of the incoming influence of a node is one.

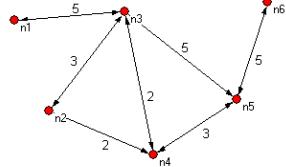


Fig. 3. Simple network with assigned edge betweenness

Fig. 3 shows normalized values of edge centrality calculated for the simple directed graph on Fig. 1. The links with highest values have the highest importance.

Let Q_i is a subset of edges from E that have direction towards node i . Let $C(e)$ is the betweenness of edge e . Since the incoming weights of a node must satisfy (8) the weight of edge e leading from node i to j will be calculated as

$$d_e = \frac{C(e)}{\sum_{k \in Q_j} C(k)} \quad (12)$$

D. Degree algorithm

The degree weight calculation algorithm, assigns weight to incoming links of a node according to the degree of nodes the links are originating from. Let P_i is the same subset of nodes from V that have outgoing links to node i and let $D(i)$ is the degree of node i . Like in the previous techniques, we first sum the degree of all neighbor nodes of i and then divide the degree of each node by the sum. This technique assigns high values of weight for links that are originating from well connected nodes. The weight of the link between nodes i and j is

$$d_{ji} = \frac{D(i)}{D(i) + \sum_{k \in P_j} D(k)} \quad (13)$$

IV. COMPLEX NETWORKS

Since one of our main goals is to analyze the behavior of different real network topologies, for that purpose we use different types of complex networks. Complex networks have certain properties that make them different from aspect of topology. The difference comes from the way nodes are connected among each other. According to the inter-link dependences several types of network topologies are defined.

A. Random Networks

The simplest and most straightforward realizations of complex networks are random networks. These networks are characterized by nodes that are connected randomly connected to each other, with certain probability p [10]. For networks with large number of links, the average number of links per node is the same and the degree distributed follows the Poisson distribution. This fact shows that the probability that a node will have large deviation from the average value is exponentially small. These networks are pioneers in complex network theory, because most of the large scale networks found in reality (WWW, internet, cellular, power, neural networks) were considered to be random. However, it was later discovered that, the real networks have different topology dependences.

B. Geographic Random Networks

A special case of random networks are geographically random networks. These networks are characterized by nodes that are randomly distributed in the space, and are connected only to the nodes in their proximity. These networks always have one giant cluster component that contains most of the nodes. A typical example of random geographic network is wireless ad hoc network where each wireless station is connected to the stations that are within its range of coverage.

C. Small-world Networks

According to the link structure, small world networks stand between random and lattice connected network. They are generated by randomly replacing fraction of links from d-dimensional lattice structure [11]. If the fraction equals zero, than the network is lattice, and if the fraction is one, than the network is random network. For fraction between the extreme values, we get a small-world network. The name of these networks comes from the property that the average shortest distance between two nodes increases logarithmically with the number of nodes. Therefore the wider the network, it is easier to connect two distant nodes with just a few links. Thus, although the network is large, at the same time it is small because any node is reachable in average in a few steps.

D. Scale-free Networks

Small world networks are composed of highly connected clusters, in which everybody knows everybody from the cluster, and very few of them provide connectivity to the rest of the world by setting links with other clusters. However, some of the real networks like the world-wide web, networks of scientific citations etc. have additional properties which classify them as a subtype of small world networks. These networks are called scale-free, meaning that they have distribution of connectivity that decays with power law. The number of nodes with exactly k links follows a power law, each with a unique degree exponent. These networks are characterized by presence of nodes called hubs, with large number of links. These nodes are dominant in the structure of all scale-free networks, making each node from the network easily reachable from any point [11]-[12].

V. RESULTS

The most important parameters which are studied for defining the behavior of different networks are mean value and standard deviation of failed nodes. These parameters for homogeneous networks are given in analytical form in [9], however, the analytical methods for calculation of mean value and standard deviation are not applicable for heterogeneous influence model. Therefore we use simulations to determine the behavior of different network topologies and weight calculation algorithms.

We are simulating the behavior of four different network topologies: scale-free, small-world, random and geographic random, each having 250 nodes. We used network generators with input parameters adjusted to values that will enable generating networks with nodes connected to an average of 6 other nodes. All the networks are connected to one giant cluster. The minimum probability that a node will fail is $p_{\min} = 0.59$ and the maximum probability is $p_{\max} = 0.99$. The simulations are executed for 500 time steps, and repeated for 50 different networks.

In all the simulations we plot the dependence of network behavior on the structure of the local Markov chain. Since the probability of failure p is calculated for each node according to (7), we plot the network behavior only against the recovery probability q . At the beginning of time $k=0$, all the nodes are in normal state, and very quickly the network reaches the mean value, deviating around it. Our goal will be finding the mean value and the standard deviation of node failures.

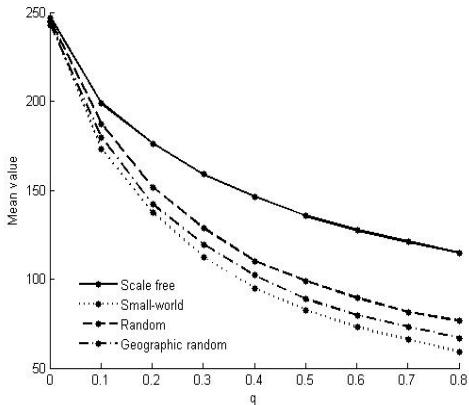


Fig. 4. Dependence of network topologies and local Markov chain structure on mean value of failed nodes for equal weight algorithm

On Fig. 4 the dependence of mean value of the four different topologies on recovery probability q is shown. The links weight is calculated according to the equal weight calculating algorithm mentioned above. It is clear that mean value strongly depends on network topology, having the highest values for scale-free networks. The other topologies have similar dependence. Random network is the second most influent topology on mean value, leaving behind geographic random and small world network.

Fig. 5 shows how the different weight calculation algorithms affect the network behavior of a scale-free

network. Most intuitive behavior can be noted when the equal weight algorithm is used, because as recovery probability q increase, the number of failed nodes decreases evenly, unlike the node betweenness algorithm which introduces very high drop of failed nodes, especially for low values of recovery probability q . This is due to the fact that node betweenness is calculated by the importance of every node. Because scale-free networks have hubs with many links, their betweenness is high, so once a hub is repaired its influence is very rapidly spread through the network. From the figure we can conclude that the edge betweenness and the degree weight algorithm are very close in nature, when number of failed nodes is concerned.

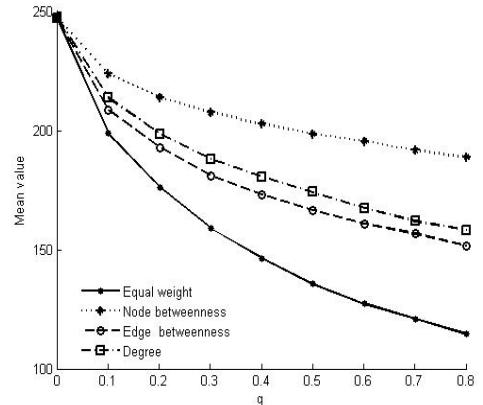


Fig. 5. Dependence of weight calculation algorithm on mean value of failed nodes for a scale-free network

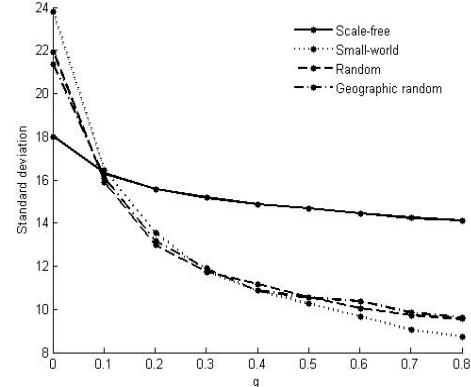


Fig. 6. Dependence of standard deviation for different topologies on recovery probability q for node betweenness algorithm

On Fig. 6 the dependence of standard deviation on network topology is shown. Again the scale-free networks are the networks which reach highest values of standard deviation. They are almost resistant to changes of value of the recovery probability q . The other types of networks have approximately the same values for the standard deviation. Although they are lower than the standard deviation of scale-free networks, for low values of recovery probability q , they reach higher values of standard deviation than the scale-free networks.

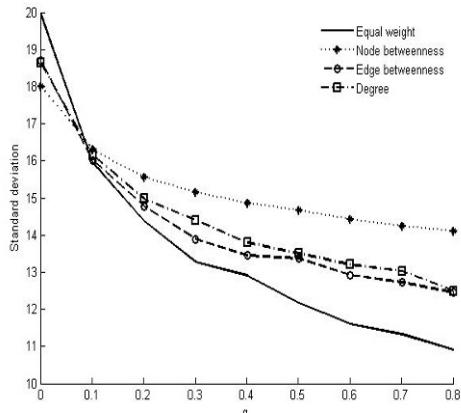


Fig. 7. Standard deviation for different weight calculation algorithms for scale-free networks

Fig. 7 presents the dependence of weight calculation algorithm on standard deviation for a scale-free network. Similarly like the mean value, the standard deviation is most sensitive to recovery probability q for equal weight distribution algorithm, and most resistant to changes of q for node betweenness algorithm. In between stand the other weight calculation algorithms.

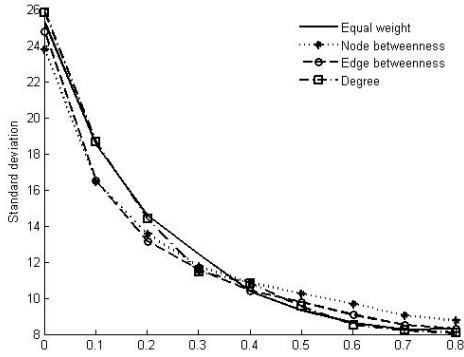


Fig. 8. Standard deviation for different weight calculation algorithms for small-world networks

Fig. 8 presents the dependence of weight calculation algorithm on standard deviation for a small-world network. It is clear that the standard deviation is almost the same for any of the algorithms for calculating the weight. The only parameter that is important in the standard deviation is the local Markov chain and the network topology. Although not presented on the figure, we can come to the similar results for all of the complex network topologies.

VI. CONCLUSION

From our simulations we can conclude that network topology has a major impact on the average number of failed/influenced nodes. The effect is mostly visible in the scale free network which have rather large number of such nodes for any values of the recovery probability, compared to the small-world, random and geographic random networks, which have similar behavior. We also conclude that besides the topology, another key concept for the network behavior is the weight that is assigned to the links. When we analyzed different weight calculation algorithms, we concluded that that a failure/influence is most rapidly spread when weights are calculated according to the node betweenness algorithm. Edge betweenness and degree algorithm give very similar results. The influence is spread most slowly when the equal weight distribution algorithm is used for assigning weights to the links.

Another conclusion from our work is that although the standard deviation depends on network topology, the scale of dependence is very low compared to the size of the network. For scale-free networks the recovery probability has hardly any affect on the standard deviation. For other types of networks, standard deviation depends on the recovery probability and is almost the same for all kinds of weight calculation algorithms.

Our future work will include analysis of influence propagation in complex networks, using other models for influence spreading like, SI, SIS and SIR.

REFERENCES

- [1] Garetto, M. Gong, W. Towsley, D: Modeling malware spreading dynamics, *INFOCOM 2003*
- [2] Akshay Java, P. Kolari, T. Finin, T. Oates. Modeling the Spread of Influence on the Blogosphere
- [3] J. Brown, P. Reinegen. Social ties and word-of-mouth referral behavior. *Journal of Consumer Research* 14:3(1987), 350-362.
- [4] F. Bass. A new product growth model for consumer durables, *Management Science* 15(1969), 215-227.
- [5] J. Goldenberg, B. Libai, E. Muller. Using Complex Systems Analysis to Advance Marketing Theory Development. *Academy of Marketing Science Review* 2001.
- [6] D. Kempe, J. M. Kleinberg, and E. Tardos. Maximizing the spread of influence through a social network. *ACM SIGKDD international conference on Knowledge discovery and data mining*, 2003
- [7] Freeman, L. C. Centrality in social networks: *Conceptual clarification*. *Social Networks* 1, 215-239, 1979
- [8] Reinhard Diestel, Graph Theory, Springer-Verlag Heidelberg, New York, 1995
- [9] C. Asavathiratham, S. Roy, B. Lesieutre, G. Verghese. The Influence Model. IEEE Control Systems, Dec. 2001.
- [10] Michael Karonski and Adrzej Rucinski: The Origins of the Theory of Random Graphs, *The Mathematics of Paul Erdos*, Berlin, Springer, 1997
- [11] L. A. N. Amaral, A. Scala, M. Barthelemy, H. E. Stanley: Classes of small-world networks, *PNAS* 97:11149-11152
- [12] A. L. Barabasi: Linked, Penguin Group, London, May, 2003
- [13] Barabási, Albert-László "Scale-Free Networks". *Scientific American*, 288:60-69, May 2003.

An Adaptive Combiner-Equalizer for Multiple-Input Receivers

Ligia Chira Cremene, Nicolae Crisan, Marcel Cremene

Technical University of Cluj-Napoca, 15, Daicoviciu, Romania

Communications Department

Ligia.Cremene@com.utcluj.ro

Abstract— Where multiple-input receivers are concerned diversity combining is one of the most efficient techniques against fading effects. In this paper we propose a multiple-input adaptive combiner-equalizer. The novelty of the solution lies in the unified combining-equalization approach - the two classical operations being performed simultaneously and not sequentially. Our simulations show significant performance in terms of outage probability for both indoor and outdoor conditions, while complexity is lower than for a classical MRC implementation. The concept of unifying certain operations along the transmission chain is feasible today more than ever as it can be easily implemented on SDR (Software Defined Radio) platforms.

Keywords – diversity combining, multiple-input receivers, adaptive combiner-equalizer, unified processing.

I. INTRODUCTION

The present work is part of a study that tries to show that certain processing operations along a wireless transmission chain are equivalent. We noticed that similar, if not the same algorithms or methods, are used at different levels, in different processing blocks (e.g. weight optimization algorithms and tapped delay lines are used in adaptive antenna arrays as well as in equalizers). For instance, we noticed similarities between receiver combining and time-equalization techniques; they both involve weighting and summation of delayed signals. In most cases equalization is performed after the combining operation. For this case we have imagined a processing block that performs the two operations simultaneously, as a unified function.

The concept of unifying certain processing functions/operations on the transmission chain is feasible today more than ever as it can be easily implemented on SDR (Software Defined Radio) platforms.

The approach is to add combining abilities to the equalizer, that is usually present on the receiver chain, and thus to transform it into a combiner-equalizer. This transformation involves the addition of a tapped delay line for each branch. The equalizer will combine the delayed signals corresponding to each branch, and will try to generate an inverse channel model, based not just on one input but on all available branches (2, 3, ...N). The equalizer becomes a MISO (Multiple Input Single Output) system.

This paper is organized as follows: the next section overviews the existing receiver diversity techniques and their established performance. Section III discusses other adaptive, hybrid approaches. Section IV describes the proposed adaptive combiner-equalizer, while section V presents our implementation in Matlab-Simulink and discusses the results. The last section contains our conclusions and envisaged future work.

II. MULTIPLE-INPUT RECEIVER PERFORMANCE

Diversity combining is an established technique for improving the mean throughput of a wireless system by mitigating fading effects.

Receiver combining techniques are a means of implementing space diversity, and they involve the use of multiple antennas at the receiver. In receiver diversity, the independent fading paths associated with multiple receive antennas are combined to obtain a resultant signal that is then passed through a standard demodulator. Most combining techniques are linear: the output of the combiner is a weighted sum of the different fading paths or branches [1]. Some techniques also require signal co-phasing before summation (e.g. MRC).

The best combining performance (the highest combining gain) is given by the most complex technique - MRC (Maximum Ratio Combining). The complexity of MRC comes from the fact that the signals need to be co-phased before summing, and the SNR must be estimated for each branch. The result is obtained by adding the co-phased signals, which are also weighted with values proportional to their SNRs.

There are several types of receiver diversity combiners, with different implementation complexity and overall performance: Threshold Combining (ThC), Selection Diversity Combining (SDC), Maximum Ratio Combining (MRC), and Equal Gain Combining (EGC). For non-dispersive channels, static diversity-combining techniques are effective because simultaneous deep fades in all sub-channels are highly improbable. MRC outperforms the others on flat fading channels, yet is not optimum in dispersive fading conditions because of inter-symbol-

interference (ISI). The challenge remains to adequate the spatial diversity solution to very specific scenarios.

In Maximum Ratio Combining (MRC) the signals from the N receiver-branches are weighted with the complex conjugate of the corresponding sub-channel and then summed. Each signal is assigned a weight, w_i (fig. 1). This technique offers a means of combining the signals from all receiver branches, so that signals with a higher received power have a larger influence on the final output. This combining technique generally requires an individual receiver for each antenna element, and this is the main disadvantage compared to Selection Diversity. Also, since the signals are summed they must have the same phase to maximize performance. This requires not only separate receivers but also a co-phasing and summing device.

On the other hand, MRC produces an output SNR equal to the sum of the individual SNRs, which is an advantage because when none of the arriving signals have an acceptable SNR, this kind of combining may produce an output with an acceptable SNR. Another advantage of MRC is that, even if we have a Rayleigh channel for each branch; the combined signal has no longer Rayleigh distribution.

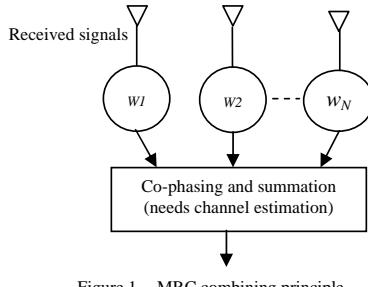


Figure 1. MRC combining principle

Regarding receiver combining, even if a performance hierarchy of these techniques is already established, we have analyzed the existing combining methods for different scenarios [9]. Our simulations, performed on an 802.11a WLAN Simulink platform, have confirmed that receiver combining techniques significantly improve performance in terms of packet error rate (PER), thus ensuring a higher link availability and reliability. Also the bit rate is increased depending on the propagation scenario. The main conclusion was that MRC outperforms the other combining techniques in terms of diversity gain, but this is only for flat fading channels, and it is not the optimum combiner in dispersive fading conditions because of inter-symbol-interference (ISI). The challenge remains to adequate the spatial diversity solution to very specific scenarios.

The aspects that increase the MRC complexity are:

a) *Co-phasing of the signals.* Before summing the signals it is very important to make sure that the signals are in phase. The same principle is used by RAKE receivers. Usually, the solution is to use delay lines and an algorithm that estimates the delay for each branch, and this obviously increases complexity. Combining more than one branch signal

requires co-phasing, where the phase θ_i of the i^{th} branch is removed through the multiplication by $w_i = a_i e^{-j\theta_i}$ for some real-valued a_i . This phase removal requires coherent detection of each branch to determine its phase θ_i .

b) *Computation of the weights.* Equation (1) computes the gain of each branch and the weights are: $w_i = a_i e^{-j\theta_i}$. This implies a method for estimating the SNR on each branch, and this in turn increases the complexity.

$$a_i = \frac{SNR_i}{\sum_{i=1}^{N_{Rx}} SNR_i} \quad (1)$$

where: a_i is the gain of branch i ;

SNR_i is the instantaneous SNR of branch i ;

N_{Rx} is the number of receiver antennas.

III. RELATED APPROACHES

We discuss here some MRC optimizations and combining-equalizing attempts that can be found in recent and old literature. An optimization idea for MRC, and also for MIMO systems, is to reduce the number of active branches, in order to reduce the system complexity. Only the “good” (high-SNR) branches will be selected [5]. This solution does not increase the performance significantly and signal quality (SNR) still needs to be estimated for each branch. By deliberately cancelling part of the information that arrives at the receiver, we affect the link availability.

In [7], a threshold-based generalized selection combining (T-GSC) scheme is proposed. In this proposal, only the branches with signal levels above a specified threshold are combined. This proposal reduces the complexity but does not increase the performance in terms of BER, the disadvantage of deliberate signal cancellation being still present.

Some adaptive solutions try to jointly use different techniques, for instance adaptive modulation and diversity combining [6]. Our solution may also be combined with other techniques (if necessary) and this is still to be tested.

The closest approach to our proposal is that of Balaban and Salz [11], [12] who demonstrate the performance advantage of joint combining and equalization, which is also used in a combiner-equalizer Alcatel patent [13] from ‘97. In both cases there are two distinct operations: first combine, then equalize or first equalize on each branch and then combine. In the patent case there are no numerical results available. Some of the Balaban & Salz versions of the dual diversity combiner-equalizer perform better than our implementation, some do not.

IV. THE PROPOSED ADAPTIVE COMBINER-EQUALIZER

The proposed combiner-equalizer (fig. 2) is based on the following principles:

- (1) tapped delay lines are a solution for correctly combining delayed signals without co-phasing, because they enable access to different delayed versions of the signals.
- (2) the combiner-equalizer may be seen as a classifier and its primary goal is to classify the received symbols (according to the modulation scheme). The classification accuracy is more important than the inverse channel modelling accuracy.
- (3) a general solution for classifying vectors is to use linear or non-linear neural networks. The simplest and fastest structure (widely used for adaptive equalizers) has one linear neuron and the weights are updated using algorithms such as LMS (Least Mean Squares) or RLS (Recursive Least Squares).
- (4) each received signal (branch) adds information that should not be ignored because this information helps the neural network classify the inputs more accurately. At the same time, too much information leads to a slower network because of additional weight computation. All branches are a priori important, and it is up to the combiner-equalizer to combine them properly.

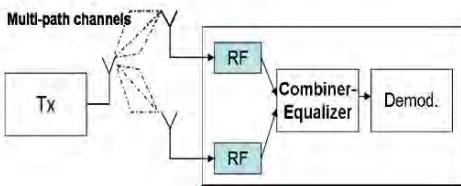


Figure 2. Positioning of the combiner-equalizer on the receiver chain

Figure 3 describes the structure of the proposed combiner-equalizer. This structure is obtained by adding tapped delay lines to a linear adaptive equalizer [4], one for each branch. We have chosen a linear equalizer because it is less complex than a non-linear one (i.e. Radial Basis Functions - RBF or fuzzy based equalizer). The same principle is applicable for non-linear equalizers also.

Additional tapped delay lines are necessary in order to have access to the previous samples of the available branches. The number of delay cells depends on the maximum delay spread supported by the system. The minimum number of cells must be higher than the maximum delay, divided by the sample time (considering the worst case scenario - outdoor conditions).

The delayed versions of the different arriving signals are the inputs of a linear neuron. The same algorithm used by the equalizer, LMS or RLS, will be applied for the additional inputs and will update all the weights. The adaptation algorithm uses the same training sequence that was used for the single-input, regular equalizer. From this

point of view, the combiner-equalizer works exactly as a regular adaptive equalizer.

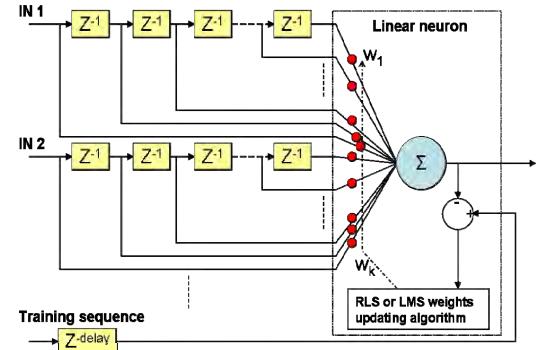


Figure 3. The proposed multiple-input adaptive combiner-equalizer (the 2Rx configuration)

The proposed structure is equivalent to a set of FIR filters using the same summing unit and the same training algorithm. There is no need to co-phase the input signals of the combining-equalizer. There is no need to estimate the SNR for each branch. Instead, the combiner-equalizer minimizes the output error and estimates the weights corresponding to each delayed signal using the training algorithm. We consider that there is no need here to explain how the weights are adapted since the LMS and RLS algorithms are well known in the adaptive filtering.

The complexity of the proposed solution is measured in the number of additional delay cells necessary for the multiple inputs, and in the extra operations needed to update the additional weights. In most of our simulations, we have used 12 delay cells for each branch, to ensure good performance even for outdoor conditions. For indoor conditions the number of delay cells may be reduced to 3 cells per branch, as some basic tests have shown. The complexity may be reduced by decreasing the number of delay cells per branch, and by using the LMS algorithm instead of RLS. For our tests we have chosen RLS for its robustness and accuracy even if the convergence rate is higher for LMS.

V. SIMULATION AND ANALYSIS

In terms of objective of the simulations, we were interested in obtaining the BER performance of the proposed combiner-equalizer under specified channel conditions. We were also interested in fine-tuning the parameters of the design in order to study some performance tradeoffs. In this respect, we consulted the WINNER II channel models specifications [10], where from we have chosen the indoor small-office and outdoor-to-indoor environments, with their corresponding cluster-delay-line models and values (including delays and angles of arrival).

As we wanted to investigate the properties of the equalizer per se, we decided not to burden the simulation with a full system model.

We have implemented the proposed adaptive combiner-equalizer in Simulink, starting from the 4-QAM (QPSK) adaptive equalization block available with Matlab-Simulink (fig. 5). The modified block now manages two or three inputs. We have also replaced the Rician channel block with a selective fading channel (Rayleigh distribution).

Our first simulations were based on three test configurations: the 1Tx-1Rx configuration, with a regular equalizer (no combining), the 1Tx-2Rx and 1Tx-3Rx configurations with the adaptive combiner-equalizer. The channel blocks were Rayleigh-based, with Doppler shift values ranging from 20 to 50 Hz, and delays from 1 μ s to 6 μ s (multipath outdoor environment – worst case scenario), table I.

From the first set of simulations we can see that the combiner-equalizer performance is very good (as depicted in figure 4). For instance, reading from the graphical representation, for a SNR = 0.5dB, 1Tx-1Rx configuration (regular equalizer), we obtain a BER=0.3444. The combiner-equalizer BER = 0.0216, for two branches, and BER = 0.00137 for three branches. The combining gain is 20dB (for 2 branches) at a BER = 0.02 and higher for lower BER values.

Figure 4 shows the test results for E_b/N_0 ranging from -5 to 20 dB (SNR between -10 and 40 dB). For instance, the 1Tx-2Rx performance for a SNR = 0dB, BER = 0.02, is comparable to that of the 1Tx-1Rx for a SNR = 20 dB. The same BER value may be obtained using three branches for a SNR = -6.5 dB.

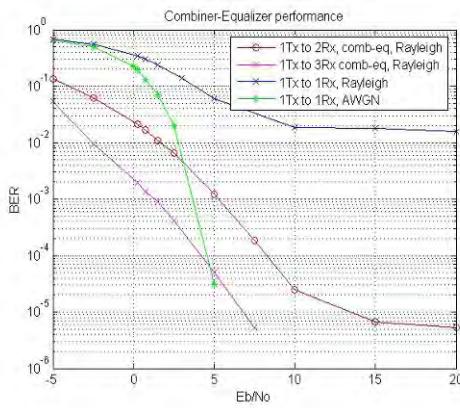


Figure 4. Adaptive combiner-equalizer performance (Rayleigh channel, QPSK transmission)

In order to make our results easier to reproduce elsewhere, we present the simulation settings. The results were obtained using a modified version of the Simulink QPSK adaptive, linear equalizer. The combiner-equalizer was obtained by modifying a LMS/RLS equalizer, and

eliminating the pre-equalization block, used in the initial block-diagram. We have used the 50-symbol training sequence of the initial implementation (per each 250-symbol frame). The equalizer is a synchronous one (the delay per tap is equal to the symbol duration). The initial training period was not used for performance evaluation, we have removed the first 5% of each simulation recordings.

For the two-input combiner-equalizer, we have used the same RLS setting, but the LMS learning step had to be reduced from 0.025 to 0.01. For the three-input combiner-equalizer, we have used a 0.005 LMS learning step, and we have also changed the RLS setting, 0.995 for lambda and 0.025+0i for delta. About 1Mb of data was transmitted for each simulation. Because of this reduced number of transmitted bits, we expect a satisfying precision in the -5 to 10dB E_b/N_0 range, and a lower precision between 10 and 20 dB.

TABLE I. INITIAL TEST SETTINGS

Configuration	Settings (dispersive fading)		
	delay	gain	Doppler shift
1Tx - 1Rx	[0 1e-6]	[0 -3]	50 Hz
1Tx - 2Rx	[0 1e-6]	[0 -3]	50 Hz
	[0 1e-6 5e-6]	[0 -3 -5]	30 Hz
1Tx - 3Rx	[0 1e-6]	[0 -3]	50 Hz
	[0 1e-6 5e-6]	[0 -3 -5]	30 Hz
	[0 1e-6 5e-6 8e-6]	[0 -3 -3 -4]	20 Hz

Tables II and III synthesize the main simulation settings for indoor and outdoor scenarios and the corresponding calculated outage probability ($BER > 10^{-5}$).

TABLE II. INDOOR SIMULATIONS

INDOOR (5ns-200ns)						
Fading	flat					
Multipath channels	2ch			3ch		
Mean SNR [dB]	5	10	20	5	10	20
DS [Hz]	10 – 20			10 – 5 – 20		
Outage ($BER > 10^{-5}$)	1	1	0	1	0.96265	0
Fading	dispersive					
Multipath channels	2ch (5paths)			3ch (6paths)		
Mean SNR [dB]	5	10	20	5	10	20
DS [Hz]	10			10		
Outage ($BER > 10^{-5}$)	1	1	0.47501	1	1	0

TABLE III. OUTDOOR SIMULATIONS

OUTDOOR (1us-20us)						
Fading	flat					
Multipath channels	2mpch			3mpch		
SNR [dB]	5	10	20	5	10	20
DS [Hz]	30 – 50			50 – 60 – 45		
Outage ($BER > 10^{-5}$)	1	1	0.36376	1	1	0.055234
Fading	dispersive					
Multipath channels	2mpch (5paths)			3mpch (6paths)		
SNR [dB]	5	10	20	5	10	20
DS [Hz]	30 – 50			50 – 60 – 45		
Outage ($BER > 10^{-5}$)	1	1	1	1	1	0.11704

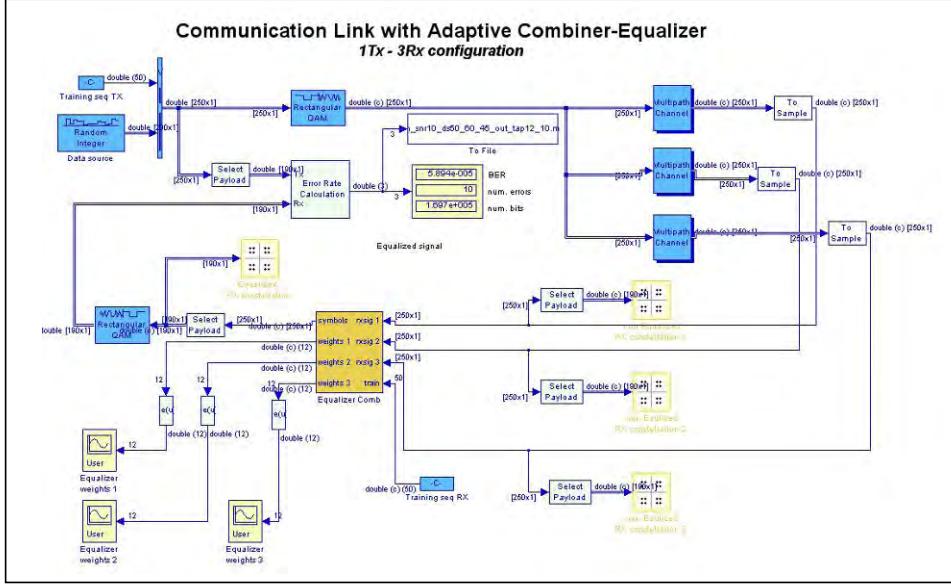


Figure 5. Integration of the multiple-input combiner-equalizer onto a QPSK transmission chain

VI. CONCLUSIONS

In this paper we propose an adaptive combining-equalizing approach for multiple-input receivers. The novelty of our solution lies in the unified combining-equalization approach - the two classical operations being performed simultaneously and not sequentially as in the examples presented in the ‘related work’ section. The advantages of the proposed solution are: easy to extend for N receiver antennas, easy to integrate in a transmission chain, low complexity, no need of co-phasing and gain computation for each branch, increased diversity gain (compared to classical MRC implementations).

The combiner-equalizer principle is simple: to classify each symbol, function of previous symbols on each branch, using the existing training sequence for error estimation.

The proposed solution enables us to adjust the complexity-performance balance, by modifying the number of delay cells per branch, and by choosing the LMS algorithm instead of RLS. The performance can probably be increased even more by using a non-linear neural network like RBF.

After an initial set of test simulations we were able to obtain the BER performance of the proposed combiner-equalizer, under specified channel conditions. We were also interested in fine-tuning the parameters of the design in order to study some performance tradeoffs. Thus we noticed that the three-input configuration ensures a better outage probability (both indoor and outdoor), and that three taps on

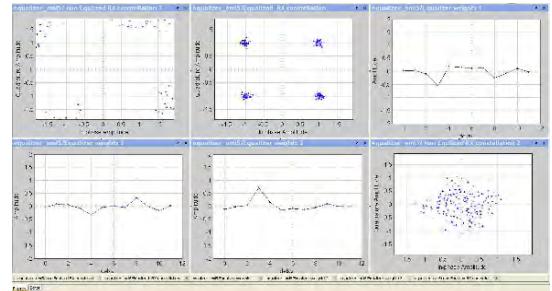


Figure 6. Snapshot of the combiner-equalizer performance (one of the worst-case scenarios – outdoor, mean SNR=10dB, high Doppler shift)
 a), f) non-equalized constellations, b) equalized Rx constellation,
 c), d), e) combiner-equalizer weights adaptation.

each branch are enough for a good indoor performance. As future work, we intend to define a cost function for this unified processing block. Another step is to add the code correction function to the proposed combiner-equalizer [8], in order to see if the hybrid approach outperforms the regular solution. An analytical final analysis is necessary - for the moment the results are based on simulations. Other MRC-based implementations also need to be simulated in the very same conditions for more accurate comparison.

REFERENCES

- [1] Angeliki Alexion, Martin Haardt, "Smart Antenna Technologies for Andreea Goldsmith, "Wireless Communications", Stanford University, Cambridge, Univ. Press, 2005.
- [2] Ramasamy Venkatasubramanian, "Beamforming for MC-CDMA", Master Thesis at Virginia Polytechnic Institute and State University
- [3] Cui, J., Falconer, D. D., and Sheikh, A. U. 1997. Performance evaluation of optimum combining and maximal ratio combining in the presence of co-channel interference and channel correlation for wireless communication systems. *Mob. Netw. Appl.* 2, 4 (Dec. 1997), 315-324.
- [4] Chong-Yung Chi, Chih-Chun Feng, Chii-Horng Chen and Ching-Yung Chen, "Blind Equalization and System Identification Batch Processing Algorithms, Performance and Applications", Springer-Verlag London Limited 2006, ISBN-10: 1846280222.
- [5] Mohamed-Slim Alouini, "Adaptive Modulation and Combining for Bandwidth and Power Efficient Communication over Fading Channels", Third BEATS/CUBAN/WIP Workshop, Sidi Bou Said, Tunisia, May 23, 2005.
- [6] Hong-Chuan Yang, Nesrine Belhaj, and Mohamed-Slim Alouini, "Performance Analysis of Joint Adaptive Modulation and Diversity Combining Over Fading Channels", *IEEE Transactions On Communications*, Vol. 55, No. 3, March.2004
- [7] Ahmed Iyanda Sulyman, Maan Kousa, "Bit Error Rate Performance Analysis of a Threshold-Based Generalized Selection Combining Scheme in Nakagami Fading Channels", EURASIP Journal on Wireless Communications and Networking 2005:2, 242–248, 2005 Hindawi Publishing Corporation.
- [8] Berber, S.M.; Kecman, V., "Convolutional decoders based on artificial neural networks," *Neural Networks, 2004. Proceedings. 2004 IEEE International Joint Conference on* , vol.2, no., pp. 1551-1556 vol.2, 25-29 July 2004.
- [9] Ligia Chira, Tudor Palade, "The Adaptive Potential of Space Diversity Techniques", *The Mediterranean Journal of Electronics and Communications*, Vol. 3, No. 3, 2007, pp.100-109, 2007 SoftMotor Ltd. ISSN: 1744-2400
- [10] IST-4-02776 WINNER II report, WINNER II channel models, 2007
- [11] Philip Balaban, Jack Salz, "Dual Diversity Digital Combining and Equalization in Cellular Mobile Radio", *IEEE Transactions On Vehicular Technology*, vol. 40, no. 2, May 1991
- [12] Philip Balaban, Jack Salz, "Optimum Diversity Combining and Equalization in Digital Data Transmission with Applications to Cellular Mobile Radio-Part I: Theoretical Considerations and Part II: Numerical Results", *IEEE Transactions On Communications*, vol. 40, no. 5, may 1992
- [13] Combiner-Equalizer Alcatel Patent, 1997

KSAm – An Improved RC4 Key-Scheduling Algorithm for Securing WEP

Bogdan Crainicu

“Petru Maior” University of Târgu Mureş
N. Iorga, No. 1
Târgu Mureş, MS 540088, ROMANIA
cbogdan@upm.ro

Florian Mircea Boian

“Babeş-Bolyai” University of Cluj-Napoca
M. Kogălniceanu, No. 1
Cluj-Napoca, CJ 400084, ROMANIA
florin@cs.ubbcluj.ro

Abstract— RC4 is one of the most widely used stream cipher. In this paper we propose a new variant of RC4 Key-Scheduling Algorithm, called KSAm, whose primary goal is to address the FMS (Fluhrer-Mantin-Shamir) weakness of WEP-like cryptosystems, where IV precedes the secret key. Security analysis of KSAm reveals that the FMS IV weakness is removed by destroying the FMS resolved condition. KSAm has a huge internal state of ≈ 3748 bits and provides a better distribution of the state table elements than original KSA. Further, based on the Roos’ experimental observation, we also found a weaker probabilistic correlation between the first three words of the secret key and the first three entries of the state table after KSAm, which causes a negligible bias of the first word of the RC4_{KSAm} output stream towards the sum of the first three words of the secret key. The effect of this negligible bias can be easily avoided by discarding only the first word from the RC4_{KSAm} output stream.

Index Terms—FMS attack, FMS resolved condition, IV weakness, KSA, KSAm, RC4_{KSA} , RC4_{KSAm} , weak keys, WEP

I. INTRODUCTION

RC4 is a stream cipher which was designed by Ron Rivest in 1987 and kept as a trade secret until it was anonymously posted to the Cypherpunks mailing list in 1994. A variable-length key is used to initialize a state table S, which is a permutation of all the $N = 2^n$ possible n bits words, along with two n-bits indices i and j (in practical applications $n = 8$).

Because of its simplicity and speed, RC4 is the most widely used stream cipher; for example, it is used in the SSL/TLS (Secure Socket Layer/Transport Layer Security) standards, WEP (Wired Equivalent Privacy), and it can be also found in email encryption products.

There have been performed many critical analyses of RC4 and RC4-based WEP implementations, and have, therefore, been discovered significant weaknesses: states that RC4 can never enter [6], correlations between the secret and the known parts of the RC4 state [16], weak IVs/keys [2], [8], [14], [18], [19], [22], [23], [30], [31], [37], [45], invariance weakness [8], bias in the second output [25], related key attack [8], [13],

state recovery attack [20], [29], [32], [40], distinguishing attack [7], [11], [25]-[28], [33], [34], ciphertext-only attack [9], key-recovery attack [17], [27], [44], active attack [3], [43], fragmentation attack [3], biased distribution of RC4 initial permutation [24], [28], flaws in the IEEE 802.11 access control mechanism [1], [4].

The most incisive attack on RC4 was described by Fluhrer, Mantin and Shamir in [8] (also known as FMS attack), where RC4 was proved to be completely insecure in mod of operation which is used in WEP protocol, in which a secret key is concatenated with known Initialization Vectors (IVs) in order to encrypt the plaintext. Stubblefield, Ioannidis and Rubin exploit this design failure and implement in [41] and [42] a passive attack against WEP; they were able to recover the 128 bit secret key used in a production network. This WEP’s mode of operation can be addressed by discarding the first $N = 2^n$ outputs or by using a secure hash function to build the session key from the IV and the secret key. Based also on own results [8], Fluhrer, Mantin and Shamir show in [9] the details of a passive ciphertext-only attack which can find an arbitrarily long key in negligible time.

In the last years, a number of proposals for modifying RC4 algorithm have been advanced, all of them aiming to address the most critical weaknesses of RC4: Paul and Preneel present in [34] a new pseudorandom bit generator called RC4A, Zoltak proposes in [46] the VMPS stream cipher, and Gong, Gupta, Hell and Nawaz also propose in [12] a new 32/64-bit RC4-like keystream generator.

In this paper, we analyze the Key-Scheduling Algorithm (KSA) and propose a modified version of KSA, called KSAm¹, which fortifies the WEP protocol against FMS IV weakness, where IV precedes the secret key. The KSAm adds a new secret key-dependent scrambling loop (*Scrambling 1*) between the initialization stage and the original scrambling (*Scrambling 2*), with a view to leaving the array S scrambled “as far as possible” from the identity permutation. This feature has impact not only on practical WEP implementations, but also in constructing ciphertext only distinguishers. From

¹ Here and in the rest of the paper RC4_{KSA} means the original RC4, and RC4_{KSAm} means RC4 with KSAm as key-scheduling algorithm. PRGA remains the same in both RC4 versions.

another standpoint, by holding two swap operations in KSAm, every entry of state table is swapped at least twice and thereby the probability of getting the FMS resolved condition with known values for $S[1]$, $S[S[1]]$ and $S[S[1] + S[S[1]]]$ becomes very small. Thus, we demonstrate that the attacker has no possibilities to manipulate KSAm permutation in order to reach the FMS resolved condition.

Besides the KSAm' effect on the FMS IV weakness, the paper investigates the randomness of the permutation after KSAm. Based on the Diehard battery of tests of randomness [5], the results show a better distribution of state table entries after KSAm than that provided by the original KSA.

KSAm has a huge internal state of ≈ 3748 bits and therefore it is much harder to reconstruct its internal state in the event of a “branch and bound” attack like that analyzed in [20]. On the other hand, KSA_m is slower than KSA since there is an additional scrambling procedure; it takes almost twice as long as KSA, but this extra computation time is negligible – a specific feature of RC4_{KSA} is that it is very fast in software implementations.

Our analyses of KSAm reveal a weaker probabilistic correlation between the first three words of the secret key and the first three entries of the state table after KSAm, which causes a negligible bias of the first word produced by RC4_{KSAm} towards the sum of the first three words of the secret key. Moreover, we test the Roos class of weak keys [37] for RC4_{KSAm}, and we ascertain that for these keys the first output is equal to $2K[2] + 3$ with a mean probability of $2^{-7.4}$. In comparison with the value of $2^{-2.85}$ obtained by Roos, our value is a real gain, since it is very close to the ideal value of 2^8 . In order to mitigate these vulnerabilities and make RC4_{KSAm} cryptographically secure, it is sufficient to drop only the first byte from the RC4_{KSAm} keystream output, and not 256 as in RC4_{KSA}. Anyway, we suggest a number of 32 bytes to be dumped, as precaution².

The rest of the paper is organized as follows. In Section 2 we propose the KSAm, which is a modified version of the original RC4 key-scheduling algorithm. We analyze here the resistance of KSAm against FMS known IV attack (when IV precedes the secret key), followed by a performance analysis in terms of resources needed and time consumption. Further in this section, we also analyze the distribution of state table entries after KSAm, a probabilistic correlation between words of the secret key and words produced by RC4_{KSAm}, and we test the effect of the Roos weak keys [37] on RC4_{KSAm}.

We conclude in Section 3, providing some future cryptanalytic directions for KSAm research.

Due to space limitations, we do not present neither the RC4 and WEP algorithms nor FMS IV attack (we presume that the reader is familiar with these concepts).

II. KSAm

A. Description

We now propose a modified version of the original KSA, which we denote as KSAm and describe it in Fig. 1.

The KSAm encompasses an additional scrambling loop (*Scrambling 1* – lines (a), (b), (c) and (d)): it takes the secret key and initializes a vector of indices u_0, u_1, \dots, u_{N-1} ; the values of indices u_i are not necessarily unique within the vector of indices, and they are kept secret. Then, it swaps the two values of S pointed to by i and u_i , so that the *Scrambling 1* stage of KSAm ends with a secret state, which is different from the identity permutation with a very high probability. The rest of operations (*Scrambling 2*) remain the same as in the original KSA: it applies the scrambling rounds $N = 2^n$ times, stepping i across S, updating j by adding the previous value of j , $S[i]$ and the next word of the key.

<u>KSA(K, S)</u>	<u>KSAm(K, S)</u>
<i>Initialization:</i>	<i>Initialization:</i>
for $i = 0$ to $N - 1$	for $i = 0$ to $N - 1$
$S[i] = i;$	$S[i] = i;$
$j = 0;$	$j = 0;$
<i>Scrambling:</i>	<i>Scrambling 1:</i>
for $i = 0$ to $N - 1$	for $i = 0$ to $N - 1$ (a)
$j = (j + S[i] + K[i \bmod \ell]) \bmod N;$	$u_i = (S[i] + K[i \bmod \ell]) \bmod N;$ (b)
swap($S[i], S[j]$);	for $i = 0$ to $N - 1$ (c)
	swap($S[i], S[u_i]$); (d)
	$j = 0;$
	<i>Scrambling 2:</i>
	for $i = 0$ to $N - 1$
	$j = (j + S[i] + K[i \bmod \ell]) \bmod N;$
	swap($S[i], S[j]$);

Fig. 1 KSA vs KSAm

B. Security Analysis of KSAm

At a glance, the first observation is that there are now two different scrambling processes, both of them based on the same secret key. Consequently, one of the questions is whether the original scrambling process (*Scrambling 2*) could be eliminated. First of all, since the *Scrambling 1* generates also non-uniform distributions of the state table entries, the coupling of these two scrambling processes provides a stronger randomness to the RC4's state than each of them taken separately (based on the Diehard battery of tests of randomness [5]). Obviously, the computation time needed to execute KSAm is almost twice as much as that used to execute KSA; but even that, the additional time is insignificant. Secondly, we are trying to outdistance the identity permutation, before the PRGA takes place, as far as possible, in a such a way that FMS IV/invariance weaknesses [8] are diminished. Thirdly, a level of compatibility with the original KSA is still required.

1) Identity Permutation

With KSAm, we have two independent scrambling processes; therefore, after running consecutively both of them, each element of the state table will be swapped at least twice (possibly with itself).

² In general, the total number of RC4 outputs that have to be dropped depends on the weaknesses discovered and the experimental data. For RC4_{KSA}, the recommendations range from 128 bytes to 3072. Mironov states in [27]: “...discarding the initial 12×256 bytes most likely eliminates the possibility of a strong attack” and “dumping several times more than 256 bytes from the output stream appears to be just as reasonable a precaution.”

Theorem 1: The probability that a particular single entry $S[i]$ remains unchanged after completion of one of the two scrambling process is:

$$P(S_N[a] = a) = \frac{1}{N} + \left(1 - \frac{1}{N}\right)^{N-1} \quad (1)$$

Proof: At a some point, the index i touches the value a . In this round, with probability $1/N$, $i = j = a$, and therefore $S[a]$ will be swapped with itself. For the rest of the $(N - 1)$ rounds we have $i \neq a$, and $j \neq a$ with probability $(1 - 1/N)$.

For $N = 256$, $P(S_N[a] = a)$ can be modeled as:

$$P(S_N[a] = a) \approx \frac{1}{256} + e^{-1} \approx 0.3637 \quad (2)$$

The probability that all entries N of table S remain unchanged after completion of one of the two scrambling process (that is, the identity permutation) is:

$$P(S_N=\text{identity_permutation}) = \left[\frac{1}{N} + \left(1 - \frac{1}{N}\right)^{N-1} \right]^N \quad (3)$$

The tests³ reveal that none of the 8, 16, 24 and 32-bits keys K produce the identity permutation after completion of KSAm (measured running times of tests were $T_{K=8} \approx 0.003$ sec, $T_{K=16} \approx 0.63$ sec, $T_{K=24} \approx 157.84$ sec, $T_{K=32} \approx 39337$ sec).

2) Internal State of KSAm

The security of KSAm comes also from its huge internal state. The internal state of RC4_{KSA} is approximately 1700 bits for 8-bits words. KSAm provides a much larger size and, as a result, it is much harder to reconstruct its internal state (the values of indices u_i are not necessarily unique; therefore, the number of all possibilities of distributing 2^n elements into 2^n cells where repetitions are allowed is $(2^n)^{2^n}$):

$$L_{\text{RC4-KSAm}} = \log_2(2^n!) \times (2^n)^{2^n} \times (2^n)^2 = [\log_2(2^n!) + (n \times 2^n) + 2n] \\ L_{\text{RC4-KSAm}, n=8} \approx 3748 \text{ bits}$$

In comparison with KSA, KSAm needs only additional 256 bytes of memory for the indices u_i ($n = 8$). Also, the tests show that the additional computational time of the KSAm is negligible – a mod256 operation can be performed with a bitwise AND with 255 (or simple addition of bytes ignoring overflow), while the loop of updating the indices u_i (Fig. 1 – lines (a) and (b)) can be parallelized on a multi-core machine, considering the independence of these updating operations.

3) KSAm and FMS IV Weakness

The proposed KSAm aims to minimize the FMS IV weakness by destroying the FMS resolved condition, and by increasing the randomness of the distribution of the state table entries, including those whose values are pointed out by $S[1]$, $S[S[1]]$ and $S[S[1] + S[S[1]]]$. Since the key is also used in the first scrambling procedure of the KSAm, where every state table entry is swapped at least once, the attacker will not know the entries $S[1]$, $S[S[1]]$ and $S[S[1] + S[S[1]]]$ after one iteration of the second scrambling procedure. Therefore, examining messages with specific IV values such that, at some stage in the second scrambling loop, the KSAm is in a resolved condition as defined in [8], and where the value of $S[S[1] + S[S[1]]]$ reveals informations about the secret key, is useless.

The idea behind the FMS IV attack was first published by Wagner in [45], and involves only looking for IVs that match $(A + 3, N - 1, X)$, for approximately 60 different values for X ; the attacker knows the first A words of the secret key $K[3], \dots, K[A + 2]$, with $A = 0$ initially, and he/she tries to find the next word $K[A + 3]$.

When the IV is prepended to the secret key, the input of KSA and KSAm is as follows:

- Initialization Vector (IV) of size I : $\text{IV}[0]\text{IV}[1]\dots\text{IV}[I - 1]$.
- Secret Key (SK) of size L : $\text{SK}[0]\text{SK}[1]\dots\text{SK}[L - 1]$.
- RC4 Key (K) of size $\ell = I + L$: $K[0\dots\ell] = \text{IV}[0\dots\text{IV}[I - 1]\text{SK}[0]\dots\text{SK}[L - 1] = \text{IV}[0\dots\text{IV}[I - 1]\text{SK}[0]\dots\text{SK}[\ell - I - 1]$.

Considering now a series of IVs of the form $(A + 3, N - 1, X)$ which precede the secret key, we simulate the following scenario for $A = 0$ (all the additions are carried out modulo N):

KSAm – Scrambling 1:

Building vector u :

$$\begin{aligned} i = 0: u_0 &= S[0] + \text{IV}[0] = 0 + 3 = 3, \text{ where } \text{IV}[0] = K[0]; \\ i = 1: u_1 &= S[1] + \text{IV}[1] = 1 + (N - 1) = 0, \text{ where } \text{IV}[1] = K[1]; \\ i = 2: u_2 &= S[2] + \text{IV}[2] = 2 + X, \text{ where } \text{IV}[2] = K[2]; \\ i = 3: u_3 &= S[3] + \text{SK}[0] = 3 + \text{SK}[0], \text{ where } \text{SK}[0] = K[3] \\ \dots \\ i = m: u_m &= (S[m] + K[m \bmod \ell]) \end{aligned}$$

...

Swapping:

$$\begin{aligned} \text{swap}(S[0], S[3]) &\Rightarrow S[0] = 3, S[3] = 0 \text{ (known results)} \\ \text{swap}(S[1], S[0]) &\Rightarrow S[0] = 1, S[1] = 3 \text{ (known results)} \\ \text{swap}(S[2], S[2 + X]) &\Rightarrow S[2] = 2 + X, S[2 + X] = 2 \text{ (known results)} \\ \text{swap}(S[3], S[3 + K[3]]) &\Rightarrow S[3] = 3 + K[3], S[3 + K[3]] = 0 \text{ (3 + K[3] is unknown)} \\ \dots \end{aligned}$$

With probability greater then $e^{-2} \approx 0.1353$ none of the values at $S[0] = 1$ and $S[1] = 3$ will be disturbed in any further swaps of the first scrambling. At this point, the required inequality $S_3[1] < 3$ does not hold, because $S_3[1] = 3$.

KSAm – Scrambling 2:

$$i = 0: j = S[0] + 3 = 4, \text{ swap}(S[0], S[4]) \Rightarrow S[0] = M_1, S[4] = 1 \text{ (M}_1 \text{ is unknown);}$$

³ The test programs were written in C and were run under Linux (kernel 2.6.18-92.1.6.el5xen), on a machine with the following hardware configuration: 1 Intel Xeon 2.33 GHz Dual-Core CPU, 8192 KB Cache, 8 GB RAM.

$i = 1: j = 4 + S[1] + (N - 1) = 6$, swap($S[1], S[6]$) $\Rightarrow S[1] = M_2$, $S[6] = 3$ (M_2 is unknown);
 $i = 2: j = 6 + S[2] + X = 8 + 2X$, swap($S[2], S[8 + 2X]$), where $S[2] = 2 + X$ with probability $e^{-1} \approx 0.3678$, before swap, and $S[8 + 2X] = M_3$ (M_3 is unknown) $\Rightarrow S[2] = M_3$, $S[8 + 2X] = 2 + X$;
 $i = 3: j = 8 + 2X + S[3] + K[3] = 11 + 2(X + 2K[3])$, swap($S[3], S[11 + 2X + 2K[3]]$), where $S[3] = 3 + K[3]$ with probability $e^{-1} \approx 0.3678$, before swap, and $S[11 + 2(X + 2K[0])] = M_4$ (M_4 is unknown) $\Rightarrow S[3] = M_4$, $S[11 + 2(X + 2K[3])] = 0$;
 \dots

Next, PRGA takes place:

$i = 1: j = S[1] = M_2$ with probability $e^{-1} \approx 0.3678$, swap($S[1], S[M_2]$),
 $Z = \text{Out} = S[S[M_2]] + S[1]$

At this moment, $Z = \text{Out}$ will be output as the first PRGA word. We assume that the attacker knows this word and he/she aims to reverse it back into the first word $SK[0]$ of the secret key SK . Based on the details of the IV attack described in [8], we test now whether we can predict the value of $SK[0]$:

$$SK[0] = K[3] = S_2^{-1}[\text{Out}] - j_2 - S_2[3] \quad (4)$$

Fluhrer, Mantin and Shamir recommend in [8] the use of the following equations immediately after the KSA to determine whether a particular IV is weak. So, for $B = 0$, we have:

$$X = S_3[1] < 3 \quad (5)$$

$$X + S_3[X] = 3 \quad (6)$$

Since the entry $S[1]$ is already affected by a secret key-dependent swapping procedure during the second scrambling ($S_1[1] = M_2$), searching for IV values that, after the first 3 steps, set up the permutation S such that $S_3[1] + S_3[S_3[1]] = 3$ ($S_1[1] + S_1[S_1[1]] = I + B$, where $I = 3$ and $B = 0$), is pointless. Moreover, taking into account that the first scrambling leaves S in a relatively random state, we have at least one unknown value in the right member of the Equation (4), namely the last term ($S_2[3] = 3 + K[3]$) whose value depends on the secret key K . Consequently, the attacker has no possibilities to manipulate KSAm in order to reach the resolved condition as it is defined in [8].

4) Considerations about Randomness of the Permutation after KSAm and Roos Weak Keys

Another goal of KSAm is to provide a better distribution of the state table elements than KSA. In order to achieve this goal, KSAm comprises two scrambling loops, called *Scrambling 1* and *Scrambling 2*. *Scrambling 1* loop makes the difference between the original RC4_{KSA} and RC4_{KSAm}. The design of KSAm tries to follow the Knuth's observation [21]: instead of swapping $S[i]$ with a random entry, it must be swapped with an entry randomly chosen from $S[i]$ to $S[N - 1]$. Although the implementation of this concept is quite problematic because of randomness of key K , the algorithm behind *Scrambling 1* is relatively simple: a (roughly) linear "growing" of u_i values so that, at least for the first entries, $S[u_i] \in [i, N-1]$. As we stated previously, *Scrambling 1* alone

did not pass all of the Marsaglia's Diehard battery of tests [5]; instead, by preceding *Scrambling 2*, they form together a scrambling block which successfully gets over ten Marsaglia's Diehard battery of tests. Within these tests, we give special attention to the values of entries $S[1]$, $S[S[1]]$ and $S[S[1]] + S[S[1]]$.

Since the most important biases found in RC4 are related to the first output words, our analysis is also focused on the value prediction of the first state table entries after both of the KSAm scramblings.

When starting with the first steps of the original KSA swapping, we have a high probability that the entries pointed to by the index j have not themselves been involved yet in any previous shuffles. Roos observes in [37]:

Result 1 [37]: Given a key length of K bytes, and $E < K$, there is a 37 % probability that element E of the state table depends only on elements $0 \dots E$ (inclusive) of the key.

Result 2 [37]: The most likely value for element E of the state table is: $S[E] = X(E) + E(E+1)/2$, where $X(E)$ is the sum of bytes $0 \dots E$ (inclusive) of the key.

We consider Result 2 [37] for KSAm:

Theorem 2: Probability that the value for the first few elements E of the state table after KSAm is $S[E] = 2X[E] + E(E+1)/2$, where $X(E)$ is the sum of bytes $0 \dots E$ (inclusive) of the key and $E < K$, is:

$$P(S[E] = 2X[E] + E(E+1)/2) = [1/N + (1 - 1/N)^{N-1}] \times (1 - 1/N)^p, \\ p = N(E+2) + [E(E-1) - 4]/2$$

Proof:

KSAm – Scrambling 1:

Building vector u_i :

$i = 0: u_0 = S[0] + K[0] = 0 + K[0];$
 $i = 1: u_1 = S[1] + K[1] = 1 + K[1];$
 $i = 2: u_2 = S[2] + K[2] = 2 + K[2];$
 $i = 3: u_3 = S[3] + K[3] = 3 + K[3];$
 \dots

Swapping:

$\text{swap}(S[0], S[K[0]]) \Rightarrow S[0] = K[0]$; with probability $(1 - 1/N)^{N-1}$ the value referenced by $S[0]$ will not participate in any further swaps of *Scrambling 1*;
 $\text{swap}(S[1], S[1 + K[1]]) \Rightarrow S[1] = 1 + K[1]$; with probability $(1 - 1/N)^{N-1}$ the value referenced by $S[1]$ will not participate in any further swaps of *Scrambling 1*;
 \dots

KSAm – Scrambling 2:

$i = 0: j = S[0] + K[0] = K[0] + K[0] = 2K[0]$ (only if $S[0] = K[0]$), $\text{swap}(S[0], S[2K[0]])$; $S[2K[0]] = 2K[0]$ with probability $[1/N + (1 - 1/N)^{N-1}] \Rightarrow P(S_{\text{after-Scrambling1+Scrambling2}}[0] = 2X[0] - 2K[0]) = P(S_{\text{after-Scrambling1}}[2K[0]] = 2K[0]) \times P(S_{\text{after-Scrambling1}}[0] = K[0]) \times \times P(S_{\text{after-Scrambling2}}[0] = 2K[0]) = [1/N + (1 - 1/N)^{N-1}] \times [(1 - 1/N)^{N-1}] \times [(1 - 1/N)^{N-1}] = [1/N + (1 - 1/N)^{N-1}] \times (1 - 1/N)^{2N-2};$
 $i = 1: j = j + S[1] + K[1] = 2K[0] + (1 + K[1]) + K[1] = 2K[0] + 2K[1] + 1$ (only if $j_0 = 2K[0]$ and $S[1] = 1 + K[1]$), $\text{swap}(S[1], S[2K[0] + 2K[1] + 1])$; $S[2K[0] + 2K[1] + 1] = 2K[0] + 2K[1] + 1$ with probability $[1/N + (1 - 1/N)^N] \Rightarrow P(S_{\text{after-Scrambling1+Scrambling2}}[1] = 2X[1] + 1 - 2K[0] + 2K[1] + 1) = P(S_{\text{after-Scrambling1+first-round-of-Scrambling2}}[2K[0] + 2K[1] + 1] =$

$$\begin{aligned}
&= 2K[0] + 2K[1] + J \times P(j_0 = 2K[0]) \times \\
&\times P(S_{\text{after-Scrambling1-and-first-round-of-Scrambling2}}[J] = J + K[1]) \times \\
&\times P(S_{\text{after-Scrambling2}}[J] = 2K[0] + 2K[1] + J) = [1/N + (1 - 1/N)^{N-1}] \times \\
&\times (1 - 1/N) \times [(1 - 1/N)^{N-1}] \times [(1 - 1/N)^N] \times [(1 - 1/N)^{N-2}] = \\
&= [1/N + (1 - 1/N)^{N-1}] \times (1 - 1/N)^{3N-2}; \\
&\dots
\end{aligned}$$

The probability $P(S/E) = 2X[E] + E(E+1)/2$ decreases exponentially with respect to N. We can also approximate the relation between probabilities of two adjacent entries as follows:

$$\begin{aligned}
P(S/E+1 = 2X[E+1] + (E+1)(E+2)/2) &= \\
&= \left[\left(1 - \frac{1}{N}\right)^{N+E} \right] \times P(S/E) = 2X[E] + E(E+1)/2
\end{aligned}$$

The results of a practical evaluation of these probabilities are given in Table 1 for the first three entries generated by a number of 1000000 64-bit random keys. For the rest of the state table entries, we consider the asymptotic value of 0.39.

TABLE 1
PRACTICAL EVALUATION OF $P(S/E) = 2X[E] + E(E+1)/2$

State table entries	Percentage of correct predictions
S[0]	3,97
S[1]	1,65
S[2]	0,54

Roos describes in [37] a class of RC4_{KSA} weak keys: for keys which have $K[0] + K[1] = 0$, the first output is equal to $K[2] + 3$ with probability $2^{-2.85}$. Paul, Rathi and Maitra theoretically prove in [35] the Roos' experimental observation related to these keys. Accordingly, applying these weak keys to RC4_{KSAm}, the first word generated by RC4_{KSAm} will be Output = $Z_1 = S[2] = 2K[2] + 3$ with a mean probability of $2^{-7.4}$. The probability obtained is very promising since it is so close to the value of 2^{-8} . Even that, as further safety precautions, in order to thwart against a prefix attack, our recommendation remains as stated in many RC4 related research papers [8], [9], [24]-[28],[38], namely discarding the initial bytes of PRGA outputs or generating the session key by a secure hash function. For RC4_{KSA} the suggestion is to drop at least 256 bytes (Mironov even suggests in [28] dropping the initial 12×256 bytes), while for RC4_{KSAm} discarding only the first byte will make RC4_{KSAm} cryptographically secure. Nevertheless, we recommend a number of 32 bytes to be dumped, as a reasonable prudence.

III. CONCLUSIONS AND FUTURE WORK

We showed a modified version of KSA, called KSAm, whose main goal is to address FMS IV weakness, where IV precedes the secret key, of WEP-like cryptosystems. We proved that KSAm removes FMS IV weakness (IV precedes the secret key) and there are no means to manipulate KSAm in order to reach the resolved condition as it is defined in [8].

RC4_{KSAm} has a huge internal state of ≈ 3748 bits (for $n = 8$), and establishes a truly permutation's randomness (tested with Marsaglia's Diehard battery of tests [5]), which therefore causes a uniform distribution of output Z.

We discovered a negligible bias of the first word of the RC4_{KSAm} output stream towards the sum of the first three words of the secret key. We also analyzed the effect of the Roos weak keys [37] on RC4_{KSAm}: our results reveal that the first output of RC4_{KSAm} is equal to $2K[2] + 3$ with probability of $2^{-7.4}$. Therefore, the Roos keys are not "so weak" for RC4_{KSAm} anymore. Discarding only the first output byte seems to be the right solution in order to protect against above mentioned weaknesses, but our suggestion is still to discard at least 32 bytes.

Since RC4 remains one of the most widely-used stream cipher, being very popular due to its simplicity, protective measures have to be provided against its vulnerabilities. We believe that KSAm can be a viable replacement for KSA, especially to WEP-like cryptosystems, where the secret key is concatenated with an 24-bits Initialization Vector. The future work should focus, first of all, on KSAm effects on FMS IV weakness, where IV follows the secret key, and then on finding, if any, another classes of weak keys and possible statistical biases in the output words which could be used to construct strong distinguisher. And, of course, ideas about general behaviour of RC4_{KSAm} are welcome to be expressed.

REFERENCES

- [1] W. A. Arbaugh, N. Shankar, and Y. C. Justin Wan, "Your 802.11 Wireless Network has No Clothes", *IEEE Wireless Communications*, Vol. 9, No. 6, pp. 44-51, 2002. Available: <http://www.cs.umd.edu/~waa/wireless.pdf>
- [2] A. Bittau, "Additional weak IV classes for the FMS attack", Department of Computer Science, University College London, 2003. Available: <http://www.cs.ucl.ac.uk/staff/a.bittau/sorwep.txt>
- [3] A. Bittau, M. Handley, and J. Lackey, "The Final Nail in WEP's Coffin", in *Proc. 2006 IEEE Symposium on Security and Privacy, S&P'06*, pp. 386-400, 2006. Available: <http://tapir.cs.ucl.ac.uk/bittau-wep.pdf>
- [4] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11", in *Proc. 7th Annual International Conference on Mobile Computing and Networking, MobiCom '01*, Rome, pp. 180-189, 2001. Available: <http://www.cryptopunks.ca/~iang/pubs/wep-mob01.pdf>
- [5] Diehard Battery of Tests of Randomness, G. Marsaglia, 1995. Available: <http://stat.fsu.edu/pub/diehard/>
- [6] H. Finney, "An RC4 cycle that can't happen", Post in sci.crypt, September 1994
- [7] S. Fluhrer and D. McGrew, "Statistical analysis of the alleged RC4 keystream Generator", in *Proc. 7th International Workshop, FSE 2000*, New York, Lecture Notes in Computer Science, Vol. 1978, Springer-Verlag, pp. 66-71, 2001.
- [8] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4", in *Proc. 8th Annual International Workshop, SAC 2001*, Toronto, Lecture Notes in Computer Science, Vol. 2259, Springer-Verlag, pp. 1-24, 2001.
- [9] S. Fluhrer, I. Mantin, and A. Shamir, "Attacks on RC4 and WEP", *CryptoBytes (RSA Laboratories)*, Vol. 5, No. 2, pp. 26-34, 2002. Available: http://www.rsa.com/rsalabs/cryptobytes/cryptobytes_v5n2.pdf
- [10] D. Goldstein and D. Moews, "The identity is the most likely exchange shuffle for large n", *Aequationes Mathematicae*, Vol. 65, No. 1-2, pp. 3-30, 2003.

- [11] J. Dj. Golic, "Linear statistical weakness of alleged RC4 keystream generator", in *Proc. International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT '97*, Konstanz, Lecture Notes in Computer Science, Vol. 1233, Springer-Verlag, pp. 226-238, 1997.
- [12] G. Gong, K. C. Gupta, M. Hell, and Y. Nawaz, "Towards a General RC4-like Keystream Generator", in *Proc. First SKLOIS Conference, CISC 2005*, Beijing, Lecture Notes in Computer Science, Vol. 3822, Springer-Verlag, pp. 162-174, 2005.
- [13] A. Grosul and D. Wallach, "A related key cryptanalysis of RC4", Technical Report TR-00-358, Department of Computer Science, Rice University, 2000. Available: www.weizmann.ac.il/mathusers/itsik/RC4/Papers/GrosulWallach.ps
- [14] D. Hulton, "Practical exploitation of RC4 weaknesses in WEP environments", 2001. Available: <http://www.datastronghold.com/security/articles/hacking-articles/practical-exploitation-of-rc4-weaknesses-in-wep-environments.html>
- [15] 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, ANSI/IEEE Std 802.11, 1999 Edition (R2003). Available: <http://standards.ieee.org/reading/ieee/std/lanman/>
- [16] R. Jenkins, "Isaac and RC4", 1998. Available: <http://burtleburtle.net/bob/rand/isaac.html>
- [17] A. Klein, "Attacks on the RC4 stream cipher", *Designs, Codes and Cryptography*, Vol. 48, No. 3, Springer-Verlag, pp. 269-286, 2008. Available: <http://cage.ugent.be/~klein/RC4/RC4-en.ps>
- [18] KoreK, *Need security pointers*, 2004. Available: <http://www.netstumbler.org/showthread.php?postid=89036&postcount=35>
- [19] KoreK, *Next generation of WEP attacks?*, 2004. Available: <http://www.netstumbler.org/showpost.php?p=93942&postcount=35>
- [20] L. R. Knudsen, W. Meier, B. Preneel, V. Rijmen, and S. Verdoollaeghe, "Analysis Methods for (Alleged) RC4", in *Proc. International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT'98*, Beijing, Lecture Notes in Computer Science, Springer-Verlag, Vol.1514, pp.327-341, 1998.
- [21] D. E. Knuth, "The Art of Computer Programming", Third edition, Volume 2, Addison-Wesley, 1997.
- [22] K. Kobara and H. Imai, "Key-Dependent Weak IVs and Weak Keys in WEP - How to Trace Conditions Back to Their Patterns -", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E89-A, No. 8, pp. 2198-2206, 2006.
- [23] K. Kobara and H. Imai, "IVs to Skip for Immunizing WEP against FMS Attack", *IEICE Transactions on Communications*, Vol.E91-B, No.1, pp. 218-227, 2008.
- [24] I. Mantin, "The Security of the Stream Cipher RC4", Master Thesis, The Weizmann Institute of Science, 2001.
- [25] I. Mantin and A. Shamir, "A practical attack on broadcast RC4", in *Proc. 8th International Workshop, FSE 2001*, Yokohama, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2355, pp. 87-104, 2002.
- [26] I. Mantin, "Predicting and Distinguishing Attacks on RC4 Keystream Generator", in *Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2005*, Aarhus, Lectures Notes in Computer Science, Vol. 3494, Springer-Verlag, pp. 491-506, 2005.
- [27] I. Mantin, "A Practical Attack on the Fixed RC4 in the WEP Mode", in *Proc. 11th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2005*, Chennai, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3788, pp. 395-411, 2005.
- [28] I. Mironov, "(Not So) Random Shuffles of RC4", in *Proc. 22nd Annual International Cryptology Conference, Advances in Cryptology, CRYPTO 2002*, Santa Barbara, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2442, pp. 304-319, 2002.
- [29] S. Mister and S. E. Tavares, "Cryptanalysis of RC4-like Ciphers", in *Proc. 5th Annual International Workshop, SAC 1998*, Kingston, Lecture Notes in Computer Science, Springer-Verlag, Vol.1556, pp. 131-143, 1999.
- [30] T. Ohigashi, Y. Shiraishi, and M. Morii, "Most IVs of FMS Attack-Resistant WEP Implementation Leak Secret Key Information", in *Proc. 2005 Symposium on Cryptography and Information Security*, Maiko, Vol. 4, pp. 1957-1962, 2005.
- [31] T. Ohigashi, Y. Shiraishi, and M. Morii, "FMS Attack-Resistant WEP Implementation Is Still Broken - Most IVs Leak a Part of Key Information -", in *Proc. International Conference, CIS 2005*, Xi'an, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3802, pp. 17-26, 2005.
- [32] T. Ohigashi, Y. Shiraishi, and M. Morii, "New Weakness in the Key-Scheduling Algorithm of RC4", *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Vol. E91-A, No. 1, pp. 3-11, 2008.
- [33] S. Paul and B. Preneel, "Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator", in *Proc. 4th International Conference on Cryptology in India, INDOCRYPT 2003*, New Delhi, Lecture Notes in Computer Science, Springer-Verlag, Vol. 2904, pp. 52-67, 2002.
- [34] S. Paul and B. Preneel, "A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher", in *Proc. 11th International Workshop, FSE 2004*, Delhi, Lecture Notes in Computer Science, Springer-Verlag, Vol. 3017, pp. 245-259, 2004.
- [35] G. Paul, S. Rath, and S. Maitra, "On non-negligible bias of the first output bytes of RC4 towards the first three bytes of the secret key", *Designs, Codes and Cryptography*, Vol. 49, No. 1-3, Springer-Verlag, pp. 123-134, 2008.
- [36] D. Robbins and E. Bolker, "The bias of three pseudo-random shuffles", *Aequationes Mathematicae*, Vol. 22, pp. 268-292, 1981.
- [37] A. Roos, "Class of weak keys in the RC4 stream cipher", Two posts in sci.crypt, message-id 43u1eh\$1j3@hermes.is.co.za and 44ebge\$llf@hermes.is.co.za, 1995.
- [38] R. Rivest, "RSA security response to weaknesses in key scheduling algorithm of RC4", Tech Notes, RSA Laboratories, 2001. Available: <http://www.rsasecurity.com/rsalslab/node.asp?id=2009>
- [39] F. Schmidt and R. Simion, "Card shuffling and a transformation on S_n ", *Aequationes Mathematicae*, Vol. 44, pp. 11-34, 1992.
- [40] Y. Shiraishi, T. Ohigashi, and M. Morii, "An improved Internal-State Reconstruction Method of a Stream Cipher RC4", in *Proc. IASTED International Conference on Communication, Network, and Information Security, CNIS 2003*, New York, pp. 132-135, 2003.
- [41] A. Stubblefield, J. Ioannidis, and A. Rubin, "Using the Fluhrer, Mantin, and Shamir attack to Break WEP", Technical Report TD-4ZCPZZ, AT&T Labs, 2001.
- [42] A. Stubblefield, J. Ioannidis, and A. Rubin, "A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP)", *ACM Transactions on Information and System Security (TISSEC)*, Vol. 7, No. 2, pp. 319-332, 2004.
- [43] E. Tews, R. P. Weinmann, and A. Pyshkin, "Breaking 104 bit WEP in less than 60 seconds", in *Proc. 8th International Workshop, WISA 2007*, Jeju Island, Lecture Notes in Computer Science, Vol. 4867, Springer-Verlag, pp. 188-202, 2008. Available: <http://eprint.iacr.org/2007/120.pdf>
- [44] S. Vaudenay and M. Vuagnoux, "Passive-only Key Recovery Attacks on RC4", in *Proc. 14th International Workshop, SAC 2007*, Ottawa, Lecture Notes in Computer Science, Vol. 4876, Springer-Verlag, pp. 344-359, 2007. Available: <http://infoscience.epfl.ch/record/115086/files/VV07.pdf>
- [45] D. Wagner, "My RC4 weak keys", Post in sci.crypt, message-id 447011Scbj@cnn.princeton.edu, 1995. Available: <http://www.cs.berkeley.edu/~daw/my-posts/my-rc4-weak-keys>
- [46] B. Zoltak, "VMPC One-Way Function and Stream Cipher", in *Proc. 11th International Workshop, FSE 2004*, Delhi, Lectures Notes in Computer Science, Vol. 3017, Springer-Verlag, pp. 210-225, 2004.

Ubiquitous Media Communication Algorithms

Kostas E. Psannis

Abstract—This paper proposes an efficient algorithm for H.264/AVC streaming over error prone channels. H.264/AVC Redundant slices feature is an error robustness feature allowing the encoder to send an extra representation of a frame region that can be used if the primary representation is corrupted or lost. Redundant slices tool allow the insertion of primary slices and one or more additional secondary slices belongs to the original frame in the same bit stream. If a primary slice is affected by errors, it can be replaced by an error-free redundant one; otherwise the redundant slices are discarded. Unlike previous methods, in which redundant slices are statically allocated, typically at the end of the transmission frame, we suggest a more effective allocation scheme. Moreover a dynamic Flexible Macroblock Ordering (FMO) type-2 technique is employed for specific slices which are dedicated for Region of Interest (ROI). Then, redundancy slices are generated representing the foreground ROI. Compared with the H.264/AVC conventional standard, our proposed approach can effectively enhance the smoothness of the video. The proposed redundant slices allocation with dynamic FMO type-2 technique can be used and integrated into H.264/AVC without violating the standard

Index Terms—Media Communications, Ubiquitous Media, Media Transmission Algorithm, Error Prone Channels.

I. INTRODUCTION

Today media are increasingly ubiquitous: more and more people live in a world of Internet pop-ups and streaming television, mobile phone texting and video clips, MP3 players and pod-casting. The media mobility means greater connectivity via smart wireless environments in the office, the car and airport. It also offers greater possibilities for recording, storage and archiving of media content. Media communications is fundamentally different from data communication, since they are delay and loss sensitive. Unlike data packets, late arriving video packets are useless to the video decoder. Therefore the retransmission techniques are not generally applicable to video communication applications with low delay requirements. There are additional challenges for supporting video communications especially over wireless networks. Due to the mobility nodes, the topology of the network may change frequently. Thus the established connection routes between senders and receivers are likely to be broken during video transmission, causing interruptions, freezes, or jerkiness in the received video signal. These constraints and challenges, in combination with the delay and

Kostas E. Psannis is with the Department of Technology Management, University of Macedonia, Greece, emails: kpsannis@uom.gr, mobility2net@gmail.com).

loss sensitive of media streaming applications, make video communications a challenging proposition [1].

H.264/AVC is the current video standardization project of the ITU-T Video Coding Experts Group (VCEG) and the ISO/IEC Moving Picture Experts Group (MPEG). The main goals of this standardization effort are to develop a simple and straight forward video coding design, with enhanced compression performance, and to provide a “network-friendly” video representation which addresses “conversational” (videotelephony) and “non-conversational” (storage, broadcast or streaming) applications. The MPEG-2 video coding standard [1], which was developed about 10 years ago, was the enabling technology for all digital television systems worldwide. H.264/AVC has achieved a significant improvement in the rate-distortion efficiency – providing, typically, a factor of two in bit-rate savings when compared with existing standards such as MPEG-2 Video. It allows an efficient transmission of TV signals over satellite (DVB-S), cable (DVB-C) and terrestrial (DVB-T) platforms. However, other transmission media such as xDSL or UMTS offer much smaller data rates. The H.264/AVC design covers a Video Coding Layer (VCL), which efficiently represents the video content, and a Network Abstraction Layer (NAL), which formats the VCL representation of the video and provides header information in a manner appropriate for conveyance by particular transport layers or storage media.[2]. Moreover the H.264/AVC standard introduces enhanced error robustness capabilities enabling resilient and reliable transmission of compressed video signals over wireless lossy packet networks. Those robustness capabilities are achieved by integrating some new error resilience tools that are essential for a proper delivery of real-time video services. Those tools include the Intra Refreshing (IR), Arbitrary Slice Ordering (ASO), Sequence Picture Parameter Sets (PPS), Redundant Slices (RS) tools and Flexible Macroblock Ordering (FMO) [1].

H.264/AVC supports five different slice-coding types. The simplest one is the I slice (where —I” stands for intra). In I slices, all macroblocks are coded without referring to other pictures within the video sequence. On the other hand, prior-coded images can be used to form a prediction signal for macroblocks of the predictive-coded P and B slices (where —P”stands for predictive and —B” stands for bi-predictive).The remaining two slice types are SP (switching P) and SI (switching I), which are specified for efficient switching between bitstreams coded at various bit-rates. The Inter prediction signals of the bitstreams for one selected SP frame are quantized in the transform domain, forcing them into a coarser range of amplitudes. This coarser range of amplitudes

permits a low bit-rate coding of the difference signal between the bitstreams .SI frames are specified to achieve a perfect match for SP frames in cases where Inter prediction cannot be used because of transmission errors .In order to provide efficient methods for concealment in error-prone channels with low delay applications, a feature called Flexible Macroblock Ordering (FMO) is supported by H.264/AVC. FMO specifies a pattern that assigns the macroblocks in a picture to one or several slice groups. Each slice group is transmitted separately. If a slice group is lost, the samples in spatially neighboring macroblocks that belong to other correctly-received slice groups can be used for efficient error concealment. The allowed patterns range from rectangular patterns to regular scattered patterns, such as chess boards, or to completely random scatter patterns. In Intra-frame prediction each macroblock can be transmitted in one of several coding types depending on the slice-coding type. In all slice-coding types, two classes of intra coding types are supported, which are denoted as INTRA-4×4 and INTRA-16×16 in the following.

In contrast to previous video coding standards where prediction is conducted in the transform domain, prediction in H.264/AVC is always conducted in the spatial domain by referring to neighboring samples of already coded blocks. When using the INTRA-4×4 mode, each 4×4 block of the luma component utilizes one of nine prediction modes. Beside DC prediction, eight directional prediction modes are specified. When utilizing the INTRA-16×16 mode, which is well suited for smooth image areas, a uniform prediction is performed for the whole luma component of a macroblock. Four prediction modes are supported. The chroma samples of a macroblock are always predicted using a similar prediction technique as for the luma component in Intra-16x16 macroblocks. Intra prediction across slice boundaries is not allowed in order to keep all slices independent of each other. Motion compensation in P slices In addition to the Intra H.264/AVC Redundant slices feature is an error robustness feature allowing the encoder to send an extra representation of a frame region that can be used if the primary representation is corrupted or lost. [1], [2].

Redundant slices tool allow the insertion of primary slices and one or more additional secondary slices belongs to the original frame in the same bit stream. If a primary slice is affected by errors, it can be replaced by an error-free redundant one; otherwise the redundant slices are discarded. Moreover, messages to the decoder interleaved in the code stream containing supplemental enhancement information may contain further information about the bit stream, which can be utilized by an error concealment scheme [2]. Coding of redundant slices may use different quantization parameters, different reference frames, and different motion vectors than those used in the encoding of the primary slice. However, the parameters for encoding the redundant slices should be selected in such a way that there is no visual discrepancy between the primary and redundant slice representations [1]. In recent years several techniques employ redundant slices technique which is powerful error resilience feature, part of the H.264/AVC standard. In [3] the authors demonstrate how H.264/AVC redundant slices can be used to generate the

Wyner-Ziv coding, and present simulation results to demonstrate the advantages of this method over traditional methods such as forward error correction (FEC). The Wyner-Ziv bit stream is decoded in order to recover the redundant video descriptions, which are used in lieu of portions lost from the original video signal due to channel errors. Another approach [4] employs redundant slices to protect important video frames, such as Intra-coded frames, by restricting the redundant slices to be identical copies of the primary slices. Alternatively [5] proposes using H.264/AVC standard features such as redundant slices and FMO to protect video packets, and demonstrate the advantage over FEC. Moreover a heuristic algorithm for redundant slice selection is proposed in [6]. The authors intuitively decided that there are two kinds of slices needing more protection. One kind is the slices with large residual error. The other kind is the slices referred by large number of samples in the subsequent frames. Since the latter kind of slices can only be determined after actual encoding, multi-loop encoding is unavoidable to adopt this scheme, which is not desired in real time video transmission system.

Region of Interest (ROI) can be used to encode objects of interest with higher quality. During the ROI formation, different FMO types can be employed. FMO type 3 allows a box-out kind of shape. This ROI formation is restricted to a square. On the other hand FMO type 2 uses one or more rectangular slice groups and a background. This paper proposes a dynamic FMO type 2 which was used by a modified H.264/AVC encoder [7] to follow an object of interest in the video by means of a rectangular region of interest (ROI). The object of interest can be dynamically specified the ROI frame by frame. Moreover an effective RS representation is proposed in order to highly protect the most important information in the frame. The paper is organized as follows. In Section 2 the preprocessing steps of the proposed method is detailed. Section 3 includes the simulation results and extensive comparative study demonstrating the performance of the proposed very efficient technique. Section 4 concludes the paper.

II. PROPOSED TECHNIQUE

H.264/AVC Redundant slices feature, is an error robustness feature allowing the encoder to send an extra representation of a frame region that can be used if the primary representation is corrupted or lost. Redundant slices tool allow the insertion of primary slices and one or more additional secondary slices belongs to the original frame in the same bit stream. If a primary slice is affected by errors, it can be replaced by an error-free redundant one; otherwise the redundant slices are discarded. In order to highly protect the most important information in the special frame, some specific slices are dedicated for Region of Interest (ROI). Whenever any of the primary frame coded slices cannot correctly decoded, the decoder can replace the primary slice with its corresponding redundant representation.

Flexible Macroblock Ordering (FMO) is a very powerful tool for error resilience [2]. FMO technique can, besides for pure error resilience, also be used for other purposes. For instance rectangular slice groups can be used as regions of interest (ROI) containing ‘interesting’ parts of a frame within a video sequence. FMO type 2 uses one or more rectangular slice groups and a background. The rectangular slice groups are allowed to overlap each other but macroblocks in overlapping areas can be part of only one slice group. The order in which the slice groups are declared in a Picture Parameter Set (PPS) determines which slice group a Macroblock resides in. The Macroblock number of the top left Macroblock and the bottom right Macroblock of each slice group is coded into a PPS by means of the syntax elements.

We propose a dynamic FMO type 2 which was used by a modified H.264/AVC encoder [7] to follow an object of interest in the video by means of a rectangular region of interest (ROI). The object of interest was not tracked in an automatic way, but can be dynamically specified the ROI frame by frame.

Frame Number	Coordinates (Top Left and Bottom Right Macroblock number)
0-20	3,63
21-39	6,66
40-65	17,77
66-80	39,99
81-105	4,64
106-119	15,75
120-133	36,96
134-142	16,76
143-150	39,99

1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22
23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63	64	65	66
67	68	69	70	71	72	73	74	75	76	77
78	79	80	81	82	83	84	85	86	87	88
89	90	91	92	93	94	95	96	97	98	99

(a)

Frame Number	Coordinates (Top Left and Bottom Right Macroblock number)
0-10	13,73
11-25	25,85
26-40	27,87
41-70	23,83
71-81	2,62
82-95	34,94
96-107	5,65
108-128	38,98
129-150	17,77

(b)

(c)

Fig. 1 QCIF Frame Coordinates (a), Coordinates of changing ROI for Coastguard (b), Coordinates of changing ROI for News (c).

Specifically based on the observation that end-users generally pay more attention to the moving objects (especially those with variant movement) in a video sequence we propose redundantly encode those MBs with potential variant movement. Generally, these MBs are more difficult to be error-concealed than the stationary MBs or the MBs uniform movement. Since we can determine the redundant encoded MBs before actually encoding the current frame, a dynamic FMO-type 2 is adopted for further enhance the error resilient performance of the proposed RS representation. Since encoding can be done offline, the encoding time is not an important concern. We consider that a QCIF frame is constructed with 99 Macroblocks (MBs). The number of frames to be encoded is 150 frames for two video traces; Foreman and Mother& Daughter. The changing coordinates for the rectangle throughout the video sequence are given in Fig 1.



BackGround	ROI	BackGround	RS
			(a)

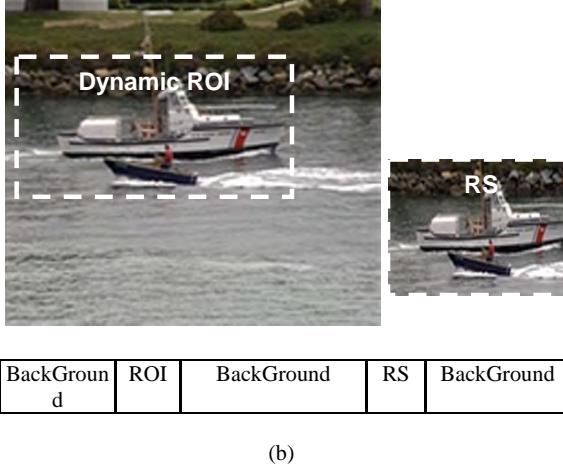


Fig. 2 Frame transmission with Redundant Slice feature. Standard redundant slice representation with static FMO type 3 (a). Effective allocation of Redundant Slice (RS) representation with dynamic FMO type 2 (b).

The H.264/AVC standard states that redundant slices representation (RS in the figure) should follow the corresponding primary frame as shown in Fig. 2 (a).

Unlike previous methods, in which redundant slices are statically allocated, typically at the end of the transmission frame, we suggest a more effective allocation scheme. In order to highly protect the most important information in the frame, some specific slices are dedicated for Region of Interest (ROI) as a foreground, exploiting the foreground with left-over FMO type 2. Then, redundancy slices are generated representing the foreground ROI. The Background was divided in three equal parts (Background A, Background B, and Background C). Fig. 2 (b) demonstrates the proposed allocation of the redundant slices within the transmitted coded frame. In this figure the first part of the background (Background A) directly follows the ROI slices, while the second part of the background (Background B) follows the RS. Then the third part of the background (Background C) is allocated at the end of transmitted coded frame. The effective allocation scheme of redundant slices in the coded transmission stream, helps decreasing the possibility of simultaneously losing both the primary and the redundant slices. Integrating the proposed redundant slices allocation algorithm and the FMO feature promises a powerful error resilient scheme.

III. SIMULATIONS RESULTS

There are two types of criteria that can be used for the evaluation of video quality; subjective and objective. It is difficult to do subjective rating because it is not mathematically repeatable. For this reason we measure the

visual quality of the interactive mode using the Peak Signal-to-Noise Ratio (PSNR). We use the PSNR of the Y-component of a decoded frame. We simulate the scenario of the H.264-based video transmission for different erroneous environments. Simulations were done using the H.264 Test Model (H.264/AVC Software Coordination, software version: JM 13.0) [7]. All test sequences are in QCIF format (176 x 144 pixels/frame) and encoded at target frame rate of 15 frames per second (fps). The number of frames to be encoded/decoded is 150 frames. Frames were partitioned into slices and the slices are organized in packets for transmission where each slice is packed in one packet. We consider that a QCIF frame is constructed with 99 Macroblocks (MBs). The simulations were carried out on the following QCIF video traces: News and Coastguard. In our experiments we compare the following ROI models, static FMO type 2, static FMO type 3 with the conventional RS Representation and Dynamic FMO type 2 with the effective RS representation under different error burst rates.

In order to evaluate the proposed very efficient technique extensive simulations were carried out with geometric analysis. Moreover to simulate the effect of the packet burst error on arbitrary blank frame we conduct several experiments with different packet burst error size. For each burst size, we examine the effect of the error location by moving the starting point of the error by one Macroblock (MB) at time. This way we cover all missing slices possibilities due to an error burst with given length. The results shown are the average of all those experiments. For instance, 95 simulations were derived for 5% error burst differ by the location of the error start point, 90 simulations were derived for 10% error burst differ by the location of the error start point, and 80 simulations were derived for 20% error burst differ by the location of the error start point. Hence for error burst ranging from 2% to 10% frame loss (i.e., loss of 10 MBs to 50 MBs for a QCIF frame) approximately 470 experiments were derived. Moreover for error burst ranging from 20% to 60% frame loss approximately 300 experiments were derived.

The average PSNR values for error burst ranging from 2% to 10% (i.e., loss of 2 MBs to 10 MBs for a QCIF frame) and from 20% to 60% frame loss (i.e., loss of 10 MBs to 60 MBs for a QCIF frame) are presented in Table 1.

Specifically, Table 1 depicts the average Y-PSNR (dB) values under different error burst rates. The largest PSNR value in each column is shown in italic and bold font. From the results shown in Table 1 the following conclusions can be drawn. Applying dynamic FMO-type 2 with the Redundant Slice representation can improve error resilient under different packet loss rates. It should be emphasized that for all the video traces the proposed dynamic FMO-type 2 RS representation outperforms the conventional H.264/AVC RS representation with the static FMO type -3 and static FMO-type 2 structure respectively. These results verify the effectiveness of the proposed technique.

Error Burst (%)	2%	4%	6%	8%	10%	20%	30%	40%	50%
FMO Type- RS. PSNR(dB)									
Static FMO type 3 with Conventional RS representation	35.61	35.01	34.55	34.0	33.55	32.98	31.91	30.62	29.36
Static FMO type 2 with Conventional RS representation	35.65	35.22	34.91	34.61	34.41	33.81	33.24	32.71	32.01
Dynamic FMO type 2 with effective RS representation	35.89	35.65	35.29	35.01	34.81	34.58	34.19	33.81	33.44

(a)

PSNR(dB)	28.1	29.8	31.2	32.6	33.9
FMO Type- RS. Bit Rate (Kbps)					
Static FMO type 3 with Conventional RS representation	30	38	49	68	97
Static FMO type 2 with Conventional RS representation	33	40	52	72	101
Dynamic FMO type 2 with effective RS representation	35	42	55	75	103

(b)

Table 1. (a) Average Y-PSNR (dB) for error burst ranging from 2% to 10% and 20% to 50% frame loss. (b) Coding Efficiency for the proposed dynamic FMO type 2 RS representation, static FMO type 2 and type 3 with the conventional RS representation.

IV. CONCLUSIONS

A very efficient dynamic FMO-type 2 with redundant slice representation is proposed in order to prevent temporal error propagation in error-prone channels. Both subjective and objective visual quality comparative study demonstrates that the proposed technique outperforms the conventional H.264/AVC Redundant Slice with static FMO type 3 and static FMO type 2 under different error burst ranging. Future work will include the impact of the proposed approach in the codec efficiency, delay and random bit errors. It should be

noted that if VCR-like interactive functions [8]-[10] were carried out the error resiliency performance of the proposed encoding technique could be better enhanced.

REFERENCES

- [1] Advanced Video Coding for Generic Audiovisual Services, ITU-T Rec. H.264 and ISO/IEC 14496-10 (MPEG-4 AVC), ITU-T and ISO/IEC JTC 1, Version 1: May 2003, Version 2: May 2004, Version 3: Mar. 2005, Version 4: Sept. 2005, Version 5 and Version 6: June 2006, Version 7: Apr. 2007, Version 8 (including SVC extension): Consented in July 2007.
- [2] Kostas Psannis and Yutaka Ishibashi, Efficient Flexible Macroblock Ordering Technique, IEICE Transactions on Communications, vol. E91-B, No. 08, pp. 2692-2701, August 2008.
- [3] S. Rane and B. Girod, Systematic lossy error protection of video based on H.264/AVC redundant slices, in Proc. Visual Communication and Image Processing VCIP-2006, San Jose, CA, Jan. 2005.
- [4] Y.-K. Wang, M. M. Hannuksela, and M. Gabbouj, Error resilient video coding using unequally protected key pictures, in Proc. International Workshop VLBV03, Sep. 2003.
- [5] P. Baccichet, S. Rane, and B. Girod, Systematic lossy error protection based on H.264/AVC redundant slices and flexible macroblock ordering, in Proc. 15th International Packet Video Workshop, Hangzhou, P. R. China, Apr. 2006.
- [6] Ziqing Mao, Rong Yan, Ling Shao and Dong Xie. An Error Resilience Scheme for Packet Loss Recover of H.264 Video, PCM 2004, August 2004.
- [7] H.264/AVC Software Coordination, software version: JM 13.0 (<http://iphone.hhi.de/suehring/tm1/>).
- [8] Kostas. E. Psannis, M. G. Hadjinicolaou, and A. Krikellis, MPEG-2streaming of full interactive content, IEEE Transactions on Circuits and Systems for Video Technology, vol. 16, no. 2, pp. 280–285, 2006.
- [9] Kostas Psannis and Yutaka Ishibashi, Enhanced H.264/AVC Stream Switching over Varying Bandwidth Networks, IEICE ELEX Journal, Vol.5, No.19, pp. 827-832, October, 2008.
- [10] Kostas Psannis and Yutaka Ishibashi, Efficient Error Resilient Algorithm for H.264/AVC: Mobility Management in Wireless Video Streaming, Telecommunication Systems Journal, vol 41, issue 2, pp. 260-292, 2009.

Balancing Streaming and Demand Accesses in a Network Based Storage Environment

Dhawal N. Thakker, Glenford E. Mapp, and Orhan Gemikonakli

School of Engineering and Information Sciences,
Middlesex University,
The Burroughs, Hendon,
London NW4 4BT, United Kingdom

{d.thakker, g.mapp, o.gemikonakli}@mdx.ac.uk

Abstract

The usage of network-based applications is increasing, as network speeds increase. Also, the use of streaming applications, e.g BBC I-Player, Youtube etc, over the network is becoming commonplace. These applications access data sequentially. However, as processor speed and the amount of memory available increase, the rate at which streaming applications access data is much faster than the rate at which the blocks can be fetched consecutively from the network storage. Therefore, there is a need to analyse prefetching and clustering techniques for network-based storage systems. In addition to sequential access, the system also needs to satisfy demand misses.

In this paper, we attempt to develop an analytical model which will be used to investigate the operational boundaries under which streaming applications can run without jitter and demand misses can be satisfied in reasonable time.

1. Introduction

Due to the increase of CPU speed and the amount of memory available, there is an increase in the use of the multimedia (streaming applications) and database applications in the working environment. These applications access files sequentially from storage devices (e.g disks) and need to be served at constantly high data rates while they are executing, e.g. High Definition video (HD) data rate is 5 MB/Sec, MPEG-4 data rate is 2.5 MB/Sec etc. Also, due to the increase in network speed, most of these applications are accessed over the network rather than using local storage.

As the future access pattern is known for applications mentioned above, prefetching could be used. Prefetching enables the file system to bring blocks of data before they are needed. This allows applications to run without waiting for the blocks to be fetched from the storage device i.e.

without stalling, thus reducing the latency experienced by the running application. Prefetching can only work, if it is relatively inexpensive. That is, at any given time, if more blocks are fetched than requested, the time to fetch additional and requested blocks should be comparable to the time it would take to fetch only the requested blocks. In addition to prefetching blocks, the operating system must also promptly satisfy demand misses i.e., block requests by an application without any prior information.

Clustering could be used to minimise the overall latency experienced, as it has the ability to fetch multiple blocks simultaneously thereby reducing the latency when compared to fetching them one block at a time. Clustering on a disk can result in speeds of up to 23 MBps compared to 200KBps¹, when blocks are fetched one at a time.

As mentioned before, the increase in speed of networks and their availability (e.g. 1 Gigabit networks are readily available and the availability of 10 Gigabit network speed is not very far in the future), most of the multimedia and database applications such as BBC I-Player, Youtube, Systems Applications and Products (SAP) etc, run over the network. Therefore prefetching and clustering techniques should be used in network storage.

2. Motivation

In most commercial environments, data to be streamed is first loaded into the memory of servers. In order to explore such environments a Network Memory Server (NMS) was developed [2, 5]. The NMS server stores all the data of the clients in the memory of the server. Hence, the latency experienced in fetching a block of data will be dominated by the characteristics of the network.

Analysis of Clustering

¹ Assuming 5 millisecond revolution time (latency) to fetch one

We have used the NMS to explore clustering over the network. From our experiments, we believe that the cost for obtaining blocks using clustering is composed of a Latency cost (L) and a constant per block cost (C). The exact value of these parameters depend on storage technology being used. In the NMS, the latency cost is the overhead time (going through the stack up and down on client and server side) and transmission time (sending the network buffer between the client and the server). It varies depending on the network load. The constant per block cost ¹ is the time taken to search for the block and copy it into the network buffer on the server, and to copy the block from the network buffer into memory on the client. These two variables summate to the time $T_{net}(y)$ which is the time taken to fetch y number of blocks requested in a network buffer, as demonstrated by the formula below:

$$T_{net}(y) = L + Cy \quad (1)$$

It has been observed from experiments that the data rates obtained through clustering could provide sustainable transfer rates, as shown in the Figure 1. For very fast network, the value of L will be very small. Hence, the value of $T_{net}(y)$ will be approximately equal to Cy . The key issue becomes whether network file systems can take advantage of the clustering characteristics to improve performance by prefetching blocks over the network.

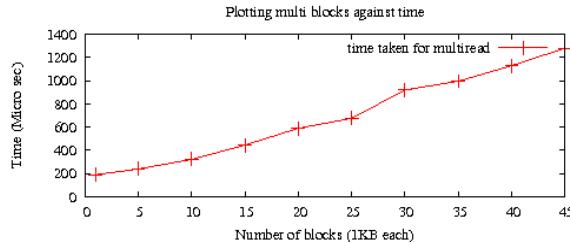


Figure 1. Multiple block Latency

Our long term goal is to develop a file system using clustering and prefetching techniques over the network which can be ideal for the working environment, where it can allow streaming applications (once they are started) to run without stalling while satisfying demand requests in reasonable time. This paper looks at the analytical model that will help us to decide the number of requests that should be clustered, from streaming applications and demand misses, into a network buffer to provide required level of service.

3. Related Work

The important research work done in the area of interest are listed below:

¹This cost will vary depending on the server load.

- Pei Cao et al.(1995) [1] proposed four rules to obtain optimal integrated strategies for prefetching and caching must satisfy. However, the prefetching work was more theoretical and the implemented prefetching strategy was static prefetching.

- Papathanasiou and Scott(2005) [7] argued that technological trends and emerging system design goals have dramatically reduced the potential costs and increased the potential benefits of highly aggressive prefetching policies. The authors proposed that memory management needs to be redesigned to embrace such policies. The authors also came up with the efficient prefetching and caching techniques [6] to maximise power-down opportunities (without performance loss).

- Li et al. work(2007) [4] used the knowledge of I/O switch time, to decide how much to prefetch, to improve performance of the sequential access.

- Patterson et al. work(1995) [8] proposed the notion of **prefetch horizon** i.e. when to initiate prefetching for the known reference, to use cache effectively and to minimise the execution time of the applications.

However, Li et al. and Patterson et al. work was disk-centric and both these research efforts did not consider the time taken to consume blocks by applications. We will explore similar ideas for the network-based storage.

- Rochberg and Gibson(1997) [9] extended the work of Patterson et al. by implementing the Patterson et al. framework over the network. But due the fact that they used NFS, which only operates on a per block basis, they were unable to use clustering over the network and so their results were not as good as the results from disks.

This research will build upon these efforts by looking at the network characteristics to develop an algorithm using prefetching and clustering techniques. This will guarantee the quality of service for applications running over the network.

4. Our approach

In the first and second sub-sections, we briefly analyse how to treat streaming access and demand access respectively.

4.1. Streaming Access

We assume that streaming applications access blocks sequentially at a constant rate. We will first derive an equation to analyse how many blocks should be prefetched so that

streaming applications can run without any jitter once they are started.

Let T_{cpu} be the time to consume a block for a streaming access, then the rate at which it will consume y blocks will be $T_{process}(y)$ i.e.

$$T_{process}(y) = T_{cpu} * y \quad (2)$$

As shown in the Equation 1, the time taken to service y blocks is given by:

$$T_{net}(y) = L + Cy \quad (3)$$

Now, for an application to run without any delay or jitter, the time taken to fetch blocks should be less than or equal to the time taken to consume them i.e.

$$\begin{aligned} L + Cy &\leq T_{cpu} * y \\ L/(T_{cpu} - C) &\leq y \end{aligned} \quad (4)$$

The equation shows that the number of blocks prefetched for streaming applications should be equal to or greater than $L/(T_{cpu} - C)$ and they should be fetched at an interval of $T_{process} * (y)$, to allow them to run without stalling³. This can be satisfied by using only double buffering as shown in the Figure 2. As discussed earlier, in addition to prefetch

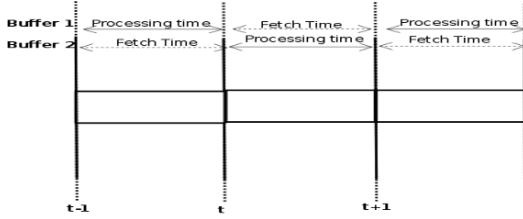


Figure 2. Double Buffering in steady state.

blocks operating system also needs to promptly satisfy demand misses. The only way to satisfy the demand misses along with prefetching is to make sure that the time taken to fetch the prefetch blocks is smaller than the time taken by applications to consume them. This will leave spare time as shown in Figure 3, which could be used to satisfy demand misses. In short, the Equation 4 guarantees the quality of service for streaming applications. There will be no overload on the network buffering system, as it only prefetches the required number of blocks in a cycle that are needed for streaming applications to keep them running.

4.2. Demand Access

Demand accesses are generated by applications without giving any prior notice and will need to be satisfied as soon as possible.

³It will experience start stall time to prefetch first y blocks. Due to the variance in the network load, we will need to buffer more than y prefetch blocks, this is will explored in an algorithm.

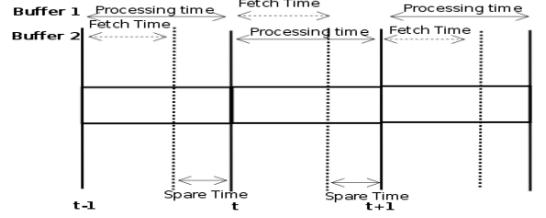


Figure 3. Double Buffering in steady state: Processing time is the time taken to consume block and fetch time is the time taken to fetch the block from the NMS. Spare time is the time difference between the processing and fetch time.

Clustering a demand miss with ongoing prefetch requests will add an additional per block cost to the overall fetch operations. To bring in additional d demand misses with ongoing prefetch requests p will be $T_{demand}(p + d)$:

$$\begin{aligned} T_{demand}(p + d) &= L + C_p + C_d \\ T_{demand}(p + d) &= L + C_{p+d} \end{aligned} \quad (5)$$

where $C_p(C * p)$ is the time to prefetch p number of prefetch blocks. The $C_d(C * d)$ is the time to bring in additional blocks with on going prefetch. Note that the number of requests clustered into a network buffer increase the time to fetch the network buffer.

Let T_{disk} represent the average time taken to satisfy the demand requests using disk access. T_{wait} is the average waiting time in the demand queue. Now as long as we can guarantee that the average time taken to satisfy each demand request over the network is less than or equal to the average time taken to satisfy a demand request in the disk, the quality of service will be better than or equal to the disk. This is important as it justifies the use of network storage rather than using local disks. From this we have,

$$T_{demand}(p + d) + T_{wait} \leq T_{disk} \quad (6)$$

Equation 6 shows that in fetching the network buffer, the sum of the time taken to fetch the demand requests ($T_{demand}(p + d)$) and the average waiting time (T_{wait}) on the demand queue should be less than or equal to T_{disk} .

Substituting Equation 5 in Equation 6 for clustering demand misses.

$$L + C_{p+d} + T_{wait} \leq T_{disk} \quad (7)$$

Equations 7 and 4, will guarantee the quality of service for demand requests and for running streaming applications respectively. It can be seen from Equation 7 that to know the value of p and d at varying rates of demand misses and streaming applications is very important, in order to maintain equilibrium state and to provide the required QoS.

To investigate these regions, we now develop an analytical model, which will be used to explore boundaries and performance of the system.

5. Analysis

In this model, there are two queues: the demand and the prefetch queue, as shown in Figure 4. Let λ_d be the rate at which demand requests are arriving to the demand queue and let λ_p be the rate at which prefetch requests are arriving to the prefetch queue. While serving, more than one requests could be taken from both the queues, clustered into a network buffer which is then sent off to the server. This can be viewed as a type of *bulk service*.

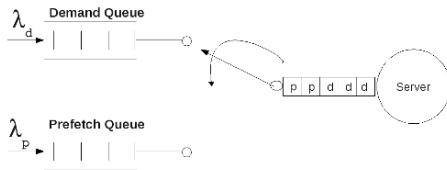


Figure 4. A model with a server serving two queues: Prefetch and Demand queue.

This analysis attempts to answer the question: Given the arrival rates of the two queues, can we find a way to calculate the average waiting time experienced in the demand queue? Since we believe that the streaming applications access blocks at a constant rate we can control the number of blocks needed to be fetch for the prefetch queue to provide required QoS. Hence, we can reduce the model to a single queueing system based on demand requests but the service time for the demand blocks will include the cost of fetching prefetch blocks.

5.1. Standard Approach (Partial Batch Model)

As a first step to analysing the average waiting time experience in the demand queue, we will use the partial batch model described in [3]. In this model a server can serve up to a maximum of K requests. If there are less than K requests in the system, the server begins service on these requests. Furthermore, when there are less than K requests being serviced new arrivals immediately enter service. The amount of time required to service requests, is an exponentially distributed random variable with mean $\frac{1}{\mu}$.

This model is represented in the Figure 5. Each state of the model is represented in terms of n and s . n is the total number of requests in the system and s is the number of requests being served. It can be seen from the figure that any arrival in the system enters in to the service immediately

as long as there are less than K number of requests being served and time taken to service those requests is exponentially distributed to a mean value of $\frac{1}{\mu}$. A balanced equation

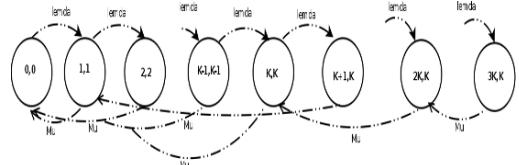


Figure 5. Partial Bulk Service model.

for the model can be written as:

$$0 = -(\lambda + \mu)p_n + \mu p_{n+k} + \lambda p_{n-1} \quad (n \geq 1) \quad (8)$$

$$0 = -\lambda p_0 + \mu p_1 + \mu p_2 + \mu p_{K-1} + \mu p_K$$

This equation can be rewritten as:

$$[\mu D^{K+1} - (\lambda + \mu)D + \lambda]p_n = 0 \quad (n \geq 0) \quad (9)$$

By finding the root (r_0) of this equation that is between 0 and 1, one can work out mean queue length (L) and average waiting time (W) for the queue, using the equations below.

$$L = \frac{r_0}{1 - r_0} \quad \text{and} \quad W = \frac{r_0}{\lambda(1 - r_0)} \quad (10)$$

This approach is extremely accurate for very heavy traffic, since on these occasions the server will always be serving the maximum batch size. However, for lighter traffic loads the model is inaccurate because according to this approach new requests will immediately enter service, when the server is serving less than maximum batch size which is not the case in our scenario. Here, the server only serves the number of people in the queue at its arrival, requests arriving after this point must be serviced in the next cycle regardless of whether or not the maximum batch size is being served in the current cycle. Hence, the scenario is gate-limited and not exhaustive-limited as seen in the partial batch model. Gate-limited models have been extremely difficult to solve and no standard solution is readily available. In the next section we attempt to develop a model which can be used to analyse the described scenario.

5.2. Our Model

In this section we attempt to develop a more accurate model which could be used under light and heavy traffic. As shown in Figure 6, the state of the model is defined by two variables i.e. n and s . n is the total number of requests in the system including the requests being served and s is the number of request being served at any given time. Therefore, for the maximum batch size $s = d$. s goes from 0 to d , so when $s = 0$, the system is empty and when $s = d$ up to

d requests are being served. Also, this will give rise to the d different stages as shown in Figure 6 with each stage having service rate depending on the number of blocks being served.

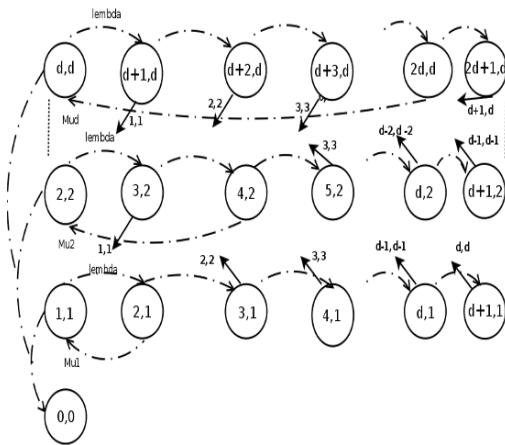


Figure 6. A model with a server which can serve up to d demand requests in a batch mode, n = Total number of requests in the system and s = Number of requests being served.

We start by looking at a simple scenario, so we restrict d to 2, as shown in the Figure 7. Having d equal to 2 there can only have three stage either server is serving 1 request or its serving 2 requests or the queue is empty. This means that with the exception of 2, 2 to 0, 0 each transition can only jump one stage at a time (i.e. 1 to 2 or 2 to 1) for e.g. 3, 1 goes to 2, 2 or 3, 2 goes to 1, 1. We will analyse each stage individually starting with stage one.

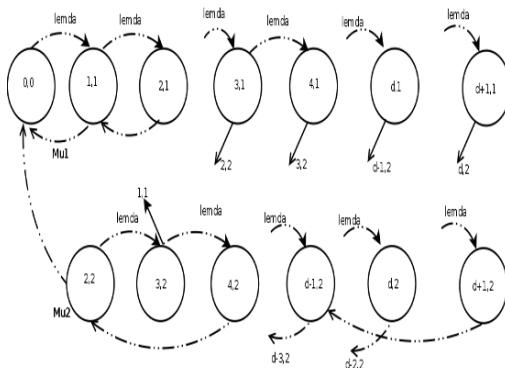


Figure 7. Two stage model, $d = 2$.

5.2.1 Considering Series One

Let us consider series one of the figure 7. In series one, $s = 1$ and for $n > s$ i.e. $n > 1$, we will have:

$$\lambda P_{n-1,1} = (\lambda + \mu_1)p_{n,1} \quad , p_{n,1} = \frac{\lambda}{(\lambda + \mu_1)}(P_{n-1,1}) \quad (11)$$

This implies that for any $n > 1$, in series one:

$$p_{n,1} = \left(\frac{\lambda}{\lambda + \mu_1} \right)^{n-1} (P_{1,1}) \quad (12)$$

And for $n = s$, we will have:

$$(\lambda + \mu_1)P_{1,1} = \lambda P_{0,0} + \mu_1 P_{2,1} + \mu_2 P_{3,2} \quad (13)$$

Finally for $n = s = 0$ i.e. $P_{0,0}$ will be:

$$\lambda P_{0,0} = \mu_1 P_{1,1} + \mu_2 P_{2,2} \quad (14)$$

5.2.2 Considering the series two i.e. when $s = 2$

Similarly, for $s = 2$, we will derive equations for $n = s$ and $n > s$, using figure 7. when $n > s$, we will have:

$$(\lambda + \mu_2)P_{n,2} = \lambda P_{n-1,2} + \mu_2 P_{n+2,2} + \mu_1 P_{n+1,1} \quad (15)$$

And for $n = s$, we will have:

$$(\lambda + \mu_2)P_{2,2} = \mu_2 P_{4,2} + \mu_1 P_{3,1} \quad (16)$$

Now using the derived equations for the stage one and stage two, we will try to obtain an equation for the stage 2 at point $P_{3,2}$, later we can find out the roots of that equations as in the partial batch, thus will be able to find out the probability of being at each point in stage two.

$$(\lambda + \mu_2)P_{3,2} = \lambda P_{2,2} + \mu_2 P_{5,2} + \mu_1 P_{4,1} \quad (17)$$

From the equation 12, $P_{4,1}$ can be substitute as $(\frac{\lambda}{\lambda + \mu_1})^3 (P_{1,1})$. Further from the equation 14, $P_{1,1}$ can be substitute as $\lambda P_{0,0} - \mu_2 P_{2,2}$. Therefore,

$$P_{4,1} = (\lambda P_{0,0} - \mu_2 P_{2,2}) \left(\frac{\lambda}{\lambda + \mu_1} \right)^3 \quad (18)$$

Substituting the value of $P_{4,1}$ in the equation 17 and finding out the root (r_0) which will be in between 0 and 1, we can find out the probability of being at each point in stage 2 in terms of $P_{0,0}$. We use the same approach as in M/M/1 queueing as well the partial batch model and so express $P_{n,2}$ in terms of $P_{0,0}$ as follows:

$$P_{n,2} = r^n P_{0,0} \quad (19)$$

Similarly, using equation 14, we can find out the probability of being at each point in stage 1 in terms of $P_{0,0}$.

$$P_{n,1} = \left(\frac{\lambda}{(\lambda + \mu_1)} \right)^{n-1} * Const * P_{0,0} \quad (20)$$

where $Const = \frac{(\lambda - \mu_2 r^2)}{\mu_1}$.

From the equations 19 and 20, we can see that the probability at any point in model can be known if $P_{0,0}$ is known. Also, the sum of the probability at stage one and two should be equal to 1. Using this,

$$\left(\sum_{n=0}^{\infty} P_{n,1} + \sum_{n=0}^{\infty} P_{n,2} \right) = 1 \quad (21)$$

Substituting value for $P_{n,1}$ and $P_{n,2}$ from equations 19 and 20.

$$(P_{0,0}) = \frac{\lambda \mu_1 (1 - r)}{(\lambda + \mu_1)^2 * C(1 - r) + \lambda * \mu_1} \quad (22)$$

Once we know $P_{0,0}$, the total number of requests (L) in the system can be easily known using:

$$L = \sum_{n=0}^{\infty} n * P_{n,1} + \sum_{n=0}^{\infty} n * P_{n,2} \quad (23)$$

and

$$W(\text{average waiting time}) = \frac{L}{\lambda} \quad (24)$$

5.3. Simulation and Results

A simulation was developed to verify the analytical model. In the simulation, the number of prefetch blocks (P) were kept constant ($P = 1$) and the arrival rate of the demand queue was varied. The results are shown in Figure 8. Our model is significantly better than the partial batch model for operational loads. These results are preliminary and more detailed results will be published later.

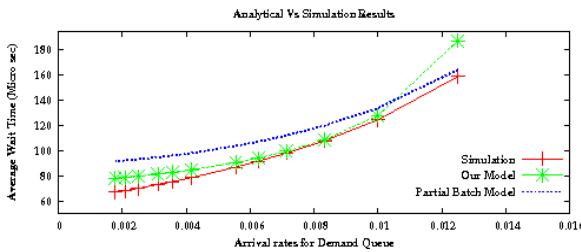


Figure 8. Waiting time for the demand queue calculated using Simulation, Partial Batch Model and Our approach.

6. Conclusion and Future work

In this paper, we have looked at prefetching blocks for streaming applications while satisfying demand misses promptly to provide required level of QoS. For future work, we are looking at developing a more detailed analytical model. We also hope to develop an algorithm to satisfy both streaming and demand requests based on our analytical model. This algorithm will be tested on an experimental file system which has already been developed to find out the real-time performance of the design.

References

- [1] P. Cao, E. W. Felten, A. R. Karlin, and K. Li. A study of integrated prefetching and caching strategies. In *SIGMETRICS '95/PERFORMANCE '95: Proceedings of the 1995 ACM SIGMETRICS joint international conference on Measurement and modeling of computer systems*, pages 188–197, New York, NY, USA, 1995. ACM Press.
- [2] O. Gemikonakli, G. Mapp, D. Thakker, and E. Ever. Modelling and Performability Analysis of Network Memory Servers. In *ANSS '06: Proceedings of the 39th annual Symposium on Simulation*, pages 127–134, Washington, DC, USA, 2006. IEEE Computer Society.
- [3] D. Gross and C. M. Harris. *Fundamentals of Queueing Theory (Wiley Series in Probability and Statistics)*. Wiley-Interscience, February 1998.
- [4] C. Li, K. Shen, and A. E. Papathanasiou. Competitive prefetching for concurrent sequential I/O. *SIGOPS Oper. Syst. Rev.*, 41(3):189–202, 2007.
- [5] G. Mapp, D. Thakker, and D. Silcott. The Design of a Storage Architecture for Mobile Heterogeneous Devices. *ICNS2007*, 0:41, 2007.
- [6] A. E. Papathanasiou and M. L. Scott. Energy efficient prefetching and caching. In *ATEC '04: Proceedings of the annual conference on USENIX Annual Technical Conference*, pages 22–22, Berkeley, CA, USA, 2004. USENIX Association.
- [7] A. E. Papathanasiou and M. L. Scott. Aggressive prefetching: an idea whose time has come. In *HOTOS'05: Proceedings of the 10th conference on Hot Topics in Operating Systems*, pages 6–6, Berkeley, CA, USA, 2005. USENIX Association.
- [8] R. H. Patterson, G. A. Gibson, E. Ginting, D. Stodolsky, and J. Zelenka. Informed Prefetching and Caching. In *SOSP '95: Proceedings of the fifteenth ACM symposium on Operating systems principles*, pages 79–95, New York, NY, USA, 1995. ACM.
- [9] D. Rochberg and G. Gibson. Prefetching over a network: early experience with CTIP. *SIGMETRICS Perform. Eval. Rev.*, 25(3):29–36, 1997.

An Energy and Distance Based Clustering Protocol for Wireless Sensor Networks

Xu Wang¹ Liyan Qian² Jianjun Wu³ Tian Liu⁴

¹Department of Machine Intelligence

²Computer Laboratory

³Department of Electronics

⁴Key Laboratory of High Confidence Software Technologies (Peking University),
Ministry of Education, CHINA, and Institute of Software

^{1,2,3,4}School of Electronics Engineering and Computer Science, Peking University,
Beijing, 100871, CHINA

eecswangxu@pku.edu.cn lyqian@pku.edu.cn just@pku.edu.cn lt@pku.edu.cn

Abstract-Wireless sensor networks (WSNs) open a new domain which has great potentials in application of gathering data in a variety of environments. It is necessary to design energy efficient routing to maximize lifetime of WSNs, because WSNs consist of a large number of sensor nodes with limited battery. In this paper, we analyze the well-known clustering routing protocol LEACH and put forward feasible measures to improve the performance. We propose an energy and distance based clustering (EDBC) protocol which optimizes the random selection of cluster heads in LEACH. Regarding residual energy of sensor nodes, we select nodes with relatively more energy as clusters. Distances between cluster heads are greater than a proper threshold D to form a well-proportioned distribution. Simulation results show that EDBC outperforms LEACH in terms of network lifetime, load balance and energy utilization.

I. INTRODUCTION

A wireless sensor network is composed of thousands of tiny sensor nodes which are deployed in a large geographical area. These nodes measure ambient conditions such as temperature, movement, sound, light, and the presence of certain objects by means of various embedded sensors and form a self-organized network system through wireless communication. This system process the collected data to reveal some characteristics about phenomena located in the area. Eventually, the data must be transmitted to a base station (BS), where the end-user can access the data [1] [2].

WSNs differ from traditional wireless ad hoc networks and have mainly the following features: (1) The total of sensor nodes can be several orders of magnitude higher than in an ad hoc network, and sensor nodes can be densely deployed so that its fault tolerance can be guaranteed via short distance communication; (2) Due to its low cost, small volume and low power consumption, a sensor node's ability of computation and storage capacity is very limited; (3) Since the power source of a sensor node cannot be changed during use, the power supply is an essential design issue that concerning the lifetime of WSNs; (4) Sensor nodes are prone to failures so that the topology of a wireless sensor network changes frequently. (5) A wireless sensor network is a data-centered system whose

chief concern is not specific observation from a certain sensor node but information on the whole.

Regarding the above characteristics of WSNs, to design good routing protocols for WSNs is an important challenge. In 2000, Heinzelman et al. proposed LEACH (low-energy adaptive clustering hierarchy) [3], which is a promising protocol but has some disadvantages meanwhile. In this paper, we give analysis on LEACH, and propose an energy and distance based clustering (EDBC) protocol to make improvement. Simulation results show that EDBC outperforms LEACH in terms of network lifetime, load balance and energy utilization.

II. LEACH PROTOCOL

LEACH is a self-organized, clustering-based routing protocol. It is based on certain assumptions, which are reasonable to a large extent due to technological advances in radio hardware and low-power computing.

A. Fundamental Assumptions

The BS is fixed far from the sensor nodes.

All nodes in the network are homogeneous, containing the same energy and synchronized all the time.

All nodes are able to transmit data with enough power to the BS initially, and to control the amount of transmit power.

Each sensor node has the computational power to support different MAC protocols and to perform signal processing functions.

Data from the nodes in the same cluster has correlation to a large extent.

Radio energy dissipation model [4]: the transmitter expends energy to run the radio electronics and the power amplifier, and the receiver expends energy to run the radio electronics. If the distance between the transmitter and the receiver is less than the threshold d_0 , $d_0 = \sqrt{\epsilon_{fs} / \epsilon_{mp}}$, the free space (fs) model is used; otherwise, the multipath (mp) model is used. To transmit an l -bit message a distance d , the radio expends

$$\begin{aligned} E_{Tx}(l, d) &= E_{Tx-elec}(l) + E_{Tx-amp}(l, d) \\ &= \begin{cases} lE_{elec} + l\epsilon_{fs}d^2, & d < d_0 \\ lE_{elec} + l\epsilon_{mp}d^4, & d \geq d_0 \end{cases} \end{aligned} \quad (1)$$

and to receive this message, the radio expends

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} \quad (2)$$

B. Algorithms

In LEACH, the nodes organize themselves into local clusters, with cluster heads chosen randomly. All nodes have a chance to act as a cluster head to balance the energy dissipated by each node.

The operation of LEACH is divided into rounds. Each round includes a set-up phase and a steady-state phase. At the beginning of a set-up phase, the node locally chooses a random number between 0 and 1. If the number is less than a threshold $T(i)$, the node becomes a cluster head for the current round. The threshold is set as:

$$T(i) = \begin{cases} \frac{p}{1 - p[r \bmod(1/p)]} & (\forall i \in G) \\ 0 & (\forall i \notin G) \end{cases} \quad (3)$$

where p is the desired percentage of cluster heads, r is the number of the current round, and G is the set of nodes which have not been selected as cluster heads in the last $1/p$ rounds [3].

The nodes selected as cluster heads broadcast an advertisement message. All the other nodes decide which cluster to join according to the received signal strength of the advertisement and send message to the cluster head. After receiving messages from non-cluster-head nodes, the cluster heads add them to its routing table, and send back to them a TDMA schedule. This ensures no collisions among data messages and allows non-cluster-head nodes to turn off their radio components except during their transmit time.

After all the non-cluster-head nodes receive the TDMA schedule, the set-up phase is complete and the steady-state phase begins. In this phase, all non-cluster-head nodes take turns to send data to the cluster head in their transmit time according to the TDMA schedule. The cluster heads perform data aggregation, and eventually transmit the resultant data to the BS.

C. Performance Analysis

Compared to plane routing protocols, LEACH prolongs network lifetime by almost 30 percent. Compared to multi-hop routing protocols, data is transmitted to the BS through at most

one hop, thus reducing the data transmit latency. However, the selection of cluster heads depends entirely on the random numbers the nodes choose at the beginning of the set-up phase. This actually causes some disadvantages as follows.

The distribution of cluster heads is not well-proportioned because of the random selection of cluster heads, thus causing more energy consumption. Experiments show that it is likely that distances between some cluster heads are rather short or rather long, which reduces the network load balance, and shortens network lifetime.

All the nodes take turns to act as cluster heads in LEACH, which is not quite energy efficient. Because the residual energy of the nodes may be remarkably different, some nodes with relatively less power can be selected as cluster heads, and run out early.

Besides, the way to balance energy consumption in LEACH requires that all the nodes have the same initial energy, which is hard to guarantee in reality.

III. AN ENERGY AND DISTANCE BASED CLUSTERING PROTOCOL

To overcome the disadvantages discussed above in LEACH and maximize network lifetime in WSNs, we propose an energy and distance based clustering (EDBC), taking into consideration the residual energy of each sensor node, and selecting nodes with relatively more energy as cluster heads. Furthermore, we make sure distances between cluster heads are greater than a threshold D to form a well-proportioned distribution.

Suppose the sensor field is an $X \times Y$ rectangle.

$$D = \sqrt{\frac{cXY}{\pi pN}} \quad (4)$$

where N is the total of nodes, p is the percentage of cluster heads, and $c(\geq 1)$ is a properly pre-fixed constant to guarantee that the clusters can cover the whole area.

We still adopt the *round* mechanism in LEACH, and also divide each round into two phases: a set-up phase and a steady-state phase. At the beginning of the set-up phase, each node broadcasts its residual energy within radius D , and receives other nodes' residual energy messages. If a node's residual energy is more than every node's within the distance D , it becomes a cluster head, and broadcast an advertisement message within radius D . Otherwise, the node becomes a non-cluster-head node, and chooses which cluster to join according to the strength of the advertisement message it receives. The cluster heads then send back to all the other nodes in the same cluster a TDMA schedule. The set-up phase is complete, and the following steady-state phase is operated the same as in LEACH. After the steady-state phase operates for t seconds, the current round ends and the next round begins.

IV. SIMULATION AND COMPARISON

Using Equations 1-3 and the networks with 100 sensor nodes randomly located in a rectangle area as is shown in Fig. 1, we simulated the operation of LEACH and EDCA under the same condition in MATLAB.

The BS is located at (50,175). All sensor nodes are randomly distributed in a $50m \times 50m$ square area. The other parameters in the model are set as follows: $N = 100$, $p = 0.05$, $c = 2$, $E_{elec} = 50nJ/bit$, $\varepsilon_{fs} = 10\text{ pJ}/bit/m^2$, $\varepsilon_{mp} = 0.0013\text{ pJ}/bit/m^2$, initial energy of each node $E_0 = 1J$, the energy for data aggregation

$E_{da} = 5nJ/bit/signal$, every data packet that contains data about sensor field condition is 4000 bits, and every data packet that contains control information to self-organize the cluster is 100 bits.

Simulation results show that the distribution of cluster heads is better proportioned in EDBC than in LEACH. As shown in Fig. 2, when the number of cluster heads is 5, they are not distributed properly with some cluster heads too near and some too far. Compared to LEACH, the distribution of cluster heads in EDBC tends to be better proportioned, in favor of reducing energy consumption, as is shown in Fig. 3. Besides, the total of cluster heads in each round can vary greatly because of the uncertainty of the mechanism used in LEACH, while the number of cluster heads is more stable in EDBC because of its consideration on distance.

Network lifetime is regarded as the time when the first dead node comes up. We simulated the performances of the wireless sensor networks of 100 random sensor nodes for 30 times. The average round number when the first dead node emerges in LEACH is 1416; while in the improved protocol is 1855. The network lifetime is prolonged remarkably in EDBC as is shown in Fig. 4.

There has been much research [5-12] on improving the LEACH since it was proposed. The modifications of LEACH include using multi-hop hierarchical clustering methods and making use of an information center that knows the location and energy of each node and thus distribute cluster heads better. Compared to these protocols, EDCA has the following advantages:

(1) Self-organization. Because WSNs are often applied to data gathering in particular environments, the location of nodes can be changed during the working period, and the topology of the network may be changing frequently while sensing the sensor field. Thus, it is of great importance that the routing protocol is self-organized. Besides, the location of sensor nodes is not easy to get and can cause delay and extra energy consumption. EDBC has the advantage of self-organization by using the communication between sensor nodes within a properly set distance D , which also reduces transmit energy dissipation.

(2) Short transmit latency. The data of a sensor node is transmitted to the BS directly if it is a cluster head, and at most through one hop of the cluster head to the BS in EDBC. Hence, transmit latency in EDBC is shorter compared to those multi-hop routing protocols, and make it suitable for application that requires instant information of the sensor field.

(3) Efficiency whether or not sensor nodes are homogeneous. While LEACH requires that every node in the network contains the same amount of energy initially, which is not quite practical, EDBC does not have this problem because sensor nodes containing relatively more residual energy are selected as cluster heads.

V. CONCLUSION AND FUTURE WORK

It has been a new challenge to design proper routing protocols for WSNs in recent years. LEACH is a self-organized, clustering-based routing protocol in which all sensor nodes take turns to act as cluster heads. The cluster heads play a vital role in the entire network, organizing the cluster, receiving and aggregating data from other cluster members, and transmitting the resultant data to the BS.

LEACH can prolong network lifetime by almost 30 percent compared to plane routing protocols [4]. However, it has some drawbacks, and can be improved in some aspects. From the analysis and the simulation results of LEACH and EDBC, we can draw the conclusion that the performance is improved under many circumstances in terms of network lifetime, load balance and energy utilization by making feasible modifications to LEACH regarding residual energy of the nodes and the proper distances between cluster heads.

Since there is no unique standard of judging the performance of routing protocols which may function remarkably differently under various conditions, as to a certain application, much work such as proper modeling, suitable choice or modification of routing protocols, and precise simulation of real environment, needs to be done before putting a routing protocol design into practice. Other influential factors for WSNs such as data transmission and density of sensor nodes should also be taken into consideration.

ACKNOWLEDGMENT

The authors would like to thank all the reviewers for their helpful comments. This project was supported by the President's Fellowship for Undergraduate Research of Peking University.

REFERENCES

- [1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Wireless Sensor Networks," *IEEE Communications Magazine*, 2002, 40(8):102-114.
- [2] Th. Arampatzis, J. Lygeros, and S. Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks," in *Proc. 13th Mediterranean Conference on Control and Automation*, June 2005, pp. 719-724.

- [3] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," in *Proc. 33rd Hawaii Int. Conf. System Sciences (HICSS)*, Maui, HI, January 2000.
- [4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans on Wireless Communications*, October 2002, vol.1, pp. 660-670.
- [5] Shen Bo, Zhang Shi-Yong, and Zhong Yi-Ping, "Cluster-Based Routing Protocols for Wireless Sensor Networks," *Journal of Software*, the China Computer Federation, 2006, 17(7), pp. 1588-1600.
- [6] Wang Daoyuan, Tian Hui, and Wang Shuang, "Energy-Efficient Routing Research for WSN," *Int. Conf. on Wireless Communications, Networking and Mobile Computing (WiCom 2007)*, September 2007, pp. 2413-2415.
- [7] Shuguang Cui, Madan R., Goldsmith A. J., and Lall S., "Cross-Layer Energy and Delay Optimization in Small-Scale Sensor Networks," *IEEE Trans on Wireless Communications*, October 2007, vol.6, no.10, pp.3688-3699.
- [8] Qian Y, Zhou JF, Qian LP, et al. "Prolonging the Lifetime of Wireless Sensor Network via Multihop Clustering," *the 6th Int. Conf. on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN 2006)*, St. Petersburg, Russia, May 2006, vol.4003, pp.118-129.
- [9] Lee HS, Kim KT, and Youn HY, "A New Cluster Head Selection Scheme for Long Lifetime of Wireless Sensor Networks," *Int. Conf. on Computational Science and Its Applications (ICCSA 2006)*, Glasgow, Scotland, May 2006, vol.3983, pp.519-528.
- [10] Gong HH, Liu M, Mao YC, et al. "Distributed Energy Efficient Data Gathering with Intra-cluster Coverage in Wireless Sensor Networks," *the 8th Asia-Pacific Web Conference and Workshops (APWeb 2006)*, Harbin, China, January 2006, vol.3841, pp.109-120.
- [11] Kim KT, and Youn HY, "Energy-Driven Adaptive Clustering Hierarchy (EDACH) for Wireless Sensor Networks," *Int. Conf. on Embedded and Ubiquitous Computing*, Nagasaki, Japan, December 2005, vol.3823, pp.1098-1107.
- [12] Cao Y, and He C, "A Distributed Clustering Algorithm with an Adaptive Backoff Strategy for Wireless Sensor Networks," *IEICE Trans. on Communications*, February 2006, vol.E89B, iss.2, pp.609-613.

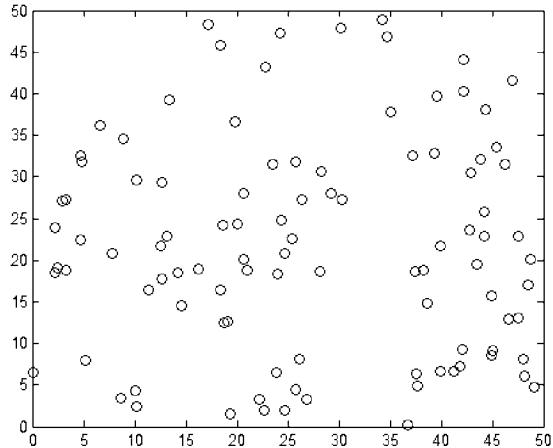


Fig. 1. 100-node random network

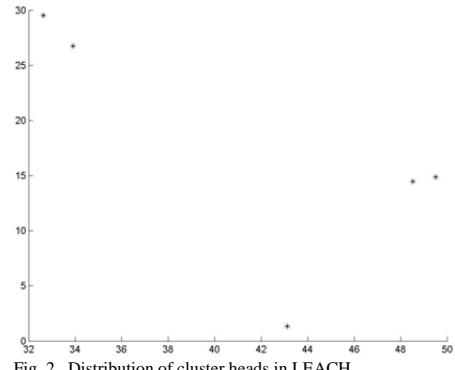


Fig. 2. Distribution of cluster heads in LEACH

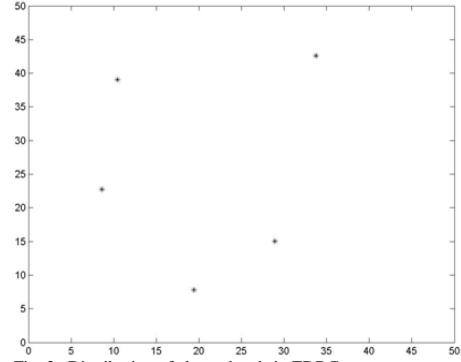


Fig. 3. Distribution of cluster heads in EDBC

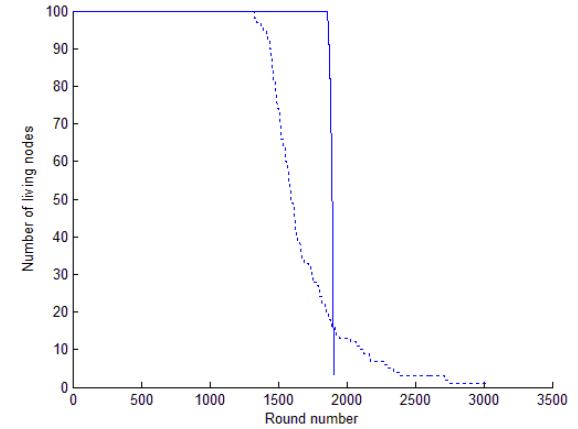


Fig. 4. Average number of living nodes in LEACH (the dotted line) and EDBC (the solid line) as round number increases.

Encoding Forensic Multimedia Evidence from MARF Applications as Forensic Lucid Expressions

Serguei A. Mokhov

SGW, EV7.139-2

Department of Computer Science and Software Engineering

Concordia University, Montreal, Quebec, Canada

Email: mokhov@cse.concordia.ca

Abstract—In this work we summarize biometric evidence as well as file type evidence extraction “exported” as formal Forensic Lucid language expression in the form of higher-order intensional contexts for further case analysis by a system that interprets Forensic Lucid expressions for claim verification and event reconstruction. The digital evidence is exported from the Modular Audio Recognition Framework (MARF)’s applications runs on a set of data comprising biometric voice recordings for speaker, gender, spoken accent, etc. as well as more general file type analysis using signal and pattern recognition processing techniques. The focus is in translation aspect of the extracted evidence into formal Forensic Lucid expressions for further analysis.

Index Terms—encoding multimedia evidence, evidence analysis, forensic case specification, Forensic Lucid, higher-order intensional contexts, Lucid, MARFL, Modular Audio Recognition Framework (MARF)

I. INTRODUCTION

Problem Statement: Authors of MARF [1] proposed to use some of its applications for biometric forensic analysis of multimedia data such as audio recordings [2] and scanned handwritten images [3] as well as file-type analysis [4]. On the other hand, they proposed an intensional scripting language for dynamic configuration management and scripting of the said applications, MARFL [5]. Yet they provide no convenient means to extract and encode the identified evidence for further processing and case analysis. In our research, we work with the Forensic Lucid specification language and need to be able to encode the extracted information as contextual expressions syntactically and semantically valid in Forensic Lucid.

Proposed Solution: We propose an adapter translator program, that translates the MARF’s data structures in a way similar to the way MARFL represents configuration details, but translated into the Forensic Lucid-compatible definitions. We add it as back-end plug-in attached to MARF to compile the resulting data structures into the Forensic Lucid expressions.

A. Forensic Lucid

Forensic Lucid [6], [7] is a forensic case specification language based on the intensional logic and programming paradigms [8], [9], [10], [11], [12], [13], [14], [15]. The authors of Forensic Lucid formally design and specify the language to be able to “script” in a tool the evidence, stories told by witnesses, and the case itself as an evidential

statement as a higher-order context specification (all Lucid dialects are context-oriented with the contexts being first-class values) as well as the case specification in terms of inference derivations of the case. Forensic Lucid was created to address the difficulties and complexity to use the earlier formal approach [16], [17] that required a potential investigator to construct a finite-state machine (FSM) and model transitions. Forensic Lucid inherited some of the terminology and formalities in the specification of events, properties, observations, observation sequences, evidential statement, and the transition function and its inverse for event reconstruction and automated verifiability of traces from the FSM approach. Forensic Lucid’s compiler and development environment is being realized in a sister project, the General Intensional Programming System (GIPSY) [13], [18], [19].

B. MARF and MARFL

MARFL is an intensional Lucid-like configuration specification language for MARF applications scripting support. It supports higher-order context definitions for nested configuration parameters. We capitalize on that notion in our research by translating the results of classification and parts of the configurations into the Forensic Lucid expressions. A comprehensive example of a context for processing a WAV file in the MARF’s pipeline can be modeled as shown in Figure 1 [5]. In that example the authors of MARFL illustrate a complex hierarchical context expression where several nested dimensions are explicitly specified. In general, MARFL’s context follows the classical Lucid definition, where it is defined as a collection of $\langle dimension : tag \rangle$ pairs. What MARFL does differently is that a single pair may not necessarily be an atomic context, but may contain sub-contextual elements. The inner-most context is always simple and atomic and typically has dimensions of primitive types, such as integer, IEEE 754 floating point value, or a string. The outer layers of context hierarchy are composite objects. Thus, a `[sample loader:WAV]` denotes a dimension of type `sample loader` with its higher-order tag value `WAV`. The `WAV` dimension value can further be decomposed to an atomic simple context if needed, that contains three dimensions of primitive types.

Such a way of context representation of the higher-order context by the MARFL authors is similar to equivalent defi-

nitions described by Swoboda et al. in [20], [21], [22], [23], where a tree of contexts is defined for languages like iHTML (with nested tags), functional intensional databases annotated with XML, etc.

II. METHODOLOGY

A. Translation into Forensic Lucid

The higher-order contextual specification of Forensic Lucid goes (top to bottom) from evidential statement, to observation sequence, to observation, to (P, \min, \max) , where the observed property P is an arbitrary object, usually a human-readable description of the state or event, and $[\min, \min + \max]$ is the duration of the observation of that property [16], [17]. Thus, at the higher order we need something similar to Listing 1's `o1`. We borrow the mapping of the properties P (that can be strings, integers, or even any-order contextual or otherwise expressions) to a human-readable rewrite string, similarly to what is in Listing 2 after the \Rightarrow sign. We also assume that a P by itself is a syntactic sugar of $(P, 1, 0)$.

```
evidential statement es = unordered {os1,os2,os3};
where
  observation sequence os1 = ordered {o1,o2,o3};
  observation sequence os2 = ordered {o4,o5,o6};
  observation sequence os3 = ordered {o7,o8,o9};
  where
    observation o1 =
    [
      p: "ID:23;JoeAverage" => "speaker ID is 23, Joe
                                   Average",
      min:1,
      max:0
    ];
    ...
  end;
end;
```

Listing 1. Forensic Lucid Contextual Expression

B. MARF Evidence

The evidence extracted from the analysis results of MARF comes from the several internal data structures, namely `Result`, `ResultSet`, `TrainingSet`, and `Configuration`.

The `Result` consists of tuples containing `ID` and `outcome`, which are the properties of a single result. The result set, `ResultSet`, is a collection of such tuples. Processed utterances (a.k.a feature vectors or clusters of `doubles`), alongside with the training file names and IDs comprise the training set data, and configuration is a collection of processing settings that led to the current results given the training set.

We need to specify what is the property P in the three categories (configuration, training set, and the result set) and what is its observed duration. We set it as follows: it is a default of $(1, 0)$, as the notion of duration varies per configuration, so we are only interested in of how we arrive from the given configuration and training set to the results.

We syntactically write `observation o = P`, which is equivalent to $(P, 1, 0)$ as mentioned earlier. We need to then

```
MrA @ es_mra
where
  evidential statement es_mra = {os_mra, os_final,
  os_unrelated};

observation sequence os_mra = ($, o_unrelated_clean, $,
  o_blackmail, $);
observation sequence os_final = ($, o_final);
observation sequence os_unrelated = ($, o_unrelated, $, (
  Ct,0,0), $);

observation o_final = (1, "u", "t2");
observation o_unrelated_clean = (1, "u", "o1");

// ...

invtrans(Q, es_mra, o_final) = backraces
where
  // list of all possible dimensions
  observation Q = lengths box left_part box right_part;

// events
observation lengths = unordered {0, 1, 2};

// symbolic labels map to human descriptions
observation left_part = unordered {
  "u" => "unrelated",
  "t1" => "threats-obscured part",
  "o1" => "other data (left part)"
};

observation right_part = unordered {
  "t2" => "threats in slack",
  "o2" => "other data (right part)"
};

backtraces = [ A, B, C, D, ];
where
  ...
end;
end;
end;
```

Listing 2. Blackmail Case Modeling in Forensic Lucid

determine what is an observation sequence. We define it as a sequence of three “observations”, each observation per category. The observations must be ordered: (1) configuration `config0`, (2) training set `tset0`, and (3) the classification result `result0`. The meaning of this observation sequence is that given some MARF configuration settings and the existing training set, the system produces the classification result. If we are performing the training, the observation sequence is slightly different, but also has three observations: configuration, incoming sample, and the resulting training set, which would be encoded accordingly as all the necessary primitives for that are already defined. With such notions in mind we come up with the complete exportable Forensic Lucid expression as a 3-observation sequence, e.g. presented in Listing 2. As with our simplifying assumption, we can remove the $(1, 0)$ syntactical constructs, and just keep the P , which in this case is a higher-order context specification, as shown in Figure 3.

We define some syntactic examples and the corresponding simplifications to illustrate a few points:

- an observation sequence `OS` is a sequence of three observations, where the last one is the “no-observation” \$ construct:

```
os = { o1, o2, $ };
```

```
[  
    sample loader      : WAV [ channels: 2, bitrate: 16, encoding: PCM, f : 8000 ],  
    preprocessing     : LOW-PASS-FFT-FILTER [ cutoff: 2024, windowsize: 1024 ],  
    feature extraction: LPC [ poles: 20, windowsize: 1024 ],  
    classification   : MINKOWSKI-DISTANCE [ r : 5 ]  
]  

```

Fig. 1. Example of hierarchical context specification for a evaluation configuration of MARF.

```
MARFos = { confo, tseto, resulto } =  
{  
    ([  
        sample loader      : WAV [ channels: 2, bitrate: 16, encoding: PCM, f : 8000 ],  
        preprocessing     : LOW-PASS-FFT-FILTER [ cutoff: 2024, windowsize: 1024 ],  
        feature extraction: LPC [ poles: 20, windowsize: 1024 ],  
        classification   : MINKOWSKI-DISTANCE [ r : 5 ]  
    ], 1, 0),  
  
    ([data:[{[5.2,3.5,7.5],[3.6,2.5,5.5,6.5]}], files:[``/foo/bar.wav'', ``/bar/foo.wav'']], 1, 0),  
    ([ID:5, outcome:1.5], 1, 0)  
}  

```

Fig. 2. Example of a three-observation sequence context exported from MARF to Forensic Lucid.

```
MARFos = { confo, tseto, resulto } =  
{  
    [  
        sample loader      : WAV [ channels: 2, bitrate: 16, encoding: PCM, f : 8000 ],  
        preprocessing     : LOW-PASS-FFT-FILTER [ cutoff: 2024, windowsize: 1024 ],  
        feature extraction: LPC [ poles: 20, windowsize: 1024 ],  
        classification   : MINKOWSKI-DISTANCE [ r : 5 ]  
    ],  
  
    [data:[{[5.2,3.5,7.5],[3.6,2.5,5.5,6.5]}], files:[``/foo/bar.wav'', ``/bar/foo.wav'']],  
    [ID:5, outcome:1.5]  
}  

```

Fig. 3. Example of a simplified three-observation sequence context exported from MARF to Forensic Lucid.

- if observations of properties $P_1 = [a : 1, b : 2]$ and $P_2 = [s : 4, g : 7]$ (which happened to be contexts themselves here) have a duration of 1 (one) they can be shortened in their expression to just P . E.g. the following observation sequences are equivalent:


```
os = {[a:1,b:2], [s:4,g:7]};  
os = {[{[a:1,b:2]},1,0], {[s:4,g:7]},1,0});
```
- in generic observation sequences where *min* and *max* duration parameters are not zero, cannot be implicit. In the below is an example of a “complex” observation sequence where P_1 and P_2 have several possible durations, e.g. in $os - \{o_1, o_2\}$, where $o_1 = (P_1, 5, 4)$ and $o_2 = (P_2, 1, 2)$, would result in:


```
os = {[{[a:1,b:2]},5,4], {[s:4,g:7]},1,2});
```
- As a “syntactical sugar” we allow a declaration of an observation sequence *os* that consists of only a single observation o_1 , we allow dropping of the curly braces:


```
os = o1; <=> os = {o1};
```

III. LIMITATIONS

There are a number of current limitations with the approach that are to be addressed in the upcoming future work. We list some of them here:

- At this point the investigator will have to “copy-paste” the produced output into their Forensic Lucid case specification for further evaluation after the output is produced, i.e. there are now friendly user-interface or any other type of integration of the exporter code, MARF, and GIPSY.
- The concrete syntax and semantics of Forensic Lucid and MARFL, are not fully finalized as of this writing as they both go through the design, formalization, and analysis phases with relatively frequent adjustments as the research moves forward.
- There are no correctness proofs yet for the Forensic Lucid code itself as well as the correctness of implementation

of MARF and GIPSY, which are necessary to be valid for the tool to be usable in court.

IV. CONCLUSION

We devised a basic methodology of exporting and translating the evidence contained within MARF's data structures represented in the higher level in the MARFL language, as a collection of contextual expressions in Forensic Lucid. The evidence of biometric origin, file type analysis, writer analysis and others can therefore be exported into Forensic Lucid for case formulation later on. An investigator can simply use the provided expression in their Forensic Lucid case as-is to maintain the library of observation sequences with the collected evidence.

V. FUTURE WORK

This section lists a number of items to improve in the near future work in the Forensic Lucid language and the surrounding systems. These are mostly there to address the limitations described earlier and enhance overall usability, applicability, and standardization of the language:

- Prove the correctness of the MARF code and its storage modules in the internal representation of the evidence.
- Complete formal definition of Forensic Lucid and MARFL, and then formally verify the correctness of the adapter/exporter code and prove its equivalence between the MARFL and Forensic Lucid representations in Isabelle [24].
- Provide equivalent translation and export tools for the JPF-based forensic toolkit [25], [26], [27] plug-ins for memory, log, and email analysis evidence as evidential expressions specified in Forensic Lucid.
- Export MARF pipeline as a transition function ψ for complete specification of the MARF-based system in Forensic Lucid.

ACKNOWLEDGMENT

The author thanks Drs. Joey Paquet and Mourad Debbabi for the helpful and detailed review, suggestions, support, and comments about this work. We acknowledge reviewers who took time to review this work and provide us with constructive feedback. This work is sponsored in part by the Faculty of Engineering and Computer Science, Concordia University, Montreal, Canada.

REFERENCES

- [1] The MARF Research and Development Group, "The Modular Audio Recognition Framework and its Applications," SourceForge.net, 2002–2008, <http://marf.sf.net>, last viewed December 2008.
- [2] S. A. Mokhov, "Study of best algorithm combinations for speech processing tasks in machine learning using median vs. mean clusters in MARF," in *Proceedings of C3SE'08*, B. C. Desai, Ed. Montreal, Quebec, Canada: ACM and BytePress, May 2008, pp. 29–43, ISBN 978-1-60558-101-9.
- [3] ——, "Writer Identification Using Inexpensive Signal Processing Techniques: Experimental Results," 2008, unpublished.
- [4] S. A. Mokhov and M. Debbabi, "File type analysis using signal processing techniques and machine learning vs. `file` unix utility for forensic analysis," in *Proceedings of the IT Incident Management and IT Forensics (IMF'08)*, O. Goebel, S. Frings, D. Guenther, J. Nedon, and D. Schadt, Eds., Mannheim, Germany, Sep. 2008, pp. 73–85, LNI140.
- [5] S. A. Mokhov, "Towards syntax and semantics of hierarchical contexts in multimedia processing applications using MARFL," in *Proceedings of the 32nd Annual IEEE International Computer Software and Applications Conference (COMPSAC)*. Turku, Finland: IEEE Computer Society, Jul. 2008, pp. 1288–1294.
- [6] S. A. Mokhov and J. Paquet, "Formally specifying and proving operational aspects of Forensic Lucid in Isabelle," Department of Electrical and Computer Engineering, Concordia University, Tech. Rep. 2008-1-Ait Mohamed, Aug. 2008, in *Theorem Proving in Higher Order Logics (TPHOLs2008): Emerging Trends Proceedings*.
- [7] S. A. Mokhov, J. Paquet, and M. Debbabi, "Formally specifying operational semantics and language constructs of Forensic Lucid," in *Proceedings of the IT Incident Management and IT Forensics (IMF'08)*, O. Goebel, S. Frings, D. Guenther, J. Nedon, and D. Schadt, Eds., Mannheim, Germany, Sep. 2008, pp. 197–216, LNI140.
- [8] E. A. Ashcroft and W. W. Wedge, "Lucid - a formal system for writing and proving programs," *SIAM J. Comput.*, vol. 5, no. 3, 1976.
- [9] ——, "Erratum: Lucid - a formal system for writing and proving programs." *SIAM J. Comput.*, vol. 6, no. (1):200, 1977.
- [10] ——, "Lucid, a nonprocedural language with iteration," *Communication of the ACM*, vol. 20, no. 7, pp. 519–526, Jul. 1977.
- [11] W. Wedge and E. Ashcroft, *Lucid, the Dataflow Programming Language*. London: Academic Press, 1985.
- [12] E. Ashcroft, A. Faustini, R. Jagannathan, and W. Wedge, *Multidimensional, Declarative Programming*. London: Oxford University Press, 1995.
- [13] J. Paquet, "Scientific intensional programming," Ph.D. dissertation, Department of Computer Science, Laval University, Sainte-Foy, Canada, 1999.
- [14] R. Lalement, *Computation as Logic*. Prentice Hall, 1993, C.A.R. Hoare Series Editor. English translation from French by John Plaice.
- [15] P. Rondogiannis, "Higher-order functional languages and intensional logic," Ph.D. dissertation, Department of Computer Science, University of Victoria, Victoria, Canada, 1994.
- [16] P. Gladyshev, "Finite state machine analysis of a blackmail investigation," in *International Journal of Digital Evidence*. Technical and Security Risk Services, Sprint 2005, Volume 4, Issue 1, 2005.
- [17] P. Gladyshev and A. Patel, "Finite state machine approach to digital event reconstruction," in *Digital Investigation Journal*, vol. 2, 2004.
- [18] J. Paquet and P. Kropf, "The GIPSY architecture," in *Proceedings of Distributed Computing on the Web*, Quebec City, Canada, 2000.
- [19] J. Paquet, "A multi-tier architecture for the distributed eductive execution of hybrid intensional programs," 2008, submitted for publication at SAC'09.
- [20] P. Swoboda, "A formalisation and implementation of distributed intensional programming," Ph.D. dissertation, The University of New South Wales, Sydney, Australia, 2004.
- [21] P. Swoboda and W. W. Wedge, "Vmake, ISE, and IRCS: General tools for the intensionalization of software systems," in *Intensional Programming II*, M. Gergatsoulis and P. Rondogiannis, Eds. World-Scientific, 2000.
- [22] P. Swoboda and J. Plaice, "A new approach to distributed context-aware computing," in *Advances in Pervasive Computing*, A. Ferscha, H. Hoertner, and G. Kotsis, Eds. Austrian Computer Society, 2004, ISBN 3-85403-176-9.
- [23] ——, "An active functional intensional database," in *Advances in Pervasive Computing*, F. Galindo, Ed. Springer, 2004, pp. 56–65, LNCS 3180.
- [24] L. C. Paulson and T. Nipkow, "Isabelle: A generic proof assistant," University of Cambridge and Technical University of Munich, 2007, <http://isabelle.in.tum.de/>, last viewed: December 2007.
- [25] M. Debbabi, A. R. Arasteh, A. Sakha, M. Saleh, and A. Fry, "A collection of JPF forensic plug-ins," Computer Security Laboratory, Concordia Institute for Information Systems Engineering, 2007–2008.
- [26] A. R. Arasteh and M. Debbabi, "Forensic memory analysis: From stack and code to execution history," *Digital Investigation Journal*, vol. 4, no. 1, pp. 114–125, Sep. 2007.
- [27] A. R. Arasteh, M. Debbabi, A. Sakha, and M. Saleh, "Analyzing multiple logs for forensic evidence," *Digital Investigation Journal*, vol. 4, no. 1, pp. 82–91, Sep. 2007.

Distributed Modular Audio Recognition Framework (DMARF) and its Applications Over Web Services

Serguei A. Mokhov

SGW, EV7.139-2

Department of Computer Science and Software Engineering

Concordia University, Montreal, Quebec, Canada

Email: mokhov@cse.concordia.ca

Rajagopalan Jayakumar

SGW, EV3.151

Department of Computer Science and Software Engineering

Concordia University, Montreal, Quebec, Canada

Email: jayakumar@cse.concordia.ca

Abstract— In this work we present the software architecture design and implementation of a Distributed Modular Audio Recognition Framework (DMARF), and its applications, such as Speaker Identification, that can run distributively over the Web Services architecture using XML-RPC. We describe some of the challenges occurred during the design and implementation, the advantages and disadvantages of such an implementation, and its possible future directions.

Index Terms—Distributed Modular Audio Recognition Framework (DMARF), Web Services, XML-PRC, MARF

I. INTRODUCTION

Problem Statement: DMARF, a distributed extension of MARF (detailed further), implemented in Java had its RMI and CORBA implementation done in a modular way (such that they can co-exist, and communicate, or replace each other), but were not flexible enough and required Java- or CORBA-enabled clients outside of MARF's own modules. The now popular Web Services paradigm that makes the components even more interoperable and platform-independent than even CORBA was lacking in DMARF.

Proposed Solution: We extend the original DMARF with the Web Services (WS) implementation such that its architecture and semantics are compatible to that of the already fully implemented RMI and CORBA services. With our contribution we add much greater interoperability of the DMARF nodes over the Internet and restricted environments where HTTP is the only protocol allowed.

A. Distributed MARF

DMARF [1] is based on the classical MARF (introduced further) whose pipeline stages were made into distributed nodes.

Classical MARF: The Modular Audio Recognition Framework (MARF) [2] is an open-source research platform and a collection of pattern recognition, signal processing, and natural language processing (NLP) algorithms written in Java and arranged into a modular and extensible framework facilitating addition of new algorithms for use and experiments by scientists. The backbone of MARF consists of pipeline stages that communicate with each other to get the data they need in a chained manner. In general, MARF's pipeline of algorithm implementations is presented in Figure 1 [3]. The pipeline consists of four basic stages: sample loading, preprocessing, feature extraction, and training/classification. There

are a number of applications that test MARF's functionality and serve as examples of how to use MARF's modules. One of the most prominent applications SpeakerIdentApp [4] – Text-Independent Speaker Identification (who, gender, accent, spoken language, etc.) [5].

Distributed Version: The classical MARF presented in the previous section was extended [1], [6], [7] to allow the stages of the pipeline to run as distributed nodes as well as a front-end, as roughly shown in Figure 2. The basic stages and the front-end were implemented without backup recovery or hot-swappable capabilities at this point; just communication over Java RMI [8], CORBA [9], and now with XML-RPC web services [10].

Applications of DMARF: Any high-volume processing of recorded audio, textual, or imagery data for pattern recognition and biometric forensic analysis are the typical applications MARF has been used on a desktop. DMARF makes this process distributed. Web Services in DMARF make it even more widely available over the Internet. Most of the emphasis in this work is in audio, such as conference recordings [3] with purpose of attribution of said material to identities of speakers. Similarly, processing a bulk of recorded phone conversations in a police department for forensic analysis and subject identification and classification, where sequential runs of the MARS instances (Modular Audio Recognition System is an implementing concrete instance of MARF) on the same machine, especially a mobile equipment such as a laptop, PDA, cellphone, etc., which are not necessarily high-performance computing devices, so an investigator has an ability of uploading collected voice samples to the servers constituting a DMARF-implementing network.

B. Requirements

MARF has several applications. The distributed application ideas in some part come from [11], [8], [9], [12], [10], [13], [14]. The classical pipeline in Figure 1 and the original applications (e.g. speaker identification service, etc.) as they stand are purely sequential with even little or no concurrency when processing a bulk of voice samples. Thus, the purpose of this work is to make the pipeline distributed and run on a cluster or a just a set of distinct computers to compare with the traditional version and do a thorough software engineering design for disaster recovery and service replication, communication technology independence, and the like.

In Figure 2 the distributed version of the pipeline is presented. It indicates different levels of basic front-ends, from higher to lower, which a client application may invoke as well as services may invoke other services through their front-ends while executing in a pipelined mode. The back-ends are in charge of providing the actual servant implementations as well as the features like primary-backup replication, monitoring, and disaster recovery modules.

There are several distributed services, some are more general, and some are more specific. The services can and have to intercommunicate. These include:

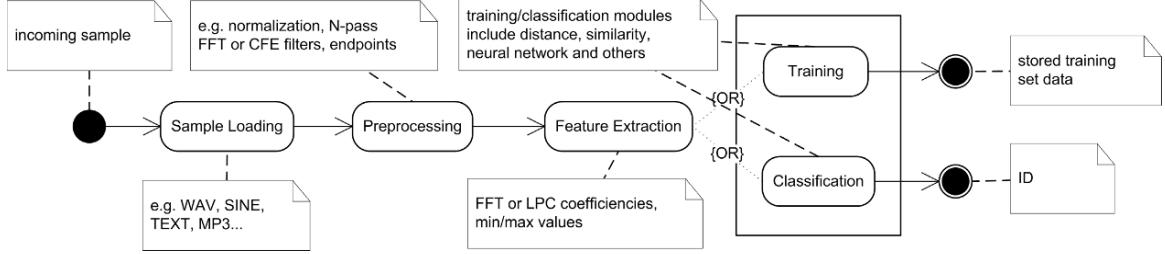


Fig. 1. MARF's Pattern Recognition Pipeline

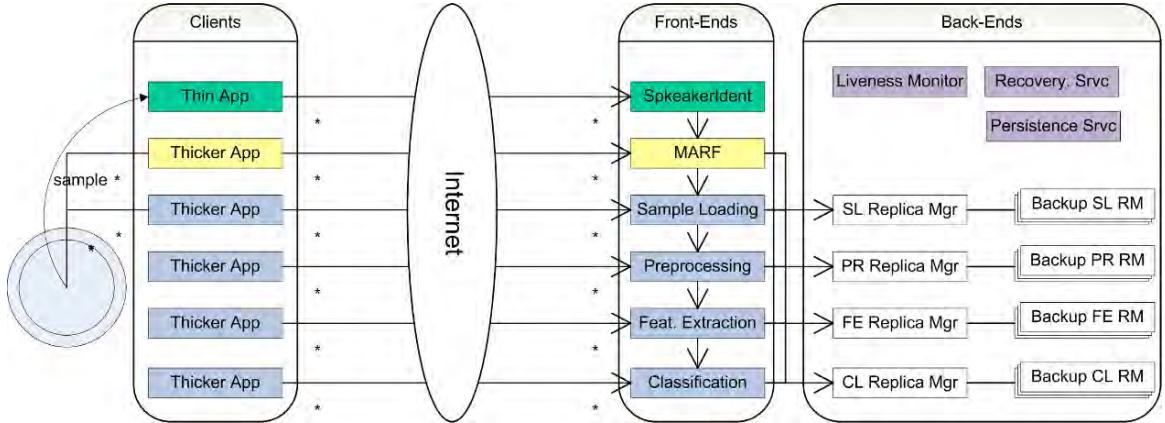


Fig. 2. The Distributed MARF Pipeline

- The General MARF Service that exposes MARF's pipeline to clients and other services and communicates with the below.
- The Sample Loading Service knows how to load certain file or stream types (e.g. WAVE) and convert them accordingly for further preprocessing.
- The Preprocessing Service accepts incoming voice, text, image, or any binary samples and does the requested preprocessing (a variety of filters, normalization, etc.).
- The Feature Extraction Service accepts data, presumably pre-processed, and attempts to extract features out of it given requested algorithm (out of currently implemented, like FFT, LPC, MinMax, etc.) and may optionally query the preprocessed data from the Preprocessing Service.
- The Classification and Training Service accepts feature vectors and either updates its database of training sets or performs classification against existing training sets. It may optionally query the Feature Extraction Service for the feature vectors.
- The Natural Language Processing Service accepts natural language texts and performs also some statistical NLP operations, such as probabilistic parsing, Zipf's Law stats, etc.

Some more application-specific front-end services (that are based on the existing currently non-distributed applications) include but not limited to:

- The Speaker Identification Service (a front-end) that will communicate with the MARF service to carry out application tasks.
- The Language Identification Service would communicate with MARF/NLP for the similar purpose to identify the written or spoken language.
- Some others (front-ends for Zipf's Law, Probabilistic Parsing,

and test applications).

The clients are so-called “thin” clients with GUI or a web form allowing users to upload the samples for training/classification and set the desired configuration for each run, either for individual samples or a batch.

C. Design Scope

In the DMARF, if any pipeline stage process crashes access to information about the pending transactions and computation in module is not only lost while the process remains unavailable, but can also be lost forever. The use of a message logging protocol is one way that a module could recover information concerning that module's data after a faulty processor has been repaired. A write-ahead message-logging (WAL) protocol is designed for DMARF. It is designed for the disaster recovery of uncommitted transactions and to avoid data loss. It also allows to be extended for backup replication and point-in-time recovery (PITR) if WAL logs are shipped off to a backup storage or a replica manager and can later be used to reconstruct the replica state via gossip or any other replication scheme.

The design of DMARF is also extended by adding a “warm standby”. The “warm standby” is a DMARF module that is running in the background (normally on a different machine), receiving operations from the primary server to update its state and hence ready to “jump in” if the primary server fails. Thus, when the primary server receives a request from a client, which changes its state, the primary sends the request to the backup server, performs the request, receives the response from the backup server and then sends the reply back to the client. The main purpose of the “warm stand by” is to

minimize the downtime for subsequent transactions while the primary is in disaster recovery. The primary and backup servers communicate using either the reliable TCP protocol on a WAN (e.g. the Internet) or a FIFO-ordered UDP on a LAN.

II. SYSTEM OVERVIEW

In this section, we examine the system architecture of the implementation of the DMARF application and software interface design issues.

A. Architectural Strategies

The main principles are:

- Platform-Independence – where one targets systems that are capable of running HTTP.
- Database-Independent API – will allow to swap database/storage engines on-the-fly. The appropriate adapters will be designed to feed upon required/available data source (binary, CSV file, XML, or SQL) databases.
- Communication Technology Independence – where the system design evolves such that any communication technologies adapters or plug-ins (e.g. RMI [8], CORBA [9], DCOM [15], Jini [16], JMS [17], Web Services [10]) can be added with little or no change to the main logic and code base.
- Reasonable Efficiency – where one architects and implements an efficient system, but will avoid advanced programming tricks that improve the efficiency at the cost of maintainability and readability.
- Simplicity and Maintainability – where one targets a simplistic and easy to maintain organization of the source code.
- Architectural Consistency – where one consistently implements the chosen architectural approach.
- Separation of Concern – where one isolates separate concerns between modules and within modules to encourage re-use and code simplicity.

B. System Architecture

1) *Module View*: The DMARF system is divided into layers. The top level has a front-end and a back-end. The front-end itself exists on the client side and on the server side. The client side is either text-interactive, non-interactive, or a web form/servlet collection of client classes that connect and query the servers. The front-end on the server side are the MARF pipeline itself, the application-specific frontend, and pipeline stage services. All pipeline stages somehow involved to the database and other storage management subfunctions. At the same time the services are a back-end for the client connecting in.

2) *Execution View*:

Runtime Entities: of the Java Virtual Machine (JVM) and on the server side there must be the naming and implementation repository service running. For the WS aspect of the application, there ought to be DNS running and a web servlet container. The DMARF uses Apache Tomcat [18] as a servlet container for DMARF's WS. The WS client in addition to the Java Runtime Environment (JRE) may require a servlet container environment and a browser to view and submit a web form.

Communication Paths: It was resolved that the modules would all communicate through message passing between methods. Further, a Java XML Remote Procedure Call (JAX-RPC)-based implementation over the Simple Object Access Protocol (SOAP) is used for Web Services (WS). While a more modern JAX-WS alternative to JAX-RPC was released, this project still relies on JAX-RPC 1.1 as it's not using J2EE and the authors found it is simpler and faster to use and more accurate tutorial and book material were available). WS influenced some technology-specific design decisions, but it was possible to abstract them as was done earlier for RMI and CORBA "agents" and delegate the business

logic to the corresponding delegate classes enabling all three types of services to communicate and implement transactions similarly. Communication to the database depends on the storage manager (each terminal business logic module in the classical MARF is the StorageManager class). Additionally, Java's reflection [19] is used to discover instantiation communication paths at run-time for pluggable modules.

Execution Configuration: The execution configuration of the DMARF has to do with where its `data/` and `policies/` directories are. The `data/` directory is always local to where the application was ran from. In the case of WS, it has to be where Tomcat's current directory is; often is in the `logs/` directory of `$(catalina.base)`. The data directory contains the service-assigned databases in the `XXX.gzbin` (generated on the first run of the servers). The "XXX" corresponds to the either training set or a module name that saved their state. For the WS, for deployment two directories `META-INF/` and `WEB-INF/` are used. The former contains the Tomcat's context file for deployment that ought to be placed in `$(catalina.base)/conf/Catalina/localhost/` and the latter typically goes to `local/marf` as the context describes. It contains `web.xml` and other XML files produced to describe servlet to SOAP mapping when generating `.war` files with the `wscompile` and `wsdeploy` tools provided with the JAX-RPC distribution.

The build-and-run files include the Ant [20] `dmarf-build.xml` and the GNU make [21] `Makefile` files. The `Makefile` is the one capable of starting the servers, and the clients in various modes. The execution configuration targets primarily the Fedora Linux platform (if one intends to use `gmake`), but is not restricted to it.

A hosts configuration file `dmarf-hosts.properties` is used to tell the services of how to initialize and where to find other services initially. If the file is not present, the default host for all is assumed to be `localhost`.

3) *Proof-of-Concept Prototype Assumptions*: Some simplifying assumptions took place that were not a part of, explicit or implied, of the specification. They are to be fulfilled in the future work as the system evolves. These in fact represent the current limitations.

- There is no garbage collection done on the server side in terms of fully limiting the WAL size or outdated data in the training sets or any other database.
- WAL functionality has not been at all implemented for the modules other than for the Classification Service.
- DMARF services do not implement nested transaction while pipelining.
- Services do not intercommunicate (TCP or UDP) other than through the pipeline mode of operation.
- No primary-backup or otherwise replication is present.

C. Software Interface

Primary communication-related software interfaces are briefly described below. A few other interfaces are omitted for brevity (of storage and classical MARF).

WS: The main WS interfaces the WS "servants" (which are actually servlets) implement are `ISpeakerIdentWS`, `IMARFServerWS`, `ISampleLoaderWS`, `IPreprocessingWS`, `IFeatureExtractionWS`, and `IClassificationWS`. They are located in the `marf.server.ws.*` packages. There are also the generated files off this interface for stub and skeleton serializers and builders for each method and non-primitive data type of Java with `wscompile` and `wsdeploy` and the "servant" implementations. There are about eight (8) files generated for SOAP XML messages per method or a data type for requests, responses, faults, building, and serialization.

Delegate: The DMARF is flexible here and allows any delegate implementation as long as `IDelegate` in `marf.net.server.delegates` is implemented. A common implementation of it is also there provided with the added value benefit that all three types of servants of the above can use the same

delegate implementations and therefore can share all of functionality, transactions, and communication.

III. DETAILED SYSTEM DESIGN

This section briefly presents the design considerations and assumptions in the form of directory structure, and UML class diagrams.

A. Directory and Package Organization

In this section, the directory structure is introduced. Please note that Java, by default, converts sub-packages into subdirectories. Please refer to Table I and Table II for description of the data contained in the directories and the package organization, respectively.

B. UML Class Diagrams

The entire design is summarized in several UML class diagrams representing the major modules and their relationships. The diagram of the overall architecture is in Figure 3. We omit others due to the shortage of space, but they can be located in the project's CVS repository online or the related talks and presentations.

In the general architecture, at the root of the hierarchy are the `IClient` and `IServer` interfaces that are independent of a communication technology type of interfaces that "mark" the would-be classes of being type server or client. This is design of a system where one is able to pick and choose either manually or automatically which communication technologies to use. These interfaces are defined in the `marf.net` package and are used in reflection instantiation utilities.

Next, the hierarchy branches to the WS marked-up sever and client interfaces (among others), `IWSServer` and `IWSClient`. The `IWSServer` allows setting and getting an in-house made `RemoteObjectReference` (which isn't a true object reference as in RMI or CORBA, but encapsulates the necessary service location information). Then the diagram shows the servants and their relationships with the exposed interfaces as well as inclusion of the WAL logging, transaction recovery, and monitoring module stubs in the process. The clients for the respective technologies are in the `marf.net.client.ws` packages. The servers for the respective technologies are in the `marf.net.server.ws` packages.

More design details are revealed in the class diagram of the storage-related aspects in Figure 4. The `Database` class contains statistics of classification and is only written by the `SpeakerIdentApp` front-end. All, `Database`, `Sample`, `Result`, and `ResultSet` and `TrainingSet` implement the `Serializable` interface to be able to be stored on disk or transferred over a network.

The serialization of the WAL instance into a file is handled by the `WALStorageManager` class. The `IStorageManager` interface and its most generic implementation `StorageManager` come from the MARF's `marf.Storage` package. The `StorageManager` class provides the implementation of serialization of class instances in plain binary as well as compressed binary formats. It also has facilities to plug-in other storage or output formats, such as CSV, XML, HTML, and SQL, which derivatives must implement if they wish.

C. Synchronization

The notion of synchronization is crucial in an application that allows access to shared resources or a data structures by multiple read-write entities in terms of clients and servers. This includes our DMARF. At the server side the synchronization must be maintained when the `Database` or `TrainingSet` objects are accessed through the server possibly by multiple clients and servers out of which at least one performs an update. The way it is designed and implemented in this version, the `Database` class instance becomes its own object monitor and all its relevant methods are made synchronized, thus locking entire object while it's accessed by a

thread thereby providing data integrity. The whole-instance locking maybe somewhat inefficient, but can be carefully re-done by only marking some critical paths only and not the entire object – a topic for another work and version.

Furthermore, multiple servers keep a copy of their own data structures, making it more concurrent. On top of that, the WS DMARF servants act through a delegate implementation allowing to keep all the synchronization and business logic in one place and decouple the communication logic from the business logic.

IV. TESTING

The conducted testing of the distributed pipeline including single training test and a batch training on maximum four computers in separate buildings. `Makefile` and `batch.sh` serve this purpose.

The tests were quite successful and terminating any of the service replicas and restarting it resumed normal operation of the pipeline in the batch mode. There more thorough testing is to be conducted as the project evolves from a proof-of-concept to a cleaner solution.

V. CONCLUSION

We successfully complemented DMARF's RMI and CORBA implementation with the Web Services for greater portability of MARF services over HTTP.

The WS implementation from the Java-endpoint provided interface and a couple of XML files was a natural extension of RMI implementation *but* with somewhat different semantics from RMI and CORBA. The implementation effort required to architect the WS aspect was not high, but the deployment within a servlet container and WSDL compilation required significant effort.

However, the highly modular design allowed swapping module implementations from one technology to another if need be making it very extensible by the means of delegating the actual business logic to the delegate classes. As an added bonus of that implementation, WS services can communicate with the RMI-, CORBA-based ones, through plain TCP or UDP and do transactions. Likewise, all the synchronization efforts are undertaken by the delegates and the delegates are the single place to fix if there is something broken.

Summary of Technologies Used: The following were the most prominent technologies used throughout the implementation of the project: J2SE (primarily 1.4), Java WS with JAX-RPC [10], Java Servlets [22], Java Networking [12], Apache Ant [20], Apache Jakarta Tomcat [18], and GNU Make [21].

Future Work and Work-In-Progress: Extend the remote framework to include other communication technologies (Jini, JMS, DCOM+, .NET Remoting) in communication-independent fashion and transplant that all for use in MARF [13]. Additionally, complete application GUI for the client and possibly server implementations. Finally, complete the advanced features of distributed systems such as disaster recovery, fault tolerance, high availability and replication, and others with great deal of thorough testing.

ACKNOWLEDGMENT

This research work was funded by the Faculty of Engineering and Computer Science of Concordia University, Montreal, Canada.

REFERENCES

- [1] S. A. Mokhov, "On design and implementation of distributed modular audio recognition framework: Requirements and specification design document," Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, Aug. 2006, project report, <http://marf.sf.net>, last viewed December 2008.
- [2] ——, "Choosing best algorithm combinations for speech processing tasks in machine learning using MARF," in *Proceedings of the 21st Canadian AI'08*, S. Bergler, Ed. Windsor, Ontario, Canada: Springer-Verlag, Berlin Heidelberg, May 2008, pp. 216–221, LNAI 5032.

TABLE I
DETAILS ON MAIN DIRECTORY STRUCTURE

Directory	Description
bin/	compiled class files are kept here. The sub-directory structure mimics the one of the <code>src/</code> .
data/	contains the database.
logs/	contains the client and server log files.
doc/	project's API and manual documentation.
lib/	libraries
src/	contains the source code files and follows the described package hierarchy.
dist/	contains distribution services <code>.jar</code> and <code>.war</code> files.
policies/	access policies for the RMI client and server granting various permissions.
META-INF/	Tomcat's context file (and later manifest) for deployment <code>.war</code> .
WEB-INF/	WS WSDL servlet-related deployment information and classes.

TABLE II
DMARF'S PACKAGE ORGANIZATION

Package	Description
marf	root directory of the MARF project; below are the packages mostly pertinent to the DMARF
marf.net.*.*	MARF's directory for the some generic networking code
marf.net.client	client application code and subpackages
marf.net.client.ws.*	Distributed MARF WS clients
marf.net.protocol.*	reserved for other protocols, like two-phase commit
marf.net.server.*	main server code and interfaces is placed here
marf.net.server.ws.*	WS-specific services implementation
marf.net.server.delegates.*	service delegate implementations are here
marf.net.server.frontend.*	root of the service front-ends
marf.net.server.frontend.ws.*	WS-specific service front-ends
marf.net.server.frontend.delegates.*	service front-ends delegate implementations
marf.net.server.monitoring	reserved for various service monitors and their bootstrap
marf.net.server.persistence	reserved for WAL and Transaction storage management
marf.net.server.recovery	reserved for WAL recovery and logging
marf.Storage	MARF's storage-related utility classes
marf.util	MARF's general utility classes (threads, loggers, array processing, etc.)
marf.gui	general-purpose GUI utilities that to be used in the applications, clients, and server status monitors

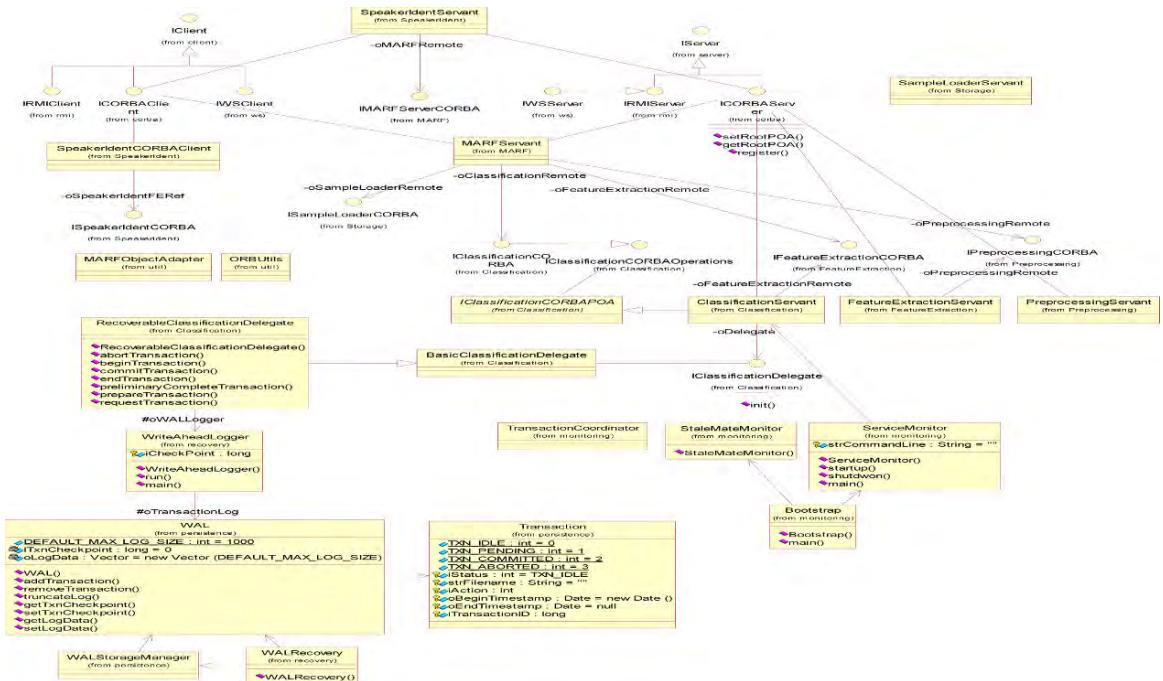


Fig. 3. General Architecture Class Diagram of marf.net

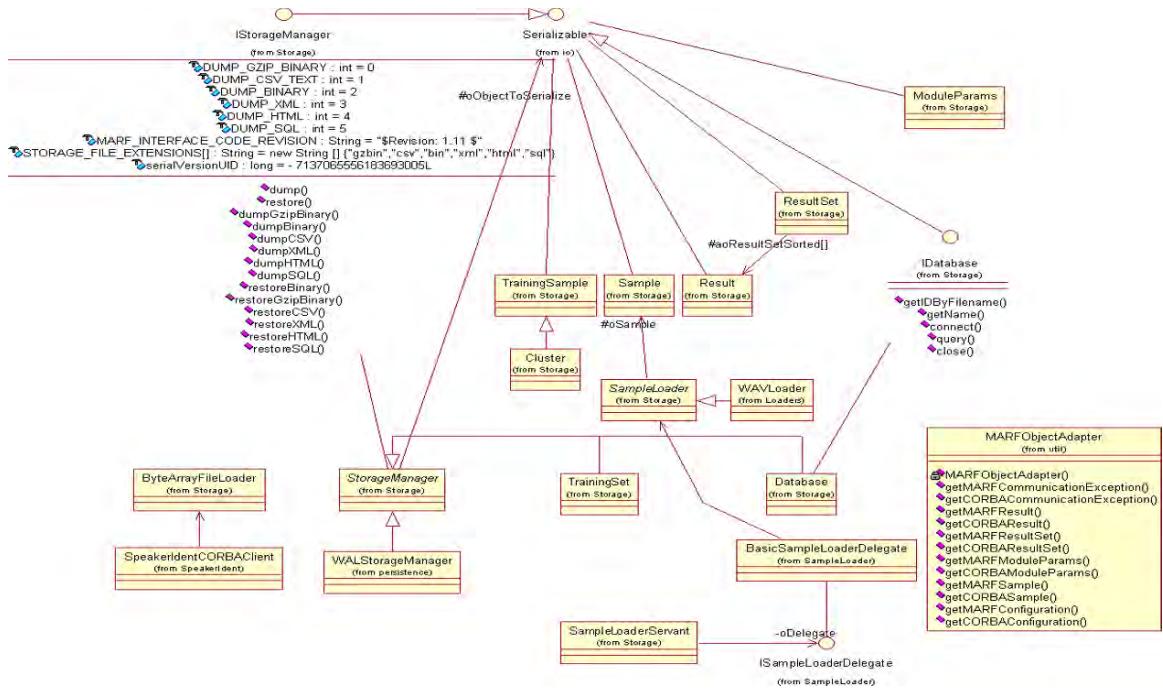


Fig. 4. Storage Class Diagram

- [3] ——, "Introducing MARF: a modular audio recognition framework and its applications for scientific and software engineering research," in *Advances in Computer and Information Sciences and Engineering*. University of Bridgeport, U.S.A.: Springer Netherlands, Dec. 2007, pp. 473–478, proceedings of CISSE/SCSS'07, cisse2007.org.
 - [4] S. A. Mokhov, S. Sinclair, I. Clement, D. Nicolacopoulos, and the MARF Research & Development Group, "Text-Independent Speaker Identification Application," Published electronically within the MARF project, <http://marf.sf.net>, 2002–2008, last viewed April 2008.
 - [5] S. A. Mokhov, "Study of best algorithm combinations for speech processing tasks in machine learning using median vs. mean clusters in MARF," in *Proceedings of C3SE'08*, B. C. Desai, Ed. Montreal, Quebec, Canada: ACM and BytePress, May 2008, pp. 29–43, ISBN 978-1-60558-101-9.
 - [6] ——, "Towards security hardening of scientific distributed demand-driven and pipelined computing systems," in *Proceedings of the 7th International Symposium on Parallel and Distributed Computing (IS-PDC'08)*. Krakow, Poland: IEEE Computer Society Press, Jul. 2008, to appear. <http://ispdc2008.ipipan.waw.pl/>.
 - [7] S. A. Mokhov, L. W. Huynh, and J. Li, "Managing distributed MARF's nodes with SNMP," in *Proceedings of PDPTA'2008*. Las Vegas, USA: CSREA Press, Aug. 2008, to appear.
 - [8] A. Wollrath and J. Waldo, "Java RMI tutorial," Sun Microsystems, Inc., 1995–2005, <http://java.sun.com/docs/books/tutorial/rmi/index.html>.
 - [9] Sun Microsystems, "Java IDL," Sun Microsystems, Inc., 2004, <http://java.sun.com/j2se/1.5.0/docs/guide/idl/index.html>.
 - [10] ——, "The java web services tutorial (for Java Web Services Developer's Pack, v2.0)," Sun Microsystems, Inc., Feb. 2006, <http://java.sun.com/webservices/docs/2.0/tutorial/doc/index.html>.
 - [11] G. Coulouris, J. Dollimore, and T. Kindberg, *Distributed Systems Concepts and Design*. Addison-Wesley, 2005, ISBN: 0-321-26354-5.
 - [12] Sun Microsystems, "Custom networking," Sun Microsystems, Inc., 1995–2005, <http://java.sun.com/docs/books/tutorial/networking/index.html>.
 - [13] S. Mokhov, I. Clement, S. Sinclair, and D. Nicolacopoulos, "Modular Audio Recognition Framework," Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, 2002–2003, project report, <http://marf.sf.net>, last viewed April 2008.
 - [14] S. A. Mokhov, "On design and implementation of an heterogeneous web services, CORBA, RMI, and TCP/IP-based distributed stock broker system," Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, Aug. 2006.
 - [15] R. Grimes, *Professional DCOM Programming*. Wrox Press Ltd., 1997, ISBN 186100060X.
 - [16] Jini Community, *Jini Network Technology*. Sun Microsystems, Inc., Sep. 2007, <http://java.sun.com/developer/products/jini/index.jsp>.
 - [17] Sun Microsystems, *Java Message Service (JMS)*. Sun Microsystems, Inc., Sep. 2007, <http://java.sun.com/products/jms/>.
 - [18] Apache Foundation, "Apache Jakarta Tomcat," [online], apache.org, 1999–2005, <http://jakarta.apache.org/tomcat/index.html>.
 - [19] D. Green, "Java reflection API," Sun Microsystems, Inc., 2001–2005, <http://java.sun.com/docs/books/tutorial/reflect/index.html>.
 - [20] Ant Project Contributors, *Apache Ant*. The Apache Software Foundation, 2000–2005, <http://ant.apache.org/>.
 - [21] R. Stallman, R. McGrath, P. Smith, and the GNU Project, "GNU Make," Free Software Foundation, Inc., [online], 1997–2006, <http://www.gnu.org/software/make/>.
 - [22] Sun Microsystems, "Java servlet technology," Sun Microsystems, Inc., 1994–2005, <http://java.sun.com/products/servlets>.

The Authentication Framework within the Java Data Security Framework (JDSF): Design and Implementation Refinement

Serguei A. Mokhov

SGW, EV7.139-2, Department of Computer Science and Software Engineering, Concordia University, Montreal, Quebec, Canada, Email: mokhov@cse.concordia.ca

Farid Rassai[†]

Ericsson Canada[†], Montreal, Quebec, Canada, Email: farid.rassai@ericsson.com

Lee Wei Huynh[‡]

SR Telecom[‡], Montreal, Quebec, Canada, Email: leewei_huynh@srtelcom.com

Lingyu Wang

Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada, Email: wang@ciise.concordia.ca

Abstract— We present a refinement design of the *Authentication Framework*, which is a part of a more general structure, that we refer to as Java Data Security Framework (JDSF) designed to support various aspects related to data security (confidentiality, origin authentication, integrity, SQL randomization), where this article focuses only on the authentication aspect. The design refinement considerations include unification of the parameters structure of concrete module implementations of the framework’s API from the software engineering point of view.

Index Terms—data authentication, Java Data Security Framework (JDSF), Modular Audio Recognition Framework (MARF), HSQLDB, outsourced data storage and databases (OSD)

I. INTRODUCTION

This work explores secure data storage related issues from the point of view of data authentication in two open-source projects: MARF [1], [2] and HSQLDB [3] and proposes a design refinement of the corresponding relatively independent reusable framework to enable the data authentication mechanisms in both projects. While we present a comprehensive list of the studied techniques, requirements, and possibilities, we begin with a smaller subset of the framework’s realization at the same time keeping the design flexible for it to grow to accommodate future extensions.

A. Background

In this section we briefly introduce the fundamentals of the technologies used for the design and implementation refinement and application as case studies of the research described in this paper, specifically JDSF, MARF, and HSQLDB that deal with data storage of the data that needs to be authenticated.

[†]Opinions expressed in this paper are solely of the author and not necessarily that of Ericsson

[‡]Opinions expressed in this paper are solely of the author and not necessarily that of SR Telecom

1) **JDSF**: Initially, as a project [4] the Java Data Security Framework (JDSF) was designed for use in the two use-cases, MARF [1] and HSQLDB [3] to allow for plug-in-like implementation of various security aspects for comparative studies, such as the data confidentiality, integrity, and authentication, and SQL randomization. Aspects, such as encrypted search, k -anonymity, l -diversity, k -uncertainty, indistinguishability, classical cryptographic primitives, integrity lock architecture, outsourced databases, etc. were considered [5], [6], [7], [8], [9] in order to extract possible parameters these aspects require for the design of an extensible framework API and its implementation. A particular challenge is the compilation of diverse approaches and algorithms into a common set of Java methods and data structures to cover all aspects, and at the same time keeping it all as simple as possible. The JDSF framework’s design is located within the MARF’s code branch at this point in time and is open-source.

2) **MARF**: The Modular Audio Recognition Framework (MARF) [1], [2], [10] is an open-source research platform and a collection of pattern recognition algorithms written in Java. It is put together into a modular and extensible framework facilitating addition of new algorithms. MARF’s based applications can run distributively (Distributed MARF or DMARF) over the network (using CORBA, XML-RPC, or Java RMI) [11], [12] and its implementation may act as a library in applications. One of MARF’s applications, SpeakerIdentApp [13] has a database of speakers, where it can identify who people are, their gender, and spoken accent biometrics regardless of what they say [14], [15].

3) **HSQLDB**: HSQLDB [3] is a popular open-source SQL relational database engine, as MARF and JDSF written in Java. It has a JDBC driver and supports a large subset of ANSI-92 SQL, SQL 99, 2003, and 2008 enhancements. It provides a small and relatively fast database engine, which provides both in-memory and disk-based tables and supports embedded and server modes. Additionally, it includes tools such as

a minimal web server, in-memory query, and management tools. HSQLDB is currently being used as a database and persistence engine in many open source software projects (e.g. OpenOffice [16]) as well as in commercial software projects.

B. Approach

As a part of the overall JDSF framework, we propose to provide a sub-framework to allow for the common algorithm implementations of the authentication aspects for MARF's and HSQLDB's database(s). Both, MARF and HSQLDB are considered independently as well as MARF is being considered as a front-end of HSQLDB to simulate various trust relationships. Depending on the trust architecture, a MARF's instance can be a trusted or untrusted front-end and so is the HSQLDB's instance that it's communicating with.

There are several ways to accomplish that, several architectures, algorithms, etc., so on the research side of the project we reviewed several techniques that achieve the required goals, compared them, and provided a framework's API design- and implementation-wise such that it is easy to add new algorithms that implement the goals, and gradually develop those techniques within the designed framework as a proof-of-concept. To summarize:

- we consulted a few research papers on the techniques for authentication of the data storage.
- we proposed and designed the framework [4] that allows easy plugging-in of such implementations within MARF and HSQLDB, with the API, etc.
- we then implemented several such techniques and compare them for the results (e.g. complexity, performance, strength, trust model, etc.).
- there is an emphasis on doing this for a high volume of a multimedia data (in the MARF's case for now mostly audio, text, or images).

Overview: For the majority of cases, the current MARF implementation uses a flat-file database to store speaker identities and a mapping to their voice samples. MARF can be instructed to use a connection to any relational database, e.g. HSQLDB, PostgreSQL [17], MySQL [18], etc. through an appropriate JDBC driver, or plain Java objects (default), XML, or comma-separated values (CSV) files. Regardless the corresponding storage model, the data travels between the implementing library components and the applications to storage generally unauthenticated. Similar observations can be made in HSQLDB.

We may decide to do not trust the underlying storage model to provide the authenticity of the MARF's database or data sets, we implement a layer at the MARF's library level to provide the authenticity checks (among other things) through an optional cryptographic framework.

If we pick HSQLDB as the backend database engine for MARF and its applications, we can either mark it as trusted or untrusted in the first iteration of the experiments as the authors participate in the design and implementation of the related JDSF and MARF components and can experiment with both tools. While HSQLDB has a comprehensive implementation of features, there is a room for improvement to tighten security

in HSQLDB by authenticating the data that are going in and out and their source by either cryptographic or watermarking techniques, some of which are summarized in our other works.

Assumptions: The article is exclusively considering the authentication of the *data* or its origin in some form of a data storage or a database. There are no users or clearance levels in our model, so there are no issues of authorization and access control, multilevel databases, etc. Therefore, we will not address confidentiality and integrity here (which are addressed separately in [19], [20]), SQL randomization (which is addressed in [21]), availability, authorization, and access control aspects in this work.

II. RELATED WORK

This section presents the shortened summary of the research done on the authentication aspects of various types of data, such that the framework being developed pragmatically covers most aspects and parameters to be flexible and uniform. The data authentication aspect in JDSF is mostly about data-origin's authentication (e.g. in DMARF [11] or the General Intensional Programming System (GIPSY) [22] the data can easily come from another host during the distributed computation that may have been spoofed and is intentionally producing incorrect results passing them off as integrity-correct). This review is primarily based on the cited works [23], [24], [25], [26] as well as the lecture notes [9] and some related techniques discussed in our integrity work [20].

A. Overview

Any type of storage management system, such as DBMS, etc. is important in the vast number of applications. It is a problem, when it involves the data owners delegating their data management needs to an external service provider (e.g. in our simple example for MARF to HSQLDB). Since a service provider most of the time is not fully trusted from a variety of security aspects point of view, there is one of the several core security requirements we study is the authenticity of the outsourced data and databases. Outsourced databases (ODB) is a relatively recent paradigm that has been proposed and received considerable attention.

There is still a lot research to do to develop the ODBs to be fully trusted. The basic idea is that data owners delegate their database needs and functionalities to a third-party storage provider, which offers services to the users of the database. Since the third party can be untrusted or can be compromised, security concerns must be addressed before this delegation takes place.

The database outsourcing paradigm poses numerous research and development challenges, which do not affect the overall performance, usability, and scalability, but impact one of the foremost challenges that is the security of stored or transmitted data. For example, a user stores their data (which are usually a critical asset or confidential matters) at an external, and potentially untrusted, data storage service provider. It is thus important to secure the outsourced data from potential attacks not only by malicious outsiders but also from the service provider itself. Consequently, whenever the

users try to query from a hosted database, the results must be demonstrably authentic (with respect to the actual data owner) to make sure that the data came from a legitimate source (and also have not been tampered with, which the integrity aspect assures).

Thus, we focus on researching to provide secure and effective means of ensuring data authentication, while incurring minimal computational and bandwidth overhead. In particular, we investigate techniques to help the ODB clients to authenticate the origin of data coming from the service provider the data owner as a query. At the end of this section we summarize a few solutions, which have been researched and published on how to authenticate data. The goal is to design and implement these methods on top the existing platforms of MARF and HSQLDB and beyond in the uniform manner, which at this point do not have data authentication system built-in.

B. Scope

In the non-relational world (Java object serialization, XML, CSV, etc.) and equivalent read/write queries have to be authenticated, to make sure the underlying store was not swapped underneath a running application (while its integrity may still be correct, but the data may no longer be authentic), but that comes from an unauthorized provider (techniques similar to those that can be borrowed from the DNSsec [27], [28], [29], [30] for host authentication). In relational databases, we are to consider only the equality queries and also logical comparison predicate clauses. In other words, one considers the standard SQL queries involving SELECT-type of clauses, which typically result in selection of a set of records (or attributes) matching a given predicate or a set thereof. In other hand, we do not consider queries that involve any kind of data aggregation for example SUM or AVERAGE. We focus on the mechanisms for origin authenticity of query replies returned by the storage service provider in the ODB model. Another issue, which is equally important, is the completeness of query replies that we consider in our integrity work [20].

One of the existing solutions is the owner creates a specialized data structure over the original database that is stored at the servers together with the database. The structure is used by a server to provide a verification object *VO* along with the answers, which the client can use for authenticating the results. In our framework design the notion of *VO* is realized in the *AuthenticatedObject* class shown in Figure 6. Verification usually occurs by the means of using classical collision-resistant hash functions and digital signature schemes. Note that in any solution, some information that is authentic to the owner must be made available to the client, and from the client's point of view, the owner cannot be differentiated from a (potentially malicious) server. Examples of such information include the owner's public signature verification key or a token that in some way authenticates the database. Any successful scheme must make it computationally infeasible for a malicious server to send incorrect query results and verification object that will be accepted by a client who has the appropriate authentication information from the owner.

C. Cryptographic Essentials

The classical digital authentication algorithms involve cryptographic signatures and hashing functions as well as more advanced data structures. Due to shortage of space and the abundance of the general knowledge of them, we mention them only briefly in this work.

Collision-resistant Hash Functions: A hash function takes a variable-length input and produces a fixed-length output $y = \mathcal{H}(x)$. This creates a possibility of collisions (two or more distinct documents might map to the same hash value). Such functions are collision-resistant if it is difficult to find such useful from the attacker's point of view documents to match the same hash value. However, computing a collision resistance flaw is in general computationally infeasible. In our work, we will be providing the components to allow heuristic hash functions, which have the advantage of being very fast to evaluate, as well as any other hash function implementations there may be, i.e. our authentication framework does not discriminate between algorithms and allows researchers to implement anything they need for comparative studies or the actual application use. As an example, a basic HMAC-based authentication (also good for the integrity checks [20]) is illustrated in Figure 1 and Figure 2. The hash functions at option are implemented using whatever algorithm implementation is available, e.g. MD5, SHA1, and others.

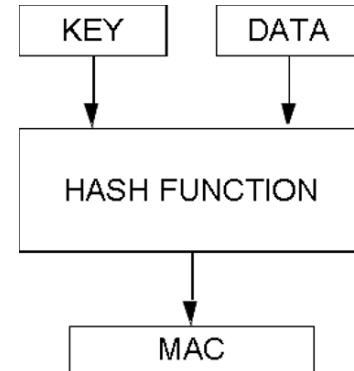


Fig. 1. Basic HMAC-based Authentication [31].

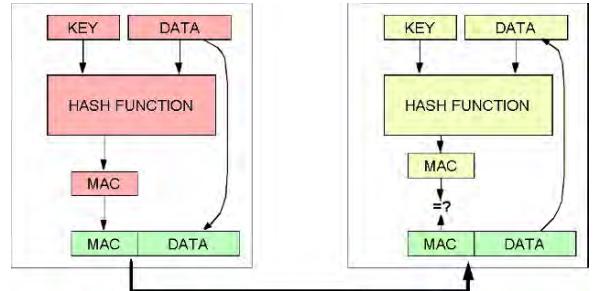


Fig. 2. HMAC-based Authentication Process [31].

Public-key Digital Signature Schemes: A public-key digital signature scheme is a methodology that can be used for authentication of both the integrity and ownership of a signed message. In such a scheme, the signer generates a pair of keys – a public, k_+ , and a private k_- , and the private key is used for data signing. The classical digital signature algorithms include but not limited to RSA, DSA, and ElGamal. For the large volumes of data, e.g. multimedia data or large relational databases, such digital signature schemes alone are computationally quite expensive, especially if applied per record.

The Merkle Hash Tree: The Merkle hash tree [32], [33] is an improvement on solution for authenticating a set of data values. It will solve the simplest form of the query authentication problem for point queries and datasets that can in main memory. The Merkle hash tree is a binary tree, where each leaf contains the hash of a data value, and each internal node contains the hash of the concatenation of its two children. The verification of data values is based on the fact that the hash value of the root of the tree is authentically published (authenticity can be established by a digital signature). To prove the authenticity of any data value, all the prover has to do is to provide the verifier, in addition to the data value itself, with the values stored in the siblings of the path that leads from the root of the tree to that value. The verifier, by iteratively computing all the appropriate hashes up the tree, at the end can simply check if the hash they have computed for the root matches the authentically published value. The security of the Merkle hash tree is based on the collision-resistance of the hash function used: it is computationally infeasible for a malicious prover to fake a data value, since this would require a hash collision somewhere in the tree (because the root remains the same and the leaf is different hence, there must be a collision somewhere in between). Thus, the authenticity of any one of n data values can be proven at the cost of providing and computing $\log_2(n)$ hash values, which is generally much cheaper than storing and verifying one digital signature per data value. Furthermore, the relative position (leaf number) of any of the data values within the tree is authenticated along with the value itself.

D. Parameters Summary

Here is the summary of the typical parameters extracted throughout our initial research to include into the framework for authentication purposes. Since we do not hardcode the list, and it is a part of the configuration, it can grow and be expanded in the future as needed as new methods and algorithms appear. It is imperative that not all of these parameters are used by all the available methods even if they all are set to some values. Each of the parameter subset is used only by the algorithm implementation that requires those parameters. The parameters can be shared among multiple instances of various algorithms at run time. Notice, the parameters constitute not only scalar values of primitive or composite types, but also algorithms as well.

- 1) AAB-tree – is an extended B+-tree structure
- 2) VO – a Verification Object that contains the hashes stored

- 3) $SAT(Q)$ – the set of records from T that satisfy all query predicates
- 4) $ANS(Q)$ – the final answer to a query Q
- 5) Q – the aggregation query
- 6) k – values that need to be authenticated
- 7) \mathcal{H} – the type of a HMAC hash function

III. METHODOLOGY

A. Overview

This section presents excerpts of the framework design based on the studied methods, algorithms, and techniques. The software design methodology is primarily based on the algorithms and their parameters referred to earlier in Section II as well as a plug-in type of architecture for various framework components whose implementation can be easily replaced. Thus, the framework presents a collection of interfaces for all technique types (in this case we focus on data authentication), followed by their generic and concrete implementations. The concrete implementations usually come from various open-source vendors and require adaptation to be used in the framework, that's why a layer of abstraction is introduced to adapt the data between algorithm implementors and the framework's components. Further, to apply the framework's implementation to MARF and HSQLDB, concrete security adapters are designed to make use of the JDSF's authentication framework "injected" into the core storage management components of both MARF (through `marf.Storage.StorageManager`) and HSQLDB (through `org.hsqldb.persist.Log`) where they make sure the data hits the storage other than the main memory and the data carries the authentication information along.

B. Framework

General Operation: In Figure 3 is a general way the framework's particular adapters (e.g. for MARF and HSQLDB) write the security-enhanced data based on the security configuration options, set by the system administrator. The reading of the security-data is usually the reverse process. While it seems the application of the security layers, and specifically the order of the authentication information it, is rigid and hardcoded, it is not the case – the design precludes for the order of operations also to be configurable as needed, and what is pictured is the default.

Design: The typical MARF's packages (see Figure 4) were extended with the two new packages that constitute the root of JDSF: `database` and `marf.security`. In Figure 5 are the primary packages and classes that correspond to the studied aspects of authentication and the utility, storage, algorithms building blocks they rely upon.

The instance of the `marf.security.Configuration` class is usually populated from the related configuration file `security.properties` that is set by the system administrator. The configuration can also be set by the applications or middleware running atop of the JDSF's authentication framework. It represents the security options desired by a

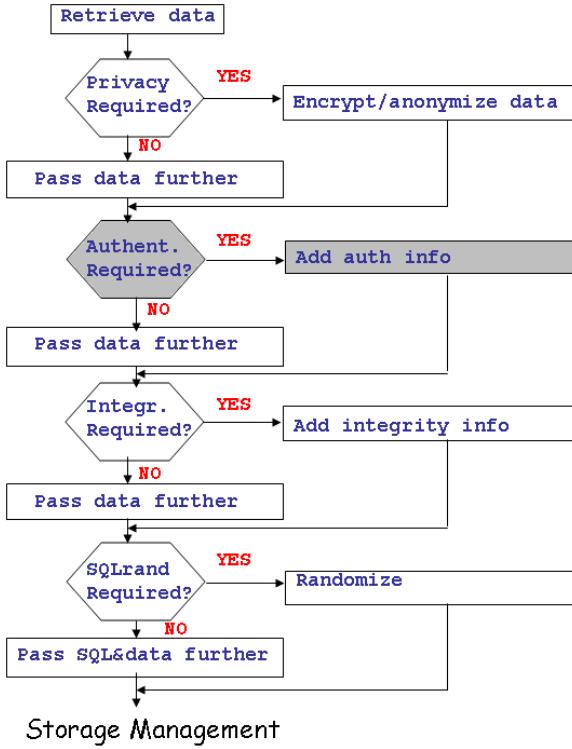


Fig. 3. Writing Data With Security Options.

given instance of the framework-enhanced data management tool (e.g. MARF or HSQLDB).

The remainder of the framework's core is captured by the main interfaces and generic classes, followed by concrete implementation and stub modules, and cryptographic algorithm providers. The interfaces allow external to JDSF plug-ins, e.g. provided by third parties, to be able to extend and compare to the existing implementations if desired. The interfaces are:

- The principal `IAuthenticationModule` interface about the authentication aspect, which is found in the `marf.security.authentication` package, shown in Figure 7.
- The abstraction over algorithms of different vendors is represented by the `IAlgorithmProvider` interface found in the `marf.security.algorithms` package, shown in Figure 8.
- The `ISecurityEnhancedObject` interface abstracts the storage aspects of the security-added objects, found in the `marf.security.Storage` package as shown in Figure 6.
- The abstraction interface `ISecurityAdapter` in the `marf.security.adapters` package is there to adapt the framework to the concrete case studies, as shown in Figure 9.

In the `marf.security.algorithms` package there are implementations of well known cryptographic algorithms,

such as CBC-DES, RSA, DSA, MD5, and SHA1. The actual implementations in Java were provided by open-source vendors, such as [34], [35], [36], [37], [38], [39]. Since these implementations have sometimes very little in common, integrating their code into the framework had to be abstracted by a common API of algorithm providers (as shown in Figure 8), so the rest of the framework does not depend on the vendors' API and can be replaced to use another implementation easier when needed.

The most complexity goes into the implementation and integration of the framework into the actual data management tools, such as MARF and HSQLDB. For this we provide their specific adapters (see Figure 9): the first of them is called `marf.security.adapters.MARFSecurityAdapter` that extends MARF-specific storage management functionality. The second one, for HSQLDB, is likewise referred to as the `HSQLDBSecurityAdapter` class found in `marf.security.adapters`, which are there to be either "injected" into the original code wrapping storage management functions of the original tools to mandatory go through the security-enhanced API or act as stand-alone proxies. The replaced and/or extended modules exactly are `marf.Storage.StorageManager` for MARF and `org.hsqldb.persist.Log` for HSQLDB as they are the ones dealing with the data serialization.

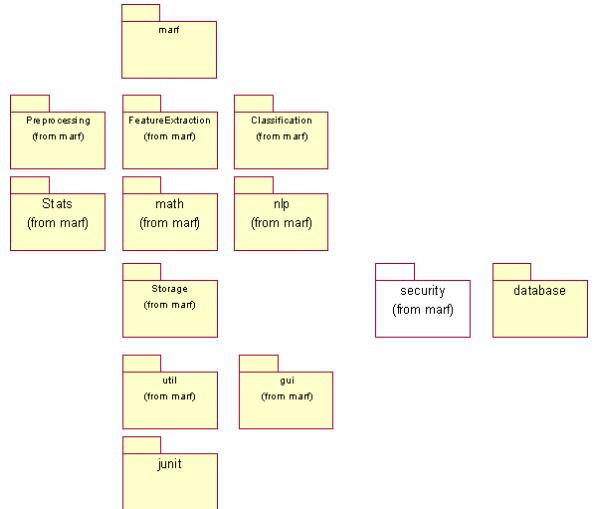


Fig. 4. MARF Augmented with Security Database Packages.

IV. CONCLUSION

The authentication framework's operation was designed to allow for addition of any number of algorithms or techniques to add as plug-ins for comparative studies or when better techniques become available for the actual application use. The parameters and the configuration of the framework were made available from the survey and the research study of the data and database security techniques presented earlier. It is also general enough to expand beyond MARF and HSQLDB,

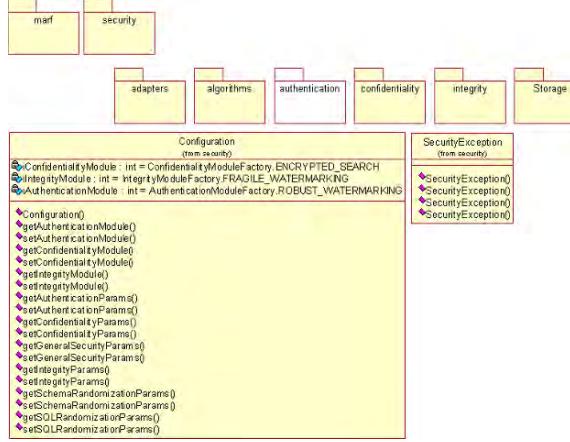


Fig. 5. marf.security Package.

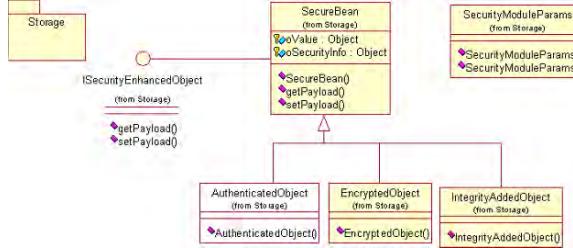


Fig. 6. marf.security.Storage Package and Classes.

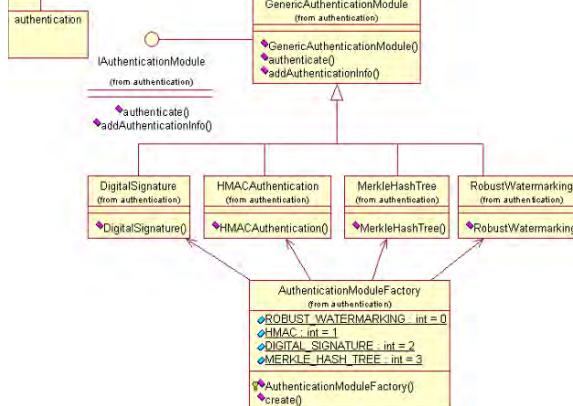


Fig. 7. marf.security.authentication Package and Classes.

and as a result the open source community can benefit as a whole. JDSF, just like MARF and HSQLDB, is open source and is hosted at SourceForge.net under the umbrella of MARF, in its CVS repository.

V. FUTURE WORK

As a future work we plan on continuing our open-source development effort of the framework and completing the

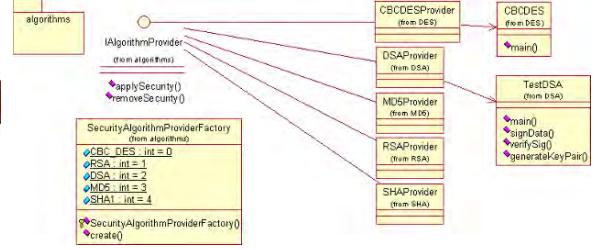


Fig. 8. marf.security.algorithms Package and Classes.

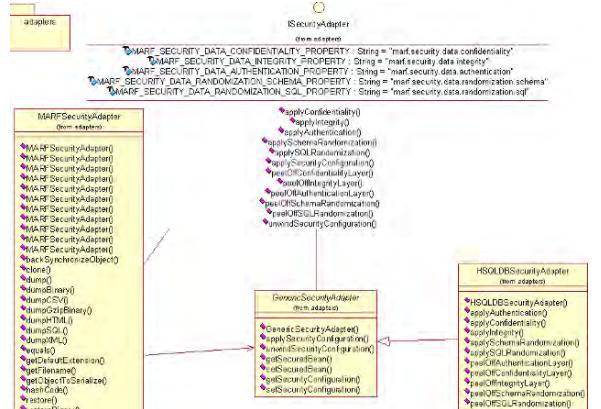


Fig. 9. marf.security.adapters Package and Classes.

full integration of it into MARF and HSQLDB, along with comprehensive testing suite and overhead statistics and new algorithm implementations. We are working on porting it to other systems that require the features provided by the framework, such as the General Intensional Programming System (GIPSY) [22] as studied e.g. in [40]. Additionally, to validate our approach further, we plan to make the open-source JDBC drivers of not only HSQLDB, but also database engines such as PostgreSQL [17] and MySQL [18] integrated with our framework thereby covering the database middleware without requiring modifications to the applications or the DBMS themselves. We also plan to explore solutions for holistic aggregates and investigate the application of our techniques to authenticate data cubes in OLAP systems.

ACKNOWLEDGMENT

This research and development work was funded in part by the Faculty of Engineering and Computer Science of Concordia University, Montreal, Canada. We also would like

to acknowledge various people for their contributions and suggestions:

- Jian Li,
- data and database security researchers,
- open-source community,
- Drs. Joey Paquet and Mourad Debbabi,
- and Dr. Chadi Assi.

During the design and implementation, integration, and testing of the framework, we resorted to a number of open-source implementations of known cryptographic and otherwise algorithms, which are compatible with our open-source license (BSD) with due credit given to the original open-source developers.

REFERENCES

- [1] S. Mokhov, I. Clement, S. Sinclair, and D. Nicolacopoulos, "Modular Audio Recognition Framework," Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, 2002–2003, project report, <http://marf.sf.net>, last viewed April 2008.
- [2] S. A. Mokhov, "Introducing MARF: a modular audio recognition framework and its applications for scientific and software engineering research," in *Advances in Computer and Information Sciences and Engineering*. University of Bridgeport, U.S.A.: Springer Netherlands, Dec. 2007, pp. 473–478, proceedings of CISSE/SCSS'07, cisse2007.org.
- [3] The hsqldb Development Group, "HSQLDB – lightweight 100% Java SQL database engine v.1.8.0.10," hsqldb.org, 2001–2008, <http://hsqldb.org/>.
- [4] S. A. Mokhov, L. W. Huynh, J. Li, and F. Rassai, "A Java Data Security Framework (JDSF) for MARF and HSQLDB," Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada, Apr. 2007, project report. Hosted at <http://marf.sf.net>, last viewed April 2008.
- [5] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," University of California, Berkley.
- [6] L. Wang, S. Jajodia, and D. Wijesekera, *Preserving Privacy in On-line Analytical Processing (OLAP)*. Springer, Berlin, 2007, ISBN: 0-387-46273-2.
- [7] L. Wang and S. Jajodia, *Security in Data Warehouses and OLAP Systems* in *The Handbook of Database Security: Applications and Trends*, M. Gertz and S. Jajodia, Eds. Springer, Berlin, 2007.
- [8] L. Sweeney, "k-anonymity: A model for protecting privacy," in *International Journal on Uncertainty, Fuzziness, and Knowledge-based Systems*, 2002, pp. 557–570.
- [9] L. Wang, "INSE691A: Database security and privacy, course notes," CI-ISE, Concordia University, 2007, <http://users.encs.concordia.ca/~wang/INSE691A.html>.
- [10] S. A. Mokhov, "Experimental results and statistics in the implementation of the modular audio recognition framework's API for text-independent speaker identification," in *Proceedings of the 6th International Conference on Computing, Communications and Control Technologies (CCCT'08)*, C. D. Zinn, H.-W. Chu, M. Savoie, J. Ferrer, and A. Munitic, Eds., vol. II. Orlando, Florida, USA: IIIS, Jun. 2008, pp. 267–272.
- [11] —, "On design and implementation of distributed modular audio recognition framework: Requirements and specification design document," Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, Aug. 2006, project report, <http://marf.sf.net>, last viewed December 2008.
- [12] S. A. Mokhov and R. Jayakumar, "Distributed modular audio recognition framework (DMARF) and its applications over web services," in *Proceedings of TeNe'08*. Springer, 2008, to appear.
- [13] S. A. Mokhov, S. Sinclair, I. Clement, D. Nicolacopoulos, and the MARF Research & Development Group, "Text-Independent Speaker Identification Application," Published electronically within the MARF project, <http://marf.sf.net>, 2002–2008, last viewed April 2008.
- [14] S. A. Mokhov, "Choosing best algorithm combinations for speech processing tasks in machine learning using MARF," in *Proceedings of the 21st Canadian AI'08*, S. Bergler, Ed. Windsor, Ontario, Canada: Springer-Verlag, Berlin Heidelberg, May 2008, pp. 216–221, LNAI 5032.
- [15] —, "Study of best algorithm combinations for speech processing tasks in machine learning using median vs. mean clusters in MARF," in *Proceedings of C3S2E'08*, B. C. Desai, Ed. Montreal, Quebec, Canada: ACM and BytePress, May 2008, pp. 29–43, ISBN 978-1-60558-101-9.
- [16] Sun Microsystems, Inc., "OpenOffice," [online], 2008, openoffice.org.
- [17] The PostgreSQL Global Development Group, "PostgreSQL – the world's most advanced open-source database," [postgresql.org](http://www.postgresql.org), 1996–2008, <http://www.postgresql.org/>, last viewed May 2008.
- [18] MySQL AB and Sun Microsystems, Inc., "MySQL – the world's most popular open source database," www.mysql.com, 1995–2008, <http://www.mysql.com/>, last viewed December 2008.
- [19] S. A. Mokhov, L. W. Huynh, J. Li, and F. Rassai, "A privacy framework within the java data security framework (JDSF): Design refinement, implementation, and statistics," in *Proceedings of the 12th World Multi-Conference on Systemics, Cybernetics and Informatics (WM-SCI'08)*, N. Callaos, W. Lesso, C. D. Zinn, J. Baralt, J. Boukachour, C. White, T. Marwala, and F. V. Nelwamondo, Eds., vol. V. Orlando, Florida, USA: IIIS, Jun. 2008, pp. 131–136.
- [20] S. A. Mokhov and L. W. Huynh, "The integrity framework within the java data security framework (JDSF): Design refinement and implementation," in *Proceedings of CISSE'08*. University of Bridgeport, CT, USA: Springer, Dec. 2008, to appear.
- [21] S. A. Mokhov, L. Wang, and J. Li, "Simple dynamic key management in SQL randomization," 2008, unpublished.
- [22] The GIPSY Research and Development Group, "The General International Programming System (GIPSY) project," Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, 2002–2008, <http://newton.cs.concordia.ca/~gipsy/>, last viewed April 2008.
- [23] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," Computer Science Department, School of Information and Computer Science, University of California, Irvine, 2006.
- [24] M. Narasimha and G. Tsudik, "Authentication of outsourced databases using signature aggregation and chaining," 2006.
- [25] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Authenticated index structures for aggregation queries in outsourced databases," Tech. Rep., 2006.
- [26] —, "Dynamic authenticated index structures for outsourced databases," in *SIGMOD 2006*. ACM, 2006.
- [27] DNSSEC.NET, "DNSSEC: DNS Security Extensions Securing the Domain Name System," 2002–2008, <http://www.dnssec.net/>, last viewed December 2008.
- [28] D. Atkins and R. Ausein, "RFC 3833: Threat Analysis of the Domain Name System (DNS)," [online], Aug. 2004, <http://www.rfc-archive.org/getrfc.php?rfc=3833>, viewed in December 2008.
- [29] R. Arends, R. Ausein, M. Larson, D. Massey, and S. Rose, "RFC 4034: Resource Records for the DNS Security Extensions," [online], Mar. 2005, <http://www.rfc-archive.org/getrfc.php?rfc=4034>, viewed in December 2008.
- [30] D. Conrad, "RFC 3225: Indicating Resolver Support of DNSSEC," [online], Dec. 2001, <http://www.rfc-archive.org/getrfc.php?rfc=3225>, viewed in December 2008.
- [31] C. Assi, *INSE7120: Advanced Network Management, Course Notes*. CI-ISE, Concordia University, 2007, <http://users.encs.concordia.ca/~assi/courses/inse7120.htm>.
- [32] R. Merkle, "A digital signature based on a conventional encryption function," in *Advances in Cryptology – CRYPTO'87*, 1988, pp. 369–378.
- [33] —, "A certified digital signature," in *Advances in Cryptology – CRYPTO'89*, 1990, pp. 218–239.
- [34] Unasccribed, "CBC-DES Java implementation," [online], 2007.
- [35] J. O. Grabbe, "Java program for RSA encryption," [online], 2001, http://www.laynetworks.com/rsa_java.txt.
- [36] Unasccribed, *Sign and Verify a DSA Signature*. java2s.com, 2004, <http://www.java2s.com/Code/Java/Security/VerifyaDSASignature.htm>.
- [37] Sun Microsystems, Inc., *Security Features in Java SE*. java.sun.com, 2007, <http://java.sun.com/docs/books/tutorial/security/index.html>.
- [38] S. Paavolainen and S. Ostermiller, "MD5 hash generator." [ostermiller.org](http://ostermiller.org/utils/MD5.java.html), 2007, <http://ostermiller.org/utils/MD5.java.html>.
- [39] A. Andreu and M.-A. Laverdiere, "SSHA digest, modified," [online], 2006, <http://www.securitydocs.com/library/3439>.
- [40] S. A. Mokhov, "Towards security hardening of scientific distributed demand-driven and pipelined computing systems," in *Proceedings of the 7th International Symposium on Parallel and Distributed Computing (ISPDC'08)*. Krakow, Poland: IEEE Computer Society, Jul. 2008, pp. 375–382.

Performance Evaluation of MPLS Path Restoration Schemes using OMNET++

Marcelino Minero-Muñoz, Vicente Alarcon-Aquino, Jose Galdino García-Fierro, Roberto Rosas-Romero, Jorge Rodriguez-Asomoza, Oleg Starostenko

Department of Computing, Electronics, and Mechatronics
Communication and Signal Processing Research Group
Universidad de las Americas Puebla
72820 Cholula, Puebla MEXICO
E-mail: {marcelino.minero, vicente.alarcon}@udlap.mx

Abstract-Multi-Protocol Label Switching (MPLS) is an alternative to integrate Internet Protocol (IP) routing and switching technologies because it provides end-to-end Quality of Service (QoS), guarantees traffic engineering, and support Virtual Private Networks (VPNs). However, MPLS must use path restoration schemes to guarantee the delivery of packets through a network. Considering that MPLS is a label switching technology, it uses a method for label distribution based on signaling protocols like LDP (Label Distribution Protocol) among others. In this paper we present the simulation of some LDP messages and assess the performance of three path restoration schemes (Haskin, Makam, and Simple Dynamic) in an MPLS network using OMNET++. The simulation results show that the Simple Dynamic scheme presents a reduced arrival time when sending a message from the source to a destination, when compared to those times obtained to Haskin and Makam schemes.

I. INTRODUCTION

During the last years, the Internet growth has taken an exponential and unstoppable course; at the same time there has been an increasing demand of new and more sophisticated services, therefore the technology has had to undergo fundamental changes with respect to the usual practices developed in the mid 90s. In this super-growth environment, the Internet Service Providers (ISPs) must find a way to adjust the dramatic growth of network traffic and number of users. Furthermore, an aspect that feeds this accelerated growth in the demand is the “best effort” nature of the Internet, in which access and distribution of contents services are emphasized instead of data transport services. But there is a growing demand for services that require a higher level of capability, especially higher predictability from the Internet (a more deterministic and less random answer). Service Level Agreements (SLAs) written to meet Layer 2, Layer 3, and even Layer 4 parameters are being request by customers to fulfill this bandwidth demand [1].

To avoid having equipment specifically designed for the new Internet applications, ISPs had to adapt any

commercially available equipment. The best option seemed to be to increase the performance of the traditional routers. As infrastructure, the ATM switching equipment was the only technology that provided the required bandwidth, the packet forwarding capacities, and traffic engineering. The idea was to combine, in many ways, the effectiveness and yield of the ATM switches with the control capabilities of IP routers. The answer was the deployment of the “IP over ATM” Model (IP/ATM). The solution that IP/ATM introduces for meeting the cell tax problem is the increasing of interconnection IP nodes. This solution creates as well the problem of exponential growth $n \times (n - 1)$ of the number of nodes that form the network; this slows down the process of packet forwarding made by the corresponding protocols, and so the necessity for a new technology that meets these demands. In this paper we explain and analyze the concepts of MPLS as well as performing a simulation and comparison of path restoration schemes using OMNET++. The remainder of this paper is organized as follows. Section II presents a description and operation of the MPLS protocol. In Section III, a brief explanation of the signaling protocol LDP is presented. In Section IV different path restoration schemes are introduced. Section V presents an overview of OMNET++ and the modeling of the MPLS module. Simulation results for different path restoration schemes under different scenarios are reported in Section VI. In Section VII the conclusions of this paper are presented.

II. MPLS COMPONENTS AND OPERATION

This section gives an overview of the terms associated with the MPLS technology. The main components associated to an MPLS network are shown in Figure 1. The function of ingress Label Edge Router (LER) is to put a label in the IP packet and forward it to the next hop in the MPLS network. This label is assigned according to the forwarding equivalence class (FEC) of the packet. In this case the IP packet is encapsulated in an MPLS Protocol Data Unit (PDU), with an MPLS shim header included in

the packet. The main objectives of MPLS are accomplished using fixed-length labels.

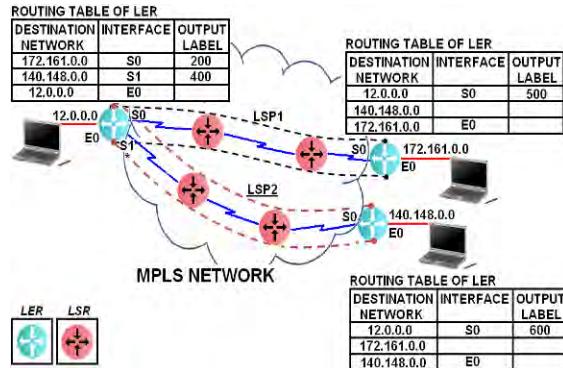


Figure 1: MPLS domain with LSRs, LERs, two LSPs and associated FECs

These labels included in an MPLS header (shim header) are assigned considering FECs that determine the route of a datagram. The FECs are a representation of a group of packets that share the same requirements to their transport. These FECs can be used to support QoS operations (e. g. real time applications) [2]. This FEC to label relationship determine the Label Switched Path (LSP) of a datagram, from the ingress point to the egress point of the MPLS network. In the MPLS domain of Figure 1 the router R0 (an LSR), using a signaling protocol, determines that it can reach the network 172.161.0.0 through the interface S0 using the label 200. Additionally, R0 determine that using the interface S1 it can send packets to the network 140.148.0.0 using the label 400. In other words, two FECs have been established. Figure 1 also shows the LSPs associated with a specific FEC. The complete path through an MPLS network is known as LSP. The LSP or “tunnel” at both ends of the MPLS network is a concatenation of the LSP segments between each node. In this tunnel the ingress node define the type of traffic and assigns a label. According to this label, the traffic is forwarded through the LSP without further examination. At the end of the tunnel, the egress node removes the label and forwards the traffic to an external network (e. g. an IP network). This type of tunnels allows the implementation of Traffic Engineering (TE). The MPLS label, among other fields, is part of a shim header with the structure shown in Figure 2.

- The Time to Live field (TTL) indicates the period of time in which the datagram is valid.
- The Stack field (S) indicates the existence of additional labels assigned to the datagram.
- The Experimental field (EXP) does not have a formal definition in the MPLS technology, but it is used in Cisco label switching for Class of Service (CoS).
- The Label field contains a 20-bit value at the front of the packet.

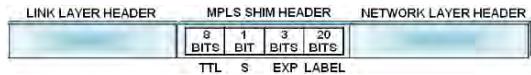


Figure 2:Structure of an MPLS shim header

Note that additional information can be associated with a label—such as CoS values—that can be used to prioritize packet forwarding.

The most used terms to describe the routing tables in the MPLS technology are the Label Information Base (LIB) and Label Forwarding Information Base (LFIB). The LIB contains the labels associated to a determined address and the address itself associated with these labels. These associations are those generated in this LSR and also those received from the LSRs in the neighborhood. The LFIB table contains only the necessary information to forward a datagram to the next hop in the LSP. This information consists on local labels (to be used between two LSRs on the same LSP and created by the LSR with this LFIB) and the output labels. This table also contains information of the interface to be used to forward the traffic to the next hop. An egress LER removes the label of the IP packet and forwards it to a traditional IP network. The Label Switch Routers (LSRs) are devices capable of forwarding packets inside an MPLS network. These routers are located inside the MPLS network and are intermediate hops between the ingress and egress LERs. Their function is to examine the labels of the received packets and replace them with another label according to the routing table of the intermediate routers.

III. SIGNALING PROTOCOL LDP

There are several methods to make the label distribution in an MPLS network. The most used is LDP (*Label Distribution Protocol*). The LDP is a complex protocol and contains more procedures, characteristics, and messages than RSVP (*Resource Reservation Protocol*). In this section a brief description of this protocol is presented. Among all the messages defined in the RFC of LDP, the most important are the following (see Figure 3) [2]:

- Hello Messages
- Initialization Messages
- Label Request Messages and
- Label Mapping Messages

These messages allow two LSRs to build the routing tables in each LSR with the following procedure. The LSR A sends Hello Messages (UDP messages) through all their interfaces to find out those LSRs with a direct connection to LSR A. After this, if LSR A needs to find those labels associated with an LSR B connected to one of their interfaces, say I2, it sends Initialization Messages through I2 and LSR B responds with another Initialization Message. After the exchange of these messages a session is

established between LSR A and LSR B. Finally, Label Request and Label Mapping Messages allow communicating the FECs and labels associations from LSR A to LSR B or vice versa. A detailed description of these LDP messages can be found in [2] and [3].

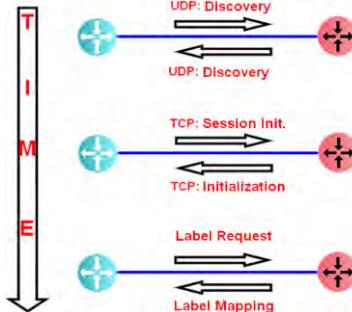


Figure 3.Signaling procedure between LSRs

IV. PATH RESTORATION SCHEMES

The implementation of MPLS must include a solution to a path or route failure, and thus the inclusion of path restoration schemes in this implementation is necessary. These schemes are based on the kind of failure and each one has characteristics that make it preferable over others [4], [5]. There are several path restoration schemes that are used for comparison purposes when a new architecture is proposed. Some of these schemes are Haskin [6], Makam [7] and Simple Dynamic [8]. Additionally to these schemes, there are others like Fast Rerouting, Reliable Fast Rerouting and Optimal Guaranteed Alternate Route (see e.g. [9]). The application of these schemes depends on the specific requirements of the network [5]. These schemes forward traffic around a failure in a primary route and their objective is to minimize the time of establishment of the alternate route and avoid the excessive lost of information. These schemes can be classified according to the following criteria:

- Local Repair: Minimize the required time for the fail propagation. Hence, if the restoration can be realized in local manner, it can be accomplished faster.
- Global Repair. Considers that the nodes and links along the primary route are protected by one restoration route. In case of failure, the restoration scheme sends a Failure Indication Signal (FIS) to the ingress node and when it receives this FIS the alternate route is activated from this node.

A. Simple Dynamic Scheme

This scheme uses local repair and dynamic activation. Hence the alternate route is established when the point of failure is detected (see Figure 4).

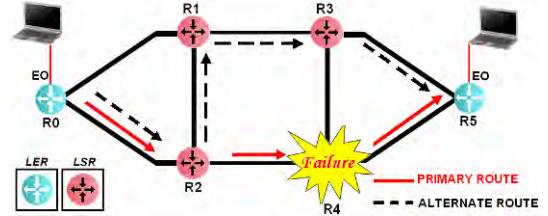


Figure 4.Simple Dynamic scheme

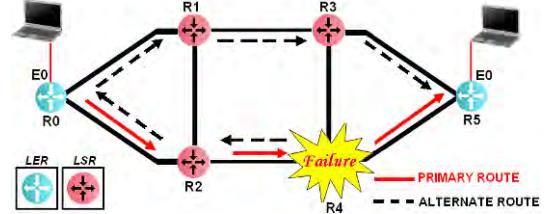


Figure 5.Haskin scheme

When a failure in the primary route occurs, this scheme finds an alternate route that continues from the node that detects the failure. This scheme can consider link failures as well.

B. Haskin Scheme

This restoration scheme uses alternate routes previously established with local repair (see Figure 5). One of the requirements of this method is that the network topology allows the establishment of the alternate route between the ingress and egress LSRs of the LSP tunnel, in such way that the alternate LSP does not share any resource with the route to be protected [6]. The main idea of this scheme is to return the traffic from the point of failure on the protected LSP to the ingress LSR, in such way that the traffic could be redirected through an alternate route between the ingress LSR and the egress LSR of the protected tunnel. The alternate route is established as follows [6]:

- The initial segment of the alternate LSP is between the last hop LSR before the point of failure and the ingress LSR in opposite direction of the protected LSP.
- The final segment of the alternate route is defined between the ingress LSR and the egress LSR.

C. Makam Scheme

This scheme uses global repair and allows dynamic and pre-negotiated activation of the alternate route (see Figure 6). However, the dynamically-established alternate routes add more time to the restoration operation compared with the pre-negotiated activation.

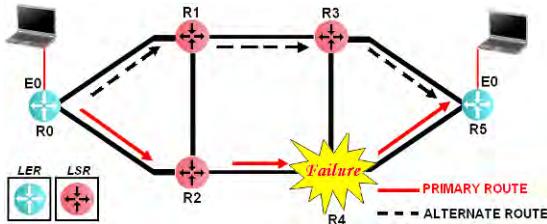


Figure 6.Makam scheme

The establishment of the alternate route for this scheme is as follows [7], [9]:

- When a failure is detected, the node detecting the failure sends a failure indication signal (FIS) to the ingress node.
- All the packets in transit between the failure detection and the moment in which the FIS arrive to the ingress node are lost.
- When the ingress node receives the FIS redirects the traffic through an alternate route to the egress node.

The main difference between this scheme and the Haskin scheme is that it does not redirect the traffic from the point of failure; instead it redirect traffic from the ingress node.

V. MODELLING OF AN MPLS NETWORK

The simulation of the path restoration schemes and the signaling protocols is accomplished using OMNET++. This section presents the principal characteristics of this software tool.

V.I. OMNET OVERVIEW

OMNET++ is free object-oriented software used to simulate in modular form discrete events establishing hierarchical structures between each component. In addition OMNET++ has a Graphical User Interface (GUI) used to develop simulations of different communication networks. The communication between different modules is accomplished using different messages. The complexity of these messages is dependent of the task related to them. For example, one message can send data directly to one module or send data using connections. The parameters of each module can be used to define its behavior or to define the network topology. OMNET++ simulations can be carried out in parallel form providing results similar to those obtained in real networks [10].

OMNET++ uses a Network Editor (NED) language to the graphical construction of the network to be used in the Graphical NED (GNED) ambient. This language defines several types of modules, the parameters associated and the interconnection between them. The GNED ambient shows the result of the code generated on NED. Some simple modules are considered the active components of the network, and they are the only modules programmed in

C++ using the library omnetpp.h included in OMNET++. This language is used to program MPLS, signaling protocols LDP, and CR-LDP and the Haskin scheme. The environment for simulations Tkenv shows the results of the NED and C++ programming and allows a complete control of the simulation programmed. This ambient show a timeline for the messages created and as a consequence shows the occurrence of events on the simulation. All these variables values (scalar or vector) modified by a module event on a simulation are stored and plotted when the simulation ends. The changes in vector variables are plotted using the graphic tool Plove and the change on scalar variables are plotted using the tool Scalars [10].

V.2. MPLS MODELLING

In this section we present the MPLS network modelling using the GNED ambient of OMNET++. Afterwards, the programming of the principal functions of the signaling protocols and the path restoration schemes using C++ are presented.

A. MPLS Network Modelling using GNED of OMNET++

The proposed MPLS network used to implement the path restoration schemes is designed using the ambient GNED of OMNET++ and the NED language. This proposed network consists of 4 hosts, each one connected to an IPv4 router. These IPv4 routers are connected to an MPLS network that consist of 10 LSRs and 4 LER (see Figure 7). The hosts consist of 4 layers (Application, Transport, Network and Data Link) and the routers consist of 2 layers (Network and Data Link). The MPLS routers consist of 2 layers but in addition these routers show the modules of LDP and MPLS. The design of each one of these elements is shown in the following sections.

B. LDP Module

In this module the signaling mechanism that establishes the LSP is carried out using the LDP protocol before label distribution. This signaling mechanism consists of the following four stages:

- Discovery
- Session establishment
- Label distribution
- LSP creation

C. MPLS Module

This module assign, swap or remove labels on the messages. The first action is to assign a label to those messages that ingress to the MPLS network. This procedure is carried out by discrimination between LDP messages and an IP datagram. These messages with a TCP or UDP port number of 646 are considered LDP messages and a message with a different port number is considered to be an IP datagram.

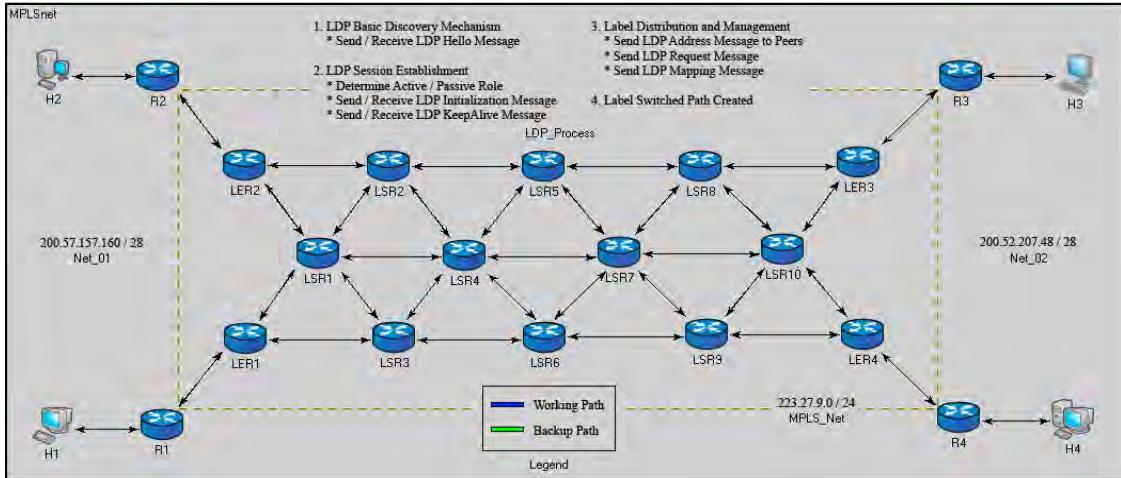


Figure 7.MPLS network designed on GNED.

The swap or remove label actions are carried out using the Incoming Label Map Table (ILM) to find the incoming label and then using the Next-Hop Label Forwarding Entry Table (NHLFE) to find the action to perform with this label: swap or remove.

The implementation of the path restoration schemes is carried out in the MPLS and ERIB (Explicit Route Information Base) modules as follows. The link failures are declared after the source module sends the seventh datagram (the link and routers involved in a failure are declared inside the program). This link failure triggers some actions on the node that detects this failure. Concerning to the Haskin scheme, each one of the labeled frames is sent to the MPLS module where a Route Restoration Label is used to send the traffic using this restoration route. This route restoration label is used to swap the previous label of the frame and to find the output interface of the frame with this new label. This output interface is found in the ERIB. Once the relabeled frames arrive to the ingress LER, this LER carries the switchover mechanism to send this frames through the restoration path and not through the active path.

VI. SIMULATION RESULTS

The simulation of this MPLS network is carried out using the Tkenv tool of OMNET++. This simulation provides a file used to plot (using Scalars) the variables defined in the program and as a consequence determine the correct behavior of the path restoration schemes. The creation of the file that contains the variables to plot is programmed in C++. The scalar variables are used to plot the received, send, and lost packets. These variables are time-independent. Figure 7 shows the active path (LER2-LSR2-LSR5-LSR8-LER3) for a packet of 28 Kilobytes (sent in 19

fragments) sent form the host H2 to the host H3.

A. Haskin Scheme

The restoration path when a link failure is present in the proposed network is shown in Figure 7 (LER2-LSR1-LSR4-LSR7-LSR10-LER3). In this network, a packet is sent from host H2 with a destination at H3. This message is fragmented and each fragment is sent through the active path until a link failure is detected. In this case the fragments are sent through the restoration path. The active path consists of the following elements: LER2-LSR2-LSR5-LSR8-LER3. The LSR2 and LSR5 process the 19 fragments of the application message. The LSR5 element sent 7 fragments to LSR8 before the link failure is detected. When the link failure is detected, the remaining fragments are sent back to the LER2, using as an intermediate node the LSR2. These fragments are received at LER2 and sent through the backup path: LER2-LSR1-LSR4-LSR7-LSR10-LER3. From the point of view of LER3 the first seven fragments are received from the active path and the remaining twelve fragments are received from the backup route.

B. Makam Scheme

The simulation of the Makam Scheme is carried out using the same network topology used for the Haskin scheme. For this scheme a packet is sent from host H2 to the host H3. This packet is divided in 19 fragments and sent through the active route until a failure occurs. If the failure occurs when the node LSR5 has processed 7 fragments, the remaining 12 are lost. The host LSR5 sent a FIS signal to LER2. When the FIS signal arrives to LER2, the host H2 retransmits a message, which is divided again in 19 fragments. This new fragments are sent through the restoration path (LER2-LSR1-LSR4-LSR7-LSR10-LER3).

When these 19 fragments arrive to LER3 it verifies if these are duplicated fragments or new fragments, when compared with the 7 fragments previously sent through the active path.

C. Simple Dynamic Scheme

Using the topology shown in Figure 7, the function of the Simple Dynamic scheme is as follows. The process considers again sending packets from H2 to H3. Before a failure exists in the topology, all the fragments are sent through the active route. When the failure exists the fragments are sent through the backup path LSR5-LSR7-LSR10-LER3. In the simulation carried out for this scheme, the packet sent from H2 to H3 is divided in 19 fragments and before the failure occurs, the LSR5 sends 7 fragments and sent them to LSR8. When a failure occurs LSR5 establishes the alternate path, which is used to send to LER3 the remaining 19 fragments. In this scheme the ingress and egress LERs do not know that a failure exists inside the MPLS network. Using this scheme there are no packets lost.

According to the results obtained in the simulation of path restoration schemes we can observe that the time used to send packets from the source H2 to the destination H3 using Haskin scheme is of 300 milliseconds (see Table 1). This time includes the creation of the message (170 ms) and the time used by the fragments to arrive to the destination (130 ms). The Haskin scheme is also compared to IP networks using NS-network simulator (see e.g., [11]). For the Makam scheme the results show that the sending time from H2 to H3 increases (320 ms) when compared to Haskin scheme. The simple dynamic scheme presents a reduced sending time (260 ms) when compared to Haskin or Makam schemes. This time includes a transit time from H2 to H3 of 90 ms and the time of creation of the message at H2 (170 ms).

Table 1. Arrival time for simulated path restoration schemes

Path Restoration Scheme	Message Time Creation at H2	Transit time from H2 to H3	Arrival Time to H3
Haskin	170 ms	130 ms	300 ms
Makam	170 ms	150 ms	320 ms
Simple Dynamic	170 ms	90 ms	260 ms

VII. CONCLUSIONS AND FUTURE WORK

In this paper we have presented the simulation of three path restoration schemes for MPLS networks using OMNET++. The principal components of this simulation tool were presented and the function of each one was described. This

tool shows the great versatility to simulate MPLS networks and to obtain simulation results similar to those obtained in a real network. Furthermore, we simulate the complete functioning of the signaling protocol LDP for the distribution of labels to each component of the proposed MPLS network. Simulation results show that it could be possible to simulate more complex schemes like OGAP (Optimal and Guaranteed Alternative Path) for the path restoration in MPLS networks. This scheme among others can offer some additional characteristics to be measured like packet reordering or recovery time for link or node failures. Further work can be done to enhance the simulation of the signaling protocol or to include the simulation of the most important characteristics of CR-LDP for Traffic Engineering. Another possible improvement can be the simulation of path restoration schemes considering optical MPLS networks.

REFERENCES

- [1] Marconi white paper, Building scalable Service Provider IP Networks, Connection-Oriented Networking Solutions, July 2000.
- [2] Ulysses Black, MPLS and Label Switching Networks, Second Edition, New Jersey, Prentice Hall 2002.
- [3] Andersson L., Doolan P., Feldman N., Fredette A., Thomas B., *LDP Specification*, RFC3036, January 2001.
- [4] V. Alarcon-Aquino, J. C. Martínez Suárez, Introduction to MPLS Networks (in Spanish). El Cid Editor, 2006.
- [5] Johan Martin Olof Petersson, *MPLS based recovery mechanisms*, Master Thesis, University of Oslo, May 2005.
- [6] D. Haskin, R. Krishnan. *A method for setting an alternative label switched path to handle fast reroute*. Draft-haskin-mpls-fast-reroute-05.txt. November 2000.
- [7] S. Makam, V. Sharma, K. Owens, C. Huang. *Protection / Restoration of MPLS Networks*. Draft-makam-mpls-protection-00.txt. October 1999.
- [8] Ahn G, Chun W. "Simulator for MPLS Path Restoration and Performance Evaluation", *Joint 4th IEEE International Conference on ATM (ICATM2001) and High Speed Intelligent Internet*, April 2001, pp. 32-36.
- [9] Hundessa Gonfa, Lemma, *Enhanced Fast Rerouting Mechanisms for Protected Traffic in MPLS Networks*, Professional Thesis, Universidad Politécnica de Cataluña, 2003.
- [10] Varga, A., "OMNeT++, User Manual", OMNeT ++ Discrete Event Simulation System. Available at: <http://www.omnetpp.org/doc/manual/usman.html>.
- [11] V. Alarcon-Aquino, J. C. Martinez, L. G. Guerrero-Ojeda, Y. Takahashi, *MPLS/IP Analysis and Simulation for the Implementation of Path Restoration Schemes*, *WSEAS Transactions on Computers, Issue 6, Vol. 3, December 2004. p. 1911-1916*.

FM Transmitter System for Telemetrized Temperature Sensing Project

Saeid Moslehpoor^{#1}, Jun Kondo^{#2} and Hisham Alnajjar^{#3}

^{#1, #2}Department of Electrical and Computer Engineering, University of Hartford, West Hartford, CT,

^{#1}moslehpoor@hartford.edu

^{#2}kondo@hartford.edu

^{#3}alnajjar@hartford.edu

Abstract— Small, inexpensive, traditional analog-type telemetric systems have been developed from 1960th. Since the cost of the device is significantly low, it still can be used for one-time use purposes. This paper highlights a methodology of sending a FM signal from the FM transmitter which is based on an inexpensive FM wireless microphone to measure high-altitude ambient air temperature. The FM signal is received by a conventional home FM receiver. This research has focused on the following three aspects;

1. Modifying a FM wireless microphone circuit to build an inexpensive telemetry system.
2. Optimizing the performance of the pulse wave generator and FM transmitter circuits using Design Entry CIS.
3. Converting the frequency of the pulse-wave generator to the corresponding temperature.

I. INTRODUCTION

Dr. Avital Fast of the Albert Einstein Medical Center and Dr. Meyer Kaplan of Levittown Animal Hospital started to measure the temperature changes in a dog's knee to establish the relationship between the temperature changes and the healing process of the injured knee tissue in 1992 [1]. Dr. Avital Fast and Dr. Meyer Kaplan did some experiments by implanting a thermocouple into a dog's knee and connecting the wire to a computer. But the dog chewed the wire and this procedure was found to be unsuccessful. Therefore, a telemeterized temperature sensing system was fabricated by Dr. Changlu Wang from the University of Hartford in 1996 [2]. He started to use the CFM-6L FM transmitter which was fabricated by Dr. Carl Enger of Biotelemetry in Boca Raton, Florida [3]. Although, there are some problems in this earlier telemetrized temperature system;

1. The temperature changes cause the carrier frequency changes of the FM transmission. Although, the carrier frequency changes are also caused by many other factors including inductance changes of foreign objects.
2. The battery for the transmitter is too big to implant. A modern transmitter, MicroStrain EmbedSense uses an inductive link to receive power and does not require a battery [4].

3. Since it uses the FM broadcast band, it has interference with FM radio stations. Today, wireless access radio systems use 2.4 GHz, also 3.5 GHz and 10.5 GHz bands for high speed communications [5].

The digital-type transmitter provides more performance than the analog-type transmitter though it is much more expensive. These two types of transmitters are shown in Figure 1 [6].



Figure 1 Two FM Transmitters; Left, CFM-6L FM (\$500) Right, TC-Link Wireless Thermocouple System (\$2,195)

Therefore, this telemetrized temperature project was dramatically changed in January 2008. The purpose of this project was changed from measuring the temperature of the injured knee tissue to measuring high-altitude air temperature. The transmitter is lifted up by a balloon to measure the high-altitude air temperature. Since the system may be used for only one time and may not come back to the ground again, it must be very inexpensive and disposable. In addition, the new system has the fixed FM carrier frequency and the frequency of the pulse wave generator is used to transmit the temperature information.

II. METHODOLOGY

The new approach is stated as follows;

1. The carrier frequency is fixed and never changes during the FM transmission.
2. The temperature changes cause the frequency changes of the pulse-wave generator and the relationship between temperature and frequency is determined by precise calibration.

The design requirements for the FM transmitter are stated as follows;

3. It can generate the enough transmission power to reach the FM receiver which is at least 100 feet away from the FM transmitter.
4. It can accurately measure the temperature changes from 0 degree Celsius (freezing point) to 10 degree

Celsius which is the temperature range of high-altitude atmosphere attained by this system.

5. It must be light and less than 6 oz. So that the system can be easily lifted up by a 38 inch diameter balloon. Figure 2 shows the FM transmitter is suspended by the balloon.



Figure 2 FM Transmitter suspended by 38" diameter Balloon

III. APPARATUS

The resistance of the thermistor changes in relation to temperature changes. The resistance changes cause the frequency changes in the pulse-wave generator and also cause the frequency modulation of the carrier signal which is 105.6 MHz. This frequency modulated carrier signal is transmitted from the antenna to send the temperature information.

Thermistor

YSI 44115 Precision Thermistor was used in this experiment and the relationship between the resistance versus temperature is stated as follows [7];

Temperature	Resistance Value
0 degree Celsius	3966 k ohms
2 degrees Celsius	3529 k ohms
4 degrees Celsius	3144 k ohms
6 degrees Celsius	2804 k ohms

FM Transmitter

This FM transmitter was based on the Radioshack FM Wireless Mike Module Kit which was sold for \$11.99. The FM carrier frequency of 105.6 MHz was used for this project.

Pulse Wave Generator

This pulse-wave generator was copied from "Radio Shack Basic Electronics Transistors and Integrated Circuits, Workbook 1 [8]" which is the instructional manual for Electronics Learning Lab.

FM Receiver

Sony STR-DE197 FM Stereo Receiver was used for receiving the FM signal from the transmitter. It has the audio frequency range of 40 Hz - 20kHz and provides the power per channel (RMS) of 100 watts at the total harmonic distortion of 0.09%.

Function Generator

BK Precision 4040A was used to determine the frequency of the pulse wave generator. It can generate the frequencies from 0.2 Hz to 20 MHz and has the frequency counter which can measure the frequency range of 5 Hz to 30 MHz.

Antenna

Channel Master 3010 Outdoor Rooftop UHF/VHF/FM Antenna was used for receiving the FM signal and it is shown in Figure 3. The size of the antenna is 52"W x 15"D x 2-1/4"H and it has the reception beam angle of 45 degrees.



Figure 3 Channel Master 3010 Outdoor Rooftop UHF/VHF/FM Antenna

Balloon

A 38 inch diameter helium balloon was used to lift the circuit board.

Kite Strings

Two 500 feet kite strings were attached to the circuit board to control the altitude of the system.

IV. IMPLEMENTATION

1. Prototyping

First, the circuit was made on the pre-punched circuit board and the following fundamental aspects were tested;

1. Transmission Frequency
2. Transmission Range
3. Frequency changes caused by different temperatures

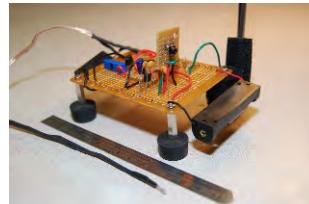


Figure 4 First Prototype of the Pulse Wave Generator and FM transmitter

2. Optimization using Design Entry CIS

Optimizer

There are seven resistors (R1-R7), seven capacitors (C1-C7) and one inductance (L1) in the circuit. R1 corresponds to the resistance of the thermistor and R2 corresponds to the resistance of the trimmer. R1, R2 and C1 determine the frequency of the pulse wave generator. L1, R5, C5, C6 and C7 determine the carrier frequency which is 105.6 MHz. Therefore, the values of R3, R4 R6, R7, C2, C3 and C4 were optimized to get the maximum output voltage which corresponds to the maximum transmission power from the antenna terminal. The results are show in the following table.

Component	Original Value	Optimized Value
R3	470k	470k
R4	33k	21k
R6	33k	3.3k
R7	180	40
C2	10u	10u
C3	100p	992p
C4	10n	10n

The original circuit is shown in Figure 5, the optimized circuit is shown in Figure 6, the frequency response of the original circuit is shown in Figure 7 and the frequency response of the optimized circuit is shown in Figure 8.

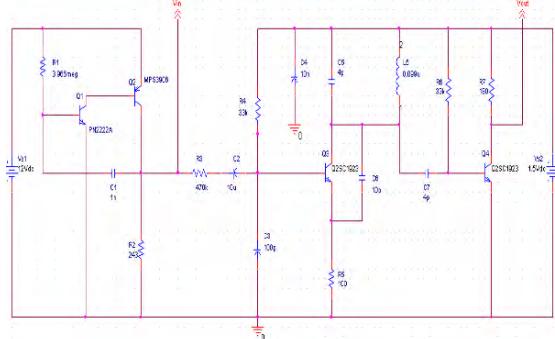


Figure 5 Original Circuit

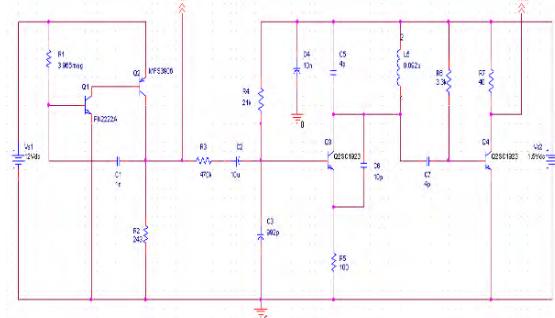


Figure 6 Optimized Circuit

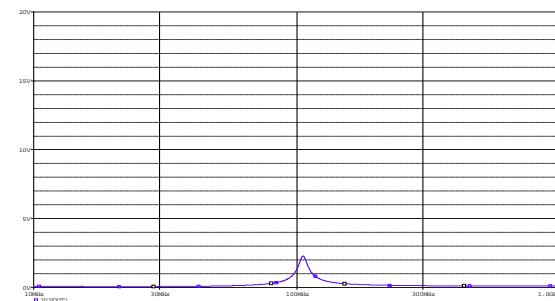


Figure 7 Original Frequency Response

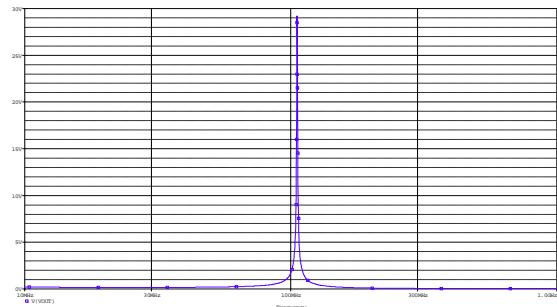


Figure 8 Optimized Frequency Response

Sensitivity Analysis

There are seven resistors (R1-R7), seven capacitors (C1-C7) and one inductance (L1) in this circuit. Although, R1 corresponds to the thermocouple and it is obviously most sensitive to the maximum output voltage. Therefore, R1 is excluded from this analysis. The relative sensitivities of the five most sensitive components to the maximum output voltage are stated as follows;

R5 100%
L1 49%
R6 20%
R7 13%
R4 11%

Monte Carlo Analysis

The tolerances of all resistance, capacitance and inductance are set to 10%. The mean output voltage is 6.58 volts and the standard deviation of the output voltage is 461 millivolts. Figure 9 shows the results of this Monte Carlo analysis.

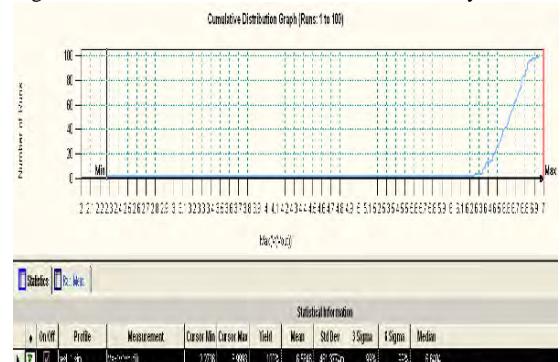


Figure 9 Monte Carlo Analysis Results(10% Tolerance)

Smoke Analysis

The smoke analysis shows that components of the pulse wave generator are risky, especially the trimmer R2, the NPN transistor Q1 and the PNP transistor Q2

Component	Parameter	Type	Rated Value	Steering	Monitoring	Measured Value	V/I/A
P2	T20	Per	200	0	0	38.00E-01	2.00
P3	T20	Per	200	0	0	30.00	2.00
P4	T20	Per	200	0	12.00	1.00E-03	2.00
P5	T1	Per	200	0	20	1.75E-04	2.00
P6	T2	Per	200	0	5	1.00E-02	2.00
P7	T3	Per	200	0	5	1.00E-02	2.00
P8	T4	Per	200	0	5	1.00E-02	2.00
P9	T5	Per	200	0	20	4.00E-03	2.00
P10	C	Per	200	0	12.00	3.00E-01	2.00
P11	Y2	Per	30	0	1.00E-02	2.00	2.00
P12	0	Per	00	1	3.00E-01	2.00	2.00
P13	Y3	Per	00	0	2.00E-02	2.00	2.00
P14	0	Per	00	0	1.00E-02	2.00	2.00

Figure 10 Smoke Analysis Results (Peak Values)

3. Circuit Board Fabrication

The tested circuit schematic form was implemented on the circuit board using PCB Editor. The PCB manufacturer, 4PCB required the following 4 files for the fabrication of the circuit board; Outline File, Top Copper File, Bottom Copper File and Drill File. They are shown in Figure 11, 12, 13, 14.

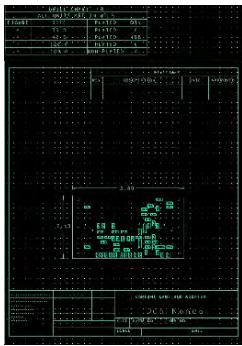


Figure 11 Outline File



Figure 12 Top Copper File



Figure 13 Bottom Copper File

```

:LEADER: 12
:HEADER:
:CODE : ASCII
:FILE : BareBones_Proto_Copper_2.drl for board master.brd - layer: TOP and BOTTOM
: : Hole size 1 = 36.000000 Tolerance = -0.000000/0.000000 PLATED MILS Quantity = 6
: : Hole size 2 = 42.000000 Tolerance = -0.000000/0.000000 PLATED MILS Quantity = 108
: : Hole size 3 = 120.000000 Tolerance = +0.000000/-0.000000 PLATED MILS Quantity = 6
: : Hole size 4 = 109.000000 Tolerance = +0.000000/-0.000000 NON_PLATED MILS Quantity = 4
:
: G90
X024000Y0115000
X024000Y0105000
X023000Y010945000
X023000Y0075000
X023000Y0095000
X023000Y0135000
M000
:
: X023000Y00112000
X023000Y0112000
X033800Y012000
X031300Y0134000
M30

```

Figure 14 Drill File

The circuit board, “BareBones Proto PCB” which was fabricated by 4PCB is shown in Figure 15 and the final circuit board which has all components is shown in Figure 16.

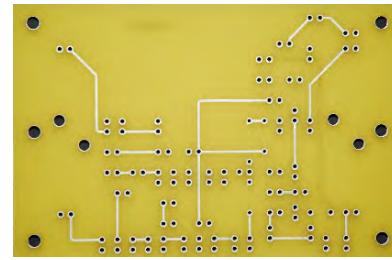


Figure 15 BareBones Proto PCB (2.5 x 3.8 inches)

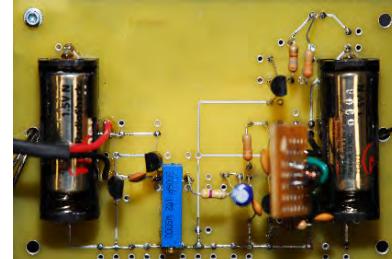


Figure 16 Final Circuit Board (2.5 x 3.8 inches)

4. Calibration

The calibration of pulse-wave generator was conducted using the water tank. The thermocouple was immersed into the water and the water temperature was gradually raised from the freezing point. The temperatures and the corresponding

frequencies were recorded. Figure 17 shows the relationship between the frequency and the temperature. If the temperature increases, the frequency of the pulse-wave generator also increases.

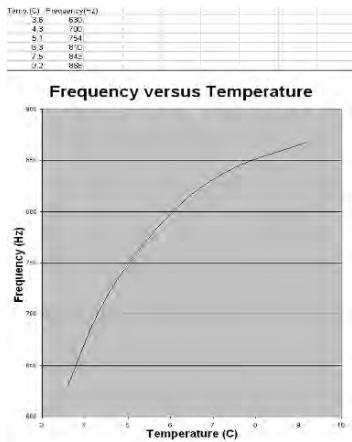


Figure 17 Frequency versus Temperature

V. EXPERIMENTS

The temperature experiments were conducted above Dana Hall at the campus of University of Hartford. Two 500 feet kite strings were attached to the PCB to control the altitude of the transmitter. The altitude was determined by measuring the length of the string.



Figure 18 Temperature Experiments above Dana Hall
A small blue dot at the top of the photograph is the balloon.

VI. RESULTS

The final test results of this telemetrized temperature project are stated as follows;

Date; April 27th, 2008
Time; 8 AM
Altitude; 258 feet above Dana Hall,

University of Hartford, West Hartford, CT USA
Pulse Wave Frequency; 744 Hz
Temperature; 4.9 degrees Celsius



Figure 19 Final Flight on April 27th, 2008

VII. CONCLUSION

The comparison between this analog-type FM transmitter and digital-type FM transmitter, TC-Link Wireless Thermocouple System is summarized as follows;

Analog-Type TC-Link Wireless System

Cost*	\$90	\$2195
Frequency	105.6 MHz	2.4 GHz
Channels	1	6
Range	258 feet	100 meters (328 feet)

* Excluding the cost of the thermocouple

TC-Link Wireless System has 6 times more channels. Since it uses the 2.4 GHz FM frequency band, it is interference free from FM radio stations. Although, the cost is 24 times higher than this analog-type FM transmitter. Therefore, the future of this telemetrized temperature project is still prospective.

VII. RELATED WORK

The atmospheric transmitter which measures various atmospheric parameters is called Radiosonde. It may operate at the frequency of 403 MHz or 1680 MHz and the weight is typically 250 grams. As the balloon ascends, it expands as the atmospheric pressure decreases. Finally, it breaks and stops ascending. The balloon size can range from 250 grams to 3000 grams and an 800 gram balloon can ascent 69,000 feet above the ground. The modern radiosonde can measure the following atmospheric parameters;

1. Pressure
2. Altitude
3. Geographical Position
4. Temperature
5. Relative Humidity
6. Wind Speed and Direction

In the United States, the National Weather Service launches radiosondes from 92 stations in North America and the Pacific Islands at 0000 and 1200 UTC(Coordinated Universal Time) and the Radiosonde data is crucially important for weather prediction[9].

ACKNOWLEDGMENT

The author would like to thank Dr. Saeid Moslehpoour of the University of Hartford, Dr. Avital Fast of the Albert Einstein Medical Center, Dr. Carl Enger of Biotelemetrics, Dr. Bill Stuhler of EMA Design Automation, Inc. and Mr. Bill Biss of 4PCB for valuable support, suggestions and recommendations.

REFERENCES

- [1] A. Fast, Facsimile sent to Dr. Devdas Shetty, Feb. 1992.
- [2] C. Wang, "Instruction to Install the Telesensor System," Dept. Elect. Eng., Univ. Hartford, Hartford, CT, Oct. 1996.
- [3] C. Enger, Facsimile sent to Jun Kondo, Sept. 1998.
- [4] MicroStrain Technical Product Overview, EmbedSense Wireless Sensor.
Available: <http://www.microstrain.com/embed-sense.aspx>
- [5] M. Danash, J. Zuniga, F. Concilio "Fixed Low-Frequency Broadband Wireless Access Radio Systems," IEEE Communications, New York, Sep. 2001.
Available: <http://www.comsoc.org/dl/sample/ci1/Private/2001/Sep/danesh.html>
- [6] MicroStrain TC-Link Wireless Thermocouple System.
Available: <http://www.microstrain.com/tc-link.aspx>
- [7] "Resistance versus Temperature," Data Sheet printed by Yellow Springs Instrument Co., Yellow Springs, Ohio.
- [8] F. Mims "Basic Electronics Transistors and Integrated Circuits," Radioshack Corp., Fort Worth, TX, July 2000.
- [9] <http://en.wikipedia.org/wiki/Radiosonde>

Enhancing Sensor Network Security with RSL Codes

Chunyan Bai and Guiliang Feng

SECCM, Roger Williams University, One Old Ferry Road, Bristol RI 02809
CACS, University of Louisiana at Lafayette, Lafayette, LA 70504

cbai@rwu.edu and glf@cacs.louisiana.edu

Abstract - Sensor networks have found their wide applications in a variety of areas such as ocean and wildlife monitoring, manufacturing machinery, performance monitoring, building safety and earthquake monitoring. How to protect the data confidentiality is a challenging problem for sensor networks because of their resource constraints such as data memory, code space and energy to power the sensor nodes. Different threats to sensor networks, compared to those happened to traditional ad-hoc networks, also bring unique requirements to the design of a secure sensor network. In this paper, we present a novel encryption scheme based on Reed-Solomon-Like (RSL) Codes. The scheme provides a solution to the secure sensor networks with the advantages of fast calculation, low power consumption and easy implementation.

Index Terms: Sensor Network, Encryption, Reed-Solomon-Like Codes, Confidentiality.

I. INTRODUCTION

A. Sensor Network Securities

Sensor network is a sensing, computing and communication infrastructure that allows us to observe, record, and respond to phenomena in the natural environment or in our physical and cyber-infrastructure. The sensors themselves can range from small passive sensors (e.g. “smart dust”) to larger scale, controllable weather-sensing platforms. Their computation and communication infrastructure will be radically different from that found in today’s Internet-based systems, reflecting the device- and application-driven nature of these systems. Current and potential applications of sensor networks include, but are not limited to: military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, distributed robotics, environment monitoring, and building and structures monitoring. Because of their wide applications, wireless sensor networks have been identified as one of the most important technologies for the 21st century [11].

The application of sensor networks indicate that many sensor systems are deployed in unattended and often adversarial environments open to attackers, bad weather and so on. The likelihood that a sensor network suffers physical attacks in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network. Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues. Also most sensor networks are distributed networks without a central management point. This will increase the vitality of sensor networks.

Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security. The sensor network security should cover data confidentiality, data integrity, data freshness, availability, authentication, robustness, survivability and so on [12]. We will focus on data confidentiality in this paper.

Due to the resource constraints, and the adversarial environment of the sensor network, traditional encryption schemes that work well for ad-hoc networks will not be applied to sensor networks. Since each bit transmitted consumes about as much power as executing 800-1000 instructions [22], it makes message expansion caused by security mechanisms come at significant cost. So it is challenging to design a proper security mechanism that provides data confidentiality for sensor networks within all above limitations.

B. Related Works

Research challenges in sensor network security include securing the communication link, securing distributed services and tolerating captured nodes. Cryptography will be the solution to address all these challenges. Avoiding complex key management and minimizing the packet overhead are the

primary concerns in designing a good encryption and authentication scheme for sensor networks. Please refer to references [1],[5],[6],and [7] for related work.

Though references [13][14][15] and [16] provide thoughts in how to make the public key encryption schemes feasible with the right selection of algorithms, most of the traditional public key cryptography techniques are unsuitable in low power devices such as wireless sensor networks. This is due largely to the fact that it is needed to keep two mathematically related key, which is usually too computationally intensive for the individual nodes to adopt public key cryptography in sensor networks.

Symmetric cryptography is therefore the typical choice for applications that cannot afford the computational complexity of asymmetric cryptography such as sensor networks. The SNEP scheme proposed in [1] provides data confidentiality, two-party authentication and data freshness using RC5 cipher. Carman et al. acknowledged in [19] that symmetric key techniques are attractive due to their energy efficiency. But they also conclude that all symmetric key based key exchange protocols analyzed exhibit limitations in their flexibility.

Error-Correcting Codes (ECC) were originally proposed to fight against noise over communication and storage channels [23]. Good structures of Error-Correcting codes can also be utilized to build cryptographic systems [24].

In this paper, we consider sensor networks in which content confidentiality should be maintained. More precisely, it is our aim that passive adversaries that eavesdrop on the communication between the sensors and the sink cannot obtain the exchanged information. We also analyze to what extent the security architecture can be maintained. This is achieved by encrypting transmitted data with the Reed-Solomon-Like codes. The scheme provides a solution to the secure sensor networks with the advantages of high speed, easy implementation and low energy consumption.

The paper is organized as follows. In section II, we review the Reed-Solomon-Like codes (RSL code) based on Circular Permutation Matrices (CPM) and their algebra, which is the mathematical foundation of our encryption scheme. We also provide notations for the rest of the paper. The details of the encryption scheme based on RSL codes will be presented in section III. Section IV provides analysis of the scheme and finally conclusions are included in Section V.

II. REVIEW OF REED-SOLOMON-LIKE CODES

In this section, we review the Reed-Solomon-Like Codes [8], which are important in understanding the encryption scheme shown in next section.

We start our review with the definition of Circular Permutation Matrix (CPM). For a $l \times l$ matrix $M = (m_{i,j})_{l \times l}$, l is any specified integer, we always assume that the order of rows (columns) is from 0 to $l - 1$.

Let $p = m+1$ be an odd prime and let

$$E = \begin{bmatrix} \vec{0} & 1 \\ I_m & \vec{0}^T \end{bmatrix}, \quad (2.1)$$

where $\vec{0}$ is a $1 \times m$ vector of 0's and $\vec{0}^T$ is an $m \times 1$ vector of 0's. It can be easily checked that

$$\{I, E, E^2, \dots, E^m\},$$

the so-called *Circular Permutation Matrices* (CPM), form a group with matrix multiplication over GF(2), where I is a $p \times p$ identity matrix. It is easy to verify that for the above CPMs,

$$E^{m+1} = I, \text{ and } E^{-1} = E^m.$$

With the definition of CPM, the following binary matrix can be defined:

$$\tilde{H} = \begin{bmatrix} \tilde{I} & \tilde{I} & \tilde{I} & \tilde{I} & \cdots & \tilde{I} \\ \tilde{I} & E\tilde{I} & E^2\tilde{I} & E^3\tilde{I} & \cdots & E^n\tilde{I} \\ \tilde{I} & E^2\tilde{I} & E^4\tilde{I} & E^6\tilde{I} & \ddots & E^{2n}\tilde{I} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \tilde{I} & E^{r-1}\tilde{I} & E^{2(r-1)}\tilde{I} & E^{3(r-1)}\tilde{I} & \cdots & E^{n(r-1)}\tilde{I} \end{bmatrix}, \quad (2.2)$$

where $r < n < m$. \tilde{I} is defined as $\tilde{I} = \begin{bmatrix} I_m \\ \vec{0} \end{bmatrix}$, where I_m is a $m \times m$ identity matrix. Matrix in (2.2) is an $r(m+1) \times (n+1)m$ matrix. It can be regarded as an $r \times (n+1)$ block matrix, where each block-column contains m columns, and each block-row contains $(m+1)$ rows.

Since the summations of all rows of $E^i\tilde{I}$ and all rows of \tilde{I} are rows of 1's, respectively (i.e., (111...1)), and the bottom row of \tilde{I} is a row of 0's (i.e., (000...0)), the bottom row in each block-row of \tilde{H} can be deleted. The reduced matrix is an $mr \times m(n+1)$ binary parity-check matrix. Deleting the bottom row in each block-row of H can be implemented by multiplying H by \tilde{I}^T . Hence, the following matrix H is equivalent to \tilde{H} as a parity-check matrix:

$$H = \begin{bmatrix} I_m & I_m & I_m & I_m & \dots & I_m \\ I_m & \tilde{E}^1 & \tilde{E}^2 & \tilde{E}^3 & \dots & \tilde{E}^{n-1} \\ I_m & \tilde{E}^2 & \tilde{E}^4 & \tilde{E}^6 & \ddots & \tilde{E}^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ I_m & \tilde{E}^{r-1} & \tilde{E}^{2(r-1)} & \tilde{E}^{3(r-1)} & \dots & \tilde{E}^{(n-1)(r-1)} \end{bmatrix}. \quad (2.3)$$

(2.3) provides a $rm \times (n+1)m$ binary matrix.

Now we can introduce the RSL codes based on CPM. Let (G, \oplus) be an Abelian group and 0 the identity element. Let $b \in \{0,1\}$ and $g \in G$, It can be defined that

$$b \times g = g \times b = \begin{cases} 0 & \text{for } b = 0 \\ g & \text{for } b = 1 \end{cases} \quad (2.4)$$

Let $\vec{v} = (v_0, v_1, \dots, v_n)$ be a vector over G and $\vec{b} = (b_0, b_1, \dots, b_n)$ be a vector over $GF(2)$, we define

$$\vec{b} \times \vec{v} = \vec{v} \times \vec{b} = (b_0 \times v_0) \oplus (b_1 \times v_1) \oplus \dots \oplus (b_n \times v_n). \quad (2.5)$$

A linear code C is called Reed-Solomon-Like Code if C is defined over an Abelian group by

$$C = \{\mathbf{c} = (\vec{c}_0, \vec{c}_1, \vec{c}_2, \dots, \vec{c}_n) \mid H \times C^T = \vec{0}^T\}, \quad (2.6)$$

where $\vec{c}_i = (c_{i1}, c_{i2}, \dots, c_{im})$ with each $c_{ij} \in G$, and H is defined in (2.3).

It was proved in reference [8] that the encoding and decoding of RSL code C need $(r^2 + n)p$ XOR operations. When 32 codewords are encoded and decoded simultaneously, a 32-fold improvement can be achieved in efficiency.

III. ENCRYPTION SCHEME BASED ON RSL CODES

In this section, we will show how to apply the RSL code (n, k, d) with parameter $p = 23$ to the encryption and decryption schemes for sensor networks, where the codeword length $n = 23$, the information length $k = 12$ and the minimum distance $d = 12$, that is, a $(23, 12, 12)$ RSL code. Each information block (one of the 12) is composed of 11 message packets (each packet has 22 bits), denoted by m_1, m_2, \dots, m_{11} , and one random packet, denoted by r_{12} and chosen for the security purpose. The rest 11 packets of the RSL codeword are redundant packets, denoted by $c_{13}, c_{14}, \dots, c_{23}$ and generated by RSL code encoding scheme.

The parity check matrix of the $(23, 12, 12)$ RSL code is represented by:

$$\tilde{H} = \begin{bmatrix} I & I & I & I & \dots & I \\ I & \tilde{E} & \tilde{E}^2 & \tilde{E}^3 & \dots & \tilde{E}^{n-1} \\ I & \tilde{E}^2 & \tilde{E}^4 & \tilde{E}^6 & \ddots & \tilde{E}^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ I & \tilde{E}^{r-1} & \tilde{E}^{2(r-1)} & \tilde{E}^{3(r-1)} & \dots & \tilde{E}^{(n-1)(r-1)} \end{bmatrix}, \quad (3.1)$$

where $r = 11$, $n = 23$, I is a 22×22 identity matrix, and \tilde{E}^i is the sub-matrix of E^i by deleting the last column and the last row from E^i . Let \tilde{G} be the $(23, 12, 12)$ generator matrix of the RSL code, from (3.1) we have

$$\tilde{G} = \begin{bmatrix} I & I & I & I & \dots & I \\ I & \tilde{E} & \tilde{E}^2 & \tilde{E}^3 & \dots & \tilde{E}^{n-1} \\ I & \tilde{E}^2 & \tilde{E}^4 & \tilde{E}^6 & \ddots & \tilde{E}^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ I & \tilde{E}^r & \tilde{E}^{2(r)} & \tilde{E}^{3(r)} & \dots & \tilde{E}^{(n-1)(r)} \end{bmatrix} = [\tilde{G}_1 | \tilde{G}_2], \quad (3.2)$$

From (3.2) we have

$$\tilde{G}_1^{-1} \tilde{G} = [I_{12 \times 12} | G], \quad (3.3)$$

where $I_{12 \times 12}$ is a 12×12 identity matrix and G a 12×11 block matrix. Obviously, $[I_{12 \times 12} | G]$ is also a generator matrix of \tilde{H} . Let $H = \tilde{H}S$, where $S = \begin{bmatrix} S_1 & 0 \\ 0 & S_2 \end{bmatrix}$ and S_1, S_2 are 11×11 and 12×12 binary non-singular block matrices, respectively. Since $\tilde{G}\tilde{H}^T = 0$, we have

$$[I_{12 \times 12} | G]\tilde{H}^T = [I_{12 \times 12} | G](S^{-1})^T \times (\tilde{H}S)^T = 0$$

Therefore, if

$$(a_1, a_2, \dots, a_{12})[I_{12 \times 12} | G](S^{-1})^T = (b_1, b_2, \dots, b_{23}),$$

We have

$$\tilde{H}(b_1, b_2, \dots, b_{23})^T = \tilde{H}S \times ((S^{-1})^T)^T \tilde{G}^T (a_1, a_2, \dots, a_{12})^T = 0. \quad (3.4)$$

Let

$$S(b_1, b_2, \dots, b_{23})^T = (d_1, d_2, \dots, d_{23})^T, \quad (3.5)$$

From (3.4) we have

$$\tilde{H}(d_1, d_2, \dots, d_{23})^T = 0. \quad (3.6)$$

Equation (3.6) shows that we can use \tilde{H} as parity check matrix to decode the codeword encoded by generator matrix G after a preprocessing with S .

Furthermore, let

$$G^* = [\tilde{e}^T | G] \times (S_2^{-1})^T, \quad (3.7)$$

where $\tilde{e}^T = [\mathbf{o}, \mathbf{o}, \dots, \mathbf{o}, I]^T$, \mathbf{o} is a 22×22 all-zero matrix, I a 22×22 identity matrix, and $[\tilde{e}^T | G]$ a 12×12 block matrix.

If we represent information message \mathbf{m} as $\mathbf{m} = (m_1, m_2, \dots, m_{11}, r_{12})$, then from (3.7) we have

$$\begin{aligned}\mathbf{m} \times \mathbf{G}^* &= (m_1, m_2, \dots, m_{11}, r_{12}) \times G^* \\ &= (m_1, m_2, \dots, m_{11}, r_{12}) \times [\bar{e}^T | G] \times (S_2^{-1})^T,\end{aligned}\quad (3.8)$$

which will be the parity check parts used in the decoding phase shown in (3.10).

Next, we will present the encryption and decryption procedures with given message vector $\mathbf{m} = (m_1, m_2, \dots, m_{11}, r_{12})$, where r_{12} is the randomly chosen vector for security purpose, by using the RSL code encoding and decoding schemes discussed above.

Encryption:

Step 1: Since each message bit-block m_i is a vector, we let $m_i = (m_{i,0}, m_{i,1}, \dots, m_{i,21})$ for $i = 1, 2, \dots, 11$ and $r_{12} = (r_{12,0}, r_{12,1}, \dots, r_{12,21})$. Modify each $m_{i,j}$ by

$$m_{i,j}^* = m_{i,j} + ((r_{12,j} \wedge r_{12,<j+1>}) \vee (\overline{r_{12,j}} \wedge r_{12,<j+2>})), \quad (3.9)$$

where \wedge is the bit-AND operation and \vee the bit-OR operation. $\overline{r_{12,j}}$ is the inverse of $r_{12,j}$ for $j = 0, 1, \dots, 21$. $(a + b) = (a + b) \bmod 22$.

Step 2: Multiply message vector $\mathbf{m} = (m_1, m_2, \dots, m_{11}, r_{12})$ by G^* , we have

$$\mathbf{m} \times \mathbf{G}^* = \mathbf{C}, \quad (3.10)$$

where $\mathbf{C} = (r_{12}^*, c_{13}, c_{14}, \dots, c_{23})$. Thus \mathbf{C} is the encrypted cipher packet sequence.

Decryption:

Step 1: From (3.8) and (3.10), we have

$$\mathbf{C} \times S_2^T = \mathbf{m} \times [\bar{e}^T | G] = (r_{12}, d_1, d_2, \dots, d_{11}), \quad (3.11)$$

which gives values for r_{12} and d_i , for $i = 1, 2, \dots, 11$. Since $(d_1, d_2, \dots, d_{11}) = \mathbf{m} \times G$ is the parity check part, $(\mathbf{m}, d_1, d_2, \dots, d_{11})$ is a codeword. Next, we will use r_{12} and d_i to recover $(m_1, m_2, \dots, m_{11})$.

Step 2: Calculate the syndrome

$$(s_1, s_2, \dots, s_{11})^T = \tilde{H}_2 \times ((r_{12}, d_1, d_2, \dots, d_{11}) \times S_2)^T, \quad (3.12)$$

where \tilde{H}_2 is the sub-matrix of \tilde{H} consisting of the last 12 block-columns.

Step 3: Find $(m_1, m_2, \dots, m_{11})$ by

$$(m_1, m_2, \dots, m_{11}) = S_1^{-1} \times H_1^{-1} \times (s_1, s_2, \dots, s_{11})^T, \quad (3.13)$$

where \tilde{H}_1 is the sub-matrix of \tilde{H} consisting of the first 11 block-columns.

Step 4: Using $\mathbf{m} = (m_1, m_2, \dots, m_{11}, r_{12})$ obtained from (3.13) and with (3.9), we can recover the information message $(m_1, m_2, \dots, m_{11})$.

IV. DISCUSSION AND ANALYSIS

A. Feasibility of the Encryption Scheme

From coding theory [9], an erasure code (n, k, d) with parity check matrix H of size $(n - k) \times n$ can be used to detect $d - 1$ errors if the error locations are known. For our case when a $(23, 11, 12)$ RSL code is adopted, the encryption stage

in (3.10) is equivalent to encoding the message with the generator matrix G of size 11×23 , which guarantees that the syndrome decoding in (3.12) and (3.13) can recover the original message $\mathbf{m} = (m_1, m_2, \dots, m_{11})$ with up to 12 errors allowed given the error locations.

For an unauthorized user who incidentally obtains the cipher packet sequence \mathbf{C} , it is infeasible for him/her to decrypt the ciphertext by figuring out the decoding parity matrix \tilde{H} with exhaustive search.

B. Advantages of the proposed encryption scheme

Symmetric cryptography is preferred to public key encryption in sensor networks because of the resource constraints. The use of the traditional symmetric cryptography like DES is quite limited due to the fact that it can be broken relatively easily. In light of the shortcomings of DES, other symmetric cryptography systems have been proposed to be applied to sensor networks including 3DES (Triple DES), RC5, AES, and so on. An analysis of the various ciphers is presented in [17] and [18] and their applications in sensor networks in [1] and [19].

Compared to the traditional symmetric cryptography such as DES, Triple DES, RC5 and AES, the whole encryption and decryption processes in our scheme require only Exclusive-OR (XOR) operations and can be implemented with small hardware requirement in high speed, which make it a fit in environment with limited memory and storage space such as sensor network nodes. The complexities of the encryption and the decryption are $O(p^4)$ bit-XOR operations. If the packet has 32b times more bits than in our encryption and decryption scheme, the complexities would be $O(bp^4)$ word-XOR

operations, where we assume that each computer word has 32 bits. This shows that if we encrypt and decrypt codewords in parallel, we can further improve the speed without consuming too much sensor node energy. In Step 2 and Step 3 of the decryption process, the calculation of $H_2 \times (b_1, b_2, \dots, b_{12})^T$ was substituted by $\tilde{H}_2 \times ((b_1, b_2, \dots, b_{12}) \times S_2^T)^T$ with reduced matrix and $H_1^{-1} \times (b_1, b_2, \dots, b_{12})^T$ substituted by $S_1^{-1} \times (\tilde{H}_1^{-1} \times (b_1, b_2, \dots, b_{12})^T)$ with reduced matrix because they will take less XOR operations to implement, which further improve the speed of the decryption.

Though cryptography is considered the right solution to the content and transaction confidentiality issues of sensor networks, cryptography usually entails a performance cost for extra computation that often increases packet size. Most of the performance overhead is attributable to the increase in packet size [1]. In our case, as indicated by the encryption process in (3.10), encryption through RSL code encoding will not bring in any redundant packets to be transmitted over sensor network channels, which is another good feature of our scheme.

The purpose of using r_{12} in step 1 of encryption has two folds. First is to increase the information confidentiality by scrambling each original message vector with different r_{12} s. Second is to achieve the semantic security [10]. That is, we can ensure that an eavesdropper has no information about the plaintext, even if it sees multiple encryptions of the same plaintext. The scrambling prevents the attacker from inferring the plaintext of encrypted messages if it knows plaintext-ciphertext pairs encrypted with the same key. Simulation results will be provided in the future to further approve the good performance of our scheme.

V. CONCLUSION

In this paper we have presented a novel encryption scheme based on Reed-Solomon-Like codes. The scheme has the advantages of fast encryption and decryption (by fast encoding/decoding), easy implementation (XOR operations only), low energy consumption and small communication overload, which makes it a better candidate for sensor networks with resource constraints.

REFERENCES

- [1]. Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, and J.D.Tygar, "Spins: Security protocols for sensor networks", *Wireless Networks*, vol. 8, pp.521, 2002.
- [2]. Ball Semiconductor Inc., "Medical Applications", *Benefits of Spherical Geometry*, 1997.

- [3]. J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Mobile networking for smart dust", *ACM/IEEE Intl. Conf. on Mobile Computing and Networking*, Seattle, WA, August 1999, Mobicom 99.
- [4]. Yordan Kostov and Govind Rao, "Low cost optical instrumentation for biomedical measurement", *J. Review of Scientific Instruments*, 2000.
- [5]. Weimerskirch and D. Westhoff, "Zero-Common Knowledge Authentication for Pervasive Networks", Proc. 10th Workshop Selected Areas in Cryptography (SAC '03), pp. 73, July 2003.
- [6]. Weimerskirch and D. Westhoff, "Identity Certified Zero- Common Knowledge Authentication", *Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN'03)*, Oct. 2003.
- [7]. Weimerskirch, D. Westhoff, S. Lucks, and E. Zenner, "Efficient Pairwise Authentication Protocols for Sensor Networks: Theory and Performance Analysis", *Sensor Network Operations*, S. Phoha, T.F. La Porta, and C. Griffin, eds. Wiley-IEEE Press, May 20
- [8]. G.L.Feng, R.H.Deng, F.Bao and J.C.Shen, "New Efficient MDS Array Codes for RAID Part I: Reed-Solomon-Like Codes for Tolerating Three Disk Failures", *IEEE Transactions on Computer*, vol. 54, no. 8, Sep. 2006.
- [9]. F.J. MacWilliams and N.J. A. Sloane, *The Theory of Error-Correcting Codes*, Elsevier Science Publishers B.V. 1977.
- [10]. Shafi Goldwasser and Silvio Micali, "Probabilistic Encryption", *Journal of Computer Security*, vol. 28, 1984.
- [11]. Neil Gross, "21 ideas for the 21st century", *Business Week*, pp. 78'C167, Aug. 30, 1999.
- [12]. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks", *Communications of ACM*, vol. 47, No.6, 2004.
- [13]. G. Gaubatz, J.P. Kaps, and B. Sunar. "Public key cryptography in sensor networks – revisited", *In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2004)*, 2004.
- [14]. N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz. "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs". *In 2004 workshop on Cryptographic Hardware and Embedded Systems*, August 2004.
- [15]. D. J. Malan, M. Welsh, and M. D. Smith. "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography", *First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, 2004. IEEE SECON'04.
- [16]. R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and et. Al., "Tinypk: securing sensor networks with public key technology", *Proceedings of the 2nd ACM workshop on Security of Ad hoc and Sensor Networks (SASN'04)*, pages 59-64, New York, NY, USA, 2004. ACM Press.
- [17]. Y. Law, J. Doumen, and P. Hartel. "Survey and benchmark of block ciphers for wireless sensor networks", *Technical Report TR-CIT-04-07*, Centre for Telematics and Information Technology, University of Twente, The Netherlands, 2004.
- [18]. P.Ganesan, R.Venugopalan and et.al., "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes", *Proceedings of Wireless Sensor Networks and Applications*, WSNA'03, San Diego, CA, 2003.
- [19]. D.W.Carman and P.S. Krus and B.J. Matt, "Constraints and Approaches for Distributed Sensor Network Security", *Technical Report*, NAI Labs, Security Research Division, Glenwood, MD, 2000.
- [20]. J. Hill, R. Szewczyk, A. Woo, D. Culler and K. Pister, "System architecture directions for networked sensors", *Proceedings of ACM, ASPLoS IX*, November 2000.
- [21]. G. Kabatiansky, E. Krouk, S. Semenov, *Error Correcting Coding and Security for Data Networks*, John Wiley and Sons, 2005.
- [22]. W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, Chapter 18, Prentice Hall, 2006.

The Integrity Framework within the Java Data Security Framework (JDSF): Design and Implementation Refinement

Serguei A. Mokhov

SGW, EV7.139-2, Department of Computer Science and Software Engineering, Concordia University, Montreal, Quebec, Canada, Email: mokhov@cse.concordia.ca

Lee Wei Huynh[‡]

SR Telecom[†], Montreal, Quebec, Canada, Email: leewei_huynh@srtlecom.com

Lingyu Wang

Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Quebec, Canada, Email: wang@ciise.concordia.ca

Abstract— We present a refinement design of the *Integrity Framework*, which is a part of a more general structure, that we refer to as the Java Data Security Framework (JDSF) designed to support various aspects related to data and database security (confidentiality, origin authentication, integrity, SQL randomization), where this article focuses only on the integrity aspect. The design refinement considerations include further unification of the parameter structure of concrete module implementations of the framework’s API for validation and comparative studies.

Index Terms—data integrity, Java Data Security Framework (JDSF), Modular Audio Recognition Framework (MARF), HSQLDB, watermarking

I. INTRODUCTION

The JDSF project explores secure data storage related issues from the point of view of data security in two open-source projects: MARF [1] and HSQLDB [2] and proposes a design refinement of a relatively independent reusable framework to enable data integrity features in both projects. We limit ourselves to the section of the research we surveyed for our design and implementation that follow.

A. Background

In this section we briefly review the technologies used for as case studies for refinement and application of the research described in this paper.

MARF: The Modular Audio Recognition Framework (MARF) [1], [3] is an open-source research platform and a collection of audio and natural language processing (NLP) algorithms written in Java. It is arranged into a modular and extensible framework facilitating addition of new algorithms. MARF’s based applications can run distributively over the network (using CORBA, XML-RPC, or Java RMI) [4], [5], [6], and its implementation may act as a library in applications. One of MARF’s applications, SpeakerIdentApp has a database of speakers, where it can identify who people are, their gender, spoken accent, etc. regardless of what they say [7], [8].

[†]All opinions expressed in this work are that of the author, and not necessarily that of SR Telecom.

HSQLDB: HSQLDB [2] is a popular open-source SQL relational database engine, as MARF and JDSF written in Java. It has a JDBC driver and supports a large subset of ANSI-92 SQL, SQL 99, 2003, and 2008 enhancements. It provides a small and relatively fast database engine, which offers both in-memory and disk-based tables and supports embedded and server modes. Additionally, it includes tools such as a minimal web server, in-memory query and management tools. HSQLDB is currently being used as a database and persistence engine in many open source software projects (e.g. OpenOffice [9]) and even in commercial projects and software projects. It generally known for its small size, ability to execute completely in memory, its flexibility and speed.

B. Approach

As a part of JDSF, we provide the sub-framework to allow for the common algorithm implementations of the integrity aspects for MARF’s and HSQLDB’s data. Both, MARF and HSQLDB are considered independently as well as MARF is being considered as a front-end of HSQLDB. Depending on the architecture, a MARF’s instance can be a trusted or untrusted front-end and so is the HSQLDB’s instance that it’s “talking” to.

There are several approaches, architectures, algorithms, etc. to the integrity problem, so on the research-and-development side of the project, we research on several techniques to achieve the required integrity goals, compare them, and provide a an abstracted framework’s API implementation-wise such that it is easy to add new algorithms that implement the goals. As a proof-of-concept, we initially implement two-three of those techniques within the designed framework for comparative studies as well as examples of how to use the framework and also to validate its design. To summarize:

- We consulted a number research papers on the techniques for integrity of the data storage.
- We proposed and designed the framework [10] that allows easy plugging-in of such implementations within MARF and HSQLDB, with the API, etc.

- We then implemented some of the techniques for comparative studies.

Proposed Design and Implementation Aspects: MARF can use plain Java objects (default), XML, a connection to any relational database (e.g. HSQLDB, PostgreSQL, MySQL, etc.) through an appropriate JDBC driver, or a comma-separated values (CSV) file. MARF and its applications use the database to store subject identities and a mapping to their biometric or otherwise digital samples.

We can also decide to do not trust the underlying storage model to provide integrity of the MARF's databases, so we propose to implement a layer at the MARF's library level to provide some integrity checks (among other things) through an optional cryptographic or watermarking framework, so the users interested to get correct, unaltered, results for their research. When we pick HSQLDB as the backend database engine for MARF and its applications, we can make it trusted or untrusted in our experiments, as both layer components and the new framework are our works.

Assumptions: The paper exclusively considers the integrity aspect of *data* in some form of a data set or database. There are no users or clearance levels in our model, so there are no issues of authorization and access control, multilevel databases, etc. We will not address confidentiality and authentication (which are discussed in [11], [12]), SQL randomization (which is addressed in [13]), availability, authorization, and access control aspects in this work.

II. SURVEY OF THE RELATED WORK

This section presents the summary of the research done on the integrity aspects of various types of data, such that the framework architected covers most aspects and parameters to be flexible. We consider several approaches to data integrity that include integrity lock architecture for data and databases, watermarking schemes for multimedia and databases, in order to extract the relevant algorithm parameters for the JDSF's integrity sub-framework refinement. For the most part, this section surveys the data integrity aspects primarily from the cited related works on the multimedia and database watermarking [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26].

A. Integrity Lock Architecture

The integrity lock architecture [27], [28] enforces integrity checks by insertion or appending of timestamps in say watermarking or data integrity (and also authentication) in the data themselves. A trusted front-end must make use of a message authentication code (MAC) function by filtering out disallowed data for read queries (e.g. SELECT) based on the stamps. It also controls the queries by updating and adding stamps in or append to the data on write. In this case, the cryptographic checksums or watermarks help to verify the data integrity. Since in our work we do not deal with users or multiple levels of access control, we simplify the integrity lock architecture as shown in Figure 1.

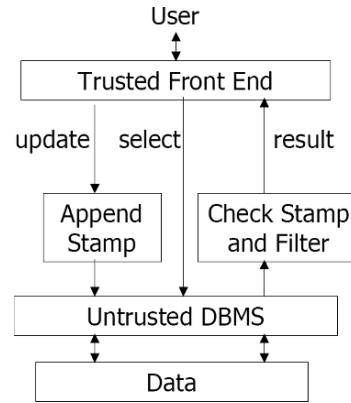


Fig. 1. Simplified Integrity Lock Architecture

B. Data Watermarking for Integrity Checks

For the assurance of data integrity, we can use authentication mechanism (see [12]) with cryptographic methods to generate an authentication signature with a key and prove the data origin by verifying with the same key. However, the authentication mechanism like signature to secure integrity has some drawbacks [27]:

- large overhead, can't be used on a per item basis (scale problem).
- if used on relations in relational databases, it can't localize the modification – once the signatures mismatch, the entire relation is useless.
- the signatures must be stored elsewhere.

The watermarking technologies come in handy to address some of these problems. The techniques have been implemented for multimedia for quite some time. They are used in multimedia products to prove the copyright ownership or to prevent piracy. Relatively recently, some research has been done for watermarking of relational databases. Moreover, more and more databases store not only primitive data types, but also multimedia data, like audio or video data, or serialized binary objects.

The researchers in the digital watermarking field have also been thinking to use it for data stream or even database integrity checking. Therefore, we would like to focus on digital watermark technologies for multimedia and data integrity. Watermarking consists of embedding a mark into the original media signal or otherwise data, which is different from classical digital signatures. The watermark attaches to the original data or is stored separately. This mark should not degrade the media quality. In order to prove the origin of content, the mark should be detectable and retrievable. In this work, we would like to review the techniques for the three types of media: audio, image, and video.

Digital Watermarking Requirements: Digital watermarking is a kind of process to inject a watermark into a media object without reducing the quality of it. Therefore, the watermark can be extracted and used to be a proof the origin of source media and its integrity. The watermark used for media should achieve four components of requirements, which are invisibility, robustness, security, and capacity. Without any one of

these requirements, the watermark will be useless to protect the integrity of the original data:

- *invisibility*: for any media object, the watermark must be invisible; otherwise, it will reduce the value of it, e.g. if music comes with a watermark noise, then it will affect the quality of the music.
- *robustness*: for any multimedia data, it is too easy to find software to “rip” from original media. The quality of multimedia can be modified to fit the users need. Therefore, in order to verify multimedia objects for modification, the watermark is supposed to keep some kind of readable quality even if the user modifies the content of a multimedia object. Then, the watermark can be an evidence in the court to prove the object belongs to the original owner.
- *security*: the watermark shouldn’t be removable. The watermarking techniques should use cryptographic algorithms to inject the watermark inside of a multimedia object such that there is no way to remove or modify it. In other words, it should be impossible to reverse the injection procedure with the purpose of removal of the watermark without knowing the secret information like private keys.
- *capacity*: the watermark should be easy and fast to embed in the multimedia object. It shouldn’t take very complicate or long process to do it.

Functionality of Watermarking: Watermarking can be used in many kind of purposes. The functionality of watermarking techniques we are interested in for our framework are about data integrity, which is about to leave to the network or disk, or just came or was read. It can be used for data origin authentication, fraud, and tamper detection. For multimedia content is used for legal purposes, medical applications, news reporting, and commercial transactions, it is important to ensure that the content not only originated from its real source, but that it had not been changed or falsified as well. This can be achieved by embedding a watermark in the data. The watermark can also include information from the original media that can help to recover any modification.

Since the specific integrity requirements vary with the application, watermarking techniques need to be designed within the context of the entire system in which they are to be “injected”. Each application implies different requirements and would necessitate different types of watermarking schemes or a combination thereof. For the rest of the section, we briefly discuss different watermarking principles and techniques for different data types.

Audio Watermarking: As we know, audio signal is kind of wave signal. Therefore, the basic idea consists in how to add an audio watermark signal to the original audio signal. The watermarked signal must have only minor distortion and perceived by the listener as identical to the original one. The watermark carries data that can be retrieved by a detector. The requirements that an audio watermarking system must satisfy are application-dependent and we can mention as general requirements, that fall in line with the requirements mentioned earlier specified more precisely for audio:

- *inaudibility*: the watermark shouldn’t be perceived by the listener and should not degrade sound quality.
- *robustness*: the watermark should resist any transformations applied to the audio signal, and sound quality is not unacceptably degraded by the modification.
- *capacity*: the audio watermark bit rate should be high enough for the application to capture, which must be balanced with the inaudibility and robustness; a trade-off must be defined.
- *low complexity*: for real-time applications, watermarking algorithms should be acceptable time-wise. Some applications (such as low bit-rate audio over the Internet) might accept the watermark to introduce a small level of sound quality degradation, while others (such as high bit-rate audio) would be extremely rigorous.
- *reliability*: the watermark must allow some portion of error bits. Data contained in the watermark should be extracted with acceptable error rates.
- *resistance*: signal-processing operations such as resampling or filtering is usually necessary for resistance. For copyright protection, resistance to attacks target on preventing watermark detection is also required; for example, if a piece of the signal is deleted, the watermark should still be detectable. On the contrary, for integrity-verification applications (such as tape of testimonies presented in the court), the watermark must be weak, fragile, and no longer be recognized once the audio is modified by unauthorized people.

The audio watermarking can be treated as a communication system. The audio signal carrying useful information and channel noise. In traditional communication systems, the useful signal is usually much stronger than the noise, and the noise is often assumed to be Gaussian and white. To avoid audible distortion, the watermark signal must be much weaker than the audio signal. Furthermore, the audio signal is generally non-stationary. Some basic approaches for audio watermarking have been proposed in the research. For example, we can mention:

- *spread-spectrum watermarking*: as in spread-spectrum communication systems [19], [20] the idea consists in spreading the watermark in frequency to maximize its power while keeping it inaudible and increasing its resistance to attacks [21], [22].
- *echo-hiding watermarking*: temporal masking properties are exploited in order to render the watermark inaudible. The watermark is an echo of the original signal [23], [24].
- *bit stream watermarking*: the watermark is inserted directly in the bit stream generated by an audio coder. For example, in [25], the watermark consists in the modification of scale factors in its bit stream.
- *masked watermark*: psychoacoustics is the study of the perception of sound. The study is, when two tones are close to each other in frequency and they are played simultaneously, then “frequency masking” happens: if one of the tones is sufficiently loud, it masks the other one [26]. Psychoacoustic models generalize the frequency-masking effect to non-tonal signals. In audio

watermarking, psychoacoustic models are often used to ensure inaudibility of the watermark. The watermark is constructed by inserting in frequency a nearly-white signal according to the masking threshold. After this operation, the watermark is always below the masking threshold and the watermark shouldn't heard in the original sound signal.

Image Watermarking: The digital image watermarking has the same problems as digital audio as it can be manipulated using a variety of sophisticated image processing tools easily. Such manipulations are so easy and emphasize the need for image verification techniques in applications. Basically, image watermarking has same requirements as audio watermarking, which are invisibility, robustness, security, and capacity, and same functionalities. However, we know that audio signal is different from image signal by their domain, same as watermarks for each. Audio watermarking focuses on audio wave frequency domain, whereas image watermarking focuses on spatial or color frequency domain. Therefore, for the image watermark injection must have different approaches to work.

The image watermarking schemes are classified into the methods of the spatial domain and the frequency domain. To hide a watermark in the frequency domain, an image has to be transformed from a spatial domain into its frequency domain. This scheme requires many computations and time to embed or retrieve the watermarks. Meanwhile in the spatial domain, the watermark can be directly embedded into the pixel values. The algorithms for embedding and recovering are simple. Traditionally, the scheme hides the watermark bits in the least significant bits (LSB), similarly like image steganography, which should make imperception for color manipulation for viewer. Several techniques can be used for a image transformation (e.g. discrete Fourier, discrete cosine, Mellin-Fourier, wavelet). Then, insert the watermark in the transformed space. Last, invert the transform back to get the marked image. The noise caused by the watermarking signal is thus spread over the whole image without being visible.

As an example, we recite the Wong's scheme is a block-based watermarking technique. In this scheme, Wong gives an $M \times N$ image X , a binary watermark image W of the same size as the original. In practice, this step is usually achieved by tiling the original image with a smaller logo image. The original image X is partitioned into $O \times P$ pixel blocks, $\{X_1, X_2, \dots\}$; where X_r denotes such blocks. The watermark image is partitioned into blocks W_r . For each block X_r , a corresponding block \hat{X}_r is formed by setting the least significant bit of each pixel to zero. A cryptographic hash, e.g. MD5 or SHA1, can be used to transform block \hat{X}_r and image dimensions is computed as: $H_r = H(M, N, \hat{X}_r)$. The hash value H_r can be treated as a random number. To get the signature, we compute: $S_r = Encrypt(H_r \oplus W_r, Key_{private})$. In the last step, we insert the signature S_r into X_r block as least significant bits of the block. The key point for this algorithm is the watermarking insertion is independent on each block. It verify the watermark, first, we partition the image \hat{X} into blocks \hat{X}_r . From the LSB of the \hat{X}_r block, we get a signature \hat{S}_r . Lastly, we get H_r by setting LSB to zero and calculate: $\hat{W}_r = Decrypt(\hat{S}_r, Key_{private}) \oplus \hat{H}_r$. Any change

in the pixel values in each block modify decrypted signature or hash value. Therefore, any modification can be detected and located in the corresponding image block.

Video Watermarking: Video consists of frames, i.e. images. Therefore, it has the same structure of an image, or rather a collection of images. However, the video watermarking have much more problems to be concerned about, like frame shift, frame dropping, cropping, scaling, rotation, and change of aspect ratio, especially when some of these are combined together.

The requirements of video watermarking are the same as image watermarking. However, the video watermarking techniques have much more sophisticated schemes than audio and image watermarking schemes do. There are many schemes proposed in the literature, like Karhunen-Loeve transform (KLT), discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT), wavelet packet transform (WPT), and others.

Database Watermarking: The database watermarking is a recent approach where one can inject a watermark into a database, then verify the integrity by retrieving the watermark later. The watermarking algorithm inserts some small error bits into the database object being watermarked. These intentional errors are called marks and all the marks together construct the watermark. The marks must not have a significant impact on the usefulness of the data and they should be placed in such a way that a malicious user cannot destroy them without making the data less useful.

Generally, the digital watermarking for integrity verification is called fragile watermarking as opposed to robust watermarking for copyright protection. In a robust watermarking scheme, the embedded watermark should be robust against attacks from removing or invalidating the watermark. However, the fragile watermarking scheme implies that the watermark should be fragile to modifications. Once the data is altered, the application can detect and localize the modifications. For example, the integrity of a database record can be controlled by means of a fragile watermark. If the watermarked record is edited, the watermark can not be verified, but the application can localize the modification. On the other hand, in relational database, any unauthorized modification can corrupt the trust of a specific range of tuples that hides a watermark inside.

The multimedia watermarking techniques discussed earlier always have similar domains to focus on. For example, audio frequency domain, pixel frequency domain, spatial/temporal domain. However, databases don't have such a patterns to follow. Therefore, we would discuss the difference between multimedia and database watermarking techniques:

- As we know a multimedia object consists of a large number of bits with considerable redundancy. Therefore, the watermarking can have a large of room to hide. However, a database consists of attributes, tuples, and relations. Each of them are objects and most or all bits of objects are likely meaningful. The watermarking method tries to insert watermark in these separate objects.
- For media files, they all have frequency or spatial/temporal domain and these attributes don't change in different media files. However, attributes consists dif-

ferent types of primitive objects and tuples in a relation constitute a set of attributes and there are no specific rules to follow.

- Portions of a multimedia object cannot be dropped or replaced without causing perceptual changes in the object. However, the modification of a relation can simply drop some tuples or substitute them with tuples from other relations without notice.
- For insertion of a watermark in the image or video, we use the techniques to transform image by various transforms we mentioned. However, applying these techniques to a database will produce errors in all of the attribute values, which might not be acceptable. Furthermore, such a watermark might not survive even minor updates to the relation.

Parameters Summary: For the design and implementation, we present the summary of the parameters of the studied integrity and watermarking techniques. Each relation or a tuple is a data object corresponding to an audio, image, video, binary signal, or a set of serialized records, or relational database tuples.

- 1) η – number of records in the relation
- 2) ν – number of attributes in the relation available for marking
- 3) ξ – number of least significant bits available for marking in an attribute
- 4) $1/\gamma$ – fraction of records marked
- 5) ω – number of records or tuples marked
- 6) α – significance level of the test for detecting a watermark
- 7) τ – minimum number of correctly marked tuples needed for detection
- 8) k_+ – a private key known only by the owner
- 9) $H(k, d)$ – the type of MAC hash/timestamp function for integrity, its optional key k , and data d

III. METHODOLOGY

This section presents the framework's software engineering design based on the studied methods, algorithms, and techniques. The design methodology is primarily based on the algorithms and their parameters presented earlier in Section II as well as a plug-in type of architecture for various components whose implementation can be easily replaced. Thus, the framework presents a collection of interfaces for all technique types (in this case integrity), followed by their generic and concrete implementations. For integrity-related algorithms please refer back to Section II as well as information in Figure 1 for Integrity Lock modification, audio frequency masking, watermark insertion and detection algorithms. The concrete implementations came from different open-source vendors and require adaptation to the framework, that's why a layer of abstraction is introduced to adapt the data between algorithm implementors and the framework. Further, to apply the framework to MARF and HSQLDB, concrete security adapters are designed to make use of the JDSF "injected" into the core storage management components of both MARF (`marf.Storage.StorageManager`) and

HSQLDB (`org.hsqldb.persist.Log`) where they make sure the data hits the storage other than the main memory.

A. Framework

1) *General Operation:* In Figure 2 is a general way the framework's particular adapters (e.g. for MARF and HSQLDB) write the security-enhanced data based on the security configuration options, set by the system administrator. The reading of the security-data is the reverse process.

```

1 Retrieve data;
2 if Privacy Required then
3   Encrypt/anonymize data;
4 end
5 if Authentication Required then
6   Add authentication information;
7 end
8 if Integrity Required then
9   Add integrity information;
10 end
11 if SQLrand Required then
12   Randomize SQL;
13 end
14 Write out data;
```

Fig. 2. Writing Data With Security Options.

2) *Design:* The typical MARF's packages were extended with the two new packages that constitute the JDSF: `database` and `marf.security`. In Figure 3 are the primary packages and classes that correspond to the studied aspects of integrity and authentication and the utility, storage, algorithms building blocks they rely upon.

The `marf.security.Configuration` class is populated from the configuration file `security.properties`, and is set by the system administrator. It represents the security options desired by a given instance of the framework-enhanced data management tool (e.g. MARF and HSQLDB).

The rest of the framework's backbone is captured by the main interfaces and generic classes, followed by concrete implementation and stub modules, and cryptographic algorithm providers. The interfaces allow external to JDSF plug-ins, provided by external, third parties to be able to extend and compare existing implementations if desired. The interfaces are:

- `IIntegrityModule` shown in Figure 5
- `IAlgorithmProvider` shown in Figure 6
- `ISecurityEnhancedObject` shown in Figure 4
- `ISecurityAdapter` shown in Figure 7

In the `marf.security.algorithms` there are implementations of well known cryptographic algorithms, such as CBC-DES, RSA, DSA, MD5, and SHA1. The actual implementations in Java were provided by open-source vendors, such as [29], [30], [31], [32], [33], [34]. Since these implementations have sometimes little in common, integrating it into the framework had to be abstracted by a common API of algorithm providers, so the rest of the framework does not depend on the vendors' API and can be replaced to use another implementation easier when desired.

The most complexity goes into implementation and integration of the framework into the actual data management tools, such as MARF and HSQLDB. For this we provide their specific adapters (see Figure 7): the first of them is called `marf.security.adapters.MARFSecurityAdapter` that extends MARF-specific storage management. The second one, for HSQLDB, is likewise referred to as `HSQLDBSecurityAdapter` in the `marf.security.adapters` package, which are there to be either “injected” into the original code wrapping storage management functions of the original tools to mandatory go through the security-enhanced API or act as stand-alone proxies. The replaced and/or extended modules exactly are `marf.Storage.StorageManager` for MARF and `org.hsqldb.persist.Log` for HSQLDB.

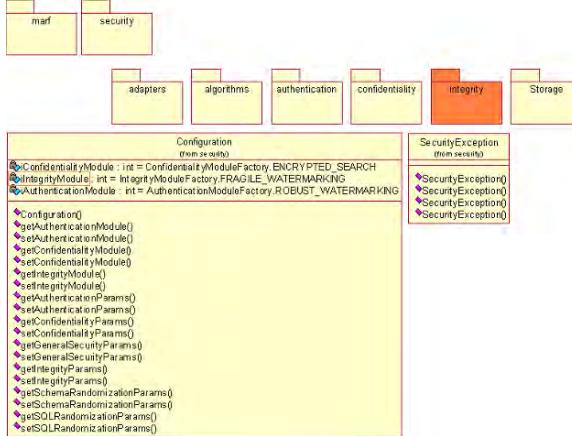


Fig. 3. `marf.security` Package.

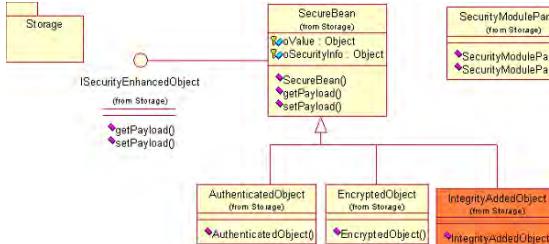


Fig. 4. `marf.security.Storage` Package and Classes.

IV. CONCLUSION

In the integrity aspect, we review the integrity lock architecture and four types of digital watermarking techniques, which are audio watermarking, image watermarking, video watermarking, and relational database watermarking. Moreover, we recite some of their methodologies and algorithms in some detail. The goal of our project is to construct a security environment for MARF and HSQLDB and then generalize it further. Since the MARF framework is primarily an audio recognition system, for integrity aspect, we can implement audio watermarking algorithms in audio file database system

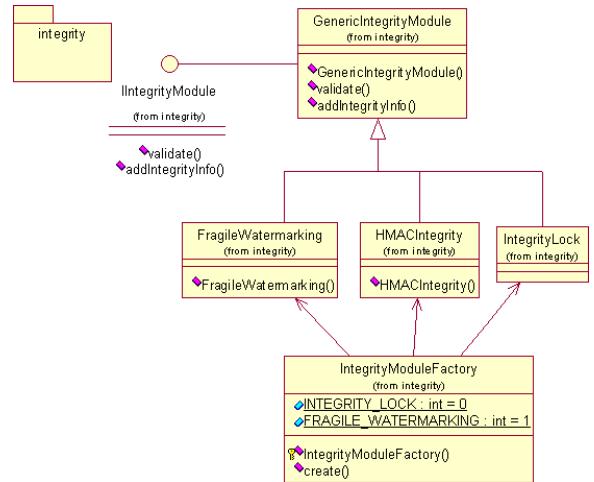


Fig. 5. `marf.security.integrity` Package and Classes.

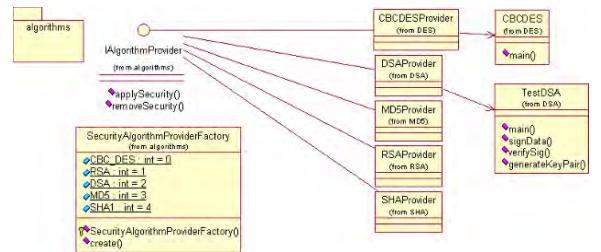


Fig. 6. `marf.security.algorithms` Package and Classes.

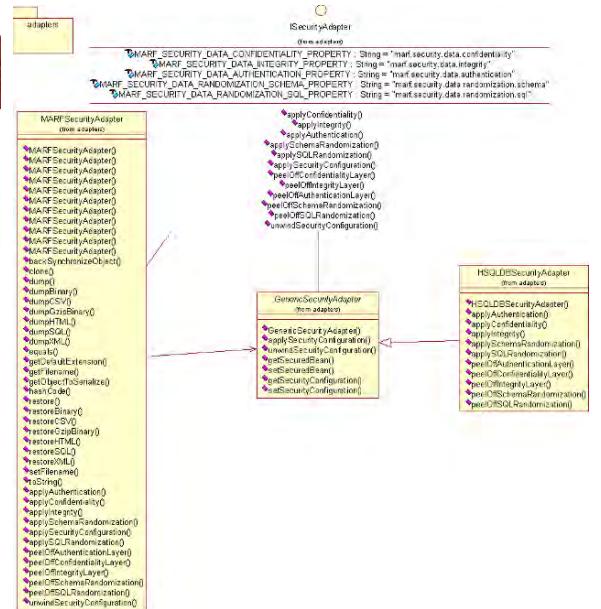


Fig. 7. `marf.security.adapters` Package and Classes.

and relational database watermarking to secure whole statistics and speaker identity attributes, tuples and relations in database.

The framework's operation was designed to allow addition of any number of algorithms or techniques as plugins for comparative studies as well as for integration into the existing systems. We extract parameters of algorithms to refine the design and implementation. The parameters and the configuration of the framework were made available from the survey and research study of the data and database security techniques presented earlier. It is also general enough to expand beyond MARF and HSQLDB, and as a result the open source community can benefit as a whole. JDSF, just like MARF and HSQLDB, is open source and is hosted at SourceForge.net under the umbrella of MARF, in its CVS repository.

V. FUTURE WORK

As a future work we plan on continuing our open-source development effort of the framework along with comprehensive testing suite and overhead statistics and new algorithm implementations and porting it to other systems that require the features provided by the framework, as studied e.g. in [35].

ACKNOWLEDGMENT

This research work was funded by the Faculty of Engineering and Computer Science of Concordia University, Montreal, Canada. We also would like to acknowledge Jian Li and Farid Rassai, database security researchers, open-source community, Drs. Joey Paquet and Mourad Debbabi, and Dr. Chadi Assi.

While implementing, integrating, and testing the framework, we resorted to open-source implementations of known cryptographic and otherwise algorithms, with due credit and citations given to their developers.

REFERENCES

- [1] S. Mokhov, I. Clement, S. Sinclair, and D. Nicolopoulos, "Modular Audio Recognition Framework," Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, 2002-2003, project report, <http://marf.sf.net>, last viewed April 2008.
- [2] The hsqldb Development Group, "HSQLDB – lightweight 100% Java SQL database engine v.1.8.0.10," hsqldb.org, 2001-2008, <http://hsqldb.org/>.
- [3] S. A. Mokhov, "Introducing MARF: a modular audio recognition framework and its applications for scientific and software engineering research," in *Advances in Computer and Information Sciences and Engineering*. University of Bridgeport, U.S.A.: Springer Netherlands, Dec. 2007, pp. 473–478, proceedings of CISSE/SCSS'07, cisse2007.org.
- [4] ——, "On design and implementation of distributed modular audio recognition framework: Requirements and specification design document," Department of Computer Science and Software Engineering, Concordia University, Montreal, Canada, Aug. 2006, project report, <http://marf.sf.net>, last viewed December 2008.
- [5] S. A. Mokhov, L. W. Huynh, and J. Li, "Managing distributed MARF's nodes with SNMP," in *Proceedings of PDPTA'2008*. Las Vegas, USA: CSREA Press, Aug. 2008, to appear.
- [6] S. A. Mokhov and R. Jayakumar, "Distributed modular audio recognition framework (DMARF) and its applications over web services," in *Proceedings of TeNe'08*. Springer, 2008, to appear.
- [7] S. A. Mokhov, "Choosing best algorithm combinations for speech processing tasks in machine learning using MARF," in *Proceedings of the 21st Canadian AI'08*, S. Bergler, Ed. Windsor, Ontario, Canada: Springer-Verlag, Berlin Heidelberg, May 2008, pp. 216–221, LNAI 5032.
- [8] ——, "Study of best algorithm combinations for speech processing tasks in machine learning using median vs. mean clusters in MARF," in *Proceedings of C3S2E'08*, B. C. Desai, Ed. Montreal, Quebec, Canada: ACM and BytePress, May 2008, pp. 29–43, ISBN 978-1-60558-101-9.
- [9] Sun Microsystems, Inc., "OpenOffice," [online], 2008, openoffice.org.
- [10] S. A. Mokhov, L. W. Huynh, J. Li, and F. Rassai, "A Java Data Security Framework (JDSF) for MARF and HSQLDB," Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada, Apr. 2007, project report. Hosted at <http://marf.sf.net>, last viewed April 2008.
- [11] ——, "A privacy framework within the java data security framework (JDSF): Design refinement, implementation, and statistics," in *Proceedings of the 12th World Multi-Conference on Systemics, Cybernetics and Informatics (WM-SCI'08)*, N. Callaos, W. Lesso, C. D. Zinn, J. Baralt, J. Boukachour, C. White, T. Marwala, and F. V. Nelwamondo, Eds., vol. V. Orlando, Florida, USA: IIIS, Jun. 2008, pp. 131–136.
- [12] S. A. Mokhov, F. Rassai, L. W. Huynh, and L. Wang, "The authentication framework within the java data security framework (JDSF): Design refinement and implementation," in *Proceedings of CISSE'08*. University of Bridgeport, CT, USA: Springer, Dec. 2008, to appear.
- [13] S. A. Mokhov, L. Wang, and J. Li, "Simple dynamic key management in SQL randomization," 2008, unpublished.
- [14] R. Chandramouli, N. Memon, and M. Rabbani, "Digital watermarking," 2002.
- [15] L. de C.T. Gomes, P. Cano, E. Gomez, M. Bonnet, and E. Batlle, "Audio watermarking and fingerprinting," 2002.
- [16] H.-C. Wu and H.-C. Lin, "Digital watermarking techniques," 2005.
- [17] R. Agrawal and J. Kiernan, "Watermarking relational database." IBM Almaden Research Center, 2002.
- [18] R. Sion, M. Atallah, and S. Prabhakar, "Rights protection for relational data," in *IEEE Transactions on Knowledge and Data Engineering*. IEEE Computer Society, 2004.
- [19] R. C. Dixon, *Spread Spectrum Systems*, 3rd ed. John Wiley and Sons, New York, 1994.
- [20] S. Haykin, *Digital Communications*. John Wiley and Sons, New York, 1988.
- [21] L. Boney, A. H. Tewfik, and K. N. Hamdy, "Digital watermarks for audio signals," in *International Conference on Multimedia Computing and Systems*, 1996, pp. 473–480.
- [22] R. A. Garcia, "Digital watermarking of audio signals using psychoacoustic auditory model and spread spectrum theory," in *107th Convention on Audio Engineering Society*, 1999.
- [23] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM System Journal*, vol. 35, pp. 313–336, 1996.
- [24] C. Neubauer and J. Herre, "Advanced audio watermarking and its application," in *109th Convention on Audio Engineering Society*, 2000.
- [25] J. Lacy, S. R. Quackenbush, A. Reibman, and J. H. Snyder, "Intellectual property protection systems and digital watermarking," in *Information Hiding (Proceedings of the Second International Workshop, IH'98)*, D. Aucsmith, Ed. Springer, LNCS 1525, Dec. 1998, pp. 158–168.
- [26] E. Zwicker and H. Fastl, *Psychoacoustics facts and models*. Springer-Verlag, Berlin, 1990.
- [27] L. Wang, "INSE691A: Database security and privacy, course notes," CI-ISE, Concordia University, 2007, <http://users.enes.concordia.ca/~wang/INSE691A.html>.
- [28] W. T. Polk and L. E. Bassham, *Security Issues in the Database Language SQL*. NIST, 1993, NIST Special Publication 800-8.
- [29] Unascribed, "CBC-DES Java implementation," [online], 2007.
- [30] J. O. Grabbe, "Java program for RSA encryption," [online], 2001, <http://www.laynetworks.com/rsa.java.txt>.
- [31] Unascribed, *Sign and Verify a DSA Signature*. java2s.com, 2004, <http://www.java2s.com/Code/Java/Security/VerifyaDSASignature.htm>.
- [32] Sun Microsystems, Inc., *Security Features in Java SE*. java.sun.com, 2007, <http://java.sun.com/docs/books/tutorial/security/index.html>.
- [33] S. Paavolainen and S. Ostermiller, *MD5 hash generator*. [ostermiller.org](http://ostermiller.org/utils/MD5.java.html), 2007, <http://ostermiller.org/utils/MD5.java.html>.
- [34] A. Andreu and M.-A. Laverdière, *SSHA Digest, Modified*. www.securitydocs.com, 2006, <http://www.securitydocs.com/library/3439>.
- [35] S. A. Mokhov, "Towards security hardening of scientific distributed demand-driven and pipelined computing systems," in *Proceedings of the 7th International Symposium on Parallel and Distributed Computing (ISPDC'08)*. Krakow, Poland: IEEE Computer Society Press, Jul. 2008, to appear, <http://ispdc2008.ipipan.waw.pl/>.

A Multi-layer GSM Network Design Model

Alexei Barbosa de Aguiar, Plácido Rogério Pinheiro,
Álvaro de Menezes S. Neto, Rebecca F. Pinheiro, Ruddy P. P. Cunha
Graduate Program in Applied Informatics, University of Fortaleza
Av. Washington Soares 1321, Sala J-30, Fortaleza, CE, Brazil, 60811-905

Abstract. GSM Network Designs usually offers big challenges for achieving an efficient cost while respecting the complex combinatorial technical constraints. This networks have hundred or thousands BTS. They have their traffic grouped in hubs, then in BSC nodes to reach the MSC. Hubs must be elected within the BTS set and BSC nodes have to be geographically allocated in the available sites. Also, the number and model of these BSC impact in the overall cost while the distances affect the transmission costs. This paper presents a mathematical model for designing a GSM network from the BTS lower layer until the MSC layer.

I. INTRODUCTION

A GSM mobile network is a very complex mix of equipments working on specific functions but in an integrated manner. These network elements are organized hierarchically.

Closer to the customers lays the BTS (Base Transceiver Station) equipments layer that is the first layer. They are responsible for interfacing the cell phones to the GSM network through radio frequency. These equipments use antennas on top of towers or buildings that are the most visible and known parts of the network by people in general. This layer is made of hundreds or thousands of equipments although each one is less expensive.

Depending on the traffic demand of a BTS its E1 link can waste its capacity. To avoid this undesirable behavior usually this equipments are shipped with units that allows cross connections between timeslots carried by E1 links. This is a very convenient resource to gather timeslots from E1 links of other BTS and carry them in fewer E1 links with better usage factor.

The elected BTS stations to group and cross connect timeslots from a set of BTS are called hubs. Hubs can be considered the second layer of the hierarchy, since it represents the first grouping function in the GSM network that increases the transmission efficiency.

Until the second layer, the timeslot handling is deterministic. It is dimensioned in a one-to-one fashion. One cell phone call uses one air voice channel timeslot in the Ater interface to the BTS. One Ater voice timeslot is associated to one sub-timeslot in the Abis

interface between BTS and BSC (Base Station Controller). Four sub-timeslots are grouped in one E1 timeslot in this Abis interface. The cross connection always preserves the internal structure of this timeslots. Therefore in a hub, the sum of all traffic timeslots from the grouped BTS side is equals to the sum of all traffic timeslots of the BSC side. There is no intelligence in this operation, only reorganization of the E1 links for better use of its capacities.

On the other side, the third layer, BSC equipments use the traffic statistical aspect to significantly reduce the number of channels need for carrying the total traffic. It is no more an one-to-one deterministic association. BSC is the first switch in the GSM network before entering in the network core. Telephony switches recalls the old switchboard that used to connect many subscribers lines to few trunk lines. The trunks are dimensioned based on the subscribers call amount and time period. Agner Krarup Erlang formulated a way of correlate the traffic (in Erlangs), the number of channels and the probability of blocking (also called grade of service or GoS). One of the most used equations to deal with telephony traffic is the Erlang B equation (1).

$$e_b = \frac{\frac{a^n}{n!}}{\sum_{i=0}^n \frac{a^i}{i!}} \quad (1)$$

where e_b is the probability of blocking, n is the number of resources (voice channels in this case) and a is the amount of offered traffic in Erlangs.

Although it is an effective way of reducing the transmission E1 lines to MSC, this equipment is significantly more expensive than a BTS.

The forth layer of a GSM network is composed by grouping up to tens of BSC in a MSC. MSC is a very complex and expensive switch that accumulates several tasks related to all telecommunication services. It integrates the core of the GSM network among other kind of equipments like HLR (Home Location

Register), EIR (Equipment Identity Register), SGSN (Serving GPRS Support Node) and others. These core equipments are out of the scope of this paper.

One significant part of a GSM network cost comes from the transmission lines. They do the duty of overcoming the distances. Hubs and switches purpose is increasing transmission efficiency and minimize this transmission cost. But one difficulty arises when a designer works on a GSM network: The search for the minimal cost design in a very complex combinational problem.

The designer have to elect BTS stations to have the hub function based on the BTS neighborhood. Distance is important in the cost but a large weight comes from the E1 lines from hub to BSC occupation rate. The BTS linked to a hub must sum time slots that maximize the E1 lines occupation rate, but each BTS has a particular time slot demand to be carried.

On the third layer, BSC also has to be allocated based on the geographical position that groups the total traffic of a set of BTS and links to MSC with a reduced amount of E1 lines. To turn the combinational problem even harder, BSC equipments have some different models with its respective traffic capacity and acquisition cost.

To address this combinational problem this work presents a mathematical model for designing a GSM network with multi-layers that respects the traffic demand and capacities, minimizing the total network cost over a time period of evaluation.

In Aguiar, Pinheiro and Rodrigues [3] a layer 2 model based on Kubat and Smith [6] and Kubat, Smith and Yum [7] is adapted to some scenarios of Brazilian mobile carriers. In Aguiar and Pinheiro [2] a layer 3 integer programming model [9] was developed to determine the association matrix between BTS and BSC, the geographical allocation of BSC nodes, The number and model of BSC and its trunk sizing based on the geographical location and traffic demand of the BTS. This work merges and expands this two isolated layer approaches in a multi-layer design of the GSM network. Ferreira, Pinheiro, Aguiar and Macambira [1] used Lagrangean Relaxation Method [4] to extend the boundaries for larger network problem instance. Rigolon, Pinheiro, Rodrigues, Macambira and Ferreira [8] extend this line of research with sub gradient methods.

Section II shows this mathematical model for the Multi-layer GSM Network Design. Afterwards section III describes the results for simulated networks problems instances. Section IV makes some considerations on the conclusion.

II. THE MODEL FOR THE MULTI-LAYER GSM NETWORK DESIGN

A. Sets

$T = \{t_1, t_2, \dots, t_m\}$	Set of BTS nodes
$H = \{h_1, h_2, \dots, h_q\}$	Set of HUB nodes
$B = \{b_1, b_2, \dots, b_n\}$	Set of BSC nodes
$W = \{w_1, w_2, \dots, w_o\}$	Set of BSC models
$C = \{c_1, c_2, \dots, c_p\}$	Set of link capacities

B. Decision Variables

u_{kc} Decision variables for choosing the capacity $c \in C$ of E1 lines trunk between BSC $k \in B$ and MSC r ;

v_{kw} Decision variables for BSC $k \in B$ model $w \in W$ choice;

x_{ijk} Decision variables for link allocation between BTS node $i \in T$, HUB node $j \in H$ and BSC node $k \in B$;

z_{jk} Decision variables for link dimensioning between HUB node $j \in H$ and BSC node $k \in B$;

C. Constants

ct_{ij} Link cost between BTS $i \in T$ and HUB $j \in H$ nodes in an analysis time period;

ch_{jk} Link cost between HUB $j \in H$ and BSC $k \in B$ nodes in an analysis time period;

cb_{kc} Link cost of capacity $c \in C$ between BSC node $k \in B$ and MSC r in an analysis time period;

cm_w BSC model $w \in W$ acquisition cost, considering an analysis time period;

ae_i BTS node $i \in T$ traffic demand in Erlangs;

at_i BTS node $i \in T$ traffic demand in timeslots;

f_c Capacity of link $c \in C$ in Erlangs;

b Capacity of one E1 link from HUB to BSC in timeslots;

e_w BSC model $w \in W$ traffic capacity in Erlangs;

D. Objective Function

The objective function (2) minimizes the HUB nodes, HUB and BSC nodes transmission cost, plus BSC acquisition total cost.

$$\min \sum_{i \in T} \sum_{j \in H} \sum_{k \in B} ct_{ij} x_{ijk} + \sum_{j \in H} \sum_{k \in B} ch_{jk} z_{jk}$$

$$+ \sum_{k \in B} \sum_{c \in C} cb_{kc} u_{kc} + \sum_{k \in B} \sum_{w \in W} cm_w v_{kw} \quad (2)$$

E. Constraints

These are the constraints adopted:

$$\sum_{j \in H} \sum_{k \in B} x_{ijk} = 1, \forall i \in T \quad (3)$$

(3) Each BTS must be connected to one and only one HUB.

$$\sum_{i \in T} \sum_{k \in B} at_i x_{ijk} \leq \sum_{k \in B} bz_{jk}, \forall j \in H \quad (4)$$

(4) Link dimensioning from HUB to BSC.

$$x_{ijk} \leq z_{jk}, \forall i \in T, \forall j \in H, \forall k \in B \quad (5)$$

(5) There must be no allocation through a hub candidate that has no link to a BSC.

$$\sum_{i \in T} \sum_{j \in H} ae_i x_{ijk} \leq \sum_{c \in C} f_c u_{kc}, \forall k \in B \quad (6)$$

(6) u_{kc} dimensioning that allows all BTS assigned to one BSC's traffic flow.

$$\sum_{i \in T} \sum_{j \in H} ae_i x_{ijk} \leq \sum_{w \in W} e_w v_{kw}, \forall k \in B \quad (7)$$

(7) BSC dimensioning accordingly to the given models and the total traffic demand.

$$\sum_{c \in C} u_{kc} \leq 1, \forall k \in B \quad (8)$$

(8) Only one trunk capacity can be chosen for one BSC.

$$u_{kc} \in \{0, 1\}, \forall k \in B, \forall c \in C$$

$$v_{kw} \in \{0, 1\}, \forall k \in B, \forall w \in W$$

$$x_{ijk} \in \{0, 1\}, \forall i \in T, \forall j \in H, \forall k \in B$$

$$z_{jk} \in \mathbb{Z}^+, \forall j \in H, \forall k \in B$$

III. COMPUTATIONAL RESULTS

A generator of problem instances was developed to study both individual networks particularities and size impacts. 10 instances of each size class were generated. This classes have the following number of BTS nodes: $\{5, 10, 15, 20, 25, 30, 35, 40\}$. For each instance this assumptions were taken: The transmission cost is a linear function of distance. The values are local market approximations. There is no price reduction based on the amount of E1 lines.

The geographical location of BTS sites is determined randomly with a configurable dispersion. Each BTS site is a candidate for hub and BSC allocation. In real networks, other site locations that have no BTS can be included for

candidates. The BTS traffic demand in timeslots is generated randomly from 3 to 10 timeslots that is the approximated value that an E1 line supports. The traffic demand in Erlangs is calculated from the number of voice channels that fits in the number of timeslots or a E1 line, with 2% of GoS. $C = \{0...40\}$ was adopted. There are three BSC models in the simulations with fictitious but reasonable capacity and costs. A small model with 512 Erlangs; a medium model with 1024 Erlangs and a large model with 2048 Erlangs of capacity. b used is equals to 31 timeslots.

These computational tests ran in an AMD Turion 1.8 MHz 64 bits processor with 1 GB of RAM memory. The model was implemented on Ilog OPL integrated environment with Cplex 10.0 solver library [5].

In Fig. 1 shows a solution for a problem instance with 30 BTS sites. In this solution we can see that there is many hubs concentrating the nearby traffic and linking to the BSC.

There are two BSC in the network to handle the traffic generated by subscribers that uses these BTS. They are represented by squares. A large model BSC was chosen to be allocated on the site of BTS 06 (on the right), since it has 21 BTS to deal with. On the other hand, a medium model BSC is allocated on the site of BTS 16 (on the left) because it works with only 9 BTS. Notice that the distance between BSC nodes and MSC (larger circle on top left) is small compared to the average distance of the other links. That happens because of the number of E1 links dimensioned. There is 9 E1 links for the larger BSC and 4 for the medium one, while links between BTS, hub and BSC sites are unitary. In this scenario the links costs increase linearly with the distance but is multiplied by the number of E1 links too.

Collected data from computational tests are resumed in tab. 1. Instance size refers to the number of BTS nodes handled by the problem instance, which affects directly the complexity in terms of memory and computational time expended.

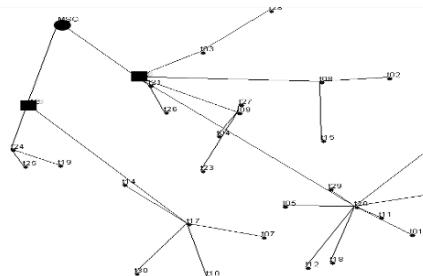


Fig. 1. Solution for 30 BTS sites.

Instance size (in BTS)	Variables	Constraints	Non-zero density	Average time (s)	Standard deviation
5	221	150	2,6998%	0,5785	0,3310
10	1241	1050	0,4866%	2,8915	1,8467
15	3811	3450	0,1585%	3,2500	1,8929
20	8681	8100	0,0695%	10,1820	8,5499
25	16601	15750	0,0363%	1314,339	1211,1110
30	28321	27150	0,0213%	1325,010	1294,9840
35	44591	43050	0,0135%	1080,436	478,6856
40	66161	64200	0,0091%	1363,216	832,9629

Tab. 1. Computational results.

Variables and constraints represent the columns and lines of the mathematical model matrix. Non-zero density is calculated as the ratio between the number of matrix coefficients that are not equals to zero and the total number of coefficients of that matrix.

Average time and standard deviation where used to describe statistically the amount of time elapsed to solve the problem instances of the integer programming model in seconds.

The elapsed time suffers a significant variation depending on the particular problem instance. Despite this fact, the average values tend to an exponential function due to Branch-and-bound algorithm [9].

IV. CONCLUSION AND FUTURE WORKS

The model works with effectiveness producing a GSM network from BTS to MSC as an integrated multi-layer design. The total cost of transmission links and BSC acquisition is reduced to the optimal value. It can be far beyond the human limited design in such exponential combinatory problem.

However, the complexity of the problem is such that the size of the handled networks is very limited compared to actual mobile carriers' networks. This is an issue that can be tackled by approximate methods.

A framework that hybridizes exact method and meta-heuristics has presented good results in expanding these boundaries in other classes of problems. Nepomuceno, Pinheiro and Coelho [10] used this framework to solve container loading problems. In the same problem category, Pinheiro and Coelho [11] presented a variation of the implementation to work with cutting problems.

We intend to overcome this challenge using this framework with some innovations aggregated in the future.

Other interesting contribution to this work is the possible incorporation of the layer 4, where the MSC allocation and sizing could be optimized together as a wider model.

ACKNOWLEDGMENT

Alexei gratefully acknowledges Capes for its financial supports through a M.Sc. scholarship.

REFERENCES

- [1] L. O. R. A. Ferreira, P. R. Pinheiro, A. B. de Aguiar, and E. M. Macambira. Design of cellular network using lagrangean relaxation algorithm. In Proceedings of International Conference on Computer, Communication and Control Technologies and The 9th International Conference on Information Systems Analysis and Synthesis. Orlando, 2003.
- [2] A. B. de Aguiar and P. R. Pinheiro. A Model for GSM Mobile Network Design, chapter Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, pages 365-368. Springer Netherlands, Dordrecht, September 2007.
- [3] A. B. de Aguiar, P. R. Pinheiro, and M. M. Rodrigues. Um modelo para telefonia celular. In Anais do XXXV Simpósio Brasileiro de Pesquisa Operacional. Instituto Doris Aragon, Rio de Janeiro, 2003.
- [4] M. L. Fisher. The lagrangian relaxation method for solving integer programming problems. Manage. Sci., 50(12 Supplement):1861-1871, 2004.
- [5] ILOG. ILOG CPLEX 10.0 User's Manual, January 2006.
- [6] P. Kubat and J. M. Smith. A multi-period network design problem for cellular telecommunication systems. European Journal of Operational Research, 134(2):439-456, October 2001.
- [7] P. Kubat, J. M. Smith, and C. Yum. Design of cellular networks with diversity and capacity constraints. IEEE Transactions on Reliability, 49(2):165-175, June 2000.
- [8] A. A. Rigolon, P. R. Pinheiro, M. M. Rodrigues, E. M. Macambira, and L. O. R. A. Ferreira. Relaxação lagrangeana com método de subgradiente aplicada no projeto de uma rede de telefonia móvel. In XXXVII Simpósio Brasileiro de Pesquisa Operacional (SBPO). Sociedade Brasileira de Pesquisa Operacional - Sobrapo, Sociedade Brasileira de Pesquisa Operacional - Sobrapo, September 2005.
- [9] L. A. Wolsey. Integer Programming. John Wiley & Sons, 1998.
- [10] N. V. Nepomuceno, P. R. Pinheiro, A. L. V. Coelho. Tackling the Container Loading Problem: A Hybrid Approach Based on Integer Linear Programming and Genetic Algorithms. Lecture Notes in Computer Science, v. 4446, p. 154-165, 2007.
- [11] N. V. Nepomuceno, P. R. Pinheiro, A. L. V. Coelho. A Hybrid Optimization Framework for Cutting and Packing Problems: Case Study on Constrained 2D Non-guillotine Cutting. In: C. Cotta and J. van Hemert. (Org.). Recent Advances in Evolutionary Computation for Combinatorial Optimization. Berlin / Heidelberg: Springer-Verlag, 2008, v. 153, p. 87-99.

Performance Analysis of Multi Carrier CDMA and DSCDMA on the basis of different users and Modulation scheme

Khalida Noori

Communication System Engineering

School of Electrical Engineering and Computer Sciences
Rawalpindi, Pakistan
khalida.noori@niit.edu.pk

Sami Ahmed Haider

Electrical Engineering Department
College of Signals
Rawalpindi, Pakistan
sami@mcs.edu.pk

Abstract

This paper analyze the comparison between the two CDMA techniques; Direct Sequence CDMA (DS-CDMA) and Multi-Carrier CDMA (MC-CDMA) systems. The objective is to evaluate these two multiple access techniques on the basis of different number of users and the different modulation schemes. Performance evaluation of the two systems is done on the basis of BERs Multipath Rayleigh fading and AWGN channel. The main intention of this paper is to identify advantages and disadvantages of MC-CDMA (Multi-Carrier Code Division Multiple Access) system in frequency selective Rayleigh fading channel. The paper deals with this issue and discusses it along with focusing on analysis of BER (bit error rate) of MC-CDMA system and comparing it with to BER of DS-CDMA system.

Introduction

Code division multiple-access (CDMA) is a mobile communications technique supporting multimedia services because it has its capability to provide higher capacity over conventional access schemes such as time-division multiple-access (TDMA) and frequency-division multiple-access (FDMA). There are various Pure and Hybrid CDMA techniques which are being used in 3G and 4G technologies[1- 2]. This paper will discuss the performance of two CDMA techniques: Direct Sequence CDMA (pure CDMA) and Multicarrier CDMA (hybrid CDMA).

In DS-CDMA just spreading is done and then the information is transmitted on a single carrier. In contrast MC-CDMA applies combination of DS-CDMA system and OFDM's multicarrier technique [3,4]. Both these systems are discussed in the following section. To have the real time effects on our transmitted signal multipath Rayleigh fading channel is used. To minimize the effects of Rayleigh fading different estimation algorithms are used at receiver side.

II. Direct spread CDMA system

In direct sequence code-division multiple access (DS-CDMA) system, the information data is transmitted after being spread with the help of spreading sequence as shown in Figure 1. The spreading is done by modulating the code signal by information signal. The code signal consists of a number of bits called "chips".To get the desired spreading of information signal, the chip rate must be much higher than the bit rate of information signal.

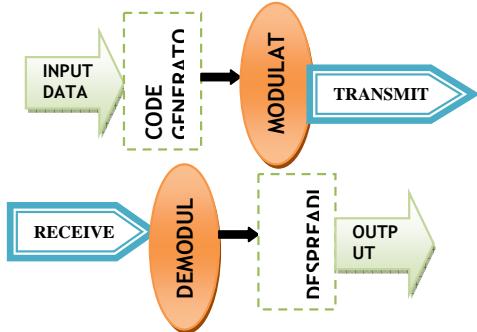


Figure 1: Block diagram of CDMA transceiver

III Multi carrier CDMA system

MC-CDMA combines the benefits of DS-CDMA with the natural robustness to frequency selectivity offered by orthogonal frequency-division multiplexing (OFDM) [5]..

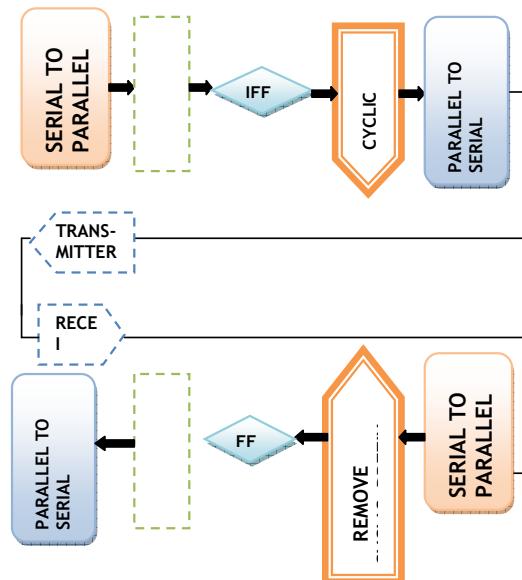


Figure 2: Block Diagram of MC CDMA system

The idea in OFDM was to divide the available bandwidth into a large number of small orthogonal bands or subcarriers each much smaller than the coherence bandwidth.

The inter-symbol interference (ISI) and inter-channel interference (ICI) in OFDM systems are reduced by the insertion of guard intervals. A central feature of OFDM is that it can take advantage of the Fast Fourier Transform (FFT) to translate the signal from the frequency to the time domain and otherwise [6]. The second component is DS-CDMA which has been discussed before.

IV. Simulation setup

DSCDMA System

On the transmitter side the input data taken is random binary numbers. Code of size 32 is used as a spreading sequence. The input data and code is then multiplied to spread the signal over large bandwidth. After that the signal is modulated. We have used four modulation techniques: BPSK, QPSK, 16-PSK and 32-PSK. The modulated signal is then passed through AWGN and Rayleigh channel to experience the effects of complete radio channel.

At the receiver side the received signal is demodulated using different modulation schemes and BER of input signal against received signal is plotted against different SNR's.

MC-CDMA System

On the transmitter side the input data is first divided into 2 channels i.e. converting it from serial to parallel. Each channel consists of 1 bit. After that each channel data is spread by multiplying with Hadamard code of length 4. The achieved signal in each channel is then modulated using different modulations and all channels data is summed together giving a single signal. Inverse fast Fourier transform IFFT is then taken and cyclic prefix is added. The length of cyclic prefix used is 2. After that the signal is passed through Rayleigh and AWGN channel having similar parameters as used in previous case. On the receiver side first the cyclic prefix is removed than FFT (fast Fourier transform) is taken. The signal is demodulated using different demodulation techniques and BER of input signal against received signal is plotted against different SNR's.

V. Simulation Results

We have compared both the systems on the basis of different modulation schemes number of user and code length. The reason for using the various modulation techniques in both the system is to compare which modulation technique gives lower bit error rate and suits both the systems the most. Performance of both systems has also been analyzed by changing the number of users and the length of Walsh code.

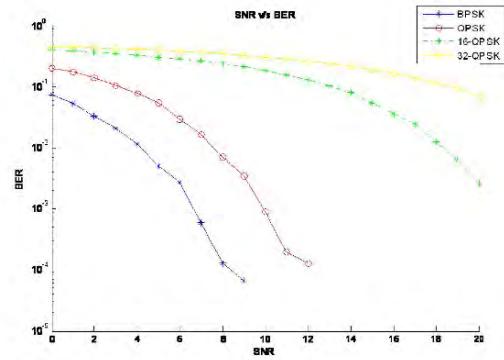


Figure 3: BER of DS CDMA system using different modulation Schemes

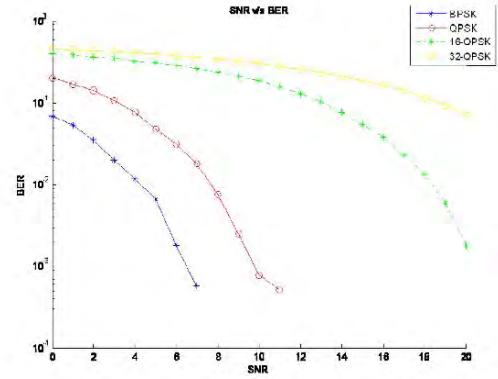


Figure 4: BER of MCCDMA system using different modulation Schemes

Two different length Hadamard codes are being used here: Hadamard 64 and Hadamard 128. Code of length 64 is used to first accommodate 30 users and then 60 users. The other code accommodates following different number of users: 30, 60, 90, and 120. After receiving the data its BER is plotted against different SNRs.

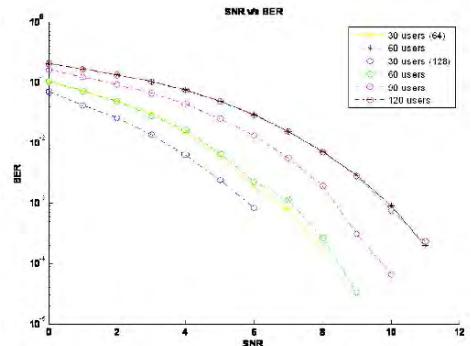


Figure 5: BER of DS CDMA on basis of different users

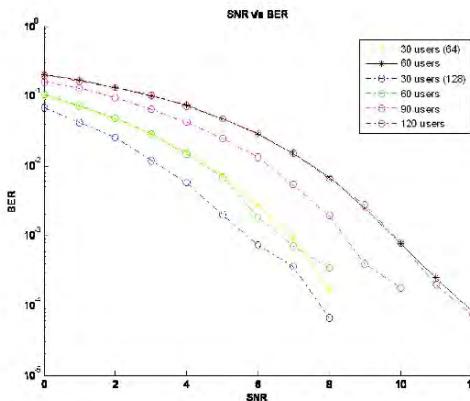


Figure 6: BER of MC-CDMA on basis of different users

VI. Conclusion

In this paper, we have discussed the advantages and disadvantages of MC-CDMA system, and analyze the performance of the two system using simulation results. Comparison between two schemes was done successfully in terms of multiple users, different modulations and code lengths. It was observed, when considered different modulation schemes the performance of MC-CDMA scheme was superior to DS-CDMA scheme and when talked in terms of multiple users or different code lengths for a particular modulation scheme the performance of both the system is approximately same.

MC-CDMA system has no major advantage over DSCDMA system in terms of required bandwidth, because the bandwidth of MC-CDMA signal spectrum is almost the same as that of DS-CDMA signal spectrum.

References

- [1] Ibars, C, Bar-Ness, Y "Analysis of time-frequency duality of MC and DS CDMA for multiantenna systems on highly time-varying and wideband channels", IEEE Transactions on Wireless Communication, Vol. 4, Issue 6, 2005, pp. 2661 - 2667
- [2] R. H. Khan, A. Hossain, R. Islam, Ju Bin Song, "SINR Performance of Multicarrier CDMA System in Frequency-Selective Rayleigh Fading Channels", International Conference on Information and Communication Technology, March 2007, pp. 201 – 204
- [3] Pingzhi Fan, "Multiple Access Technologies for Next Generation Mobile Communications", 6th International Conference on Telecommunications Proceedings, 2006, pp. P10 - P11
- [4] Shinsuke Hara, Ramjee Prasad, "Design and Performance of Multicarrier CDMA System in Frequency-Selective Rayleigh Fading Channels", IEEE Transactions on vehicular technology, vol. 48, no. 5, 1999
- [5] Peter O'Shea, Seedahmed S. Mahmoud, Zahir M. Hussain, "BER Performance of DS-CDMA System Over a Frequency Selective Multipath Rayleigh Fading Channel", RMIT University, Melbourne, Australia.
- [6] Khan, Razib Hayat; Ahsan, Abul; Haque, Mahmudul; Kabir, A.F.M. Sultanul; Hossen, Sakhawat, "MC-CDMA: An Alternative Multiple Access Technique in 3G Wireless Architecture", International Conference on Complex, Intelligent and Software Intensive Systems, 2008, pp. 573 - 578

Scalability Analysis of a Model for GSM Mobile Network Design

Rebecca F. Pinheiro, Alexei Barbosa de Aguiar, Plácido Rogério Pinheiro,
Álvaro de Menezes S. Neto, Ruddy P. P. Cunha, Domingos Neto
Graduate Program in Applied Informatics, University of Fortaleza
Av. Washington Soares 1321, Sala J-30, Fortaleza, CE, Brazil, 60811-905

Abstract - This work shows a scalability analysis of the mathematical model 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]. Other important contribution 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.

I. 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 focus 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 RF 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.

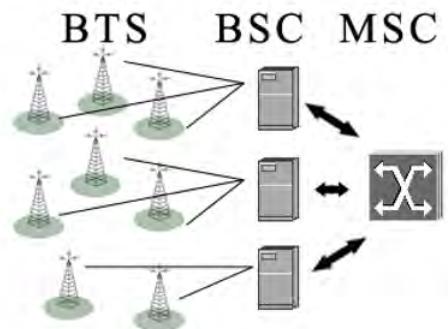


Fig. 1. Mobile Network Design

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, hotspots 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 allocated in a triangular grid pattern, where it is possible. This allocation 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 holds voice channels slots configured deterministically in a one-to-one basis with

BTS's radio channels slots. It is 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 is 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 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:

$$e_b = \frac{a^n}{\sum_{i=0}^n \frac{a^i}{i!}} \quad (1)$$

Where in (1) 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 bound 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 bound to the radio voice channel on demand, when a call is made. This feature raises 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. These lines waste 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 waste 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.

II. THE MATHEMATICAL PROGRAMMING MODEL

This is the proposed Integer Programming model [8].

 $T = \{t_1, t_2, t_3, \dots, t_m\}$ 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;

 Decision variables for link allocation between BTS node i and BSC node j;

 Decision variables for choosing the capacity c of E1 (2 Mbps) lines between BSC 1 and MSC;

 Decision variables for BSC 1 model w choice.

 Link cost between BTS i and BSC j nodes in an analysis time period;

 Link cost of capacity c between BSC 1 nodes and MSC in an analysis time period;

 BSC model w acquisition cost, considering an analysis time period;

 BTS i traffic demand in Erlangs;

 Link capacity c in Erlangs;

 BSC model w traffic capacity in Erlangs.

A. 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.

$$(1) \text{minimize} \sum_{i \in T} \sum_{j \in B} ct_{ij} x_{ij} + \sum_{l \in B} \sum_{c \in C} cm_{lc} y_{lc} + \sum_{d \in B} \sum_{k \in W} cb_k z_{dk}$$

B. 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  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.

$$(4) \sum_{i \in T} x_{ij} a_i \leq \sum_{k \in W} e_k z_{jk}, \quad \forall j \in B$$

$$(5) x_{ij} \in \{0,1\}, \quad \forall i \in T \quad \forall j \in B$$

$$(6) y_{lc} \in \{0,1\} \quad \forall l \in B \quad \forall c \in C$$

$$(7) z_{lw} \in \{0,1\} \quad \forall l \in B \quad \forall k \in W$$

III. 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 average 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 the allocation of the needed BSC will be.

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.

IV. COMPUTATIONAL RESULTS

Simulations were made with many network sizes. The bigger network sizes that could be solved in a reasonable time has about 50 sites. The different generated data caused big differences in the solving time. For instance: The smaller time for 50 sites with 3201 integer variables and 150 restrictions was 42 seconds and 4 hundredths of a second, 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 were 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.

OPL integrated modeling environment and Cplex 10.0 solver library [9] from Ilog Inc. were 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 ran in a 64 bits Intel Core 2 Quad processor with 2.4 GHz clock and 4 GB of RAM memory.

Despite the fact that 50 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 take account, since the amount of E1 lines was greater than one.

$$y = 0,851e^{0,244x} \quad (8)$$

20 instances were used with 5, 10, 15, 20, 25, 30, 35, 40 45 and 50 sites, with randomly generated data. The results are shown in table 1.

TABLE 1
CHARACTERIZATION OF THE

BT S	Var.	Const.	Density	Avg. Time	Std. Deviat.
5	96	15	9,72%	50,0	12,773
10	241	30	5,95%	40,0	8,208
15	436	45	4,43%	332,0	28,802
20	681	60	3,57%	853,5	86,418
25	976	75	3,01%	3561,5	371,594
30	1321	90	2,60%	19689,0	2872,227
35	1716	105	2,29%	46287,5	4890,274
40	2161	120	2,05%	600431,1	80263,118
45	2656	135	1,86%	363032,5	44981,655
50	3201	150	1,70%	752724,0	87873,235

INSTANCES USED IN THE EXPERIMENTS

V. SCALABILITY ANALYSIS

Due to the wide range of random generated values the problem instances have a very high complexity variation. Thus, there were problem instances with 40 BTS that could not be solved within a reasonable time threshold. Some times the solver crashed because of memory lack. But, for the same reason, there are problems instances larger than 50 BTS that can be solved in a time interval even smaller than some particular instances of 40 BTS.

The proposed model here is an Integer Programming one. This class of model requires an algorithm like Branch-and-bound , Branch-and-cut or others. This sort of algorithms have an exponential complexity. This fact limits the larger instance size that can be handled.

Actual networks often have hundred of BTS that is far beyond the range of this exact method. Aguiar and Pinheiro [13] used Lingo solver library and it was not able to handle problem instances larger than 40 BTS. The adoption of Cplex [9] expanded this boundary to 50 BTS, but it remains too small.

A mean squares non-linear regression of the average times was made to determine the observed asymptotic complexity function. It is shown on equation 8 and fig. 2.

BIBLIOGRAPHICAL REFERENCES

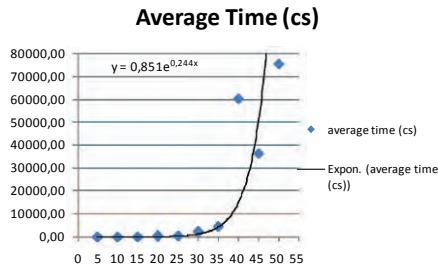


Fig. 2. Average time versus instance size

The key to break this limitation and turn big network designs feasible is to use approximate approaches. Some methodologies like Lagrangean relaxation in Simple Subgradient, Bundle Methods and Space Dilatation Methods (Shor *et al* [6, 7]) can be used. Rigolon *et al* [3] shows that the use of this tool in the first model extends the size of the mobile network to be designed.

A framework that hybridizes exact method and meta-heuristics has presented good results in expanding these boundaries in other classes of problems. Nepomuceno, Pinheiro and Coelho [11] used this framework to solve container loading problems. In the same problem category, Pinheiro and Coelho [12] presented a variation of the implementation to work with cutting problems.

VII. 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. The scalability analysis was made and some conclusions were 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.

[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.

[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.

[9] ILOG. ILOG CPLEX 10.0 User's Manual, January 2006.

[10] Shrage, L., Optimization Modeling with Lingo. Lindo Systems Inc., 1998.

[11] N. V. Nepomuceno, P. R. Pinheiro, A. L. V. Coelho. Tackling the Container Loading Problem: A Hybrid Approach Based on Integer Linear Programming and Genetic Algorithms. Lecture Notes in Computer Science, v. 4446, p. 154-165, 2007.

[12] N. V. Nepomuceno, P. R. Pinheiro, A. L. V. Coelho. A Hybrid Optimization Framework for Cutting and Packing Problems: Case Study on Constrained 2D Non-guillotine Cutting. In: C. Cotta and J. van Hemert. (Org.). Recent Advances in Evolutionary Computation for Combinatorial Optimization. Berlin / Heidelberg: Springer-Verlag, 2008, v. 153, p. 87-99.

[13] A. B. de Aguiar and P. R. Pinheiro. A Model for GSM Mobile Network Design, chapter Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, pages 365-368. Springer Netherlands, Dordrecht, September 2007.

Location Management in 4G Wireless Heterogeneous Networks using Mobile Data Mining Techniques

Sherif Rashad

Mathematics and Computer Science Department
Morehead State University
Morehead, KY 40351
s.rashad@morehead-st.edu

Abstract—The design of the location management technique aims to reduce the signaling overhead in the mobile networks and to deliver the calls correctly. None of the current location management techniques have been designed for the new structure of 4G wireless heterogeneous networks (WHN). In this paper, we propose and evaluate a new location management technique (LM-WHN) for 4G WHN using data mining technology. Multidimensional sequence mining techniques are used in this to extract the mobility patterns of the mobile users. The new location management technique uses these patterns to predict the location of the mobile users inside the 4G WHN. This helps to reduce the communication overhead that is required to determine the location of the mobile users. Data mining tasks in the proposed technique are distributed between the mobile handsets (MHs) in the 4G WHN. Simulation was conducted to evaluate the performance of the posed location management technique and to compare its performance with other techniques. Simulation results show that we can predict the user locations with high accuracy using the proposed technique. Also simulation results show that the delay in the proposed technique is slightly higher than the delay in the non-predictive location management technique

I. INTRODUCTION

It is expected that the fourth generation (4G) mobile networks will support more multimedia communications and provide mobile services every time and everywhere. Location management enables mobile networks to track the locations of the mobile users between consecutive communications [18-20]. The future mobile communication networks will be integrated with heterogeneous access methods and various kinds of cells. This can be accomplished by integrating several radio access networks (RANs) (such as cellular networks (2G, 3G, etc.) and Wireless LAN (WLAN)) in developing what is called “wireless heterogeneous networks” (WHN). Accordingly, effective location management is required to determine the location of mobile terminals in the new heterogeneous system.

Location management in mobile networks consists of two basic operations [2]: locations updating (or location registration) and paging (or search). Location updating procedure provides the network with initial information about the mobile handset (MH) location (i.e. the location

area where the MH is found). Since the mobile users are free to move within the coverage area, the network can only maintain the approximate location of each user [2]. When a connection needs to be established for a certain user, the network has to determine the exact location of the mobile user inside the coverage area. Paging procedure is used to determine the exact location information about the mobile user (i.e. the Base Station to which the subscriber is connected in a specified location area.) [1].

There is a trade-off between the costs for location updating and paging [1]. If the mobile terminals update its location whenever it crosses a cell boundary, the network can maintain its precise location, thus obviating the need for paging. But, the cost for location updating will be very high. On the other hand, if the mobile terminal does not perform location updating frequently, a large coverage area has to be paged when a call arrives to determine the location of the called user and the cost for paging will be very high. Thus, the basic problem of location management is to develop an algorithm that can be used to minimize the overall cost of location updating and paging.

The problem of location management will be more complex in WHN because different types of radio access networks (RANs) have different interfaces and different capabilities [15]. Managing the location of the mobile users in WHN is important to complete the communication between different RANs. This is also one of the important and hot research problems for the next generation of mobile networks. Most of the existing location management techniques that have been proposed by researchers in this area deal with a single RAN and none of these schemes was designed for multiple RANs as in the WHN.

The current location management techniques that can be applied in single RAN [17-20] are also inefficiently in the case of the mobile terminals are moving between the same location areas during day periods. For example, if the subscriber movements are done according to his life habits such as work, study, travel, visiting, etc., then using the current location management technique will produce unnecessary overhead due to the movement between the locations which could be known with less cost. The new researches are interested in introducing new methods for location management, which attempt to reduce the overhead traffic. In [3, 4], techniques which make use of location areas

(LAs) and paging areas (PAs) of different sizes are introduced. In these techniques a LA is divided into several PAs. In [5, 6, 18] various database architectures are proposed with the aim of organizing the database. In [7] the multilayer concept is introduced. In this method, there are groups of MHs and each MH is assigned to a given group, and each group is assigned one or several layers of LAs. The method proposed in [8] uses a process which predicts the movements of the MH according to its direction of movement, velocity, and so on. Processing and prediction are made at both the MH and the HLR. When actual movements of the MH do not fit with those predicted, a registration is triggered by the mobile to inform the network of its actual location. Otherwise, no exchange is required, which allows savings in LU processing and signaling. In [9, 10, 20], the alternative strategy (AS) is introduced. Its main goal is to reduce the location updates by taking advantage of users' highly predictable patterns. In this AS, the system handles a profile recording the most probable LAs patterns of each user. The profile of the user which contains the visited LAs can be provided and updated manually. When the user receives a call the system pages him sequentially over the LAs until getting an acknowledgment from the mobile. The main savings allowed by this method are due to the non-triggered LUs when the user keeps moving inside his profile LAs. In [11], a technique similar to AS is defined. It is called Statistical Paging Area Selection (SPAS) and is based on location statistics collected by each MH, which periodically reports them to the network. These statistics consist of a list of the average duration the MH has been located in each LA. A priority rule is determined to settle the sequence of LAs visited by the mobile. If this sequence is different from the last one reported to the network, the MH transmits it; otherwise, nothing is done. The paging process is achieved in the same way as in AS. A variant of this method, called the Two-Location Algorithm (TLA), is proposed and studied in [12]. In this strategy, a mobile stores the two most recently visited LA addresses. The same is done at the HLR level. Obviously, the main advantage of this method relies on the reduction of LUs when a mobile goes back and forth between two LAs.

The goal of our research is to develop a new predictive location management technique for WHN (LM-WHN) that integrates cellular networks and WLANs. LM-WHN takes into account the different characteristics of the cellular networks and the WLANs. Data mining technology are used in this technique to predict the location of mobile users. This will be done by using the spatial and temporal information of the mobile users to predict the mobility profiles. A data mining technique called MobilePrefixSpan [16] is used in the proposed WHN to build these mobility profiles.

II. ARCHITECTURE OF 4G MOBILE COMMUNICATION SYSTEMS SUPPORTED BY LM-WHN

The architecture of the proposed heterogeneous wireless networks includes WLANs and cellular networks and

assumes an All-IP based. All-IP wireless and mobile networks represent the convergence of two key technologies: Internet and wireless cellular systems [16]. The core IP network will serve as the backbone network with internet connectivity and packet data services [1, 2, 7].

The architecture of the proposed wireless heterogeneous network is shown in Fig. 1. As we can see, there are four basic components of the proposed architecture: 1) Base Stations, 2) Access Points, 3) Mobile Hosts, and 4) IP Core Network. The WLAN access points (APs) represent the fixed communication points for the WLAN while the base stations (BSs) represent the fixed communication points for the cellular networks. Mobile hosts (MHs) are supposed to be designed to work in two different modes: dual-mode and single-mode. Dual-mode mobile hosts will be able to support services provided by WLANs and cellular networks while single-mode mobile hosts will support only one type of mobile technology. The proposed WHN will be able to support dual mode mobile hosts as well as single-mode mobile hosts.

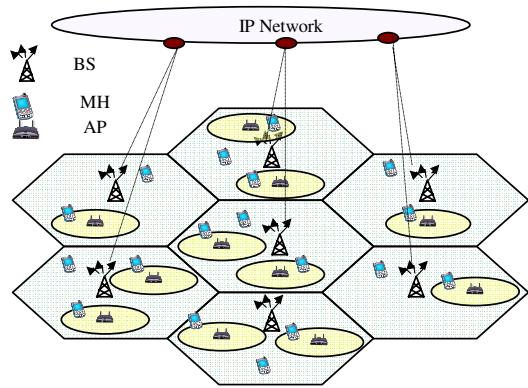


Fig. 1 Architecture of Proposed Wireless Heterogeneous Networks

By design, cellular networks are aimed at users with high mobility and low connection rates while WLAN networks are aimed at users with low mobility and high connection rates. The configuration of the wireless heterogeneous networks will be based on the connectivity to IP networks. The advantages of using IP as a core network protocol are:

- Internet connectivity
- Efficient transmission of IP packets,
- Co-existence with other access systems
- Ease of system introduction and expandability.
- IP networks can also connect with or accommodate wireless access systems other than 4G systems.
- Providing better security requirements.

The MH will be able to communicate with one BS/AP according to the coverage area and its mode of communications. The connection can be handed off from one AP to another AP (or from BS to another BS), and this called *horizontal handoff*. The connection can also be handed off from WLAN to cellular networks or vice versa and this is called *vertical handoff*. In our system model, we can have several WLANs inside the same cell but they do not have overlapped coverage. So the mobile user at every moment has the following possibilities of coverage:

- Covered by cellular network only
- Covered by cellular network and WLAN.

III. MOBILE DATA MINING TECHNIQUE

Data mining is the search for new, valuable, and nontrivial information in large volume of data. There goal of applying data mining techniques in the location management problem is to predict the mobility patterns. This will help to reduce the overall cost of location updating and paging. The key here is how we can effectively record and analyze the previous behavior of mobile users to generate these mobility profiles.

The proposed LM-WHN technique is mainly based on generating users' mobility profiles using a sequence mining technique called MobilePrefixSpan [16]. The mobility profiles are generated individually for each user by his/her MH. The MH will have the responsibility to collect the mobility data of its user. This data is used to build the mobility profile of the user and is continually updated based on its users' movements.

A. Data Collected by Mobile Host

The data collected by the MH is used to build the local mobility model that can describe the behavior of mobile users for a period of time. The data items collected for this model is shown in Table 1, where:

L_i : represents the ID of the current visited cell or access point as shown below.

VST_i : represents the time stamp when this MH enters L_i

VET_i : represents the time stamp when this MH exits L_i

W_i : a binary value describes if the information was recorded during the weekend or not. We will use the letter Y if it was on a weekend day, otherwise we use the letter N (this means $W_i \in \{Y, N\}$).

Table 1 Data Collected by the MH

Visited BS/AP	Visit Start Time	Visit End Time	Is this on Weekend?
L_1	VST_1	VET_1	W_1
L_2	VST_2	VET_2	W_2
...
L_n	VST_n	VET_n	W_n

Note that a new record will start if the mobile user enters a new BS/AP or if the current type of service is changed. The type of service can be "idle" if the mobile phone was not communicating at the time of data recording. Also, note that

the day at which this service was accessed (weekend or not) is included as an important factor. We believe that the behavior of the users is totally different during the weekends. To generate the mobility paths, it is necessary to transform the collected data from Table 1 at the MH into a sequence of symbols, where each symbol represents BS/AP. Every path is composed of a sequence of BS/AP IDs for each recorded visit. In addition, each path also contains the information regarding the duration of MH stay in a cell. This is achieved by collecting mobility data of a MH at fixed time slots Δt . For example if $\Delta t = 2$ minutes, this means that movements data are collected every two minutes. In this case, the time between movements is included in the generated sequence of movements. This information is used to estimate the time at which the user will move from one location to another.

Any generated path P_{MH} can be represented as:

$$P_{MH} = \langle L_1 \ L_2 \ \dots \ L_n \rangle$$

where $L_i \in \{B \cup A\}$

$$B=\{C_1, C_2, \dots, C_m\} \text{ and } A=\{P_1, P_2, \dots, P_k\}$$

and

C_i : is a cell ID.

B : is the set of all cells IDs in the system.

P_j : is an access point ID.

A : is the set of all access points IDs in the system.

B. Building Mobility Patterns

A data mining technique, called MobilePrefixSpan, which we have developed to analyze the information collected from the mobile users will be used to build mobility patterns. MobilePrefixSpan technique (which is shown in Fig. 2) is a modified version of the well-known Prefix-Span [21, 22] sequence mining technique and its modified version for multidimensional sequences UNISEQ [23].

0. Prepare the multidimensional sequences and convert the problem to one-dimensional sequence mining.
1. Apply the first scan to find all of the single-item frequent sequences (prefix).
2. Find the projected dataset corresponding to the single-item frequent sequences.
3. We continue by finding out the single-item frequent sequences in each projected dataset.
4. Find the frequent sequences using this prefix:
 - If the items represent BSs or APs, then consider the consecutive order.
 - Otherwise consider the order only.
5. Record the frequent sequences that have been found using this prefix.
6. Use each of these recorded frequent sequences as a prefix to find its projected dataset.
7. Repeat steps from 4 to 7 until we find all sequential patterns.

Fig. 2 MobilePrefixSpan Algorithm

The goal of MobilePrefixSpan technique is to extract the movement patterns of the mobile users using the collected information. There are two types of user information collected for generating the mobility patterns:

- Spatial Information: this indicates the location of the mobile user at every recording time. This information is collected by recording the ID of BS and AP.
- Temporal Information: indicates the time and the day information collected during the navigation of the mobile users. We divide the day into several intervals.

The detailed steps of MobilePrefixSpan algorithm are explained in [24] with the help of an example.

IV. LOCATION MANAGEMENT TECHNIQUE (LM-WHN)

A. Location Updating Procedure

The location updating will be made into two levels. The first level is at the stored mobility profile in the MH. And the second level is at the database of the BS or AP in the network. The updating of the stored data profile in the MH will be done by updating the collected data. The important thing here is to know the BS or AP that will be deleted from this profile, these nodes are called the expired nodes. The registered BS or AP will be considered as an expired node if the mobile user did not use connect through it during a certain period of operation. These expired nodes will be replaced with new nodes, which will be determined from the user mobility profile generated in the MH. The sequence mining software installed on the MH can analyze the collected data stored in MH and make its processes on it to build the user mobility profile. This profile will be sent to the database of the visitor location register (VLR) where the user is most probably to be found within nodes in that VLR region. These VLR will be in the BS or AP nodes. The address of this VLR is sent to home location register (HLR) in the IP core network. Here, the profiles of the users will be distributed in the several VLRs in the network and the corresponding addresses of these VLRs for the users will be stored in the HLR. Hence, the user profile was updated. This updating process can be initiated after a specified number of movements for each user or after a specified time interval. If the MH enters a new LA (where the location area will be a set of BS and AP Nodes), then the location updating will be done immediately and this new location will be added to the user profile.

B. Paging and Incoming Call Procedure

In the case of the incoming call, paging will be performed to determine the exact location (BS or AP) of the mobile user. The incoming call procedure can be described in the following steps:

- The calling MH will send a message through the current BS or AP to obtain the location of the dialed MH.
- The message will be forwarded to the database at HLR which contains the address of the VLR database where the user profile of the called user is stored.

- The control software at the VLR database will determine the current parameters of the time and the day according to the time of calling.
- Then the location nodes (BS or AP) with highest probability corresponding to this called user will be obtained from the stored mobility profile according to the current parameters.
- The paging (search) process will start by sending messages to these location nodes. If the MH is not found at these location nodes, then we page the next set of location nodes according to the mobility profile. We continue to do this until one of the paged nodes will answer. At this point, the connection can be started between the two MHs.

V. EVALUATION OF THE PROPOSED TECHNIQUE

The evaluation of the proposed LM-WHN technique is based on the total cost of the location updating (LU) and paging (P). This evaluation is mainly depends on the cost formulation used in [13]. This cost formulation for the location management consists of two parts: *location updating cost* (C_{LU}) and *paging cost* (C_P). Each of these two parts will include the *network cost* (messages cost for signaling) and *database cost (required to access the database)*. The database cost consists of the following two types of costs:

- D_h : The cost of accessing the Home Location Register (HLR).
 - D_v : The cost of accessing the Visitor Location Register (VLR).
- The network cost consists of the following two types of costs:
- N_f : The cost of sending a message through the fixed network(wired).
 - N_w : The cost of sending a message through the wireless network.

Using the cost of the location updating and the cost of paging, the total cost for LM-WHN (C_{LM-WHN}) technique can be calculated as:

$$C_{LM-WHN} = \lambda_{lu} C_{LU} + \lambda_c C_P$$

Where λ_{lu} is the location updating rate (location updates/sec) and λ_c is the call arrival rate in the WHN (calls/sec).

Simulation is used to evaluate the performance of the proposed LM-WHN technique. The call to mobility ratio (*CMR*) is used as an important parameter in our simulation. This parameter determines the ratio between the number of incoming calls and the number of movements between BSs/APs. This parameter will be in the range from 0.25 to 2. The performance of the proposed LM-WHN technique in terms of total cost will be compared with a Benchmark technique which will have the same location management technique with important assumption that the prediction is

perfect. This means that for the Benchmark technique, we know exactly what will be current BS/AP for every MH in the network.

A. Experimental Results

The simulation was conducted to evaluate the performance of the LM-WHN technique and compare its performance with the Benchmark technique. Benchmark technique is based on the same LM technique and it assumes that the prediction is perfect. For the Benchmark technique, we know exactly what will be the next path for every user, and what will be the exact handoff time. This will enable us to compare the performance of the proposed LM-WHN with the best approach. The results are shown in Fig. 3. Here we can see that the LM-WHN have an acceptable performance compared to the performance of the benchmark technique. This means that using the LM-WHN we can predict the mobility of the users with high accuracy comparing to the Benchmark. This is because using the LM-WHN techniques allows us to predict the location of the BS/AP with high accuracy.

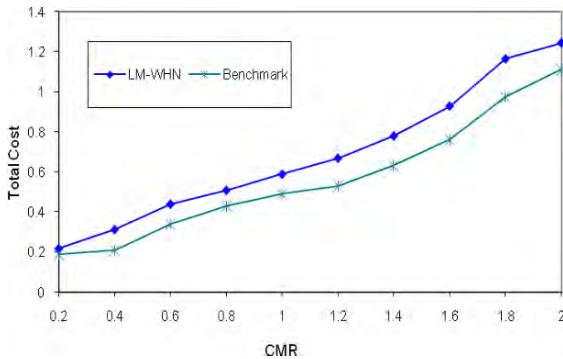


Fig. 3 Total cost for LM-WHN and Benchmark techniques

Also, the simulation was conducted to compare the performance of the LM-WHN with the performance of the traditional location area based location management technique (LM-LA) where we update the location with every movement between location areas. LM-LA is a non-predictive technique. This will help us to see the effect of the prediction in the proposed LM-WHN technique. The results are shown in Fig. 4. Here we can see that the LM-WHN have a significantly better performance compared to the performance of the LM-LA technique. This means that using LM-WHN reduces the communication signals that are required to update the location. The cost required for location updates and paging signals have been reduced significantly. The high accuracy prediction in LM-WHN techniques helps to determine the correct location of mobile users with less communication signals which reduces the overall cost.

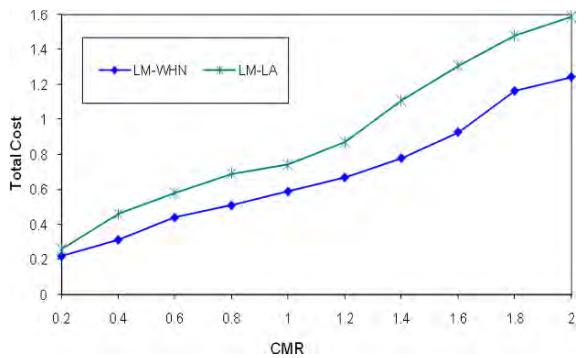


Fig. 4 Total cost for LM-WHN and LM-LA techniques

To handle the incoming calls, we need to search the MH (by paging the BS/AP) to determine its location, so there will be a delay for incoming calls which is required to search the MH. We calculate it as a normalized value with respect to corresponding LM-LA value. Simulation was conducted to study the effect of the delay on the proposed technique. The results are shown in Fig. 5. The delay in the proposed technique is slightly higher than that of the delay in LM-LA technique as shown in Fig. 5. This is because we use a sequential paging for the BS/AP. This delay is acceptable and can be reduced in future by enhancing the prediction accuracy of the proposed technique.

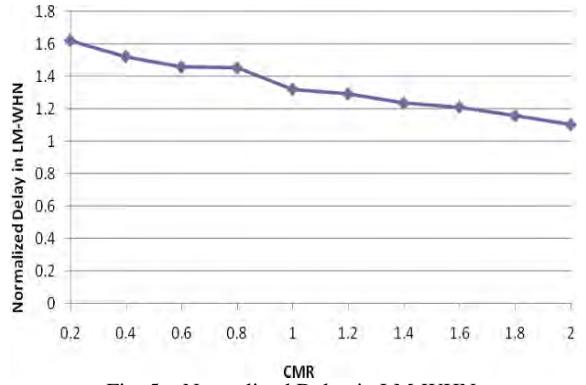


Fig. 5 Normalized Delay in LM-WHN

VI. CONCLUSION AND FUTURE WORK

Location management techniques aim to reduce the signaling overhead in the mobile networks and to deliver the calls correctly. The main objective of this research is to solve the problem of location management in the fourth generation (4G) of wireless mobile networks using predictive data mining techniques. In this paper, we proposed and evaluated a new location management technique for 4G wireless heterogeneous networks (LM-WHN) using mobile data mining technology. The new location management technique utilizes the mobility patterns of mobile users to predict their location inside the 4G WHN. Mobile Data mining tasks in the proposed technique are distributed between mobile handsets. Simulation was used in this project to evaluate the

performance of the proposed location management technique. Simulation results show that the proposed predictive technique (LM-WHN) has better performance compared to the non-predictive location management technique. Also the performance of the LM-WHN technique was compared to the Benchmark technique. Simulation results show that we can predict the user mobility with high accuracy using the proposed LM-WHN technique. Also simulation results show that the delay in the proposed technique is slightly higher than the delay in the non-predictive location management technique. This is because we use a sequential paging for the BS/AP. This delay is acceptable and can be reduced in future by enhancing the prediction accuracy of the proposed technique.

Future work includes enhancing the prediction accuracy by adding new mobility parameters such as the speed and the direction of mobility. Also, similar location management techniques can be developed for integrated WLAN, Ad-hoc networks, and cellular networks.

REFERENCES

- [1] Igor Brusic, Vesna Hassler and Wolfgang Lugmayr, "Deployment of Mobile Agents in the Mobile Telephone Network Management", Proceedings of the 33rd Hawaii International Conference on System Sciences - 2000.
- [2] Tabbane, S., "Location Management Methods for Third-Generation Mobile Systems", IEEE Communication Magazine, August 1997, pp. 72-84.
- [3] D. Plassmann, "Location Management for MBS," Proc. IEEE VTC, Stockholm, Sweden, June 8-10, 1994, pp. 649-53.
- [4] D. Goodman, P. Krishnan, and B. Sugla, "Design and Evaluation of Paging Strategies for Personal Communications," Wksp. Multiaccess, Mobility and Teletraffic for Pers. Commun., Paris, France, May 1996.
- [5] N. and S. Tabbane, "Database Architectures and Location Strategies for Mobility Management in Mobile Radio Systems," Proc. Wksp. Multiaccess, Mobility and Teletraffic for Pers. Commun., Paris, France, May 1996.
- [6] D. C. C. Wang, "A Survey of Number Mobility Techniques for PCS," Proc. IEEE Int'l. Conf. Pers. Commun., Tokyo, Japan, Nov. 6-10, 1995.
- [7] S. Okasaka et al., "A New Location Updating Method for Digital Cellular Systems," Proc. IEEE VTC '91, Saint Louis, MI, May 1991.
- [8] C. H. Rokitansky, "Knowledge-Based Routing Strategies for Large Mobile Networks with Rapidly Changing Topology," Proc. ICCC '90, New Delhi, India, Nov. 1990, pp. 541-50.
- [9] S. Tabbane, "Comparison between the Alternative Location Strategy (AS) and the Classical Location Strategy (CS)," WINLAB Tech. Rep. 37, Aug. 1992.
- [10] S. Tabbane, "An Alternative Strategy for Location Tracking," IEEE JSAC, vol. 13, no. 5, June 1995.
- [11] M. Shirota, Y. Yoshida, and F. Kubota, "Statistical Paging Area Selection Scheme (SPAS) for Cellular Mobile Communication Systems," Proc. IEEE VTC '94, Stockholm, Sweden, June 8-10, 1994.
- [12] Y.-B. Lin, "Reducing Location Update Cost in a PCS Network," IEEE/ACM Trans. Networking, vol. 5, no. 1, Feb. 1997, pp. 25-33.
- [13] Kibom Kim, Kwon Woo Yang, Joon-Ming Gil, and Chong-Sun Hwang, "Traking Mobile User Locality in Mobile Computing Systems", International Workshop on Parallel Processing, Wakamatsu, Japan, September 21-24, 1999.
- [14] Narumi Umeda, Toru Otsu, and Tatsuro Masamura, "Overview of the Fourth-generation Mobile Communication System", NTT Technical Review, Vol.2 No.9, pp. 12-17, September 2004.
- [15] Cavalcanti, D.; Agrawal, D.; Cordeiro, C.; Bin Xie; Kumar, A; "Issues in integrating cellular networks, WLANs, and MANETs: a futuristic heterogeneous wireless network", IEEE Wireless Communications Magazine, Volume 12, Issue 3, pp. 30 - 41 , June 2005.
- [16] Sherif Rashad, Mehmed Kantardzic, and Anup Kumar, "MSP-CACRR: Multidimensional Sequential Patterns Based Call Admission Control and Resource Reservation for Next-Generation Wireless Cellular Networks", the 2007 IEEE Symposium on Computational Intelligence and Data Mining (CIDM 2007), Honolulu, Hawaii, April 1-5, 2007.
- [17] Ng, C.K.; Chan, H.W.; " Enhanced Distance-Based Location Management of Mobile Communication Systems Using a Cell Coordinates Approach", IEEE Transactions on Mobile Computing, Vol. 04 , Issue 1, pp. 41 - 55 , Jan.-Feb. 2005.
- [18] Quintero, A.; Garcia, O., "A profile-based strategy for managing user mobility in third-generation mobile systems", IEEE Communications Magazine, Vo.142 Issue 9 , pp. 134 - 139, Sept 2004.
- [19] Xiao, Y.; Pan, Y.; Li, J.; "Design and analysis of location management for 3G cellular networks", IEEE Transactions on Parallel and Distributed Systems, , Vol. 15 , Issue 4 , pp. 339 – 349, April 2004.
- [20] Il Han; Dong-Ho Cho; "Group location management for mobile subscribers on transportation systems in mobile communication networks", IEEE Transactions on Vehicular Technology, Vol. 53 , Issue 1 , pp. 181 – 191, Jan. 2004.
- [21] Jian Pei; Jiawei Han; Mortazavi-Asl, B.; Jianyong Wang; Pinto, H.; Qiming Chen; Dayal, U.; Mei-Chun Hsu, "Mining sequential patterns by pattern-growth: the PrefixSpan approach", IEEE Transactions on Knowledge and Data Engineering, Vol.16, Iss.11, pp. 1424- 1440, Nov. 2004.
- [22] J. Pei, J. Han, B. Mortazavi-Asl, H. Pinto, Q. Chen, U. Dayal, and M.-C. Hsu, "PrefixSpan: Mining Sequential Patterns Efficiently by Prefix-Projected Pattern Growth," Proc. 2001 Int'l Conf. Data Eng. (ICDE '01), pp. 215-224, Apr. 2001.
- [23] Helen Pinto, Jiawei Han, Ke Wang, Qiming Chen, Umeshwar Dayal, "Multi-dimensional Sequential Pattern Mining" , Proceedings of the 2001 ACM CIKM International Conference on Information and Knowledge Management, Atlanta, Georgia, pp. 81-88, November 2001.
- [24] Sherif Rashad, Mehmed Kantardzic, and Anup Kumar, "PAC-WHN: Predictive Admission Control for Wireless Heterogeneous Networks", Proceeding of the 2007 IEEE Symposium on Computers and Communications (ISCC'07), pp. 139-144, Aveiro, Portugal, July 1-4, 2007.

A new clustered Directed Diffusion Algorithm based on credit of nodes for wireless sensor networks

Farnaz Dargahi, Amir Masoud Rahmani, Reza Samadabadi

Department of Computer Engineering, Science and Research branch, Azad University, Tehran, Iran, e-mail:
farnazdargahi@gmail.com, rahmani@sr.iau.ac.ir, samadabadi.reza@gmail.com

Abstract— for data gathering in wireless sensor network, sensors extract useful information from environment; this information has to be routed through several intermediate nodes to reach the destination. How information can effectively disseminate to the destination is one of the most important tasks in sensor networks. Due to limited power and slow processor in each node, algorithms of sensor networks must be designed carefully. Directed Diffusion (DD) is typical data-centric algorithm has been used to provide efficient data transmission. We enhance this algorithm by clustering all nodes into clusters and select a few nodes as cluster head according to their credits. This credit is computed at each node by considering three factors. Simulation results show that our proposed algorithm is more energy efficient than DD and has the ability of traffic load distribution.

Keywords— Directed Diffusion, Data gathering, Nodes' Credit, Cluster, Sensor network.

I. INTRODUCTION

A Sensor network is a group of wireless nodes randomly distributed in a region. In most data gathering applications, information produced by one or more sources usually has to be routed through several intermediate nodes; these wireless nodes have the ability of packet forwarding, i.e. relaying incoming packets to one of its neighbor nodes. Problem arises when intermediate nodes fail to forward incoming packets. Sensor nodes have many failure modes. Each failure decreases the performance of data gathering procedure. Our approach is designed by considering that nodes may not be available during the dissemination procedure. Directed Diffusion [1] is a routing mechanism for data gathering in which data consumer (sink) search for the data sources by sending interest packets and find the best route to receive the data. Many researches have been done to meet specific need of wireless sensor network applications [6], [8], [11], [12].

Yu et al. [9] discussed the use of geographical information while disseminating queries to appropriate regions. The protocol, called Geographical and Energy Aware Routing (GEAR), uses energy aware and geographically-informed neighbor selection heuristics to route packets towards the

destination region. By doing this, GEAR can conserve more energy than directed diffusion. Each node in GEAR keeps a cost. The cost is a combination of residual energy and distance to destination. Raicu et al. proposed E3D diffusion (Energy-efficient Distributed Dynamic Diffusion routing algorithm) in [13], in which each node keeps a list of neighbors and chooses the next hop neighbor based on the location information, power and load towards the base station. In this scheme, when a receiver's queue is full, or its power is lower than the sender's power or when it is below a threshold, it will tell its sender to stop forwarding packets.

HDA [2] (hierarchical data aggregation) is proposed for enhancing DD. In HDA, nodes between the sink and the source are arranged in different levels (i.e. hierarchy). Packets are only transmitted between two nodes in neighboring level. This new feature can save energy significantly.

In this paper, a new clustered, reliable and energy efficient DD algorithm is introduced

The rest of the paper is organized as follows. In section 2 we briefly review the original directed diffusion algorithm. Section 3 presents our algorithm in details. A simplified schema of the proposed algorithm is shown in section 4. Simulation based performance studies are conducted in section 5. Finally; we conclude our work in section 6.

II. REVIEW: DIRECTED DIFFUSION

Directed Diffusion [1] consists of three phases: a) interest propagation, b) Initial gradients setup, and c) Data delivery reinforced path as shown in Fig 1. Sink node send out its query whenever it wants to obtain some information from sensor nodes. This query is carried by interest packet. When a node receives an interest packet, the packet is cached and broadcast to other neighbors to ensure every node in the network will receive it. Propagation of interest packets also setup the gradient in the network for delivering data to the sink. Gradient is a reply link to a neighbor from which the interest was received. When a node matches an interest, it generates a sample sensed data, which is called exploratory

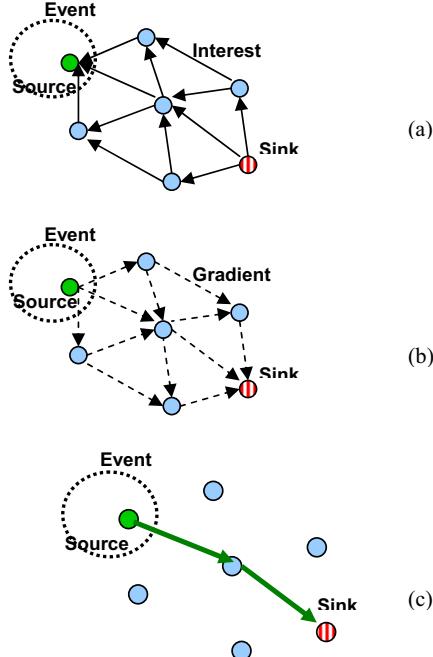


Fig 1.Directed Diffusion (a) Interest Propagation (b) Initial gradients setup (c) Data delivery reinforced path.

data and sends individually to the neighbors from which the gradient established before. As these exploratory data reach the sink from some neighbors, several paths are established between sink and source.

The sink reinforces one of these paths by increasing the data rate in the interest packet. Usually this path is the one which has the least delay. Eventually only one path remains while other paths are torn down. Finally the real data will send from the source, following the selected path.

III. THE PROPOSED ALGORITHM

Interest message in DD is flooded through the whole sensor networks. In other hands each node has to relay such message to all its neighbors. As a result, many unnecessary nodes in the networks are involved in this communication.

To solve such problems, we proposed clustered Directed Diffusion based on credit of nodes. Instead of flat structure, in our scheme all sensor nodes are arranged in different clusters, each with a cluster head. Only one cluster head is allowed in a radio range so that a cluster head will not encounter any other cluster head in its radio range as shown in Fig 2.

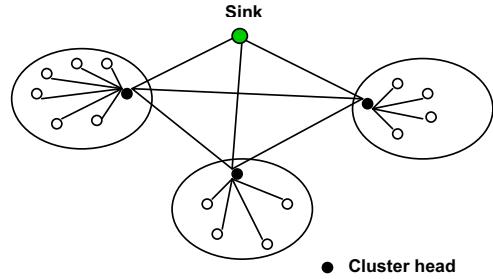


Fig 2. A snapshot of the cluster-based architecture

Sink node sends interest message only to cluster heads. Cluster heads send interest message to its member to ensure every node in their cluster will receive it. Gradient are established between cluster head (CH) and cluster members when a node matches an interest. Cluster members send the data along the gradient path.

A. Cluster head election by nodes' credit

This subsection describes the way of cluster head election by using credit of nodes. Each node has a credit. Computation of nodes' credit is done by using three factors; at each node. This credit is computed according to (1).

$$\begin{aligned} V &= \alpha_1 \times V_s + \alpha_2 \times V_E + \alpha_3 \times V_B \\ \alpha_1 + \alpha_2 + \alpha_3 &= 1 \end{aligned} \quad (1)$$

Each of the parameters of above formula has specific coefficient (α) that is amount between [0,1]. Different alternatives have been considered for finding the best value of coefficients in order to provide desired result.

The first parameter (V_s) is the number of successful or unsuccessful transmission and how nodes succeeded to deliver packets in the past. A low amount of this parameter of a node means that the node failed to route message in the past. This parameter is increased with each successfully routed packet and decrease with each failing in routing packets.

The second parameter (V_E) is the residual energy in candidate node's battery. Equation (2) is used for calculating this parameter.

$$V_E = \frac{\text{existing energy}}{\text{capacity of battery}} \quad (2)$$

This parameter has an important effect on increasing the network lifetime.

The third parameter (V_B) is traffic load at each node (Fig 3). This parameter is computed according to (3).

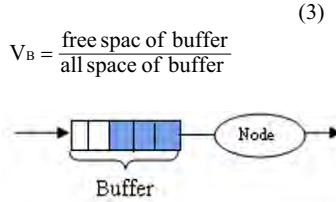


Fig 3 .Scheme of traffic load in buffer

If there would be high traffic load in candidate cluster member end to end delay will increase in the sink node, in addition this high traffic load will cause more spending energy in candidate cluster member.

Each node computes its credit based on these factors according to (1).

We define nodes state as follows: Cluster head (CH), cluster member (CM) and candidate cluster head (CCH). Before the interest is propagated throughout the sensor network, the base station sends a cluster formation message(CFM) with a credit threshold THc to its neighbor nodes, if the node's current credit is less than THc, keep silence, otherwise, sets its node state as CCH, and declares its state to its neighbors, if the nodes with the state of CCH have the same credit then the node who declares first wins the competition. The winners set their node state as CH, and declare the CH message to their neighbors. Node who receives cluster head message, join the cluster and set its node state as CM.

B. Interest diffusion

Interest message are broadcasted by sink to all cluster heads. Each cluster head broadcasts interest message to its cluster member after it receives interest message. Each cluster member will record a time stamp and the cluster head which interest message is sent from.

C. Data propagation and Reinforcement

In clusters, cluster members receive interest message form their cluster head. When a cluster member detects a data matched with the interest message, it will send exploratory data to its cluster head. Cluster head will aggregate them and then send to nearest cluster head in its neighboring or sink, if the sink node were nearest node to it. In this phase gradient are established.

After the sink starts receiving these exploratory data it reinforces one particular neighbor. The sink will choose that cluster head from which it first received the last event matching the interest and send reinforcement message through selected node.

Once a source receives the reinforcement message, it sends out actual data.

IV. A SIMPLIFIED SCHEMA OF THE PROPOSED ALGORITHM

Fig 4 is a simplified schema of the proposed algorithm, (a) is the interest propagation; (b) is the initial gradients set up; (c) is the reinforced path.

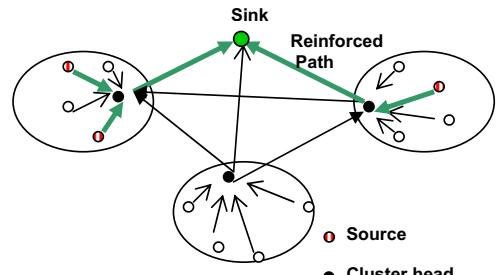
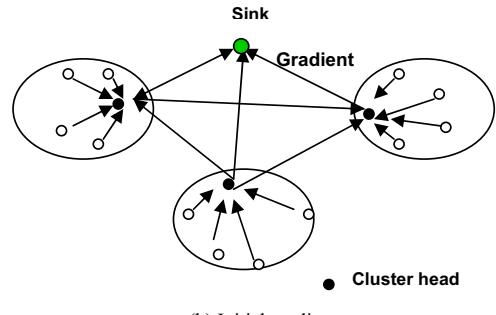
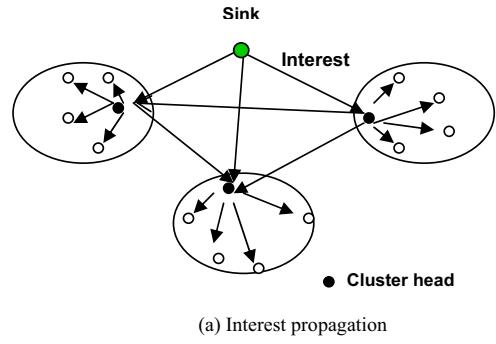


Fig 4. A simplified schema of the proposed algorithm

V. PERFORMANCE EVALUATION

In this section, we compare our proposed algorithm with Directed Diffusion. We implement algorithm in NS-2 simulator and use the following model for our simulation study.

- the number of nodes which are distributed randomly over a rectangular area of 900m \times 900m is 100.

- a sensor node's transmitting, receiving and idle listening power consumption rate are 0.660W, 0.395W and 0.035W respectively.

- initial power is 5000 joules.
- the size of data packet is 64 byte.

The value of α_1 , α_2 and α_3 are set to 0.2, 0.5 and 0.3 respectively.

Two metrics are chosen for evaluating and comparing the performance of our algorithm with DD: system lifetime and load distribution.

System lifetime is used as the measure of energy consumption. The system lifetime is the total time which a wireless sensor network experiences. Fig 5 shows the system lifetime in terms of nodes' failures. As simulation result shows, using suggested policy causes to increase system lifetime under variant nodes' failure.

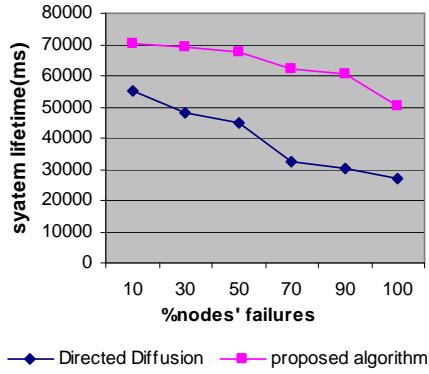


Fig.5. System lifetime

Next we analyze the traffic load distribution on the surface of network. Fig 6 shows that, as the number of sources increases, DD's performance decreases faster than our proposal. This is because of giving higher priority to the reliable nodes in our proposed algorithm. Here higher priority nodes are nodes which have higher level of energy and empty buffer for receiving more packets. Fig6 shows the simulation result and algorithm ability to distribute traffic load in terms of increasing source nodes.

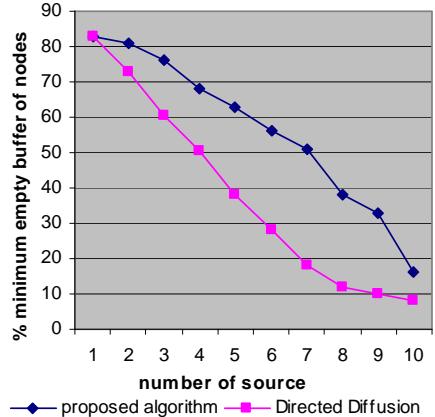


Fig 6.Trafic load distribution

VI. CONCLUSION

In this paper, a new clustered directed diffusion based on credit of nodes is presented. The aim of this paper is making the directed diffusion of data centric algorithm of sensor networks in a good order. For this purpose, each node is classified into clusters. A node with higher credit will choose for cluster head. Credit of nodes is computed according to three factors. The sink node send interest message only to the cluster head and cluster head send this message to its members. After the cluster members sense the data that matches the interest message, it will send exploratory data to cluster head in order to establish gradients. When sink node receives these exploratory data from one of the cluster heads, it will reinforce one particular path and send reinforce message to selected cluster head. The proposed approach is deduced an energy efficient with supporting traffic load distribution.

ACKNOWLEDGMENT

This work was supported by the Iran Telecommunication Research Center (ITRC).

REFERENCES

- [1] C.Intanagonwiwat, R.Govindan, D.Estrin, J.Heidemann, F.Silva, "Directed Diffusion for wireless sensor networking" Networking Volume 11, Issue 1, Feb. 2003 Page(s):2-16 Digital Object Identifier 10.1109 /TNET .2002 .808417
- [2] B.Zhou, L.H.Ngoh, B.S.Lee, C.Peng "HDA: A hierarchical data aggregation scheme for sensor networks" Computer Communications, Volume 29, Issue 9, 31 May 2006, Pages 1292-1299.
- [3] C.Schurgers, M.B.Srivastava "Energy Efficient Routing in Wireless Sensor Network" Electrical Engineering Department University of California UCLA .CA 2006.

- [4]C.Yanrong, C.jaheng."An improved Directed Diffusion for Wireless Sensor Networks" Wireless Communications, Networking and Mobile Computing, 2007. International Conference on 21-25 Sept. 2007 Page(s):2380 - 2383 Digital Object Identifiers 10.1109/WICOM.2007.593. Technical Report TR-01-0023, UCLA Computer Science Department Technical Report, May 2001.
- [5]Max do V. Machado, Antonio A. F. Loureiro and Jose Marcos Nogueira, "Data Dissemination Using the Energy Map", Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS.05), 2005.23-34
- [6]Jae-Hwan Chang, Leandros Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks", Networking, IEEE/ACM Transactions on Volume 12, Issue 4, Aug. 2004 Page(s):609 - 619 Digital Object Identifier 10.1109/TNET.2004.833122
- [7] Q.Han, S.Mehrotra, N. Venkatasubram "Application-aware integration of data collection and power management in wireless sensor networks" Journal of Parallel and Distributed Computing, Volume 67, Issue 9, September 2007, Pages 992-1006
- [8] Pai-Hsiang Hsiao, Hwang, A., Kung, H.T., Vlah, D "Load-balancing routing for wireless access networks" INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE Volume 2, 22-26 April 2001 Page(s):986 - 995 vol.2 Digital Object Identifier 10.1109/INFCOM .2001.916291
- [9] Y.Yu, D. Estrin, and R. Govindan. "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks"
- [10] I. Raicu, L. Schwiebert, S. Fowler, and S. K.S. Gupta"Local load balancing for global efficient routing in wireless sensor networks". International Journal of Distributed Sensor Networks, 1:163 – 185, 2005.
- [11] E.Fasolo, M.Rossi, J.Widmer,M. Zorzi, "In-network aggregation techniques for wireless sensor networks: a survey" Wireless Communications, IEEE Volume 14, Issue 2, April 2007 Page(s):70 87 Digital Object Identifier 10.1109/MWC .2007.358967.
- [12].S.Wu, K. Selçuk Candan" Power-aware single and multipath geographic routing in sensor networks Ad Hoc Networks, Volume 5, Issue 7 ,September 2007, Pages 974-997.
- [13].Min Chen, T.Kwon, Yanghee Choi "Energy-efficient differentiated directed diffusion (EDDD) in wireless sensor networks" Computer Communications, Volume 29, Issue 2, 10 January 2006, Pages 231-245.
- [14].J.Lipman, M.Abolhasan, P.Boustead, J.Chicharo"An optimised resource aware approach to information collection in ad hoc networks" Ad Hoc Networks, Volume 3, Issue 5, September 2005, Pages 643-655

Multiview Media Transmission Algorithm for Next Generation Networks

Kostas E. Psannis

Abstract—It has been widely recognized that multi-view video coding (MVC) is one of the key technologies for a wide variety of future interactive media applications, e.g. 3D television over next generation networks. Due to the large data volume, transmission the multi-view media requires much more bandwidth than traditional media. Consequently, how to efficiently compress multi-view media becomes more important than any other data. This paper proposes an efficient algorithm for Multiview Media Transmission over Next Generation Networks. The proposed approach is detailed examined through extensive simulations. Both subjective and objective visual quality comparative study demonstrates that the proposed approach outperforms the conventional approach.

Index Terms—Multiview Media, 3D Media Over Next Generation Networks, Free-viewpoint Media over High Speed Networks.

I. INTRODUCTION

Multiview video coding possesses a wide variety of applications, including free-viewpoint video/television, three dimensional (3D) TV and surveillance applications. Currently, the Joint Video Team (JVT) of the International Organization for Standardization (ISO)/International Engineering Consortium (IEC) Motion Picture Expert Group (MPEG) and International Telecommunication Union (ITU)-T Video Coding Expert Group is working to develop a multiview video coding (MVC) standard, which is becoming an extension of the ITU-T H.264 standard, also known as ISO/IEC MPEG-4 Part-10 [1]-[2].

The need for multiview video coding is driven by two recent technological developments: new 3D display technologies and the growing use of multi-camera arrays. A variety of companies are starting to produce 3D display technologies that do not require glasses and can be viewed by multiple people simultaneously. The immersive experience provided by these 3D displays are compelling and have the potential to create a growing market for 3D video and hence for multiview video compression over next generation networks [2]. In recent years several multiview techniques have been devised.

Kostas E. Psannis is with the Department of Technology Management, University of Macedonia, Greece, emails: kpsannis@uom.gr, mobility2net@gmail.com).

The basic idea employed in all related works on efficient multiview video coding is to exploit both spatial and temporal redundancy for compression.

Since all cameras capture the same scene from different viewpoints, inter-view redundancy is present. As the video data originate from the same scene, the inherent similarities of the multi-view imagery are exploited for efficient compression. These similarities can be classified into two types. First, inter-view similarity is observed between adjacent camera views. Second, temporal similarity is noticed between temporally successive images of each video. Temporal similarities can be exploited with motion compensation techniques that are well known from single-view video compression. Extending that idea, disparity compensation techniques make use of inter-view similarities for multi-view video compression [3], [4].

To exploit these temporal similarities, sophisticated motion compensation techniques have been developed in the past [5]. Frequently used are so-called block matching techniques where a motion vector establishes a correspondence between two similar blocks of pixels chosen from two successive images [6]. Practical compression schemes signal this motion vectors to the decoder as part of the bit-stream. Variable block size techniques improve the adaptation of the block motion field to the actual shape of the object [7]. Lately, so-called multi-frame techniques have been developed. Classic block matching techniques use a single preceding image when choosing a reference for the correspondence. Multi-frame techniques, on the other hand, permit choosing the reference from several previously transmitted images; a different image could be selected for each block [8]. Finally, superposition techniques are also used widely. Here, more than one correspondence per block of pixels is specified and signaled as part of the bit-stream [9].

On the other hand in order to employ these inter-view similarities, disparity compensation techniques are used. The simplest approaches to disparity compensation are block matching techniques similar to those used for motion compensation [10]. These techniques offer the advantage of not requiring knowledge of the geometry of the underlying 3D objects. However, if the cameras are sparsely distributed, the block-based translatory disparity model fails to compensate accurately. More advanced approaches to disparity compensation are depth-image-based rendering algorithms [11]. They synthesize an image as seen from a given viewpoint by using the reference texture and depth image as input data. These techniques offer the advantage that the given view-point image is compensated more accurately even when

the cameras are sparsely distributed. However, these techniques rely on accurate depth images, which are difficult to estimate [1].

This paper proposes a coding efficient approach in order to transmit the multiview sequences over next generation high bandwidth networks. The paper is organized as follows. In Section 2 the preprocessing steps of the proposed method is detailed. Section 3 includes the simulation results and extensive comparative study demonstrating the performance of the proposed very efficient technique. Section 4 concludes the paper.

II. PROPOSED TECHNIQUE

A H.264 video stream comprises Intra (I)-frames, Predicted (P)-frames, and interpolated-Bidirectional (B)-frames. According to H.264/AVC, I-, P- and B-frames have been extended with new coding features, which lead to a significant increase in coding efficiency. For example, H.264/AVC allows using more than one prior coded frame as a reference for P- and B-frames. Furthermore, in H.264/AVC, P-frames and B-frames can use prediction for subsequent frames. The H.264/AVC syntax permits the use of B-frames or P-frames as reference frames with the feature called stored B- or P-frames. These new features are described in detail in [1]. Moreover an H.264/AVC coded video sequence is typically partitioned into small intervals called GOP (Group Of Pictures). In comparison to older video coding standards (MPEG-1, MPEG-2), H.264/AVC supports much more flexibility at a picture/sequence level. The coding and display order of pictures is completely decoupled, and any picture can be marked as reference picture and used for motion compensated prediction of following pictures independent of the coding types of the corresponding slice types. The set of pictures that is stored in the decoded picture buffer and used for the prediction of following picture can be adaptively controlled. These features allow the selection of arbitrary coding/prediction structures, which are not supported by previous standards [12]-[17].

The conventional straightforward approach (CSA) to the multiview coding problem is to temporally encode the individual video streams independent of one another and simulcast each of the views. A typical coding scheme with hierarchical B-frames is illustrated in figure 1 for a sequence with eight cameras and a GOP length of 8. In Figure 1, S_n denotes the individual view sequences and T_n the consecutive time-points, and the video stream from each camera is coded separately. This conventional approach could be applied by a normal H.264/AVC video codec [18].

The proposed approach to multiview video compression is to achieve better compression performance in order to transmit the multiview sequences over next generation high bandwidth networks. The proposed method also uses hierarchical B-frames for each view as shown in Figure 2. Moreover the correlations between views are utilized and thus inter views prediction are applied to every view. This prediction structure might have coding efficiency advantages over the upper configurations at the disadvantage of being more complex.

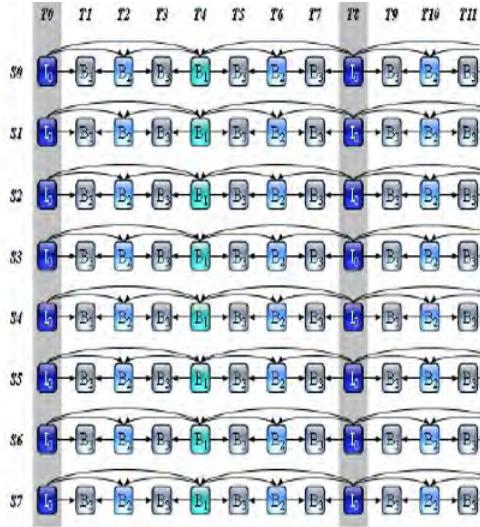


Fig. 1 Conventional straightforward approach (CSA)

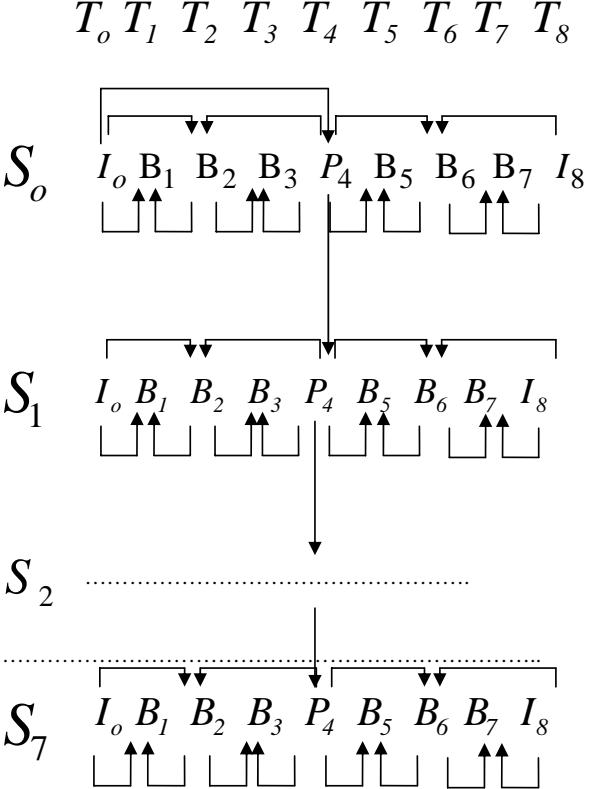


Fig. 2 The proposed approach. Arrows depict motion compensation prediction relationships.

III. SIMULATIONS RESULTS

In order to verify performance and effectiveness of the above hierarchical prediction structures, experiments are implemented on the H.264/AVC reference codec [27]. There are two types of criteria that can be used for the evaluation of video quality; subjective and objective. It is difficult to do subjective rating because it is not mathematically repeatable.

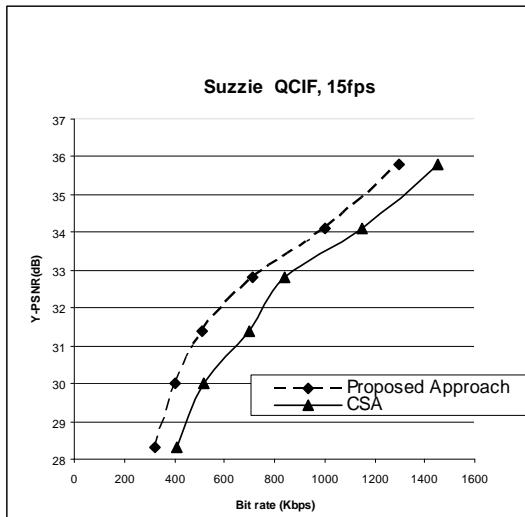
As a descriptive measure for the prediction performance, the peak signal-to-reconstructed image measure which is called PSNR (peak signal-to-noise ratio) is widely used. PSNR measures are estimates of the quality of the decoded video samples compared with the original video samples [24], and PSNR of the luminance signal is given as:

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right)$$

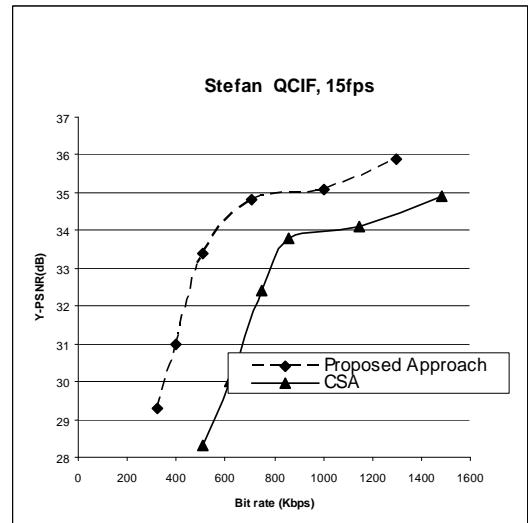
To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

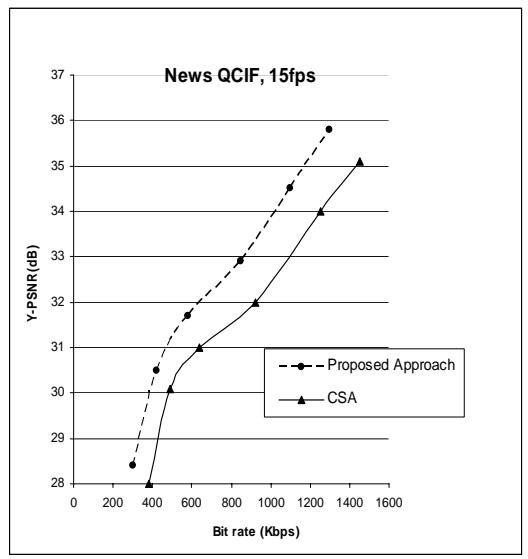
In the previous equation, M and N are the number of rows and columns in the input images, respectively. It should be noted that a higher PSNR would normally indicate that the reconstruction is of higher quality. The experiments we presented are performed with H.264/AVC conforming software version JM 13.2 [17], using typical settings for multiview video coding (MVC), like variable block size, Reference frame selection (RFS), and a search range of ± 32 .



(a)



(b)



(c)

Fig.3 Comparison of coding efficiency for the Suzie video sequence (a) for the Stefan video sequence (b) and for the News video sequence (c).

The proposed approach compared with the conventional straightforward approach (CSA) on Suzie, Stefan and News video sequences as shown below. The cameras are both linearly aligned, representing the simple and complex local disparities, respectively.

Specifically three different QCIF video sequences, Suzie and Stefan and News are used to evaluate the performance of the proposed scheme. These three sequences are chosen for their

different texture complexity and motion activity. Suzie is active sequences which include a moving background and a fair amount of motion of the foreground object. On contrary, Stefan sequence has rapid foreground motion with a fair amount of motion of the background object. News sequence has constant motion. Figure 3 illustrates the comparison of the average PSNR improvements among the different approaches. 'CSA' denotes conventional straightforward coding using hierarchical B pictures in temporal dimension only (Fig.1) and 'Proposed Approach' donates the proposed efficient approach utilizing hierarchical B pictures in interview and temporal dimension. From the figure, we can see that the 'Proposed Approach' outperforms the 'CSA' scheme significantly, it gain achieved is up to 20% bit rate saving for Suzie sequence , 12% bit rate saving for Stefan sequence, 10% bit rate saving for News sequence . The coding performance is about, 2 dB for the Stefan, 1 dB for the News sequence , 0.5 dB for the Suzie sequence, higher than that of the H.264/AVC conventional coding.

Evaluation of the video quality is an important task in the area of video processing. Often quality is required to be measured automatically (without human's interference), and this goal is achieved with objective metrics. However, objective metrics can only serve as an estimation of the real quality of video, which is the subjective opinion of actual viewers. Hence the coding performance is finally judged by subjective tests, where humans evaluate visual quality, thus a reconstructed frame for the previous schemes are compared in Figure 4. As it can be seen, fine-detailed regions especially of the background are noticeable better preserved with the proposed approach than with the conventional coding.



(a)



(b)



(c)



(d)



(e)



(f)

Fig.4. Subjective Comparison of the Stefan (a)-(b) and the Suzie (c)-(d) and News (e)-(f) video sequences for the CSA (a)-(c)-(e) and the proposed approach (b)-(d)-(f).

IV. CONCLUSIONS

A very efficient approach is proposed in order to support feasible multiview media transmission over next generation high bandwidth networks. Both subjective and objective visual quality comparative study demonstrates that the proposed approach outperforms the conventional straightforward approach (CSA) in terms of PSNR and coding efficiency. Future work will include the impact of the proposed approach in the decoding complexity. Moreover we will examine the impact of the proposed method in error prone channels, random access and VCR interactive functions and switching from wireless to wired channels and vice versa.

REFERENCES

- [1] Advanced Video Coding for Generic Audiovisual Services, ITU-T Rec. H.264 and ISO/IEC 14496-10 (MPEG-4 AVC), ITU-T and ISO/IEC JTC 1, Version 1: May 2003, Version 2: May 2004, Version 3: Mar. 2005, Version 4: Sept. 2005, Version 5 and Version 6: June 2006, Version 7: Apr. 2007, Version 8 (including SVC extension): Consented in July 2007.
- [2] R.-S. Wang and Y. Wang, "Multiview video sequence analysis, compression, and virtual viewpoint synthesis", IEEE Transactions on Circuits and Systems for Video Technology, vol. 10, no. 3, pp. 397-410, April 2000.
- [3] B. Wilburn, et al., "High Performance Imaging Using Large Camera Arrays," ACM Transactions on Graphics, vol. 24, no. 3, pp. 765-776, July 2005.
- [4] C.L. Zitnick, et al., "High-quality video view interpolation using a layered representation," ACM SIGGRAPH and ACM Trans. on Graphics, Los Angeles, CA, Aug. 2004, pp. 600-608.
- [5] M. Flierl and B. Girod, Multi-View Video Compression .Exploiting Inter-Image Similarities, IEEE Signal Processing Magazine, 2007.
- [6] J. Jain and A. Jain, Displacement measurement and its application in interframe image coding., IEEE Transactions on Communications, vol. 29, no. 12, pp. 1799.1808, Dec. 1981.
- [7] P. Strobach, .Tree-structured scene adaptive coder., IEEE Transactions on Communications, vol. 38, no. 4, pp. 477.486, Apr. 1990.
- [8] T. Wiegand, X. Zhang, and B. Girod, .Long-term memory motion-compensated prediction., IEEE Transactions on Circuits and Systems for Video Technology, vol. 9, no. 1, pp. 70.84, Feb. 1999.
- [9] M. Flierl and B. Girod, Video Coding with Superimposed Motion-Compensated Signals: Applications to H.264 and Beyond. Boston .Dordrecht .London: Kluwer Academic Publishers, 2004.
- [10] M. Lukacs, .Predictive coding of multi-viewpoint image sets., in Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Tokyo, Japan, Apr. 1986.
- [11] L. McMillan and G. Bishop, .Plenoptic modeling: An image-based rendering system., in Proceedings of the ACM SIGGRAPH, Los Angeles, CA, Aug. 1995, pp. 39.46.
- [12] Kostas Psannis and Yutaka Ishibashi, Efficient Flexible Macroblock Ordering Technique, IEICE Transactions on Communications, vol. E91-B, No. 08, pp. 2692-2701, August 2008.
- [13] Kostas Psannis and Yutaka Ishibashi, Enhanced H.264/AVC Stream Switching over Varying Bandwidth Networks, IEICE ELEX Journal, Vol.5, No.19, pp. 827-832, October, 2008.
- [15] Kostas Psannis, Interactive Compression Algorithms for Streaming Media over High Speed Networks, Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics, Sobh, T.; Elleithy, K.; Mahmood, A.; Karim, M. A. (Eds.), Publisher Springer, Signals and Communications, pp 415-420 (2008).
- [16] Kostas Psannis, Dynamic Rate Control Algorithm for Streaming Media over Wireless Channel, Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics, Sobh, T.; Elleithy, K.; Mahmood, A.; Karim, M. A. (Eds.), Publisher Springer, Signals and Communications, pp 409-414 (2008).
- [17] Kostas Psannis and Yutaka Ishibashi, Efficient Error Resilient Algorithm for H.264/AVC: Mobility Management in Wireless Video Streaming, Springer Telecommunication Systems Journal, vol 41, issue 2, 2009. H.264/AVC Software Coordination, software version: JM 13.2 (<http://iphome.hhi.de/suehring/tm/>).

A 4GHz Clock Synchronized Non Coherent Energy Collection UWB Transceiver

U Bala Maheshwaran^{1*}, Reshma Raj^{2*}, S Sindhu Tharangini^{3*} Dr. K A Narayanan Kutty⁴,
1,2,3,4 Amrita school of Engineering, Ettimadai, Coimbatore
balamaheshwaran@gmail.com¹,reshma_raj87@yahoo.co.in²,sindhu.tharangini@gmail.com³

Abstract-- In this paper, a 4GHz clock synchronized non coherent energy collection approach based Ultra Wideband transceiver for biomedical sensor signals like ECG is proposed. The system is based on a non-coherent architecture which enables the receiver to be extremely simple and largely insensitive to the transmitted pulse shape. The energy collection makes the reception efficient in a multipath environment. It is realised by using a bank of integrators which determine the energy of the transmitted signal for specific intervals of time. The proposed model is implemented in SIMULINK. The Bit Error Rate (BER) performance of the transceiver in additive white gaussian noise multipath channel is determined and the result is found to be satisfactory.

Keywords: Ultra Wideband, Non coherent receivers, Energy collection approach, Binary phase modulation.

I. INTRODUCTION

Ultra Wideband (UWB) is one of the key emerging short-range wireless technologies that can answer many of the problems faced by the conventional narrowband technologies. Impulse UWB technique considered in this paper is the transmission of very low power, wideband radio signal achieved by using very short, and sub-nanosecond electrical pulses. It offers good robustness against jamming and multipath fading, and has low probability of detection and high user-capacity [1].

The Federal Communications Commission (FCC) defines a radio system to be an UWB system if the fractional bandwidth is greater than 20% of the center frequency or if the absolute bandwidth is greater than 500MHz. The allowed frequency range of operation for UWB communication is from 3.1 to 10.6 GHz. UWB communication systems operates by spreading small amounts of average Effective Isotropic Radiated Power (EIRP) below -41.3dBm/MHz across a very wide band of frequencies relative to its centre frequency [2]. The FCC spectral mask for indoor communication is shown in Fig 1. The low power levels allows this technology to overlay already available services such as the global positioning system (GPS) and the IEEE 802.11 wireless local area networks (WLANS) that coexist in this band.

The availability of huge bandwidth opens the door for unprecedented number of bandwidth-demanding position-critical low-power applications in wireless communications, networking, radar imaging, and localization systems. These include short-range, high-speed access to the Internet, accurate

personnel and asset tracking for increased safety and security, precision navigation, imaging of steel reinforcement bars in concrete or pipes hidden inside walls, surveillance, and medical monitoring of the heart's actual contractions.

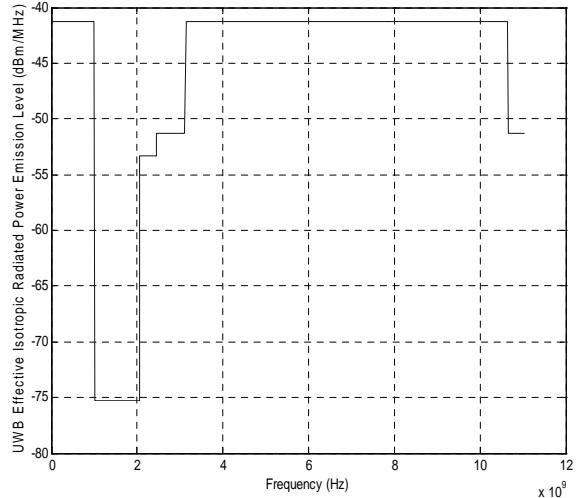


Fig 1. FCC mask for indoor communication

The system concept involves indoor wireless sensor network consisting of a number of ECG sensors, UWB transmitters and receivers [4]. The receivers are connected to a central system that analyses the ECG data. The sensor network can thus be configured specifically for automated diagnosis of heart diseases like arrhythmia. Data rate in the order of 1Gbps can be easily achieved through multiplexing. The sensors continuously sense the ECG from the mobile and immobile patients present within the sensor network. The analog signal is subsequently sampled, modulated and transmitted at a frequency of 4GHz. At the receiver, the energy of the multipath rich signal is computed and the transmitted bit is detected.

The paper is organised as follows. Section II presents the proposed architecture. The transmitter and receiver architectures are described in Section III and Section IV respectively. Section V explains the simulation results and bit error rate analysis of the proposed architecture followed by conclusion in Section VI.

II. PROPOSED ARCHITECTURE

The block diagram of the proposed transceiver architecture is shown in Fig 2.

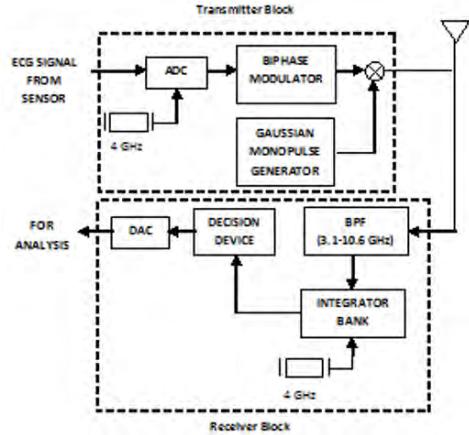


Fig 2. UWB Transceiver Architecture

The Analog ECG signal is obtained from the sensor placed on the chest of mobile or immobile patient. The signal is digitised, modulated and transmitted. At the receiver, the signal is first band pass filtered in order to eliminate signals outside the frequency range of 3.1 to 10.6 GHz. Filtered signal is then integrated at equal time intervals. The maximum energy corresponding to the maximum value of the integrator is determined using a decision device. The digital data is then fed to DAC to reconstruct the ECG signal.

III. TRANSMITTER

A. Analog to Digital converter

The ECG signal is fed to an Analog-to-Digital converter. The signal is sampled at 11Hz and quantised using a 16 bit resolution ADC. Each sample is thus encoded with a unique four bit code. It is designed with non-uniform quantisation levels i.e. closely spaced levels for the low frequency P and T waves and widely spaced levels for high frequency QRS complex of the ECG. This helps in tracking minute variations in the ECG signal. The digitised ECG signal constitutes the data to be transmitted.

B .Gaussian pulse generator

The shorter the pulse, more the bandwidth it occupies. An ideal impulse signal thus occupies infinite bandwidth. Practical UWB systems operate using Gaussian monocycle in order to utilize the entire bandwidth and also to fit appropriately within the design constraints of FCC as shown in Fig 1. A Gaussian monocycle is modelled by the equation:

$$p(t) = \left(\frac{t}{\tau} \right) e^{-\left(\frac{t}{\tau} \right)^2} \quad (1)$$

It is obtained by the first differentiation of the standard Gaussian wave. Gaussian pulse as shown in Fig 3 is preferred to other pulse shapes because its spectrum contains lowest energy in its side-loops.

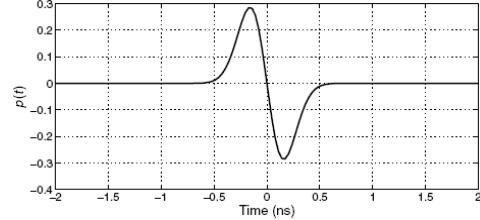


Fig 3. Gaussian monocycle

There are two approaches to cover the desired frequency spectrum: 1) Shaping of the pulse to achieve the desired spectrum 2) Up-conversion of the baseband signal. In most of the cases the generated pulse is passed through a pulse shaping network to produce the desired pulse shape in order to fulfill the FCC spectrum regulations. However, if the shaping circuits become complex for a given center frequency and bandwidth, the second approach is adopted [2].

C. Bi-phase Modulation

In bi-phase modulation the pulses are sent as shown in Fig 3 or upturned, depending on whether the pulse is a "1" or a "0". In this type of modulation pulses can be sent at a much higher rate and hence longer coding sequences can be added to the signal [1]. This enables the receiver to "lock on", filtering out random noise and eliminating interference and multipath. The technique is also more power efficient.

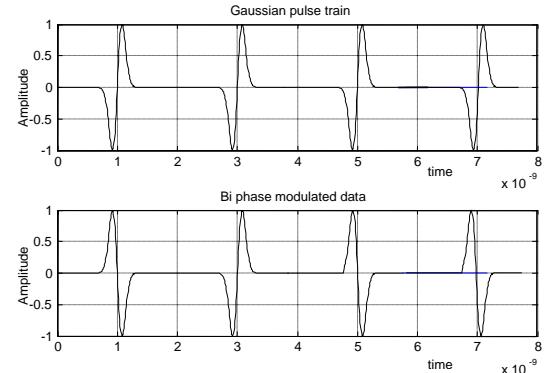


Fig 4.Biphase Modulation

Fig 4 shows the Gaussian monocycle train and the bi-phase modulated pulse train for the binary data 1 0 1 1. For bit “1” the pulse is the same as that generated. For bit “0” an inverted pulse is transmitted.

IV. RECEIVER ARCHITECTURE

Non coherent energy collection approach is used at the receiver. This approach eliminates the need for a bank of correlators or template generators, thus greatly reducing the receiver complexity. The main disadvantage of non coherent approach is the amplification of noise along with the desired signal. However this is compensated by collecting most of the energy of the transmitted data by using a bank of integrators at the receiver. To collect most of the energy, duration of the transmitted bit is required. This is achieved by synchronizing the clocks at both transmitter and receiver. After synchronization energy collection approach is used to detect the transmitted bit.

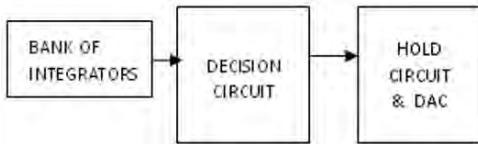


Fig 5. Basic Receiver architecture

A. Bank of Integrators

The energy collection is performed by the integrator bank. Each integrator works for the same duration but at different consecutive time intervals. The time of integration for each integrator is given by,

$$T_s = T_b / N \quad (2)$$

Where T_s is the time of integration of each integrator, T_b is the duration of a transmitted bit and N is the number of integrators.

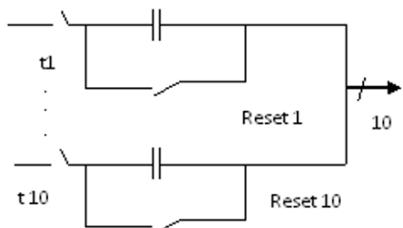


Fig 6 Bank of Integrators

Since the model proposed here is for 4GHz, duration of each bit is 0.25 ns. A total of 10 integrators are used at the receiver

side, the time duration of each integrator can be calculated by (2) as 0.025 ns (0.25 ns/10).

As shown in Fig.6 the first integrator works for 0-0.025 ns, second integrator works for 0.025-0.05 ns and so on. As shown in Fig 6, at any time only one integrator is ON. Ten integrations are performed on a single bit; the computed energy is passed to a decision circuit. The integrators are then reset to repeat the process for the next bit.

B. Decision Circuit

Decision circuit decides on the transmitted bit based on the integrator outputs. It selects the maximum value out of the ten values passed from the integrator and compares it with a threshold to decide if the transmitted bit is a 0 or a 1. Energy collection approach makes the receiver reliable even in a multipath channel. The modulation is orthogonal in time domain, thus threshold can be fixed easily as shown in Fig 7.

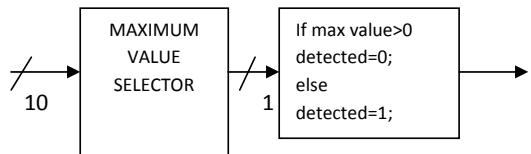


Fig 7. Block diagram of decision circuit

The decision circuit selects the maximum value before the arrival of next set of integrator values to prevent erroneous detection. Thus if the maximum value is greater than 0 the decision is in favour of bit “0” else it is bit “1”.

C. Hold Circuit and DAC

The digitized ECG is reconstructed using the DAC at the receiver to get back the analog ECG signal. A 4 bit shift register is used to store the four consecutive bits at the receiver. After receiving the four bits the DAC reconstructs the ECG signal.

V. SIMULATION RESULTS

The proposed model is tested in SIMULINK and ECG pulses are transmitted for every 69 ns. These ECG pulses are sent to server for automated diagnosis of arrhythmia. The first derivative of Gaussian pulse is used for transmission. All values or samples are taken from SIMULINK and plotted using MATLAB. The simulink blocks for transmitter and receiver are shown in Fig8 and Fig9.

As shown in the Fig 10, Single ECG data 0.1 is decoded as 0110. It is then transmitted as pulses as shown in Fig 11. The channel is modelled with three multipath and an LOS signal as shown in Fig 12.

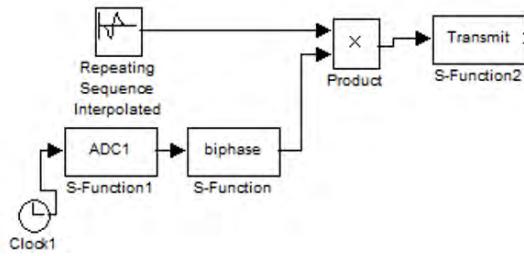


Fig 8. Transmitter Block

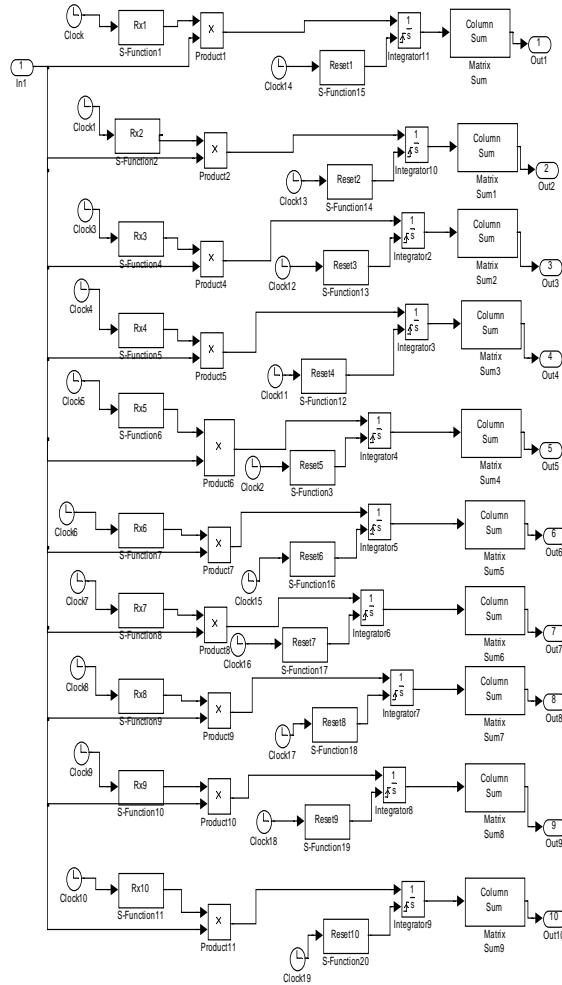


Fig 9. Receiver Block

Receiver then follows energy collection approach to detect the transmitted bit. Corresponding waveforms are shown in Fig 13 and Fig 14. Since the multipath situation is accounted for

while designing the receiver, only noise in the channel affects the bit error rate.

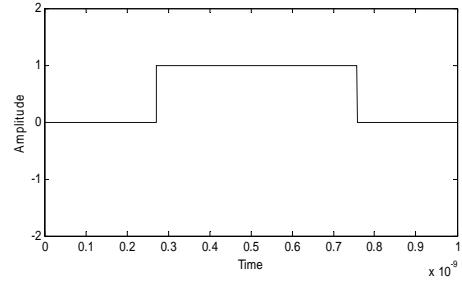


Fig 10. Output of ADC for value 0.1(0110).

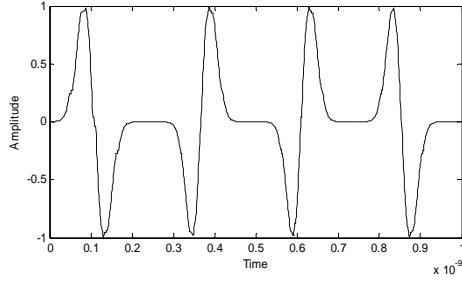


Fig 11. Gaussian pulse equivalent of 0110,

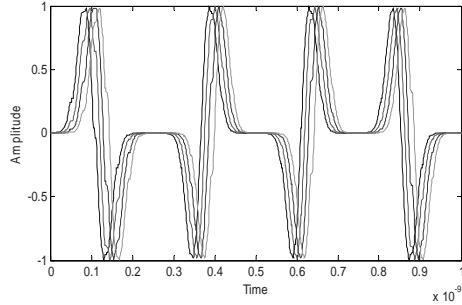


Fig 12. Effect of Multipath and AWGN on transmitted bit,

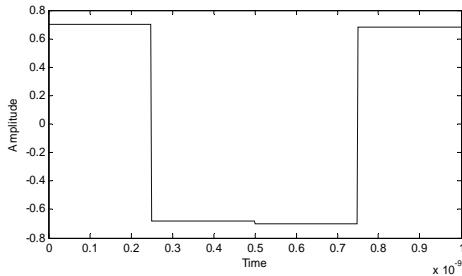


Fig 13. Output of the maximum value selector

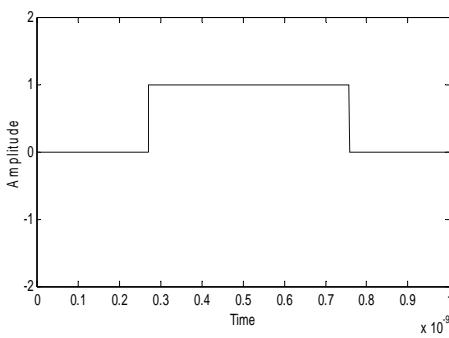


Fig 14. Output of the Decision circuit.

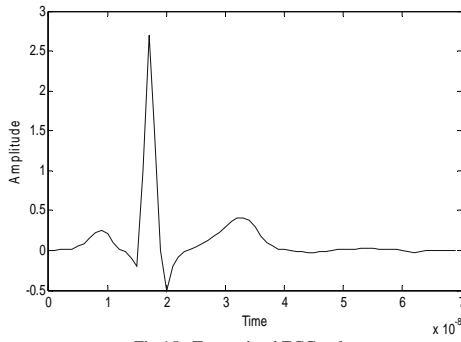


Fig 15. Transmitted ECG pulse

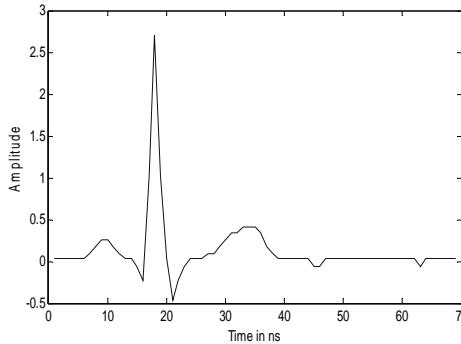


Fig 16. Received ECG pulse

Thus a gradual variation in transmitted signal as shown in Fig 15 takes a step variation in the received signal as shown in Fig 16. This can be reduced by increasing the size of DAC or increasing the sampling rate of ECG. Since most of the applications do not require exact shape, a medium sampling rate is sufficient

For Signal to Noise Ratio (SNR) of less than 2 dB, there is a higher probability for erroneous results. For SNR greater than 5dB there is a steep decrease in BER. Performance is found to

be better for SNR values greater than 8. The BER plot is as shown in Fig 17.

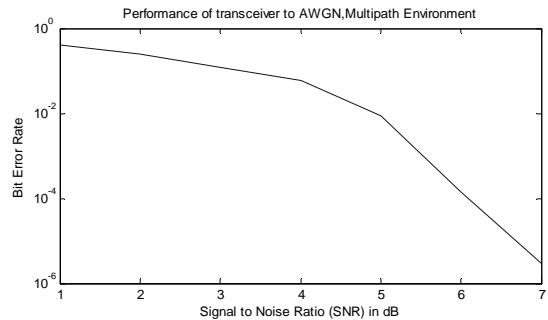


Fig 17. BER plot

VI. CONCLUSION

In this paper, an impulse-radio energy collection UWB system is adopted due to its simplicity and as it is a base band carrier-free technique which requires no up/down conversions or mixers. The pulse shape chosen for transmission is Gaussian. The modulation scheme adopted is Bi-phase modulation. The non-coherent approach employed at the receiver overcomes the need for channel estimation. There is no distortion seen in the received signals with an SNR of 4.5dB. The architecture presented here is thus ideal for wireless sensor network such as automated arrhythmia analysis in mobile patients.

REFERENCE

- [1] Takahide Terada, Shingo Yoshizumi, Yukitoshi Sanada and Tadahiro Kuroda," Transceiver Circuits for Pulse-Based Ultra-Wideband".
- [2] A.T. Kalghatgil, "Challenges in the Design of an Impulse Radio Based Ultra Wide Band Transceiver", IEEE - International Conference on Signal Processing, Communications and Networking, Madras Institute of Technology, Anna University, Chennai, India. Feb. 22-24, 2007. pp. 1-5.
- [3] Payam Heydari, "A Study of Low-Power Ultra Wideband Radio Transceiver Architectures," IEEE Communications Society / WCNC 2005.
- [4] Lucian Stoica, Alberto Rabbachin, Heikki Olavi Repo, Teemu Sakari Tiuraniemi, and Ian Oppermann, "An Ultrawideband System Architecture for Tag Based Wireless Sensor Networks," IEEE transactions on vehicular technology, vol.54, no.5, September 2005
- [5] G.Roberto Aiello and Gerald D.Rogerson, "Ultra-Wideband wireless systems", IEEE microwave magazine, June 2003

Comparison of Cascaded LMS-RLS, LMS and RLS Adaptive Filters in Non-Stationary Environments

Bharath Sridhar I.Akram Sheriff Dr. K.A.Narayanan Kutty S.Sathish Kumar
s.bharath@live.com akram4u28@yahoo.com ka_narayanankutty@ettimadai.amrita.edu s_sathishkumar@ ettimadai.amrita.edu

Abstract- This paper proposes a cascaded LMS-RLS prediction filter for improved performance in non-stationary environments. In this proposed filter, an LMS filter with varying step-size is used as the initial filter for achieving faster convergence rate and then a RLS filter for obtaining improved convergence. Theoretical analysis shows that the proposed technique improves the behavior of the adaptive filter in steady state. Computer simulations using MATLAB SIMULINK validate its performance as the error is found to be significantly less compared to the error rates of individual LMS and RLS filters.

Key words- Adaptive filter, linear prediction, LMS filter, RLS filter.

I. INTRODUCTION

Adaptive signal processing algorithms have a strong impact on Modern Communications where the multipath effects of the channel can degrade the performance of the system. The various applications of adaptive algorithms are in channel equalization, Channel estimation, to avoid Inter symbol interference (ISI), system identification and in Echo cancellation. Adaptive equalizers and interference cancellers can effectively mitigate interference (ISI) and adapt to time-varying channel environments. Adaptive signal processing plays a significant role in improving the performance of receivers, which may be limited by interfering signals. Adaptive linear filters work on the principle that the desired signal or parameters can be extracted from the input through a filtering or estimation operation. The adaptation of the filter parameters is based on minimizing the mean squared error between the filter output and a desired signal.

In the classical adaptive filtering, given an input signal $u(n)$ and a desired signal $d(n)$ we determine the filter weights, w , that minimizes the error $e(n)$ between $z(n)$ and $d(n)$. In addition adaptive algorithms can play a pivotal role estimating the errors of certain channel parameters, for example the channel impulse response (CIR).

After every iteration, more information about the interfering signals or channel parameters becomes available. Then, the interference cancellation is more precise and the channel parameters can be estimated more accurately [3]. Adaptive algorithms find the equalization vectors without explicit knowledge of the channel. The choice of an adaptive filtering algorithm depends on the following factors: rate of convergence, tracking, misadjustment, robustness, computational requirements, structure of information flow and numerical properties. An optimum balance of all these conditions is necessary for an efficient adaptive filter implementation.

The LMS and RLS are two different approaches in adaptive filtering. The LMS follows a stochastic gradient method which results in computational simplicity but the solution hovers around the Weiner solution in a Brownian motion and never manages to reach it. On the other hand, though it is complex, the RLS algorithm has a better rate of convergence having a theoretical zero misadjustment. The number of complex multiplications required in a LMS filter is $2M+1$ whereas the RLS requires $3M(M+3)/2$ complex multiplications for every M tap input vectors [4].

In this paper, we implemented a cascade technique to effectively combine the merits of both LMS and RLS algorithms for obtaining an efficient system performance. A real-time adaptive algorithm implementation demands better order of convergence even in non-stationary environments. Here, LMS and RLS adaptive filters are effectively combined in a differential iterative procedure in such a way that a tradeoff between complexity and order of convergence is obtained.

This paper is structured into the following sections. Section II reviews the LMS algorithm while Section III deals with the RLS algorithm. The proposed Cascaded filter approach is presented in Section IV. The experimental comparison between these filters and their simulation results are detailed in Section V. The design considerations and the shortcomings are also presented.

II. LMS ALGORITHM

The LMS is an important member of the family of stochastic gradient algorithms [4]. The simplicity of this algorithm results from the fact that there are no computations of the pertinent correlation functions or matrix inversions. It basically consists of two processes:

1. A filtering process that computes the output of a linear filter in response to an input signal and generates an estimation error by comparing this output with the desired response.
2. An adaptive process, which involves the automatic adjustment of the parameters of the filter in accordance with the estimation error.

The combination of the above processes constitutes a feedback loop which results in an adaptive weight-control mechanism. The recursive equation for updating the tap-weight vector is given by:

$$\hat{w}(n+1) = \hat{w}(n) + \mu u(n)[d^*(n) - u^H(n) \hat{w}(n)] \quad (1)$$

$$= \hat{w}(n) + \mu u(n)e^*(n) \quad (2)$$

$$\mu_{\text{opt}} = (1/\sigma_v)^2 (\text{tr}[R_w]/\text{tr}[R_u])^{1/2} \quad (3)$$

where, $\text{tr}[R_w]$ denotes the trace of the correlation matrix R_w , $\hat{w}(n+1)$ denotes the updated value of tap weight vector, $\hat{w}(n)$ denotes the previous value of the weight vector, $u(n)$ represents the input signal, $d(n)$ the desired signal, $e(n)$ the error signal and μ denotes the step-size updation parameter. The value of the step size plays an important role in determining the convergence rate of the filter.

III. RLS ALGORITHM

The RLS algorithm is a recursive form of the Least Squares (LS) algorithm. It is recursive because the coefficients at time n are found by updating the coefficients at time $n-1$ using the new input data. The LS algorithm is a block-update algorithm, where the coefficients are computed from scratch at each sample time. The *matrix inversion lemma* is used to derive the RLS algorithm from the LS algorithm[4]. The rate of convergence of the RLS adaptive filter is an order of magnitude faster than that of the LMS filter, due to the fact that it whitens the input data by using the inversion correlation matrix of the data, assumed to be of zero mean.

The iterative inversion is usually performed as,

$$R^{-1}(k) = \frac{1}{\lambda} \left[R^{-1}(k-1) - \frac{R^{-1}(k-1)x(k)x^T(k)R^{-1}(k-1)}{\lambda + x^T(k)R^{-1}(k-1)x(k)} \right] \quad (4)$$

$$\hat{w}(n) = \hat{w}(n-1) + k(n)[d^*(n) - u^H(n) \hat{w}(n-1)] \quad (5)$$

$$= \hat{w}(n-1) + k(n)\xi^*(n) \quad (6)$$

Here, $u^H(n)\hat{w}(n-1)$ represents an estimate of the desired response $d(n)$, based on the old least-squares estimate of the tap weight vector that was made at time $n-1$ and $k(n)$ is the gain factor which is discussed in later sections.

IV. CASCDED LMS-RLS FILTER

In our proposed method, LMS and RLS filters are cascaded. The input signal $u(n)$ along with the desired signal $d(n)$ is applied to the LMS filter. The step size parameter μ has been made as a function of n , the number of iterations.

$$\mu = (2/(\lambda_{\max}+1))^n \quad n=1, 2, \dots, 3N/4 \quad (7)$$

Thus the μ value is exponentially decrementing function of the number of iterations. The variable step size increases the accuracy of the system by adaptively modifying the rate of convergence. Initially the system progresses at a faster pace and the effects due to external noise are minimized. Gradually as the number of iterations increase, the value gets adjusted to μ_{opt} . The output of the LMS filter is given as the input to the RLS filter and the same desired signal is used. The output obtained at this stage represents the output of the cascaded system. Fig.1 demonstrates the comparison of the proposed cascaded architecture over LMS and RLS filters.

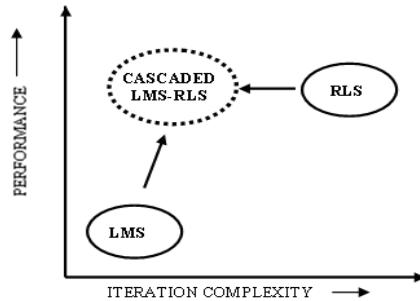


Fig.1. Performance comparison of various filter architectures

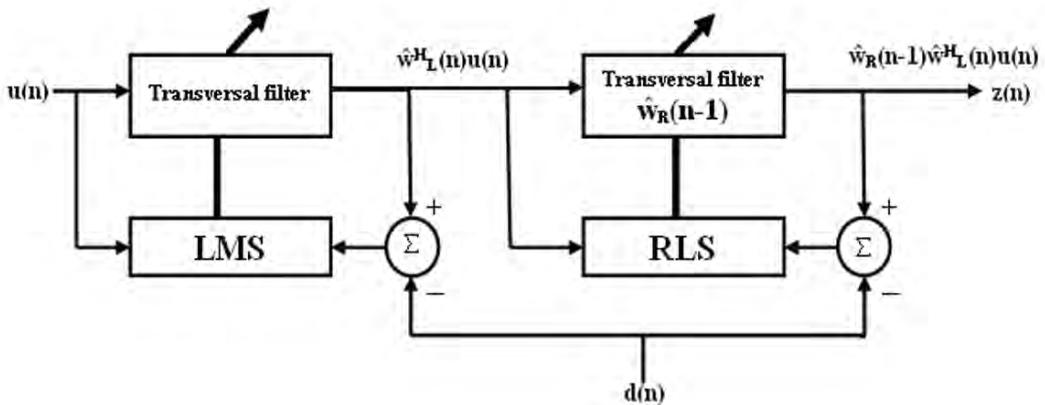


Fig.2 Block diagram of the cascaded filter

The general block diagram of the cascaded architecture is presented in Fig. 2. We propose to increase the system efficiency by differential mode of filter operation. If N denotes the total number of iterations, the first $3N/4$ iterations are performed by the LMS filter and the rest $N/4$ by the RLS filter. This results in the optimum use of both the filters taking into account their computational complexity and performance efficiency.

Let $e(n)$ and $\epsilon(n)$ denote the errors of the LMS and RLS filters respectively and $u(n)$ be the input signal given to the cascaded filter .

$$e(n) = d(n) - \hat{w}_L^H(n)u(n) \quad (8)$$

$$\epsilon(n) = d(n) - \hat{w}_R^H(n-1)y(n) \quad (9)$$

Here, $y(n)$ is the output of the LMS filter given by

$$y(n) = \hat{w}_L(n)u(n) \quad (10)$$

$$z(n) = \hat{w}_R^H(n-1) \hat{w}_L(n)u(n) \quad (11)$$

$$\xi_{TOT} = d(n) - \hat{w}_R^H(n-1) \hat{w}_L(n)u(n) \quad (12)$$

$$\xi_{TOT} = d(n)[1 - \hat{w}_R^H(n-1)] + \hat{w}_R^H(n-1)e(n) \quad (13)$$

The total error of the system is defined by (13) and its value can be approximated as in (14) when error of the LMS filter becomes negligibly small.

$$\xi_{TOT} = (1 - \hat{w}_R^H(n-1))d(n) \quad (14)$$

The input $u(n)$ and output $z(n)$ of the system are related as

$$z(n) = u(n)[\hat{w}_R(n) - k(n)\epsilon^*(n)][\hat{w}_L(n+1) - \mu u(n)\epsilon^*(n)] \quad (15)$$

In (15), $k(n)$ is the gain vector of the RLS filter given by

$$k(n) = R^{-1}(n)u(n) \quad (16)$$

where, $R^{-1}(n)$ is the inverse of the correlation matrix. The performance of the system thus depends on the efficiency of formulation of the inverse matrix. Normally the computational complexity involved in solving a system of equations is $O(N^3)$ where N is the number of equations present.

The idea behind using Levinson algorithm for inverse calculation is that it can reduce the computation of $R^{-1}(n)$ which is actually dependent upon the autocorrelation matrix $R(n)$ [1]. Reducing the computation time implies that we can achieve a faster rate of convergence thereby improving the performance of the system. The symmetric property of the Toeplitz matrix $R(n)$ is exploited in Levinson algorithm to reduce the computation to $O(N^2)$. The problem of solving N equations reduces to solving just two equations instead of N by using the symmetry property. The periodicity of the autocorrelation matrix (Cyclostationarity) is exploited for constructing the $R^{-1}(n)$ matrix. As like other Matrix inversion techniques Levinson algorithm holds good only for Positive definite matrices ($DET(A) \neq 0$).

The Levinson idea is to use the $(p-1)^{\text{th}}$ order forward and backward Levinson estimation vectors as a basis to construct those of order p . This can be done if the backward vector is shifted one (time) notch down. Because the entries in the covariance matrix repeat themselves along main diagonals, the same matrix is found one notch down those diagonals, which results in the pattern of zeros. This operation is done successively and the previous iteration coefficients are used to construct the $\varphi^{-1}(n)$ matrix.

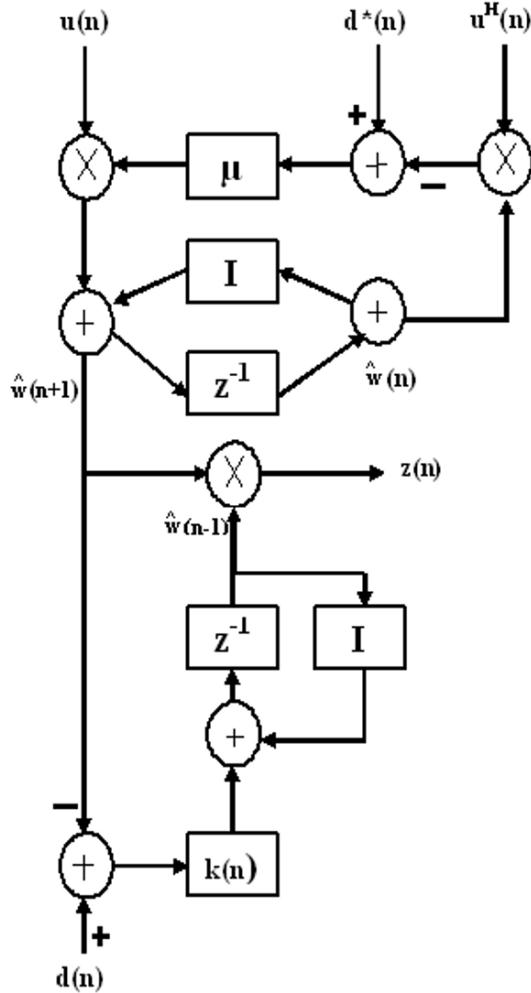


Fig. 3. Cascaded LMS-RLS Filter Architecture

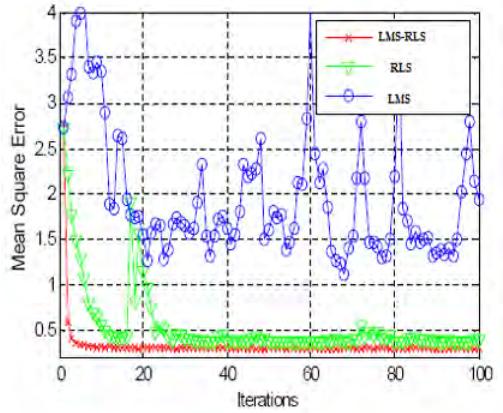


Fig. 4 Mean Square error convergence of the LMS-RLS Cascade, RLS and LMS algorithms

V EXPERIMENTAL ANALYSIS

The proposed architecture of the LMS-RLS cascaded filter is presented in Fig.3. Input signal $u(n)$, its hermitian matrix $u^H(n)$, the desired signal $d(n)$ and its complex conjugate $d^*(n)$ are given as input and the output obtained is $z(n)$. Initially when the noise (randomness) in the system is high, the LMS filter works well resulting in a faster movement towards the Weiner solution. Further when the number of iterations is increased, the system reaches a stable state and now the RLS outperforms the LMS filter in giving a solution that is more close to the optimum solution. Thus the cascaded technique on the whole provides a better solution than that obtained by the use of individual filters.

A comparison of the convergence of the mean square error of our Cascaded method, LMS and RLS is provided in Fig. 4. The desired signal was equal to the reference signal filtered by a sinusoidal bandpass filter, with unit gain at the center frequency [2]. The reference signal had unit power and the RMS of the measurement error was 0.3. Some care had to be taken in the initial stages, when the filter buffer was not full. The same process was implemented using Kalman-LMS algorithm. In the case of the KLMS the buffer can be left at zero, as long as care is taken in choosing the prior standard deviation of the filter coefficients. Both KLMS and our Cascade technique have similar performance with the LMS-RLS showing superior performance at initial stages in a non-stationary environment.

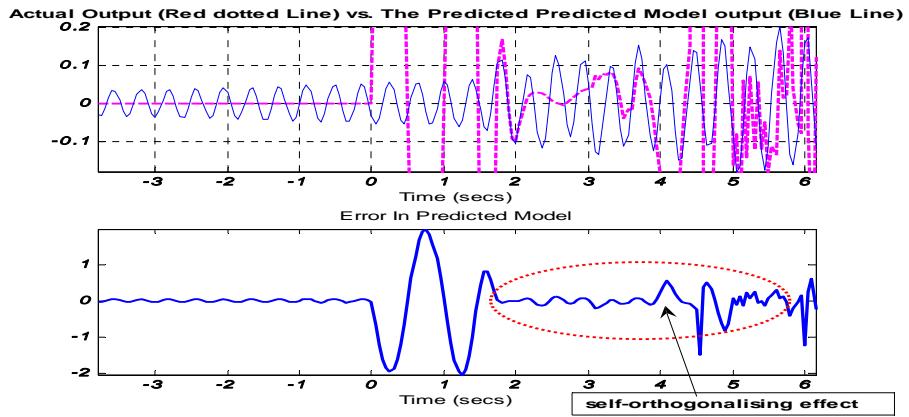


Fig.5 Error plot of the Cascaded LMS-RLS Filter

The error simulation of the cascaded LMS-RLS filter is shown in Fig.5. Initially the error is high as the system chooses a random point as the initial weight vector. Then the error is minimized as the iterations increase. Then the error is minimized as the iterations increase. There are sudden fluctuations due to the non-stationarity of the environment which can be mathematically accounted to a phenomenon known as self-orthogonalising effect. This repeats at periodic intervals as the iterations increase.

There are some drawbacks in the present cascaded filter architecture. Though the rate of convergence and the probability of the solution to reach the optimum Weiner solution is high, the hardware complexity and time delay is comparatively higher than the LMS. But in comparison to the RLS filter, the time delay is less. On the same lines, performance is comparatively higher in RLS than the cascaded filter. Thus a tradeoff between performance and cost (time delay) has been achieved using the proposed architecture.

CONCLUSION

In this paper, a cascaded approach to adaptive filtering is presented. The error plot of the Cascaded LMS-RLS filter exemplifies the fact that error is reduced in comparison to the individual error plots of the LMS and RLS filters. Thus the optimal performance of Cascaded filter can be used in non-stationary environments providing a higher rate of convergence at reduce computations.

Initially for faster tracking and for providing directionality towards Weiner solution the LMS filter with variable step size is incorporated. Then for improving the convergence beyond the capability of the LMS, the RLS filter is employed. All this comes with the limitation of time delay and hardware complexity.

REFERENCES

- [1] Murat Çabuk “Adaptive Step Size and Exponentially Weighted Affine Projection Algorithms”, MS Thesis, Boğaziçi University
- [2] Rongshan Yu and Chi Chung Ko, “Lossless Compression of Digital Audio Using Cascaded RLS-LMS Prediction” *IEEE Transactions on Speech and Audio Processing*, Vol. 11, No.6, November 2003.
- [3] Xu Sun and Sen M. Kuo, “ Active Narrowband Noise Control Systems Using Cascading Adaptive Filters ”, *IEEE Transactions on Audio, Speech and Language Processing*, VOL. 15, NO. 2, February 2007.
- [4] Simon. Haykin, *Adaptive Filter Theory*, 4th edition. Pearson Education,2002.
- [5] Kushner, H. J. and J. Yang, “Analysis of adaptive step size SA algorithms for parameter tracking”, *IEEE Transactions on Automatic Control*, Vol. 40, No. 8, pp. 1403-1410, August 1995.
- [6] Farhang-Boroujeny, B., “Variable-step size LMS algorithm: new developments and experiments”, *IEE Proceedings Visual Image Signal Processing*, Vol. 141, No. 5, pp. 311-317, October 1994.
- [7] Paulo A. C. Lopes, Gonçalo Tavares and José B. Gerald A New Type of Normalized LMS Algorithm Based on the Kalman Filter.

Data Mining Based Network Intrusion Detection System: A Survey

Rasha G. Mohammed Helali

College of Computer Science and Information Technology

Sudan University of Science and Technology

Morgan, Khartoum, Sudan

rasha_800@hotmail.com

Abstract. Significant security problem for networked systems is hostile trespass by users or software. Intruder is one of the most publicized threats to security. Network Intrusion Detection Systems (NIDS) have become a standard component in network security infrastructures. This paper presents the features of signature based NIDS in addition to the current state-of-the-art of Data Mining based NIDS approaches. Moreover, the paper provides general guidance for open research areas and future directions. The intention of this survey is to give the reader a broad overview of the work that has been done at the intersection between intrusion detection and data mining.

Key words: Clustering, Knowledge Discovery and Data Mining cup, Hidden Makov Models, Network Intrusion Detection System, Signature – based IDS.

1. INTRODUCTION

INFORMATION technology has become a key component to support critical infrastructure services in various sectors of society. “In an effort to share information and streamline operations, organizations are creating complex networked systems and opening their networks to customers, suppliers, and other business partners “[1]. While most users of these networks are legitimate users, an open network exposes the network to illegitimate access and use. Increased network complexity, greater access, and a growing emphasis on the Internet have made network security a major concern for organizations [1]. The number of computer security breaches has risen significantly in the recent years. As security incidents become more numerous, IDS tools are becoming increasingly necessary. They round out the security arsenal, working in conjunction with other information security tools, such as firewalls, and allow for the complete supervision of all network activity [2]. Traditional network security approaches have focused on prevention, intrusion detection is therefore needed as another wall to protect computer systems. It becomes increasingly important in recent years to enable firms to reduce undetected intrusions.

This paper reviews the current state of art for using data mining in network intrusion detection context. Moreover it attempts to provide a general guidance in this area enclosed with the major challenges and open research areas.

2. CURRENT USED TECHNIQUES

Traditional methods for intrusion detection which known by signature-based method are based on extensive knowledge of signatures for previously known attacks (attacks already discovered and have signatures). Monitored events are matched against the signatures to detect intrusions. These methods extract features from various audit streams, and detect intrusions by comparing the feature values to a set of attack signatures provided by human experts. The signature database has to be manually revised for each new type of intrusion that is discovered [3].

A significant limitation of such methods is that they can not detect emerging cyber threats which do not have signatures or labeled data corresponding to them. In addition, even if a new attack is discovered and its signature developed, often there is an estimated latency in its deployment across networks [3]. Moreover, the current techniques have several limitations such as producing loads of false alarms and they need extensive training data for the associated technique. These limitations have led to an increasing interest in intrusion detection techniques based on data mining in place of the conventional methods to reveal attacks efficiently.

Intrusion detection techniques can be categorized into misuse detection, which uses patterns of well known attacks or weak spots of the system to identify intrusions and anomaly detection, which tries to determine whether deviation from the established normal usage patterns can be flagged as intrusions. “Misuse detection systems, encode and match the sequence of “signature actions” (e.g., change the ownership of a file) of known intrusion scenarios. The main shortcomings of such systems are: known intrusion patterns have to be hand-coded into the system and they are unable to detect any future (unknown) intrusions that have no matched patterns stored in the system “[4].

Anomaly detection (sub)systems, establish normal usage patterns (profiles) using statistical measures on system features, for example, the CPU and I/O activities by a particular user or program. The main difficulties of these systems are: intuition and experience is relied upon selecting the system features, which can vary greatly among different computing environments; some intrusions can only be detected by studying

the sequential interrelation between events because each event alone may fit the profiles. [5]

3. DATA MINING TECHNIQUES

Data mining has become a very useful technique to reduce information overload and improve decision making by extracting and refining useful knowledge through a process of searching for relationships and patterns from the extensive data collected by organizations [6]-[3]. “The extracted information is used to predict, classify, model and summarize the data being mined. Data mining technologies, such as rule induction, neural networks, genetic algorithms, fuzzy logic and rough sets are used for classification and pattern recognition in many industries”[1]. They have been extensively used in discriminating normal from abnormal behavior in a variety of contexts [7]. In recent years data mining techniques have been successfully used in the context of network intrusion detection [8], [9], [10],[11]. The recent rapid development in data mining has made available a wide variety of algorithms, drawn from the fields of statistics, pattern recognition, machine learning, and database. Several types of algorithms some of them are particularly relevant to what this paper is investigating such as:

- Classification which maps a data item into one of several predefined categories. These algorithms normally output “classifiers” has ability to classify new data in the future, for example, in the form of decision trees or rules. An ideal application in intrusion detection will be together sufficient “normal” and “abnormal” audit data for a user or a program. Here audit data refers to (pre-processed) records, each with a number of features (fields). Then a classification algorithm has been applied to train a classifier that will determine (future) audit data as belonging to the normal class or the abnormal class.
- Clustering which maps data items into groups according to similarity or distance between them. The best use of clustering in NIDS for discovering the deviation from normal use of network “anomaly detection” .
- Link analysis: determines relations between fields in the database. Finding out the correlations in audit data will assist of selecting the right set of system features for intrusion detection.
- Sequence analysis: models sequential patterns. These algorithms can help in understand what (time based) sequence of audit events are frequently encountered together. These frequent event patterns are important when creating behavior profile of a user or program. [1].

4. CURRENT SOLUTIONS

The above sections highlights a general overview on current used tools and it is problems .Moreover, it surveys main techniques of data mining .The next section will shed some light on current solutions which have been adopted begging by how standard dataset have been released.

4.1 GENERATING STANDARD DATASET

Most intrusion detection techniques and basic pattern matching require sets of data to train on. When work on advanced Network Intrusion Detection Systems started in the late of 1990’s, researchers quickly recognized the need for standardized datasets to perform this training.[3]

Brunder discussed this issue in [3]. He started by considering first widely cited datasets for the Information Exploration Shootout which unfortunately, is no longer available. Then he moved to the most famous available datasets Defense Advanced Research Projects Agency DARPA which mentioned in early papers from Lee and Stolfo [12]. They noted the anticipated arrival of a new dataset from the Air Force’s Research Laboratory (AFRL) in Rome. The AFRL, along with MIT’s Lincoln Lab, collected network traffic from their network and used it as the basis for a simulated network. After series of processing data was made available to researchers in 1998 as the DARPA Off-line Intrusion Detection Evaluation. Lee did a great deal in [10] by analyzing DARPA data, and identifying 41 features which can be used in a data mining based NIDS. He provided a copy of the DARPA data that was already preprocessed, by extracting these 41 features, for the 1999 Knowledge Discovery and Data Mining cup 1999 KDD Cup contest, held at the Fifth Association for computing machinery ACM International Conference on Knowledge Discovery and Data Mining.

DARPA and KDD datasets have become a benchmark that can be used without any further processing. Researchers use these datasets to evaluate their models [13], [14], [15], [16], [17], [18].

4.2 DATA MINING TECHNIQUES FOR NIDS

Using data mining in context of NIDS becomes very popular nowadays. The current researches in intrusion detection are on anomaly detection (semi-supervised) and unsupervised approaches. In intrusion detection research, the use of clustering to reduce data for anomaly detection had been popular [19]. Lane and Brodley detail that k-means to compress data and report that Hidden Markov Models HMMs performed slightly better than Instance-Based Learning (IBL) for semi-real user level data [20]. Similarly, Cho focuses on decreasing data for HMM modeling [21]. The author shows that using of fuzzy logic can reduce false positive rates. Also, Stolfo et al advocate Sparse Markov Transducers [22]. However, Yeung and Ding conclude that simple static approaches, such as occurrence frequency distributions and cross entropy between distributions, outperform HMMs [17]. Other anomaly detection studies trialed with RIPPER [16], Apriori [10], frequent episodes [5] [9], attribute-oriented induction [23], and k-means [24]. Fortuna et.al, in [25] propose the use of linear support vector machines (SVMs) for detecting abnormal traffic patterns in the KDD Cup 1999 data. Most studies conclude that anomaly detection does not perform as well as misuse detection [19]. Unsupervised approaches include [17] and [27] which advocate replicated neural networks to detect outliers.

4.3 FRAMEWORKS IMPLEMENTED USING DATA MINING

Different models which define different measures of system behavior have been implemented. An ad hoc presumption that normal and anomaly behavior (or illegitimacy) will be accurately manifested in the chosen set of system features that are modeled and measured [28]. Lee, et al, tried to develop systematic method in [29] for intrusion detection by using data mining techniques. Thus, they attempted to build IDS concentrates on the idea that the short sequence of system call made by program during it's normal execution are very consistent and different from abnormal ones. The proposed a framework consists of classification, association rules and frequent episodes programs to construct detection models. They investigate using of machine learning program – Repeated Incremental Pruning to Produce Error RIPPER – to produce rules to control the classification process. The main weakness of their model that learning algorithm requires training data nearly complete with regard to all possible normal behavior of program or user behavior. Although, they suggested that the addition of temporal-statistic feature would provide good accuracy of classification model, it will be more difficult and time consuming. The reached results are very important since, they confirm that the accuracy of detection model depends on sufficient training data and feature set. In [29] Lee et.al, benefited from their previous experiments. They have suggested a new data mining framework for building intrusion detection models as an attempt to solve the problems related to the need for continues manual update of signature database such as effort and time consumption. They extend the basic association rules and frequent episodes algorithms to accommodate the special requirements in analyzing audit data for both misuse and anomaly detection. The results show that the use combined classifiers–Lean classifiers - each with different set of features is more effective to detect attacks.

An attempt was made by Dokas and Ertoz in [30] to develop a model focuses on the prediction of rare classes. Their experiments take place in DARPA and KDD cup 99 dataset. The results show that the use of Synthetic Minority Over-sampling Technique SMOTE algorithm for misuse detection provides best classification performance. On the other hand, Density-Based Local outlier Detection (LOF) proof high successful for anomaly detection over other schemes.

Simple framework is presented in [31] by Bloedorn,et al. That assists in getting start in building network Intrusion Detection System based on data mining techniques Experiments take place on Massachusetts Institute of Technology Research & Engineering MITRE (MIRE Corporation). They conclude that the use of distance based clustering algorithms is the best solution for anomaly detection. Minnesota University [32] presents an example of combining signature based tool with data mining. It enjoys great operational success, routinely detecting brand new attacks that signature-based systems could not have found. At 2008 Rajeswari etal, introduce a multiple level hybrid classifier for an intrusion detection system in [33]. That uses a combination of tree classifiers which uses Enhanced C4.5 which rely on labeled training data and an Enhanced Fast

Heuristic Clustering Algorithm for mixed data (EFHCAM). The main advantage of this approach is that the system can be trained with unlabelled data and is capable of detecting previously “unseen” attacks. Verification tests have been carried out by using the 1999 KDD Cup data set. From this work, it is observed that significant improvement has been achieved from the viewpoint of both high intrusion detection rate and reasonably low false alarm rate.

In context of integrating fuzzy logic in NIDS different attempts were made. In [34] an attempt was made by Idris and Shanmugam. They proposed a dynamic Intelligent Intrusion Detection System model mixed between anomaly and misuse detection techniques and fuzzy logic. Their idea concentrates on using fuzzy logic to create fuzzy rules to classify audit data. Apriori presented in [5] and Kuok's algorithm [20] was integrated. Their initial experiments showed promising and encouraging results. At 2008 [35] a similar idea has been pursued by Prasad et.al. Genetic Algorithms based on fuzzy logic was used to produce better results. Another challenge was made by Dhanalakshmi and Babu in [36] by proposing architecture for Intrusion Detection methods by using data mining algorithms to mine fuzzy association rules by extracting the best possible rules using Genetic Algorithms. They investigate two reasons for using fuzzy logic, the first, being the involvement of many quantitative features where there is no separation between normal operations and anomalies. The second, fuzzy association rules can be mined to find the abstract correlation among different security features.

A great contribution was introduced in term of real time detection by Peng and Zuo[18]. The use of new adopted techniques such as Frequent-Pattern tree FP-tree structure and Frequent-Pattern growth FP-growth mining method have been investigated. Although, the reached results are evaluated to be satisfied, it concentrates on misuse detection only.

Nowadays, data mining based NIDS moves through different direction that integrates agent concept into NIDS implementation to accommodate real time detection. This issue was investigated firstly in [28]. An agent based solution was proposed for real time detection. An adaptive NIDS using data mining technology with multi-agent concept is developed in [37]. The proposed system is constructed by a number of agents, which are totally different in both training and detecting processes. Each of the agents has its own strength on capturing a kind of network behavior and hence the system has strength on detecting different types of attack. The experimental results showed that the frequent patterns mined from the audit data could be used as reliable agents, which outperformed from traditional signature-based NIDS. In [38] multi-agent becomes as a solution for limitations of anomaly detection approaches that suffer from comparatively higher error rate and low performance. Experiments performed on-line on real campus network illustrate system suitability for real-time network surveillance.

5. OPEN RESEARCH AREAS

In the previous sections we survey what have been done in the cross sections of data mining NIDS. Although there is a

great progress in detection accuracy, still there is a limitation on context of using data mining for online detection especially for anomaly detection scheme. The usage of agent based technique represents good contribution for overcoming the offline limitation of data mining. But still no optimum solution is found. Future directions expected to go deep on integrating intelligent agent technique with data mining for NIDS.

6. CONCLUSION

This paper reviews the state-of-art for using data mining in network security context. Especially on Network Intrusion Detection Systems. As we notice most of the studies aim to find the most optimum solutions. But till now we can't say they really found it. Thus, still there is much research needed in this area.

REFERENCES

- [1] Zhu, Dan, Premkumar, G, Zhang, Xiaoning, Chu, Chao-Hsien (2001) A comparison of alternative methods. [Online] Available from:
http://findarticles.com/p/articles/mi_qa3713/is_200110/ai_n8954240.
- [2] Marinova V,(2007) A Short Survey of Intrusion Detection Systems*, problems of engineering cybernetics and robotics, 58.
- [3] Brugger ,T(June 9, 2004) University of California, Davis Data Mining Methods for Network Intrusion Detection 1...56.
- [4] Kuok C., Fu A., Wong M.,(2001) "Mining fuzzy association rules in databases" SIGMOD Record 17 (1) 41-46.
- [5] Julisch, K. & Dacier, M. (2002). Mining Intrusion Detection Alarms for Actionable Knowledge. Proc. of SIGKDD02, 366-375.
- [6] Dunham M (2003) Data mining Introductory and advance Topics, Pearson Education. Inc.
- [7] Forrest, S., S. A. Hofmeyr, and A. Somayaji (1997, October). Computer immunology. Communications of the ACM 40 (10), 88-96.
- [8] Hofmeyr, S. A. and S. Forrest (1999). Immunizing computer networks: Getting all the machines in your network to fight the hacker disease. In Proc. of the 1999 IEEE Symp. on Security and Privacy, Oakland, CA. IEEE Computer Society Press.
- [9] Dokas P., Ertöz L.(2002), Data Mining for Network intrusion detection ,- Proc.NFS workshop on next generation data mining , csee.umbc.edu , 21-29.
- [10] Lee, W. and S. J. Stolfo (2000). A framework for constructing features and models for intrusion detection systems. Information and System Security 3 (4), 227–261.
- [11] Chandola V, Eilertson E, Ertöz L, Simon G, and Kumar V,, Data Mining for Cyber Security,(2006) Data Warehousing and Data Mining Techniques for Computer Security, editor Anoop Singh, Springer.
- [12] Lee, W. K. W. Mok, and S. J. Stolfo(1998). Mining sequential patterns: Techniques, visualization, and applications. Submitted for publication, August 1998.1-9.
- [13] Ert'oz, L , Eilertson, E, Aleksandar Lazarevic, Pang-Ning Tan_, Vipin Kumar (2004) MINDS - Minnesota Intrusion Detection System , Technical report at university of Minnesota 1..21.
- [14] Chittur, A. (2001). Model generation for an intrusion detection system using genetic algorithms. High School Honors Thesis, Ossining High School. In cooperation with Columbia University, 3 – 19.
- [15] Neri, F. (2000a, 16–19 July). Comparing local search with respect to genetic evolution to detect intrusion in computer networks. In Proc. of the 2000 Congress on Evolutionary Computation CEC00, La Jolla, CA, pp. 238– 243. IEEE Press.
- [16] Fan, W. (2001). Cost-Sensitive, Scalable and Adaptive Learning Using Ensemble- based Methods. Ph. D. thesis, Columbia Univ.
- [17] Yeung, D.-Y. And C. Chow (2002, 11–15 August). Parzen- window network intrusion detectors. In Proc. of the Sixteenth International Conference on Pattern Recognition, Volume 4, Quebec City, Canada, pp. 385–388. IEEE Computer Society.
- [18] Peng, †. T, Zuo, W,(February 2006) IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B.
- [19] Phua1C, lee1 V, Smith1 K & ross gayler2, A Comprehensive Survey of Data Mining-based Fraud Detection Research Final version 2: 9/02/2005
- [20] Mukkamala, S., A. H. Sung, and A. Abraham (2002). Identifying key variables for intrusion detection using soft computing. <http://citeseer.nj.nec.com/544845.html>.
- [21] Cho, S. (2002). Incorporating Soft Computing Techniques into a Probabilistic Intrusion Detection System. IEEE Transactions on Systems, Man and Cybernetics 32(2): 154-160.
- [22] Lee, W., S. J. Stolfo, P. K. Chan, E. Eskin, W. Fan, M. Miller, S. Herschkop, and J. Zhang (2001, June). Real time data mining- based intrusion detection. In Proc. Second DARPA Information Survivability Conference and Exposition, Anaheim, CA, pp. 85–100. IEEE Computer Society.
- [23] Jiawei, H, and Micheline Kamber(2001). Data Mining:Concepts and Techniques. Higher Education Press,3-10
- [24] Sequeira, K. & Zaki, M. (2002). ADMIT: Anomaly-based Data Mining for Intrusions. Proc. of SIGKDD02, 386-395.
- [25] Fortuna a, Fortuna b, mohorčič m,(2007) anomaly detection in computer networks using linear svms
- [26] Hawkins, S., He, H., Williams, G. & Baxter, R. (2002). Outlier Detection Using Replicator Neural Networks. Proc. of DaWaK2002, 170-180.
- [27] Williams, G., Baxter, R., He, H. & Hawkins, S. (2002). A Comparative Study of RNN for Outlier Detection in Data Mining. Proc. of ICDM02, 709-712.
- [28] Lee W. Salvatore J. Stolfo Kui W. Mok.(1999) A Data Mining Framework for Building Intrusion Detection Models (This research is supported in part by grants from DARPA (F30602-96-1-0311) and NSF (IRI-96-32225 and

- CDA-96-25374).submitted to the 1999 IEEE Symposium on Security and Privacy.
- [29] Lane, T. & Bradley, C. (2003). An Empirical Study of Two Approaches to Sequence Learning for Anomaly Detection. *Machine Learning* 51:73-107.
- [30] Didaci, L., G. Giacinto, and F. Roli (2002). Ensemble learning for intrusion detection in computer networks. <http://citeseer.nj.nec.com/533620.html>.
- [31] Bloedorn E, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot, and Jonathan Tivel(2002). Data mining for network intrusion detection: How to get started. Technical report, The MITRE Corporation, 2001. 1-9.
- [32] Minnesota university, Minnesota Intrusion Detection System.[Online] Available from: www.cs.umn.edu/research/MINDS [Accessed 15 November 2007] .
- [33] Rajeswari, L. Prema; Kannan, A., (4-6 Jan. 2008) An Intrusion Detection System Based on Multiple Level Hybrid Classifier using Enhanced C4.5 , Communications and Networking, 2008. ICSCN aps, International Conference, Page(s):75 – 79.
- [34] Idris , N, Shanmugam ,B, (2006) Novel Attack Detection Using Fuzzy Logic and Data Mining. *Security and Management*: 26-31.
- [35] Prasad G, Dhanalakshmi Y, Dr.Vijaya V Kumar Dr Babu R, Modeling An Intrusion Detection System Using Data Mining And Genetic Algorithms Based On Fuzzy Logic, *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.7, July 2008.
- [36] Dhanalakshmi and Babu,(February 2008) Intrusion Detection Using Data Mining Along Fuzzy Logic and Genetic Algorithms, *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.2.
- [37] Cheung-Leung Lui Tak-Chung Fu Ting-Yee Cheung Agent-based network intrusion detection system using data mining approaches, *Information Technology and Applications*, 2005. ICITA 2005. Publication Date: 4-7 July 2005: 131- 136 vol.1, ISBN: 0-7695-2316-1.
- [38] Bartoš K, Grill M, Krmíček V, Rehák M, Celeda P,(July 2008) Flow Based Network Intrusion Detection System using Hardware-Accelerated NetFlow Probes, abriela Krčmárová, Petr Sojka (Eds.): CESNET Conference 2008, Proceedings, pp. 49–56.

VDisaster recovery with the help of real time video streaming using MANET support

Abdelshakour Abuzneid, Chennaipattinam Raghuram Vijay Iyengar, Ramaswamy Gandhi Dasan Prabhu
University of Bridgeport, Bridgeport, CT
abuzneid@bridgeport.edu, vchennai@bridgeport.edu, gramaswa@bridgeport.edu

Abstract- The calamities occurs unfortunately in the neighbourhood, which deteriorates the communication infrastructure completely. To recover completely from this disaster the wireless communication infrastructure should be replaced immediately, so that it can be in mobility everywhere and at the same time be connected to the headquarters base station as well. In this paper we try to implement the Mobile Ad Hoc communications (MANET) as the primary mode of communication between the nodes, which forms the rescue team. An Ad-Hoc communications infrastructure, with support for multimedia traffic such as voice over IP and videotostreaming, must be quickly replaced to support the command, control and communication needs of the rescue and recovery operations. Moreover the realtime video communication possibility is analyzed along with the conventional voice communication systems. In this paper we examine the combination of the Wi-Fi, Wi-Max and the MANET to efficiently transmit the data across the wide area networks to meet the necessity of the disaster recovery operations.

INTRODUCTION

Conventionally, the wired infrastructure was used for the disaster recovery to signal the rescue team and the recovery operations was performed. The conventional process was much time consuming and by the time salvage is implemented full fledgedly, a lot of life is forfeited. To avoid this new innovative way of communication should be instilled so that we can save many lives. In the recent past the disaster recovery operations was implemented by the wired voice communication by informing the rescue team or the fire department and it takes quite a lot of time to arrive at the location. Tentatively, some advancements have been tested and implemented which proved to support the VOIP telephony voice quality calls, which was limited as well. The next biggest challenge was to relay this information to a base station which was located many kilometers away. The communication was made between the rescue team and the headquarters base station with the aforesaid VOIP telephony system which supported the limited number of quality calls. But, there was no provision available to relay the real time images, to the base station constantly without any

hassles or the interference. This communication is in practice within a short range of campuses or an office with the live relay of video images or the broadcasting through the satellite. But these systems were having some delays or the interference. Many experiments have been conducted to overcome these problems and implemented as well, but none of them proved efficient. Moreover, the real time video conferencing or communicable relaying of information was not in place to support the disaster recovery efficiently. In this paper we have tried implementing a Mobile Ad Hoc Network (MANET) as a rescue team in various places as a hotspot, which will be capable of this real time video communication within themselves and between the base stations also. This setup would support the conventional voice communication with more number of quality calls too.

BACKGROUND

The background of this project is the idea that triggered the need of the real time efficient communication for both voice and the video on a wide bandwidth and data rate available. The resources available should not be wasted instead of making the most out of it. The high end evolving application WiMAX can also be used instead of the satellite gateway at each point reducing the implementation cost on a large scale. WiMAX has its own advantages than the Wi-Fi which is based on the IEEE 802.11 standard. WiMAX covers a vast distance of more than 35 kilometers which is more than enough for the effective communication. Basically, the Ad Hoc networking is the new trend evolving in the usage of primary needs such as military operations, security, etc., But, if we have it implemented on the day to day activity needs it would play a vital role in saving more lives. The basic structure on which it works has been shown at the following screenshot. The MANET also is connected with a local gateway to the headquarters base station through the towers. Here in this project we propose an idea of implementing the WiMAX instead of the satellite communication or the IP networks. But in the near future this can be conceived

with the coverage of vast area and efficient communication.

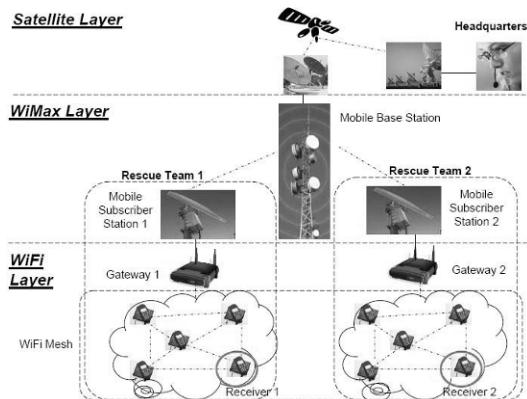


Figure 1. Basic Model showing the Network Scenario

METHODOLOGY

In this project, the attempt made to combine the high-end technologies like MANET, Wi-Fi, wired with the IP network has been analysed. To achieve this, commendable simulator called OPNET Modeler (version 14) has been used. OPNET Modeler is very advantageous in terms of research works and the network design in the real time network conditions. It can be used to visualize the need and realize the possibilities. Opnet modeler is used to create the geographical terrain in an interactive scenario and allows us to add the components and edit the attributes. The simulator itself is built with the vast number of components which can be used to create our network scenario efficiently. Simulation project is functionally divided into network level, node level, process level. The network level has the functionalities of the large IP networks, node level serves the individual devices like Routers, Switches and servers. Process level deals with the individual protocols like MAC, IP, TCP, UDP. Traditional Internet applications can be used to generate traffic. Few of the applications are web browsing, FTP, Telnet, Email, Voice over IP.

The Opnet modeler is used here to implement few of the MANETs and the Base Station which can be the control base to monitor the activities of these MANETs. We name these MANETs as the rescue teams since they will carry out the rescue operations. The main concentration is on the MANETs where the communication between the nodes has to be carried out efficiently. The disaster place needs more attention than any other place. Now these MANETs should be connected to the main Base station to

monitor the activities. At the same time the information has to be sent to the base station to give the feedback. In the next section we have briefly described about our scenarios and the network setup.

DESCRIPTION

In this section we give a clear description of the network scenarios of the connection made and the method of editing the attributes for each components. Firstly, Opnet modeler has the provision for choosing the work space as per the user needs. Accordingly we choose the following network space to support our scenario.

Initial Topology	Create Empty Scenario
Network Scale	USA Map
Model Family	None

Table 1: Table showing Network Preferences

We choose the network scale as USA map because we are trying to portray the network created in the terrain of various zones in the USA where rescue teams should be installed. The Base Station should be installed at one fixed point. The main scenario which shows the overall connection has been shown in the following screen shot.



Figure 2. Panoramic view of the whole network

The screen shot shown above has the Base Station connected to the MANETs through the 100 Mbps links and the in depth setup will be explained in the following discussions. Here in this view the USA map is shown where the network has been arranged to serve a diverse area in USA where disaster can be presumed to occur.

We have the base station shown up in the following discussion where the Wi-Fi has been put in place of the Wired Ethernet which can again be in mobility for a few meters and still deliver the efficient communication possible as the wired ethernet communications. The following screen shot shows the in depth connection of the base station which has the source information which can back up the MANETs and give the feedback to them by

monitoring. In turn the MANETs can support the same applications which the base station shares with them immediately.

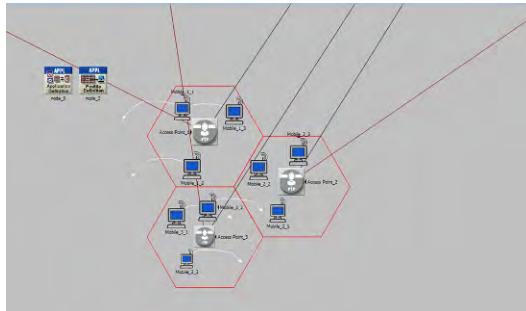


Figure 3: Screen Shot showing the Base Station

As we have shown in the above screen shot there are 3 access points installed with three BSS identifiers with 3 nodes in each cell modified to act according to the trajectory path motion. Here we enable the applications of the real time video streaming and the voice conferencing on the application config and enable the same at the Profile config. Now when we do this the applications that we have designed will be enabled to support in the overall scenario so we can choose accordingly. Moreover in this base station scenario the ip back bone has been connected to give the access to the outside world for accessing the web browsing and other additional facilities to create traffic as required.

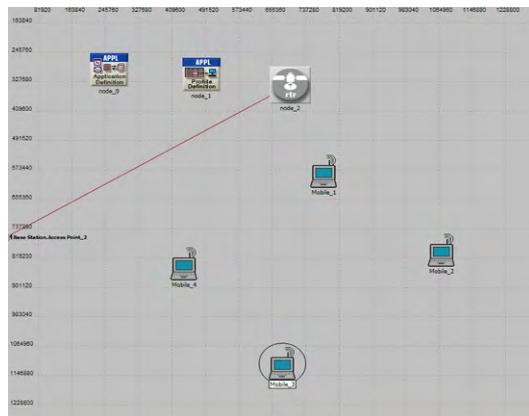


Figure 4: Screen Shot showing the MANET scenario

The above figure shows the screen shot of one of the MANETs, and the nodes are in constant mobility. We establish a Gateway to connect the MANET to the outside world.



Figure 5: Screen Shot showing the MANET 2

The above figure 5 again shows the same kind of the MANET with the same kind of attributes edited according to the need of the user.

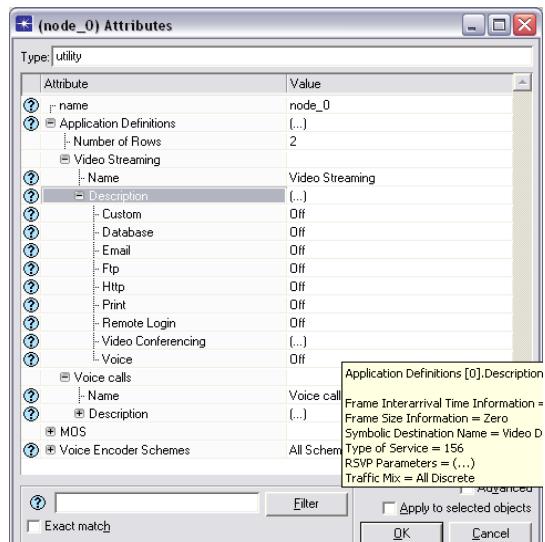


Figure 6:Modifying Applications of the Base Station

The above figure shows the application config editing where we add the necessary applications like the video conferencing and the voice conferencing at the same time. In the voice call attribute we can choose the codec that can be supported to efficiently support the highest number of quality calls with the less amount of hassles.

After we create the applications that can be supported we have to generate the traffic within the nodes and the access points to show the output.

This section completely describes about the network setup used to create the network. The Video streaming is the crucial attribute needed in our scenario along with the voice parameter using the codecs that supports efficient voice communication.

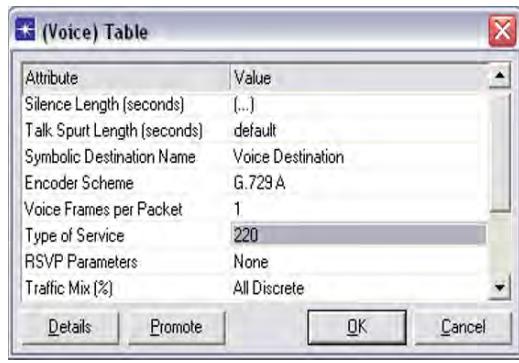


Figure 7: Configuration of the Voice Parameter

Likewise, in the screen shot shown above the voice parameters has been modified to the need of the user. Accordingly we choose the G.729 A which can be supported to give the highest number of quality calls in any terrain region.

As we said earlier, the attributes edited are based on the access points which enables the wireless networking possible and the access point functionality should be enabled. This access points act based upon the Basic Service Set (BSS) identifier, where each and every node in that particular cell should be directed to the BSS number of the particular access point of the same cell. Likewise, each and every access point in each cell will be allotted with a BSS identifier.

The video conferencing within the MANET can be enabled by defining the applications that has to be supported. We can define to support the video streaming and the voice conferencing within the MANET and the base station.

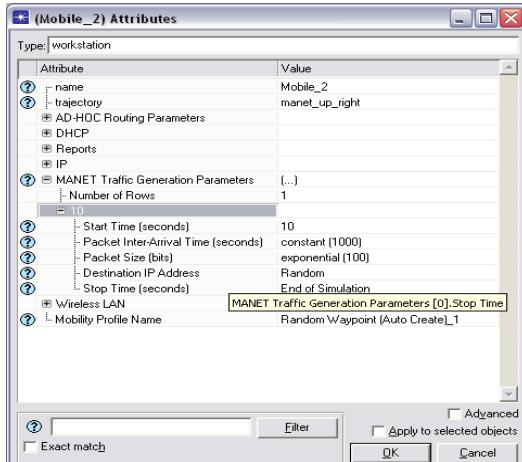


Figure 8: Generating the Traffic within the MANET

The above figure shows the generation of traffic within the nodes of the MANET. Here the start time has been set to the constant in seconds along with the constant interarrival time. Moreover the nodes should be allotted with the Class B IP Addresses to enable the path taken by the network to reach its destination.

RESULTS

The results has been shown up after the proposed establishment of the network connections. We have to choose the required statistics to be shown as a result. According to that we choose few of the attributes which will support the disaster recovery scenario that we anticipate. The few of the statistics that we chose like MANET, Wireless LAN, AODV would satisfy our need to explain the Ad-Hoc parameters, Wi-Fi functionality and the routing analogy respectively.

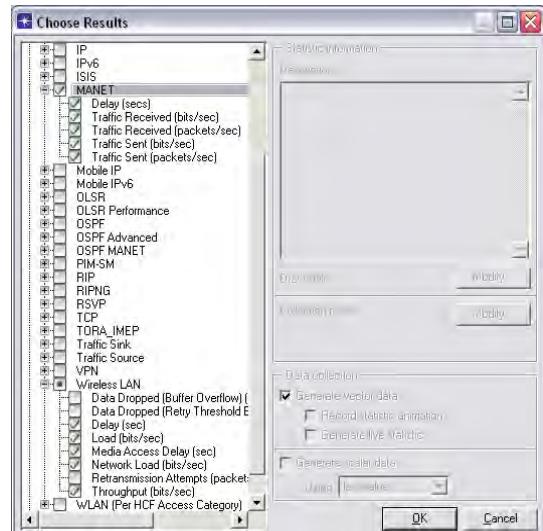


Figure 9: Choosing Global Statistics for the result

After we choose all these results we simulate the whole scenario, which will collect all the information and combine it to produce the output. Based on each and every selection we can analyze the topology and conclude about the efficiency of the networking. In the following screen shots we provide few of the analogy that can be made based on the outputs. Moreover in the OPNET modeler the output windows can be modified to show the output on varying kinds like As Is mode, Average mode, Multiplier, Exponential, Probabilty function etc., We can design the multiple outputs to be shown as stacked output or the overlaid output as shown in the following outputs. Along with the Global Statistics we can choose the

Object Statistics to define about the individual objects behaviour to the proposed networking.

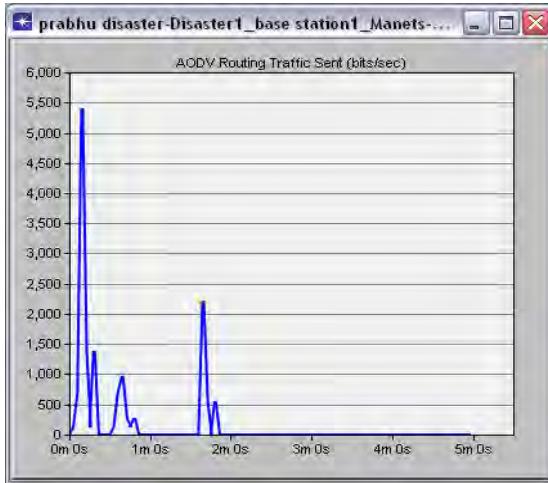


Figure 10: AODV Routing Traffic (Bits/Sec)

The above screen shot show the traffic sent in the AODV where initially the traffic reaches a peak and when the network gets distributed it goes down gradually.

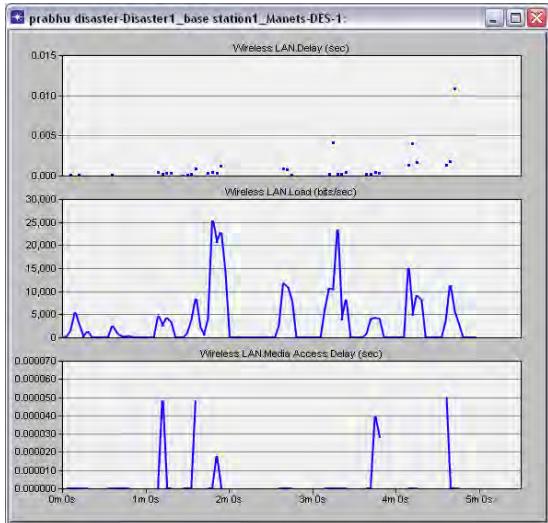


Figure 11: Parameters in the Wireless LAN

The above figure shows the various parameters of the wireless LAN stacked on a single window. The first parameter shows the delay in the Wi-Fi, the second parameter shows the load imposed on the Wi-Fi, and the third parameter shows the Media Access Delay based on the video streaming and the voice conferencing.

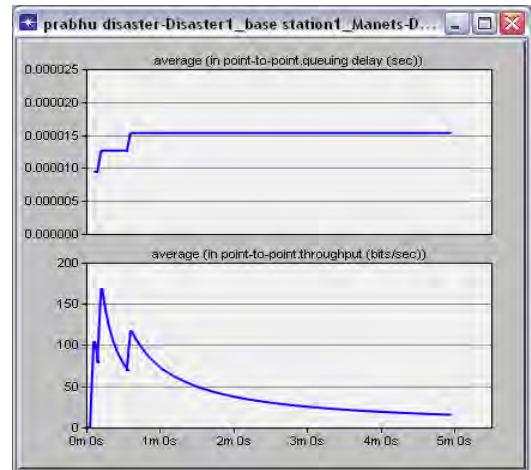


Figure 12: Queuing delay and throughput on MANET

The above figure shows the queuing delay and the Throughput of the MANET and the Base Sation combined together. It helps us to identify that the information from the MANET reaches the Base station with out any hassles or obstructions. From the above shown screen shot we infer that the relay of information has been constant all way through which proves the fact that our scenario works perfectly fine.

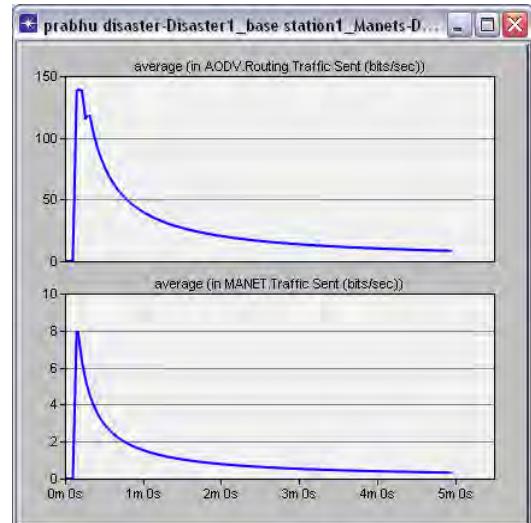


Figure 13: Traffic sent on the AODV and MANET

The above figure shows the traffic generated in the AODV routing and the MANET rescue teams. We infer that the MANET i.e., rescue teams strictly follow the AODV routing parameter to route the packets to the destination. Both the output shown above are almost the same which proves the above explained fact of routing path that it takes. All the rescue teams follow the same rule to keep intact.

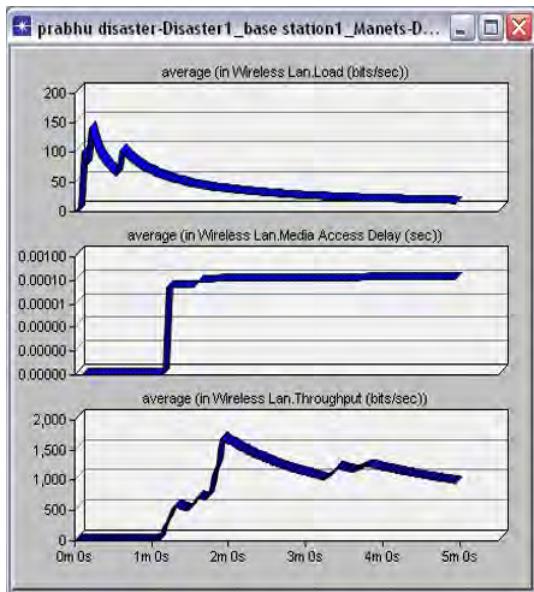


Figure 14: 3D View of the Wireless LAN parameters

The above figure shows the possibility of the Opnet to show the output in three dimensional view to make the output more interactive.

Moreover, the scalar statistics outputs can be combined with each other on the result window on the basis of time average. The following screen shots show those output.

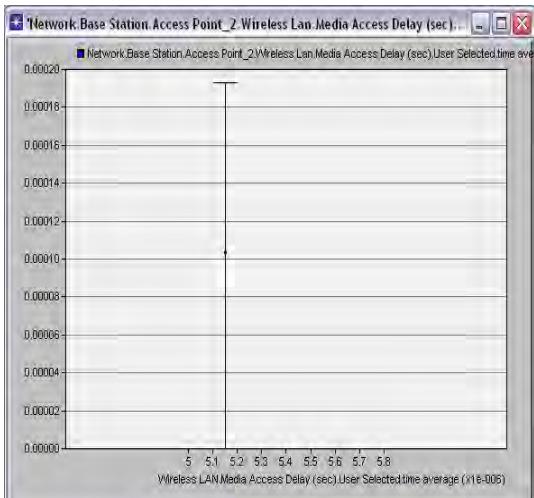


Figure 15: Media Access Delay on the Base Station

The above figure shows the media access delay on the base station the wireless LAN within the access point 2. There are various other analogy that we can do based on various other attributes.

The improvisation can be made on the design by adding either the satellite communication or the WiMax towers in the vicinity of the subnet network domain to eliminate the direct connection of the base station and the MANET using the high power network link. But, in the near future this can be affordable and be realized for the betterment.

CONCLUSION

The disaster like earthquake, fire, tsunami can cause a vast destruction of lives and the networking. Specifically, the wired network can be destroyed on a wide range which can lead to furthermore life savage. To overcome this problem we have come up with the proposal of collaborative action of the Wi-Fi and the Ad-Hoc networks with the combination of the real time video streaming and the voice conferencing within the MANET nodes and within the MANET (Rescue team) and the Wi-Fi (Base Station). This can be made possible while the individual nodes are in continuous mobility. On implementing this the simulation results showed up a positive output where the video and voice conferencing can reduce the network misconception and in turn the number of life savages drastically.

In the near future, the steps can be taken to improve the communication infrastructure by implementing the WiMax towers to connect these end infrastructures to cover up a wide area of terrain region with more viability of the signals and the applications.

REFERENCES

- [1] Weiquan Lu, Winston K. G. Seah, Edwin W. C. Peh, Yu Ge, "Communications Support for Disaster Recovery Operations using Hybrid Mobile Ad-Hoc Networks" Network Technology department, Institute for Infocomm Research, A*STAR, Singapore National University of Singapore, Singapore
- [2] Gil Zussman and Adrian Segall, "Energy Efficient Routing in Ad Hoc Disaster Recovery Networks" Department of Electrical Engineering ,Technion – Israel Institute of Technology, in IEEE INFOCOM 2003
- [3] Victor Carrascal Frias', Guillermo Diaz Delgado, Monica Aguilar Igualt, "Multipath Routing for video-streaming services over IEEE 802.11e Ad hoc Networks" in Technical University of Catalonia (UPC), Telematics Engineering Department Barcelona, Spain , Queretaro State University (UAQ), Faculty of Informatics, Queretaro, Mexico, Unpublished
- [4] Yi-Sheng Su, Szu-Lin Su, and Jung-Shian Li, "Topology-Independent Link Activation Scheduling Schemes for Mobile CDMA Ad Hoc Networks" IEEE Transactions on mobile computing 2007.

Index

A

Access

control, 9, 41, 72, 77, 100, 159–160, 295, 298, 391, 424, 450
technologies, 5, 7, 161, 305

Adaptive combiner-equalizer, 385–389

Adaptive filter, 495–499

Additive White Gaussian Noise (AWGN), 49–50, 162, 164, 185, 350, 462, 492

Address

information, 140–141
management, 223–228

Ad-Hoc networks, 217–221, 223, 357, 443, 476, 512

Admission threshold, 17–18, 21–22

Advanced applications, 155, 158

Agent-based parallel implementation, 189–194

Allocation of changes, 362–363, 365–366

Alternative Multi-hypothesis Motion

Compensated Prediction (AMCP), 311–315

Ambient air temperature, 437

Angle of arrival (AoA), 264

Ant colony algorithms, 223

Artificial neural networks, 355–360

Attack

detection, 129, 132–133, 317
subgraph, 135–138

Authenticated group key agreement protocol, 245–250

Authentication information alignment, 65–70

Authentication test, 245–246, 248

Authorization, 67–68, 71–73, 77–78, 293–294, 297, 355, 424, 450

Auto regressive (AR), 258, 349–353

Average waiting time, 257–258, 284–286, 405–406

B

Balancing streaming, 403–408

Bandwidth, 4, 9, 60, 64, 87, 93, 99, 109, 111, 121, 150, 152–153, 155, 157–158, 160–161, 168–169, 172, 184–185, 191, 195, 239, 251, 253, 255–256, 281–282, 287–288, 311, 343–345, 425, 431, 443, 462, 483–484, 487, 489–490, 507

Basestation antenna, 189, 347

Base Station Controller (BSC), 457–460, 465–468

Base Transceiver Station (BTS), 457–460,

465–469

BBC I-Player, 403

Besides tracking, 143–147

Binary phase modulation, 490–491, 493

Binding data to geographic coordinates, 207

BioAPI, 69–70

Bit error rate (BER), 42, 49–51, 164–165, 195, 288, 291, 352–353, 386–389, 462–463, 489, 492–493

Blocking probability, 149, 151–152, 154, 466

Border Gateway Protocol (BGP), 105–110, 159

Broadband Wireless Access (BWA), 47, 161

Browser, 5, 130, 298, 323–328, 419

C

Capacity analysis, 275

Cellular systems, 99, 238, 472

Cellular telephony, 465

Checksum, 140, 196, 450

CIS, 437–438

Cluster, 11, 42–45, 123–127, 212, 245–246, 248–250, 347, 382–383, 387–388, 409–411, 417, 478–480

Code division multiple access (CDMA), 124, 288–291, 461–463, 465, 467

Cognitive networks, 9–10

Collaborative approach, 239–244

Collision avoidance regulations, 373

Communication integration, 323, 328

Complex networks, 211–216, 379, 382, 384, 501

Computer

networks, 93, 129, 133–134, 191, 355, 379, 381

performance, 192, 339

Confidentiality, 35, 37–38, 54, 239, 293–294, 300, 331, 423–424, 443–444, 447, 450

Congestion control, 1, 67–169, 81–82, 93–97, 251–256

Connectivity, 41, 44–45, 47, 99, 213–214, 281, 287–288, 296, 355, 382, 397, 472

Context-aware system, 305, 309

Control mechanisms, 168, 251–256

Convolutional code, 161–162

Convolutional turbo code (CTC), 47–49, 161, 163–165

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), 53–57

Cross domain federation, 65–70

Cross-layer, 9–14

Cryptosystem, 87, 395

D

Data

authentication, 423–426

gathering, 343–348, 411, 477

integrity, 35, 38, 87, 293, 295–296, 420, 443, 449–451

protection, 31, 35–39

segment, 140–141

throughput, 281–282, 284–286

Demand accesses, 403–408

Denial of services (DoS), 3, 31, 43, 317–318, 355–357, 359

Detection phase latency time, 299, 302

Differentiated services networks, 93–97

Digital signature, 87, 294, 296, 329–331, 425–426, 450

Directed diffusion, 477–480

Direct sequence code division multiple access (DS-CDMA), 291, 349, 461, 463

Disaster recovery, 417–420, 507–512

Distance based clustering protocol (DBCP), 409–411

Distance source routing (DSR), 269–274

Distributed modular audio recognition

framework (DMARF), 417–420, 423–424

Distributed virtual NOC (dvNOC), 155–160

Diversity combining, 385–386

3D media over next generation networks, 483

DUT, 209

Dynamic spectrum allocation (DSA), 9, 426–427, 453

E

Elitism, 229–233, 237

Elliptic curves, 87–92

Encoding multimedia evidence, 413–416

Encrypted database technique, 293–298

Encryption, 31, 37, 53–57, 66, 87, 161, 197, 239, 241, 293–295, 297–298, 330–331, 391, 443–447

End-to-end communication, 111

Energy Adaptable Distance Aware Routing Protocol (EADARP), 99–104

Energy collection approach, 491–492

Enhanced Distributed Coordination Function (EDCF), 195, 197–200

Error prone channels, 398, 401, 487

Error reduction, 111–115

Event reporting, 167–172

Evidence analysis, 416

External network, 41–45, 432

F

Faculty nodes, 293–294, 297–298

Fading channels, 49, 288, 311–315, 349–353, 385–386, 388, 461

Fairness, 167–172, 195, 293, 332

Fake customers, 147

Feed forward neural network, 130

Field programmable gate arrays (FPGAs), 55, 91–92, 134

Fitness of a genetic algorithm, 229–233

Flag, 11–12, 141, 150, 208–209, 242, 318

Fluid flow model, 94

FM wireless microphone, 437

Forensic case specification, 413

Forensic Lucid, 413–416

Formal modeling, 23–25, 71–72, 78

Form-factor shrinking, 32

Forward error correction (FEC), 161–162, 398, 431–432

Frame, 47–49, 54–55, 139, 157, 159–160, 165, 195–200, 231, 252, 288, 299–301, 303, 311–315, 352, 358, 364, 367, 388, 397–401, 435, 452, 483–486

Free-viewpoint media over high speed networks, 483

Frequency of packet, 59–64

FSM attack, 413

Fuzzy sets, 373–377

G

Galois field, 87–92

Game theory, 211, 213–214

Genetic algorithm, 144, 189–190, 193, 229–233, 235–238, 375–376, 502–503

Global positioning system (GPS), 6, 61, 207–210, 263–264, 305, 345–346, 489

Glomosim, 104

Group communication protocol, 246–247

GSM mobile network design, 465–469

H

Handover, 7, 81–86, 190, 299–303

Haskin, 433–436

Heterogeneous network, 199, 257–261, 379, 471–476

Hidden Markov models (HMM), 10, 13, 502

Higher-order intensional contexts, 413

High-level network protocol, 129–134

Hold time, 151

HSQldb, 423–428, 449–450, 453–455
 Hybrid Coordination Function (HCF), 195, 197–200
 Hypercube network, 281–286

I

IEEE 802.11i, 54, 356
 Imitation modeling, 201–205
 Influence, 119, 121, 144–147, 173, 193, 201, 353, 379–384, 386
 Information security, 35–40, 228, 330, 501
 Integer programming (IP), 458, 460, 466, 468, 472
 Integrated Dynamic Congestion Controller (IDCC), 93
 Interleaved Cipher Block Chaining, 53–57
 Internet based voting, 329–332
 Internet protocol application test framework (IPAT), 1–7
 Intrusion detection system (IDS), 129–130, 132–134, 239–244, 355–360, 501–504
 IT governance, 35, 361
 IV weakness, 391–393, 395

J

Java data security frame-work (JDSF), 423–429, 449–455
 Jitter, 107, 155, 160, 195, 200, 336, 343, 405
 Job scheduling, 257–261
 JPEG, 173–176, 325

K

Kalman filtering, 349–351, 353
 Karatsuba multiplier, 87–92
 Key management, 245, 329, 443–444
 Key-Scheduling Algorithm (KSA), 391–395
 Knowledge discovery and data Mining cup, 502
 KSAm, 391–395

L

Label Distribution Protocol (LDP), 432–434, 436
 LabMap, 333–337
 LabVIEW, 334–336
 Linear prediction, 495
 Linux security, 71–78
 LMS filter, 495–499
 Load scalability, 284–286
 Localization, 59–64, 192, 263–267, 345–346, 348, 356, 367, 371, 489
 Location management wireless heterogeneous, 471–476

Low-Cost computing platforms, 189
 Low energy adaptive clustering hierarchy (LEACH), 123–127, 347, 409–411
 Lucid, 413–416
 Lyapunov approach, 94–97

M

Makam, 433–436
 Malicious commands, 129
 Management system, 35–40, 66–68, 72, 156–157, 217, 257, 424
 Maneuverability parameters, 373
 Markov model, 9–14
 Media communications, 397–401
 Media transmission algorithm, 483–487
 Medium access control, 100
 Mesh clients, 287–289
 Mesh routers, 287
 Mesh topology, 42, 105–106
 Middleware, 41–42, 44–45, 333–337, 426, 428
 Mining techniques, 471–476, 502–503
 Mobile ad hoc network (MANET), 53, 59, 99, 104, 211, 223–228, 269–278, 507–512
 Mobile context handoff, 305–309
 Mobile handsets (MHs), 472–475
 Mobile manipulator RISCbot, 367
 Mobile platform, 367–372
 Modeling and simulation, 1
 Modular Audio Recognition framework (MARF), 413–428, 449–450, 453–455
 MSC, 457–460, 465–466, 467–468
 Multi-Carrier Code Division Multiple Access (MC-CDMA), 288, 461–463
 Multicast wireless ad hoc networks, 99–104
 Multidimensional scaling (MDS), 264
 Multihomed environment, 81–86
 Multihop, 42–43, 99, 347, 411
 Multi-layer GSM, 457–460
 Multi-path fading, 264, 311
 Multiple description coding, 173, 311
 Multiple description scalar quantization (MDSQ), 173–175
 Multiple-Input-Multiple-Output (MIMO), 117–122, 386
 Multiple-input receivers, 385–389
 Multi-Protocol Label Switching (MPLS), 431–436
 Multi-sensor, 367–372
 Multiuser communication, 269
 Multiview media, 483–487

N

Network attack graph (NAG), 135–138
 Network based storage environment, 403–408

Network intrusion detection system, 501–504
 Network management, 155–160
 Network operations center (NOC), 155–160
 Network performance, 41, 43, 45, 94, 123, 132, 133, 150, 155–156, 160, 195, 211, 213, 215, 269, 274, 326, 359
 Network topology, 10, 43, 59, 61, 107, 110, 136, 155, 157, 159, 191, 214–215, 223, 251, 317–318, 379–384, 433–435
 NMEA, 207–210
 Nodes' credit, 478–479
 Non coherent receivers, 491
 NS simulator, 252

O

Ontology, 23–27
 Operations research, 465
 Optimal timer, 105
 Optimization, 35–40, 56, 120, 135–138, 144, 185, 189–194, 197, 257–262, 264, 269–274, 281–286, 299, 343, 345, 348, 361, 385–386, 438, 469
 Optimum design, 189
 Orthogonal frequency division multiplexing (OFDM), 47, 161–162, 288–291, 349–353, 461–462
 Orthogonal sequences, 177
 Orthogonal Space Combining (OSC), 117–120, 122
 OSI reference model, 139
 Outsourced data storage and databases (OSD), 423
 Overlay networks, 156, 339

P

Packet loss, 43, 59–60, 106, 157, 173, 195, 219, 273–274, 311, 315, 343, 400
 Packet size, 99–104, 253–256, 277–278, 300, 447
 Passive steady state RF Fingerprinting, 183–187
 Path failure effect, 81–86
 Peer-to-peer network (P2P network), 339–340, 342
 Perfect periodic autocorrelation function, 177
 Performance of TCP, 111
 Pixel-patch antenna, 120
 Plug-in alignment, 70
 Point Coordination Function (PCF), 195–198, 200
 Positioning, 121, 143–144, 207, 210, 263, 344, 387, 489
 Power consumption, 54, 87, 99, 103, 207–208, 210, 406, 480

Prediction, 5, 186, 211, 235–238, 311–312, 345, 394–395, 397–398, 442, 472, 474–476, 484–485, 503
 Presence, 10, 12–14, 26–27, 61, 82, 96–97, 107, 190, 225–226, 238, 243–244, 269–273, 278, 281–282, 284–286, 318, 323–324, 326–328, 360, 372, 382, 409
 Protection, 31–32, 35–39, 71–78, 125, 149–154, 311, 398, 451–452
 Public key cryptography, 329–330, 444
 Pulse-wave generator, 437–438, 440–441

Q

Quality of service (QoS), 7, 9, 11, 17, 19–22, 47, 93, 95, 106, 155, 189–190, 194–200, 203, 336, 404–406, 408, 432
 Queue size, 94, 168, 252–256

R

Rayleigh fading, 49–51, 349–351, 461
 RC4_{KSA}, 391–395
 RC4_{KSAm}, 391–392, 394–395
 Real-life ad-hoc network, 217
 Real-time, 44, 60, 82, 131–132, 143–144, 147, 167–170, 172, 201–205, 309, 333, 335–336, 369, 372, 397, 451, 495, 503
 Real-time network, 201–205, 503
 Real time shopping behavior, 143
 Reasoning, 24, 72, 289
 Recurrent neural network, 129–134
 Reed-Solomon-Like (RSL), 443–447
 Reno techniques, 111
 Representational State Transfer (REST), 323–328
 Resolved condition, 392–395
 Resource overbuild, 149, 151
 Return-on-investment (ROI), 31, 144, 398–400
 RFID technology, 29–32
 RLS filter, 496–499
 Robust transmission, 311–315
 Routing, 99–104, 269–274, 281–286
 Routing convergence, 105

S

Safe ship control, 373–377
 Sales-price margin, 143
 Scaling, 235, 264, 281, 452
 Security, 1, 3, 5, 27, 29–32, 35–40, 43–44, 53–55, 59, 64–65, 67–69, 71–72, 77–78, 87, 89, 123–126, 129, 156, 211, 228, 239, 244–250, 293–294, 296–298, 308, 317, 326, 329–332, 355–357, 392–395, 423–429, 443–447, 449–455, 472, 489, 501, 503–504, 507

Selective acknowledgement schemes, 111
 Self-localization, 343–348
 Sensor network, 41–45, 53–54, 123, 126–127, 167–172, 239–244, 263–267, 343–348, 409–411, 443–447, 477–480, 489, 493
 Sensor nodes, 41–44, 167–171, 239–240, 263–267, 288, 343, 345–347, 409–411, 447, 477–478, 480
 Sequence number, 112, 140–141, 252
 Sequential implementation, 361
 Service-Oriented Wireless Context-Aware System (SOWCAS), 305, 309
 Session initiation protocol (SIP), 81–86
 Shared path protection (SPP), 149–152
 Signature-based NIDS, 503
 Simple dynamic, 433, 436
 SIRF-Star, 207
 Software bus, 334
 Software testing, 23–25, 27
 Spectrometer, 207, 210
 Stand alone system, 293
 Standard deviation, 204, 265, 379, 383–384, 439, 460, 498
 Statistical discriminators, 317, 320
 Strand space, 245–247
 Stream Control Transmission Protocol (SCTP), 81–86
 Support vector machines, 183–187, 502
 Survivability, 149–150, 152, 443
 Synthesis of signals, 177
 System development, 6, 35–40
 System integrity, 35

T

TCP/IP compression, 111, 116
 Telemetrized temperature, 437–442
 Telephony, 192, 195, 323–324, 327, 397, 457, 465–466, 507
 Temporal interleaving, 311, 315
 Test automation, 23
 Test pattern, 210
 Test sequences generator, 208–209
 Threshold call admission control, 18–22
 Throughput, 56–57, 62–63, 81, 171–172, 251, 253–256, 277, 285–286, 318, 511
 Time difference of arrival method (TDoA), 264
 Time varying, 94, 111, 224, 349–350, 495
 Traffic analysis, 201, 317
 Transmission delay, 83, 273, 275–278, 303
 Transport control protocol (TCP), 9, 11, 41–42, 45, 81, 111–116, 192, 225–227, 251–256, 308, 317–318, 340, 360, 419–420, 434, 508
 Turbo codes, 47–49, 51, 161–165

U

Ubiquitous media, 397–401
 Ultra wideband, 489
 Unified processing, 389
 Universal Mobile Telecommunication System (UMTS), 7, 47–49, 183–186, 397

V

Vehicular ad hoc networks, 59–64
 VHDL hardware, 87
 Virtualized parametric antenna, 117, 122
 Virtual private networks (VPNs), 431
 Vulnerability, 31, 137, 144, 211, 213–216

W

Watermarking, 424, 450–455
 Wavelength Division Multiplexing (WDM), 149–150
 Weak keys, 392, 394–395
 Web application, 5, 23–27, 298
 Web services, 23–24, 26, 69, 156, 158–159, 417–420, 444
 White and Gaussian, 349
 Wi-Fi, 45, 287, 355, 357, 507–508, 510–512
 Wired equivalent privacy (WEP), 10, 54, 391–395
 Wireless ad-hoc networks, 217–221
 Wireless intrusion detection, 355–360
 Wireless local area networks (WLANs), 10, 53, 81, 195–200, 305–309, 349, 472–473, 489
 Wireless mesh network (WMN), 287–291
 Wireless network, 9, 11, 17–22, 42, 53–55, 58, 81, 100, 111, 113, 120, 123–127, 189–190, 194, 217, 275, 287, 299–303, 306–309, 355–358, 397, 472, 474, 510
 Wireless security, 53–54
 Wireless sensor network (WSN), 41–45, 53–54, 123, 167–172, 239–244, 263–267, 343–348, 409–411, 443–444, 477–480, 489, 493
 Worldwide interoperability for microwave access (WiMAX), 5–7, 47–49, 161–165, 287, 507, 512
 Worst case scenario, 29–32, 227, 300, 387–389

X

Xilinx VirtexE, 91
 XML-RPC, 417, 423, 449

Z

Z notation, 72