

S. Smys
Robert Bestak
Álvaro Rocha *Editors*

Inventive Computation Technologies

Lecture Notes in Networks and Systems

Volume 98

Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,
Warsaw, Poland

Advisory Editors

Fernando Gomide, Department of Computer Engineering and Automation—DCA,
School of Electrical and Computer Engineering—FEEC, University of Campinas—
UNICAMP, São Paulo, Brazil

Okyay Kaynak, Department of Electrical and Electronic Engineering,
Bogazici University, Istanbul, Turkey

Derong Liu, Department of Electrical and Computer Engineering, University
of Illinois at Chicago, Chicago, USA; Institute of Automation, Chinese Academy
of Sciences, Beijing, China

Witold Pedrycz, Department of Electrical and Computer Engineering,
University of Alberta, Alberta, Canada; Systems Research Institute,
Polish Academy of Sciences, Warsaw, Poland

Marios M. Polycarpou, Department of Electrical and Computer Engineering,
KIOS Research Center for Intelligent Systems and Networks, University of Cyprus,
Nicosia, Cyprus

Imre J. Rudas, Óbuda University, Budapest, Hungary

Jun Wang, Department of Computer Science, City University of Hong Kong,
Kowloon, Hong Kong

The series “Lecture Notes in Networks and Systems” publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

**** Indexing: The books of this series are submitted to ISI Proceedings, SCOPUS, Google Scholar and Springerlink ****

More information about this series at <http://www.springer.com/series/15179>

S. Smys · Robert Bestak ·
Álvaro Rocha
Editors

Inventive Computation Technologies



Editors

S. Smys
Computer Science and Engineering
RVS Technical Campus
Coimbatore, Tamil Nadu, India

Robert Bestak
Faculty of Electrical Engineering
Czech Technical University in Prague
Prague 6, Czech Republic

Álvaro Rocha
Departamento de Engenharia Informática
Universidade de Coimbra
Coimbra, Portugal

ISSN 2367-3370 ISSN 2367-3389 (electronic)

Lecture Notes in Networks and Systems

ISBN 978-3-030-33845-9 ISBN 978-3-030-33846-6 (eBook)

<https://doi.org/10.1007/978-3-030-33846-6>

© Springer Nature Switzerland AG 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*We are honored to dedicate the proceedings
of ICICT 2019 to all the participants and
editors of ICICT 2019.*

Foreword

It is with deep satisfaction that I write this Foreword to the proceedings of the ICICT 2019 organized by RVS Technical Campus, Coimbatore, Tamil Nadu, on August 29–30, 2019.

This conference was bringing together researchers, academics, and professionals from all over the world, experts in computation technology, information and control engineering.

This conference particularly encouraged the interaction of research students and developing academics with the more established academic community in an informal setting to present and to discuss new and current work. The papers contributed the most recent scientific knowledge known in the field of computation technology, information and control engineering. Their contributions helped to make the conference as outstanding as it has been. The Local Organizing Committee members and their helpers put much effort into ensuring the success of the day-to-day operation of the meeting.

We hope that this program will further stimulate research in networks and information systems, fuzzy control, smart grid, and artificial intelligence and also provide practitioners with better techniques, algorithms, and tools for deployment. We feel honored and privileged to serve the best recent developments to you through this exciting program.

We thank all authors and participants for their contributions.

S. Smys

Preface

This conference proceedings volume contains the written versions of most of the contributions presented during the conference of ICICT 2019. The conference provided a setting for discussing recent developments in a wide variety of topics including cloud computing, artificial intelligence, and fuzzy neural systems. The conference has been a good opportunity for participants coming from various destinations to present and discuss topics in their respective research areas.

ICICT 2019 Conference tends to collect the latest research results and applications on computation technology, information and control engineering. It includes a selection of 101 papers from 328 papers submitted to the conference from universities and industries all over the world. All of accepted papers were subjected to strict peer-reviewing by 2–4 expert referees. The papers have been selected for this volume because of quality and the relevance to the conference.

ICICT 2019 would like to express our sincere appreciation to all authors for their contributions to this book. We would like to extend our thanks to all the referees for their constructive comments on all papers; especially, we would like to thank Organizing Committee for their hardworking. Finally, we would like to thank the Springer publications for producing this volume.

S. Smys

Acknowledgments

ICICT 2019 would like to acknowledge the excellent work of our conference organizing the committee, keynote speakers for their presentation on August 29–30, 2019. The organizers also wish to acknowledge publicly the valuable services provided by the reviewers.

On behalf of the editors, organizers, authors, and readers of this conference, we wish to thank the keynote speakers and the reviewers for their time, hardwork, and dedication to this conference. The organizers wish to acknowledge Dr. Y. Robinson, Dr. S. Smys, Dr. Robert Bestak, Dr. Álvaro Rocha, and Dr. Vasile Avram for the discussion, suggestion, and cooperation to organize the keynote speakers of this conference. The organizers also wish to acknowledge for speakers and participants who attend this conference. Many thanks are given for all persons who help and support this conference. ICICT 2019 would like to acknowledge the contribution made to the organization by its many volunteers. Members contribute their time, energy, and knowledge at a local, regional, and international level.

We also thank all the chair persons and conference committee members for their support.

Contents

Automated Data Acquisition and Controlling System in Housing Line Using Internet of Things (IoT)	1
T. L. Pooja and M. Supreetha	
Slotted Microstrip Patch 4×4 MIMO Antenna for Ultra Wide Band Applications	11
P. Ramya, R. S. Valarmathi, C. Poongodi, and P. Hamsagayathri	
An Effective Logic Obfuscation Technique with AES Encryption Module for Design Protection	18
Binu P. Kumar and M. Nirmala Devi	
Unequal Energy Aware Secure Clustering Technique for Wireless Sensor Network	29
Simran R. Khiani, C. G. Dethe, and V. M. Thakare	
Robust Smart Home Monitoring System Based on 802.11 Mesh Network	38
S. Loyola Samraj, Nisha V. Bhalke, A. Aarthi, R. Srinath, and E. Prabhu	
A Comprehensive Analysis of the Most Common Hard Clustering Algorithms	48
Aditya Vardhan, Priyanshu Sarmah, and Arunav Das	
Development and Validation of Engine Start/Stop Strategy for P2 Hybrid Electric Vehicle	59
MeghRaj V. Palwe and Pramod Kanjalkar	
Security Landscape for Private Cloud	67
Sheeja Shaji Manakattu, Shivakumar Murugesh, and Rajashekhar Ningappa Hirekurabar	
An Efficient Medium Access Control Mechanism Using Multiple Data Rates in Ad Hoc Networks	79
Arundhati Arjaria, Priyanka Dixit, Shivendra Dubey, and Uday Chourasiya	

Ranked Keyword Search Result Verification to Detect Misbehaving Cloud Servers	87
L. Ashwini and N. R. Sunitha	
Miniaturized Device for SHM Using Electromechanical Impedance Technique	94
Ashutosh K. Kedare and Kapil Mundada	
Malicious User Detection in Cooperative Sensing Environment Using Robust Distance	104
N. Swetha, D. L. Chaitanya, HimaBindu Valiveti, and B. Anil Kumar	
Smart Irrigation Alert System Using Multihop Wireless Local Area Networks	115
C. V. N. S. Lalitha, M. Aditya, and Manoj Panda	
Real Time Health Monitoring System Using IoT	123
Bhagyashree Behara and Manisha Mhetre	
Performance Analysis of Optimization Algorithms Using Chirp Signal	132
K. Anuraj and S. S. Poorna	
Dual RSA Based Secure Biometric System for Finger Vein Recognition	138
Satyendra Singh Thakur and Rajiv Srivastava	
TUDocChain-Securing Academic Certificate Digitally on Blockchain	150
Sugandha Budhiraja and Rinkle Rani	
Enhancing Energy Efficiency in IoT (Internet of Thing) Based Application	161
Utkarsha Singh and Inderveer Chana	
Smart Home Automation Using Fuzzy Logic and Internet of Things Technologies	174
Jignasha Sosa and Jyoti Joglekar	
A Survey of Block Cluster-Based Routing Schemes in Wireless Sensor Network	183
Vasudeva Pai and Neetha Janis Tellis	
Designing Features of Parallel Computational Algorithms for Solving of Applied Problems on Parallel Computing Systems of Cluster Type	191
Gennady Shvachych, Volodymyr Busygyn, Khohlova Tetyana, Boris Moroz, Fedorov Evhen, and Kholod Olena	

A Multi-parameter Based Resource Management Approach for Cloud Environment	201
Akkrabani Bharani Pradeep Kumar and Venkata Nageswara Rao Padmanabhuni	
A New (3, 3) Secret Sharing Cryptography Scheme for Efficient Secret Data Transmission	209
Ariba Tariq and Rajitha Bakthula	
Comparison Between RSA Algorithm and Modified RSA Algorithm Used in Cloud Computing	218
Bushra Shaheen and Farheen Siddiqui	
Database as a Service for Cloud Based Video Surveillance System	225
Sumit Kumar, Vasudeva Rao Prasadula, and Shivakumar Murugesh	
Relative Hand Movement and Voice Control Based Home Automation and PC	232
Shashwat Sanket, Jayraj Thakor, Piyush Kapoor, Karrmany Pande, Suyash V. Shrivastav, and R. Maheswari	
Design Strategies for Handling Data Skew in MapReduce Framework	240
Avinash Potluri, S. Nagesh Bhattu, N. V. Narendra Kumar, and R. B. V. Subramanyam	
Implementation of Visible Foreground Abstraction Algorithm in MATLAB Using Raspberry Pi	248
M. L. J. Shruthi, B. K. Harsha, and G. Indumathi	
A New Hardware Design and Implementation of QPSK Modulator in Normal and 4-QAM Mode for 5G Communication Networks	255
R. Rameshkumar and J. N. Swaminathan	
A Novel Approach for the Run-Time Reconfiguration of Heterogeneous Applications in a Smart Home Monitoring System	263
K. S. Rekha, A. D. Kulkarni, and H. D. Phaneendra	
Implementation of Internet of Things and Protocol	272
Rishabh and Hemant Gianey	
Hacker Forum Exploit and Classification for Proactive Cyber Threat Intelligence	279
Apurv Singh Gautam, Yamini Gahlot, and Pooja Kamat	
A Systematic Approach on Design of Automation System for Tea Farming Based on Embedded Wireless Sensor Network	286
Hemarjit Ningombam and O. P. Roy	

Effect of Fault Tolerance in the Field of Cloud Computing	297
A. H. M. Shahriar Parvez, Md. Robiul Alam Robel, Mohammad Abdur Rouf, Prajjoy Podder, and Subrato Bharati	
Disaster Site Map Generation Using Wireless Sensor Networks	306
P. S. Mohan Vaishnav, K. Sai Haneesh, Ch. Sai Srikanth, Ch. Koundinya, and Subhasri Duttagupta	
LRD: Loop Free Routing Using Distributed Intermediate Variable in Mobile Adhoc Network	315
O. S. Gnana Prakasi and P. Kanmani	
Activity Classifier: A Novel Approach Using Naive Bayes Classification	323
G. Muneeswari, D. Daniel, and K. Natarajan	
Virtual Machine Allocation in Heterogeneous Cloud for Load Balancing Based on Virtual Machine Classification	331
Badshaha Mulla, C. Rama Krishna, and Raj Kumar Tickoo	
Task Scheduling Algorithms in Cloud Computing: A Survey	342
Linz Tom and V. R. Bindu	
Securing Color Image Using Combined Elliptic Curve Crypto-System and Hill Cipher Encryption Along with Least Significant Bit - Steganography	351
N. Faizal, S. Sharan, Panchami S. Nair, and Devi S. Sankar	
Comprehensive Study of Existing Stream Ciphers	362
S. Chaithanya and V. Anitha	
An Analysis of Scheduling Algorithms in Real-Time Operating System	374
Jayna Donga and M. S. Holia	
A Novel Approach for Cluster Head Selection By Applying Fuzzy Logic in Wireless Sensor Networks with Maintaining Connectivity	382
Aaditya Jain and Bhuwnesh Sharma	
Simple and Coverage Path Planning for Robots: A Survey	392
R. S. D. Pragnavi, Akhileshwar Maurya, Bharath N. Rao, Akash Krishnan, Srijan Agarwal, and Maya Menon	
Secrecy Capacity of Symmetric Keys Generated by Quantising Channel Metrics Over a Fading Channel	404
L. Srividya and P. N. Sudha	

Orthogonal Frequency Division Multiplexing-Multiple Input Multiple Output Channel Estimation for Rayleigh and Rician Channel Models	414
R. B. Hussana Johar and B. R. Sujatha	
An Efficient Training Strategy for a Temporal Difference Learning Based Tic-Tac-Toe Automatic Player	423
Jesús Fernández-Conde, Pedro Cuenca-Jiménez, and José María Cañas	
Detection of Causative Attack and Prevention Using CAP Algorithm on Training Datasets	431
D. Suja Mary and M. Suriakala	
Discrete Wavelet Transform Based Multiple Watermarking for Digital Images Using Back-Propagation Neural Network	441
C. Ananth, M. Karthikeyan, and N. Mohananthini	
Multilevel Converter for Renewable Energy System	450
Vishal Anand and Varsha Singh	
Comprehensive Study on Methods that Helps to Increase the Life of the Wireless Sensor Networks	458
Aaditya Jain, Akanksha Dubey, and Bhuvnesh Sharma	
Implementation of IDS Within a Crew Using ID3Algorithm in Wireless Sensor Local Area Network	467
K. Raja and M. Lilly Florence	
A Hybrid Technique for Unsupervised Dimensionality Reduction by Utilizing Enriched Kernel Based PCA and DBSCAN Clustering Algorithm	476
D. Hemavathi, H. Srimathi, and K. Sornalakshmi	
A Survey on Quality of Service Metrics Using Cross Layer Optimization Technique	489
Amutha R, Sivasankari H, and Venugopal K R	
A Hybrid Approach for Energy Efficient Routing in WSN: Using DA and GSO Algorithms	506
R. Vinodhini and C. Gomathy	
Retrospective Analysis of Wireless Body Area Network	523
A. Angel Cerli and K. Kalaiselvi	
Cross Layer Aware Optimization of TCP Using Hybrid Omni and Directional Antenna Reliable for VANET	530
S. Karthikeyini and S. Shankar	

Enhanced TCP to Improve the Network Communication Performance in Smart Metering Applications	547
M. Rajiv Suresh and V. Subedha	
Enhancing Spectrum Efficiency and Energy Harvesting Selection for Cognitive Using a Hybrid Technique	556
M. Balasubramanian, V. Rajamani, and S. Puspha	
Maximize Body Node's Lifetime Through Conditional Re-transmission	569
J. Karthik and A. Rajesh	
Modeling and Analysis of Energy Efficient Media Access Control Protocols for Wireless Sensor Networks Using OMNET++	579
Harish Joshi and Ravindra V. Eklarker	
Privacy Preserving Approach for Proficient User Revocation in Cloud Environments	587
S. Suganthi Devi and V. Asanambigai	
An Energy - Efficient Approach for Restoring the Coverage Area During Sensor Node Failure	594
G. T. Bharathy, S. Bhavanisankari, T. Tamilselvi, and G. Bhargavi	
Design of Effective Grid-Connected Solar System	606
Iram Akhtar, Mohammed Asim, Raj Kumar Yadav, Piyush Agarwal, and Sheeraz Kirmani	
Efficient Load Scheduling Algorithm Using Artificial Neural Network in an Isolated Power System	615
Vijo M. Joy and S. Krishnakumar	
Integrated Static Analysis for Malware Variants Detection	622
Rinu Rani Jose and A. Salim	
Data Storage in Cloud Using Key-Policy Attribute-Based Temporary Keyword Search Scheme (KP-ABTKS)	630
Nallella Thirupathi, K. Madhavi, G. Ramesh, and K. Sowmya Priya	
Single Source Divisible Load Scheduling on Distributed Heterogeneous Environments	637
Murugesan Ganapathy	
Fog Computing and Deep CNN Based Efficient Approach to Early Forest Fire Detection with Unmanned Aerial Vehicles	646
Kethavath Srinivas and Mohit Dua	
Implementing a Role Based Self Contained Data Protection Scheme in Cloud Computing	653
G. N. Beena Bethel and S. Anitha Reddy	

Contents	xix
Smart Waste Management System Using IoT	661
V. Pavan Sankeerth, V. Santosh Markandeya, E. Sri Ranga, and V. Bhavana	
Wireless Sensor Networks for Healthcare Monitoring: A Review	669
Suraiya Tarannum and Shaista Farheen	
A Survey on Efficient Internet of Things Based Techniques for Efficient Irrigation and Water Usage	677
Ruthesh Chandran, P. Rekha, and Balaji Hariharan	
An Energy Efficient Routing Protocol for Internet of Things Based Precision Agriculture	684
T. Aishwarya Lakshmi, Balaji Hariharan, and P. Rekha	
Reducing Network Downtime by Intelligent Fault Analysis	692
B. Bipin	
A Novel Access Control for Cloud Services Using Trust Based Design	702
Manikonda Aparna and N. Nalini	
An Intelligent Recommendation Engine for Selecting the University for Graduate Courses in KSA: SARS Student Admission Recommender System	711
Zeba Khanam and Salwa Alkhaldi	
Smart Cloud: A Self-organizing Cloud	723
Gayatri Hegde and Madhuri Rao	
A High Linearity Shunt Capacitive Feedback LNA for Wireless Applications	730
Gaurav Srivastava and Malti Bansal	
Transparent Watermarking QR Code Authentication for Mobile Banking Applications	738
Saiteja Ityala, Oshin Sharma, and Prasad B. Honnavalli	
Network Intrusion Detection System Using Two Stage Classifier	749
Devakunchari, Sourabh, and Prakhar Malik	
Priority Queue Scheduling Approach for Resource Allocation in Containerized Clouds	758
Madhumathi Ramasamy, Mathivanan Balakrishnan, and Chithrakumar Thangaraj	
Hybrid Evolutionary Approach for IDS by Using Genetic and Poisson Distribution	766
Riya Bilaiya and Priyanka Ahlawat	

A Novel Approach to Overcome the Limitations of Power Iteration Algorithm Designed for Clustering	774
D. Jayalatchumy, P. Thambidurai, and D. Kadhirvelu	
Design of Reliable Dense Wavelength Division Multiplexing System for Metropolitan Area Network	782
K. Sheela Sobana Rani, R. Gayathri, R. Lavanya, and K. Uthayasuriyan	
Secure Outlook View of Trustworthiness and Attacks in Cloud Computing	794
S. Mercy, R. Nagaraja, and M. Jaiganesh	
Recruitment Data Analysis Using Machine Learning in R Studio	801
R. Devakunchari, Niketha Anand, Anusha Vedhanayaki, and Y. J. Visishta	
Security Enabled Smart Home Using Internet of Things	808
Y. Swathi, M. B. Shanthi, Swati Kumari, and Priya Batni	
Review of Software Defined Networking: Applications, Challenges and Advantages	815
Upendra Singh, Vikas Vankhede, Shyam Maheshwari, Devesh Kumar, and Narendra Solanki	
Trust Based Model for Mobile Ad-Hoc Network in Internet of Things	827
Upendra Singh, Mukul Shukla, Ashish Kumar Jain, Mohan Patsariya, Ravikant Itare, and Sakshi Yadav	
Offset Generator for Offset Quadrature Phase Shift Keying Modulation	840
Alphyn Stanley and R. K. Sharma	
Quantitative Analysis of Radio Frequency Spectrum Occupancy for Cognitive Radio Network Deployment	847
Sheetal Borde, Kalyani Joshi, and Rajendrakumar Patil	
Multiprocessor Systems Design: Reliability Analysis of Multistage Interconnection Network	858
Amit Prakash and Dilip Kumar Yadav	
An Approximative Study of Database Partitioning with Respect to Popular Social Networking Websites and Applications	865
S. V. G. Sridevi and Yogesh Kumar Sharma	
A Novel Approach for Gigantic Data Examination Utilizing the Apache Spark and Significant Learning	874
Anilkumar V. Brahmane and B. Chaitanya Krishna	

Multiple Linear Regression Analysis of Factors Affecting the Consumption	883
Jesús Silva, Omar Bonerge Pineda Lezama, and Darwin Solano	
Collaborative Spaces in Virtual Environments: Socio-Cultural Support for the University Beginning Teacher	890
Jesús Silva, Juliana Ferrer, Mercedes Gaitán, and Jenny Paola Lis	
Competitions of Multi-agent Systems for Teaching Artificial Intelligence	898
Jesús Silva, Omar Bonerge Pineda Lezama, and Noel Varela	
Implementation of an E.R.P. Inventory Module in a Small Colombian Metalworking Company	905
Jairo R. Coronado-Hernandez, Holman Ospina-Mateus, Danneris Canabal-Gómez, Diana Peña-Ballestas, Javier Baron-Villamizar, Nohora Mercado-Carusso, Alfonso R. Romero-Conrado, Carlos Paternina-Arboleda, and Jesús Silva	
Simulation Model of Internal Transportation at a Container Terminal to Determine the Number of Vehicles Required	912
Carlos J. Uribe-Martes, Doris Xiomara Rivera-Restrepo, Angélica Borja-Di Filippo, and Jesús Silva	
Internet of Things Enabled Device Fault Prediction System Using Machine Learning	920
Kotte Bhavana, Vinuthna Nekkanti, and N. Jayapandian	
Author Index	929



Automated Data Acquisition and Controlling System in Housing Line Using Internet of Things (IoT)

T. L. Pooja^(✉) and M. Supreetha

Department of Electronics and Communication, JSS Science and Technology University, S.J.C.E., Mysuru 570006, India
ananya.0032@gmail.com, supreetha.manjanna@sjce.ac.in

Abstract. The Internet of Things (IoT) based automated data acquisition and controlling system conceptualizes the idea of connecting, monitoring and capturing data from machines in real-time is called as industry 4.0. It expresses the essential features required for industry development in order to achieve a smart manufacturing process. Here, the system will monitor the condition of machines from various sensors and captures the process parameters in order to send the data to edge server, where it will be displayed or take intelligent decisions automatically by using IoT framework. For data collection, data analysis, evaluation of company development and performance improvement for housing line allows process, machines, employees, and product to be coupled into a single integrated network. The emerging advancements of industries include cyber physical systems, IoT, machine to machine (M2M) communication, cloud computing, big data are embedded with the manufacturing process. The smart factory increases the production, marketing and has deliberated a control over the entire life cycle of the production process associated with the housing line.

Keywords: Industry 4.0 · Sensor · Internet of Things (IoT) · M2M communication · CPS · Cloud

1 Introduction

Smart equipment will bring stronger integration of top floor and shop floor and thus more intelligence and flexibility to the production. The industrial revolution stages from manual work towards industry 4.0 concept, which can be introduced as a path through the four industrial revolution. The first industry follows introduction of water and steam powered with mechanical production machines in 18th century. First revolution improves the quality of life. The iron and textile industries played central roles in the first revolution. The second industry follows the introduction of electrically powered mass production in the 20th century. In second revolution the industries were grown and also expansion of new industries, such as steel and oil by using electric powered mass production [1] has been initiated. The third revolution has integrated electronics and IT to achieve automation in manufacturing in 20th century. The first programmable logic controller (PLC) used in third revolution has facilitated a flexible production in the industrial production lines with programmable machines [3]. Today

we are in the fourth revolution called industry 4.0, which is mainly based on cyber physical systems (CPS). The CPS are integrated with physical and engineered systems, whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. The ability of CPS, human and machine to connect and communicate with each other by using the internet of things framework and it also has the capability of collecting and analyzing data to provide an immediate and accurate information.

Internet of Things (IoT) can be viewed as a three layer structure as depicted in Fig. 2. The three layers are namely physical layer, network layer and application layer. The physical layer has the physical devices sensor and actuators, which is typically used for sensing and actuation. In network layer it has the gateways servers to collect the data from the physical layer and gives the output by communicating it through the servers. The application layer has storage, processing, analytics and management models. The data collected from the first two layers are stored in cloud and later it is controlled and managed in this layer. These three layer architecture of IoT allow sensing to analyzing and actuation. By this way we can monitor the condition of machines [13].

An edge server is a type of edge device that provides an entry point into a network. Edge devices allow different networks to connect and share transit. There are three virtual machines in edge server and overall storage of this server is 500 GB. This server has three layers first layer is for quality analysis, second layer will have the complete information about the production and third layer of the server will store the complete data present in the line.

Sensors are used for each parameter that is placed to identify the different condition parameters of the machine during the runtime of a machine. Here we can use proximity sensor for position monitoring, accelerometer for machine vibration monitoring, pressure sensor for clamping, color detection sensor for oil level and coolant level monitoring, temperature sensor for oil temperature monitoring is important for machine condition monitoring. The system generates automated maintenance alerts whenever anomalies are noted.

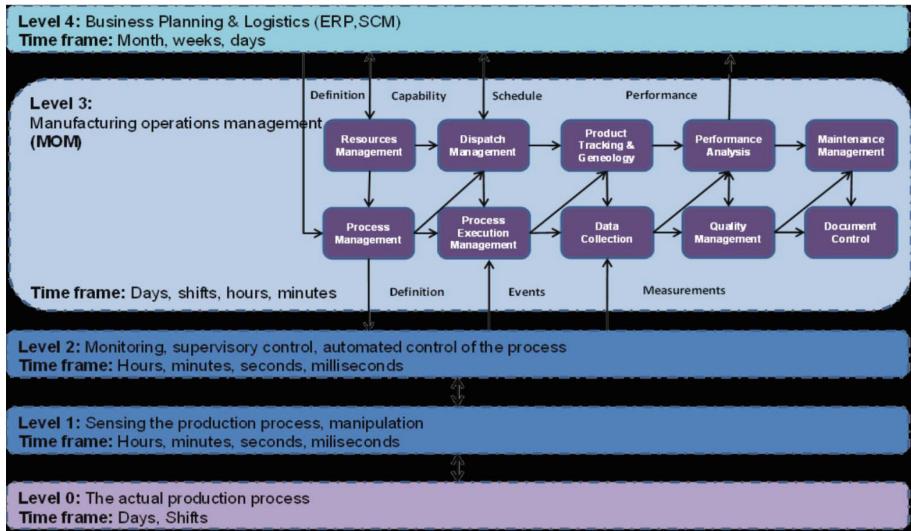
The rapid growth in the internet creates a huge data, which cannot be managed by using the traditional tools. The technology will efficiently manage the huge data collected is called as big data analytics [10]. The data from the beginning to the end of manufacturing process of product should be collected, managed and protected for the efficient product supply chain. It is possible or allowed by big data. Cloud computing store and access data and program over the internet instead of computer's hard drive. It plays a key role towards enabling industry to digitalization. As we discussed in big data there will be huge data to store this we require large data base hence, we store in cloud with the internet access, this can be accessed easily anywhere, anytime [8]. It facilitates real time exchange of data digital collaborating and integration. These techniques will help to improve the process monitoring in real time.

2 Literature Review

Industry 4.0 is linked with a supply chain and manufacturing process that connects to Internet of Things (IoT). As the real world and virtual world grows rapidly together with internet of things, this inspired organization has started the journey towards industry 4.0. There is a need for the adoption of Industry 4.0 in various industries (manufacturing) to study the impact of the improvement on the outcome of a company [4]. The industry 4.0 uses the CPS to connect all physical systems to internet and operations are monitored, coordinated, controlled and integrated by a computing and communication [15]. Technologies involved in industry 4.0 are CPS, IoT, big data, cloud computing. By using industry 4.0 the machines can communicate with each other and with the manufacturers to create what we now call a cyber-physical production system (CPPS). This helps industries to integrate the real world into a virtual one and enable machines to collect current data, analyze them, and even make decisions based upon them. But in the present system it is not possible to communicate between one machine to the another.

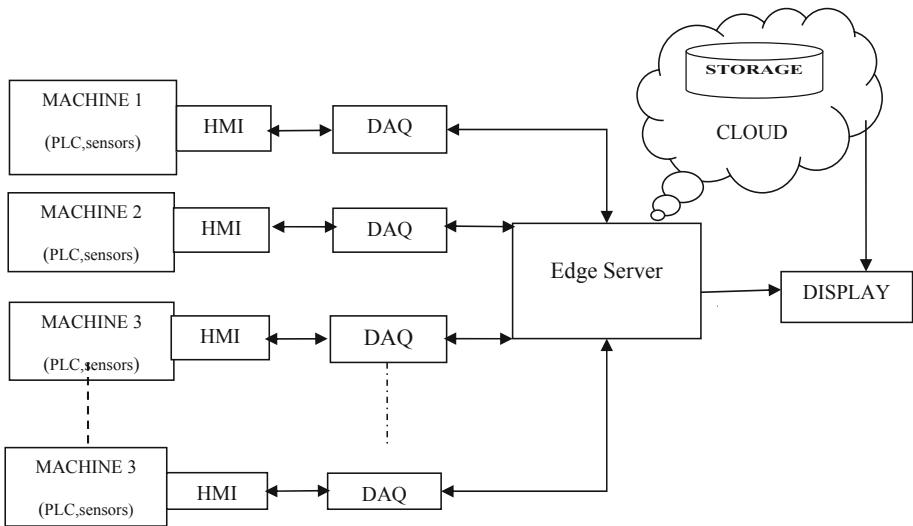
3 Positioning Among Production Supply Chain

Level 0 is considered as the lowest and then the first level is called component level, where all the hardware components like sensor, and actuator are present. These devices are connected to control systems in the next levels, where these devices respond to the signals they receive and generate the feedback signals. Level 1 is the second level and it is called as field 1 level. This level is also called as automation control because programmable logic controller (PLC), CNC and DCS will be present in this level. The basic operations were controlled in this level it is crucially important for a successful production. Level 2 is a third level and is called as supervisory/operation/control level. In this level the input and output data management, process management, data acquisition management, learning, reporting will be monitored and controlled. This level as the connection between MOS and ongoing process in shop. Level 3 is fourth level and is also called as the manufacturing operation system (MOS) level and it is also called as plant level. It doesn't focus on only on machine or one production it focus on all machines in plant and gather all information and it will share and communicate with all machines in plant. It has a functionality like quality management, product management, resource management, and its main goal is to increase production by increasing the traceability of production status in real time. Level 4 is the last level and it is also called as enterprise resource planning level or simply it can be called as enterprise level. This level is connected to the level 3 which is MOS they communicate with each other. It focus on the finance, accounting and human resource which are not directly connected to shop floor activities (Fig. 1).

**Fig. 1.** Process levels

4 Methodology

All the hardware components like, sensor, actuator present in machines are connected to control systems (PLC) and these devices respond to the signals they receive and they generate feedback signals and the data will be collected or acquired from the HMI of corresponding machines as shown in Fig. 2. Edge server allow different networks to connect and share transit. There are three virtual machines in edge server and overall storage of this server is 500 GB. This server has three layers first layer is for quality analysis, second layer will have the complete information about the production and third layer of the server will store the complete data in the line. It function is data collection, scheduling, process management, performance analysis, document management. The integration of these servers will increase operational clarity and equip organization with the ability to monitor and adjust performance against business plans. The data contains about the present state of the machines like operator, about model, operator information, productivity, problems regarding machines, defects in machine, part issues etc. The data collected from the housing line machines (20 machines) will be monitored by the server and it is sent to the server or controlled by the edge server by TCP/IP communication protocol by using internet of things. Then the collected data from the housing line will be sent to the cloud and then it will be displayed on the and on display. Monitoring and cloud computing stages are explained in Sect. 4.2 and features used in this project are explained in the Sect. 4.1.

**Fig. 2.** Block diagram

4.1 Features

The features used in housing line are attendance monitoring, downtime monitoring, traceability, condition monitoring, management transactions this is explained in the Table 1.

Table 1. Features used in housing line

Feature	Instrument	Method
Attendance monitoring	Biometric finger print scanner	Operator scans the finger print with the scanner to associate with the machine and also to know exactly who is operating the machine
Downtime monitoring	Relay and energy meter	Based on the run hours, the downtime hours are identified. The system logs the downtime and the operator can choose the downtime in the 7 th table placed near the control panel.
Traceability	Data capture (Scanner)	Every component will be individually identifiable and can be located up and down the value chain. History, current status, as well as alternative and more efficient production paths can be easily and directly recognized and adopted
Condition monitoring	Energy monitoring	Sensors for each parameter as mentioned would be placed to identify the different condition parameters of the machine during running of the machine. Here we can use proximity sensor for position monitoring, accelerometer for machine vibration, pressure sensor for clamping, color detection sensor for oil level monitoring, temperature sensor for oil temperature monitoring and current, voltage monitoring is also important for machine condition monitoring. The system generates automated maintenance alerts whenever anomalies are noted
Management transactions	<ul style="list-style-type: none"> • Job allocation • Setup approval • Role based MIS views • Reports • Adhoc analytics 	Job Allocation for job cards and operator allocation, approvals for the setups on the machine, role based MIS views (supervisor, plant head, management etc.), standard reports (OEE, downtime, maintenance etc.) and adhoc reports based on need would be generated from the system

4.2 Stages in Operating Process

As shown in Fig. 2 there are 20 machines in line it will be monitored and the data will be collected automatically and controlled using IoT platform. For this it require three stages they are sensing, monitoring, data controlling and storing in cloud and finally alerting/displaying.

Sensors are used for each parameter that is placed to identify the different condition parameters of the machine during running of the machine. Here we used storage level indication sensor, accelerometer for machine vibration, current, voltage monitoring, pressure sensor for load and oil pressure monitoring, temperature sensor, proximity sensor, color detection sensor for oil level monitoring. The system generates automated maintenance alerts whenever anomalies are noted. These sensors measures a physical properties like heat, motion, pressure and produce an output signal to PLC/HMI this information or data is monitored or transferred to the cloud using software.

Monitoring Stage

The sensors measures a physical properties like heat, motion, pressure and produce an output signal to PLC/HMI this information or data is monitored or transferred to the cloud using software. The monitoring of machines through keeware software has three stages as depicted in Figs. 3 and 4 i.e. one is creating a channel, inserting a device, and creating tags for communicating.

For creating a channel, first we have to select new project and click edit and take a new channel and then we have to name the channel as per our requirement and click next then we need to select the device driver which we need to assign to channel, the list of device drivers will be shown which are installed on our system here we can take example, select TCP/IP Ethernet and click on next and select the perfect IP address to communicate a channel over a network or we can also select default then operating system will choose the network adopter, then click next for write optimization by this we can control how the server processes writes on the channel and set the optimization method and write-to-read duty cycle below, here there are 3 options to select the optimization method one is write all value for all tags, second one is write on latest value for non-Boolean tags, third one is write only latest value for all tags, here we choose third one and click on next and last is summary page here we can check whether all information given is correct or wrong if it is wrong we can click back and we can change, if it is correct then click finish. Once we click finish we can't change. By this way we can create a channel for monitoring. Creating a channel and summary of channel is depicted in Figs. 3 and 4.

For creating a device, after creating a channel click edit and choose new device and name it and then choose a device model (modbus) and device id (IP address) then we need to set communication timing parameters like connection time out (ex: 5 s) request timeout (1000 ms) this device has the ability to generate a tag database automatically, hence, next we have to mention when the database should generate, what action should be performed after generating, if the database generate database at startup what action should perform this has to be mentioned then ethernet setting is to be done that IP protocol is selected (TCP/IP) and then data access setting, then choosing block sizes when reading data from this devices then a summary page here we can check whether all information given is correct or wrong if it is wrong we can click back and we can

change, if it is correct then click finish. Once we click finish we can't change. By this way we can create a device for monitoring.

For creating a tag: click to add tag and then we have to do general settings to create a tag like tag name, address, description, data type, client access and then it create tag. for example as depicted in figure we need to check the temperature tag name (temp_c) tag address (40001) description (temperature in degree_c) data type as float client access to only read then click run button then it will monitor the temperature and shows the result this is shown in the Fig. 5.

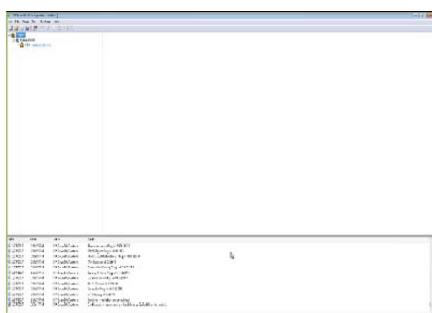


Fig. 3. Creating a channel

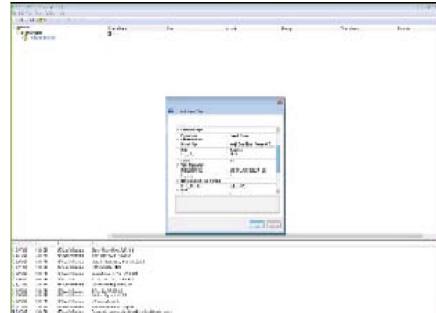


Fig. 4. Channel summary wizard

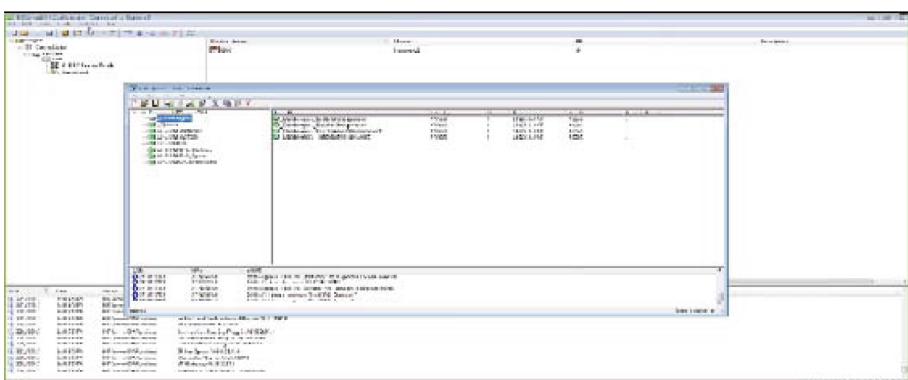


Fig. 5. After creating a tag sensor data is monitoring

Cloud Computing Stage

After monitoring the machines the data should be stored for the future use so we need a database to store the data but there will be huge data to store for this we require large data base hence, we store it in cloud with the internet access, this can be accessed easily anywhere, anytime by using thingworx software. It stores and analyse the data and

sends data to be displayed. Everyone can't access data in the cloud only few members who will give user name and password can access the data over the cloud. Finally web server sends data to PC that data will be displayed on andon display it may be about machine condition, machine downtime, about production. By this way the data will be monitored and controlled using internet of things.

5 Result and Discussion

The improvement of production and quality is shown in Fig. 6. By this we can improve production, it decreases cost and increases the product quality and this is directly impacts on efficiency. It provide reports on production analytics they are product reports, operations reports, add-on reports, analysis reports which broadly examine relationship of events, lines, products and time periods, operator metrics reports: provide performance information about operators, fastening analytics, which includes fastening data, lock counts, resolution reasons, and duration.

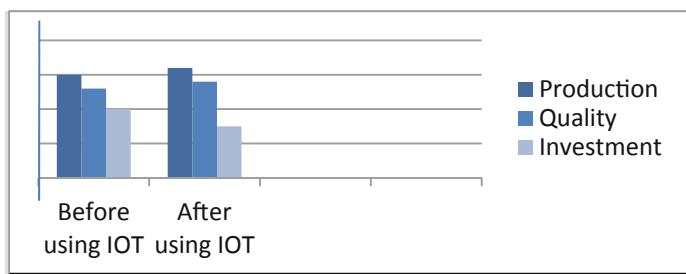


Fig. 6. Improvement in production, quality after using IoT



Fig. 7. Andon display for OEE analyzer for production

The production, overall equipment effectiveness and machine condition, downtime of machine and reason for the down time will be displayed on the display as depicted in figure, we can visualize the production in plant, which gives information about operators and operations of the current production events on displays. Objectives, outcome data and information on order progress and machine states support the staff and lead to an overall higher responsibility and quality. For production displays our OEE Analyzer can serve as a data source, this is shown in Fig. 7. By using IoT framework, it increases the production, marketing and has deliberated an intelligent control over the entire life cycle of production process associated with the housing line. With this the industry has achieved paperless integrated quality assurance, condition and energy management of machines, real time capable production controlling and this leads to some clearly visible and measureable benefits such as lower costs, easier inventory management and enhanced productivity.

6 Conclusion

Automated data acquisition and controlling system for housing line using IoT will change the entire manufacturing system. By implementing industry 4.0, it gives the fusion of the reality and the virtual world and becomes very affordable for many industries. By this way the supply chain is digitized and integrated with the traditional industrial processes. By implementing this system, the industry has significantly increased the productivity and it has deliberated an efficient control over the entire life cycle of products present in the manufacturing process. With this the housing line has achieved paperless integrated quality assurance, traceability of product, condition and energy management of machines, real time capable production controlling which leads to some clearly visible and measureable benefits like lower costs, easier inventory management and enhanced productivity. It increases the product quality, efficiency, and reduces the energy consumption. In future, the android app can be introduced, which will enable the technology to monitor the line condition in any place by just using the login. In the near future, industry 5.0 can also be introduced. The research is already started on fifth revolution of industry with a main focus on the cooperation between human, machine and workers to become up skilled to provide different value added tasks in the manufacturing of products.

References

1. Vaidya, S., Ambad, P., Bhosle, S.: Industry 4.0 – a glimpse. Procedia Manuf. **20**, 233–288 (2018)
2. Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., Yin, B.: Smart factory of industry 4.0: key technologies, application case, and challenges, pp. 2169–3536. IEEE (2017)
3. Rojko, A.: Industry 4.0 concept: background and overview. Int. J. Interact. Mob. Technol. iJIM **11**(5), 77–90 (2017)
4. Raja Sreedharan, V., Unnikrishnan, A.: Moving towards industry 4.0: a systematic review. Int. J. Pure Appl. Math. **117**(20), 929–936 (2017)

5. Barata, J., Rupino da Cunha, P., Gonnagar, A.S., Mendes, M.: A systematic approach to design product traceability in industry 4.0: insights from the ceramic industry. In: 26th International Conference on Information Systems Development (ISD 2017), Cyprus (2017)
6. Dohale, V., Kumar, S.: A Review of Literature on Industry 4.0, September 2018
7. Yen, C.T., Liu, Y.C., Lin, C.C., Kao, C.C., Wang, W.B., Hsu, Y.R.: Advanced manufacturing solution to industry 4.0 trend through sensing network and cloud computing technologies. In: 2014 IEEE International Conference on Automation Science and Engineering (CASE), Taipei, 18–22 August 2014 (2014)
8. Petrasch, R., Hentschke, R.: Process modeling for industry 4.0 applications. In: 2016 13th International Joint Conference on Computer Science and Software Engineering (JCSSE) (2016)
9. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications. *IEEE Int. Things J.* **4**(5), 1125 (2017)
10. Mert Gokalp, M.O., Kayabay, K., Akyol, M.A., Eren, P.E.: Big data for industry 4.0: a conceptual framework. In: 2016 International Conference on Computational Science and Computational Intelligence (2016)
11. Bocciarelli, P., D'Ambrogio, A., Giglio, A., Paglia, E.: A BPMN extension for modeling cyber-physical-production-systems in the context of industry 4.0. *IEEE* (2017). 978-1-5090-4429-0/17/\$31.00 ©2017
12. Li, C.H., Lau, H.K.: A critical review of product safety in industry 4.0 applications. In: Proceedings of the 2017 IEEE IEEM (2017)
13. Shahzad, K., O'Nils, M.: Condition monitoring in industry 4.0 – design challenges and possibilities: a case study. *IEEE* (2018). 978-1-5386-2497-5/18/\$31.00 ©2018
14. D'Emilia, G., Gaspari, A.: Data validation techniques for measurements systems operating in a industry 4.0 scenario. *IEEE* (2018). 978-1-5386-2497-5/18/\$31.00 ©2018
15. Elmustafa, S.A.A., Zeinab, K.A.M.: Internet of Things applications, challenges and related future technologies (2017). www.researchgate.net/publication/31365115. Accessed Jan 2017



Slotted Microstrip Patch 4×4 MIMO Antenna for Ultra Wide Band Applications

P. Ramya^{1(✉)}, R. S. Valarmathi², C. Poongodi¹,
and P. Hamsagayathri¹

¹ Department of Electronics and Communication Engineering,
Bannari Amman Institute of Technology, Sathyamangalam, India

{ramyap, poongodic, hamsagayathri}@bitsathy.ac.in

² Department of Electronics and Communication Engineering, Vel Tech
Dr. Rangarajan Sagunthala R&D Institute of Technology, Chennai, India
atrmatthy@gmail.com

Abstract. In this article four element MIMO antenna design for Ultra wide band 3–7 GHZ is presented. The antenna is designed based on microstrip annular framework with rectangular slot. To enhance the separation between the elements an annular slot antenna with I shape patch on the ground plane is used as an element of multi-input-multi output antenna. Ant1 and Ant2 cover the lower band. Further the Ant3 and Ant4 covers the upper band. The proposed antenna is compressed in order to occupy a volume of $51 * 51 * 0.8$ mm³. 19 dB isolation, which is measured between the antenna elements. The proposed antenna shows the good radiation characteristics with a high gain of 4.5 dBi. The performance characteristics of MIMO antenna is analyzed in terms of the scattering parameters, VSWR, antenna gain and radiation patterns. Analysis of these parameters indicates that the design is appropriate for ultra wide band applications.

Keywords: MIMO antenna · Annular ringslot · UWB · Isolation

1 Introduction

In MIMO antenna multiple antennas are operated on the same band to the high transmission speed and channel capacity. The radiation characteristic of each element is important to enhance the performance of MIMO antenna. In addition to the software approaches, shielding [1], split ring resonator [2], electronic band gap structure [3], spatial filter [4] are the common methods. To improve the radiation characteristics of MIMO antenna. These strategies are unsuitable for some applications.

In this a paper, we propped a MIMO antenna with improved isolation to achieve the requirements of UWB (2–7 GHZ) and WiMax. In the proposed antenna, each antenna element is slotted like annular ring and feed of the each element is placed on ground plane to reduce the size of the MIMO antenna. If any one element is radiated, the induced current of the other element is reduced so the mutual couplings are effectively reduced. Simulation results show that the mutual isolation of the proposed antenna are

improved by more than 30 dB. The radiation properties of the proposed antenna is analyzed using ADS Ver 2011.

2 Antenna Design

The structure of the proposed antenna is shown in Fig. 1. It consists of annular ring based circular slot with a radius r_1 and circular patch of radius r_2 , fed by the insert feed through ground plane. In the proposed antenna each element has separate feed length of L_1 and L_2 . The optimized parameters of the proposed antenna is shown in Fig. 1. The optimized size of the antenna is to $51 * 51 * 0.8$ mm³.

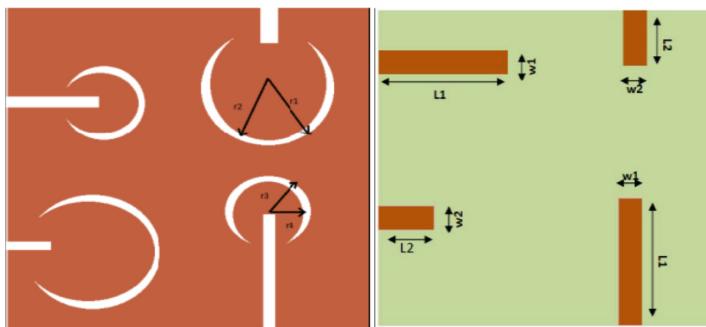


Fig. 1. Geometry of the proposed antenna (a) top view (b) bottom view

3 Results and Discussion

3.1 Reflection Coefficient

In this section, the proposed circular slot antenna is simulated and experimental reflection coefficient, isolation, radiation pattern results are presented also the effect of isolation is discussed. Figure 2 represents the S11 response of the proposed antenna ant1 ant2 covers the lower band and ant3 and ant4 covers the upper band of frequencies.

The effect of return loss and mutual isolations of antenna elements are shown in Figs. 3 and 4. It is clear that the band are sensitive to gap parameter the optimal value of gap is 0.8 mm. To reduce the antenna size the feed is placed on ground plane and to control the resonance frequency the radius of the patch is optimized.

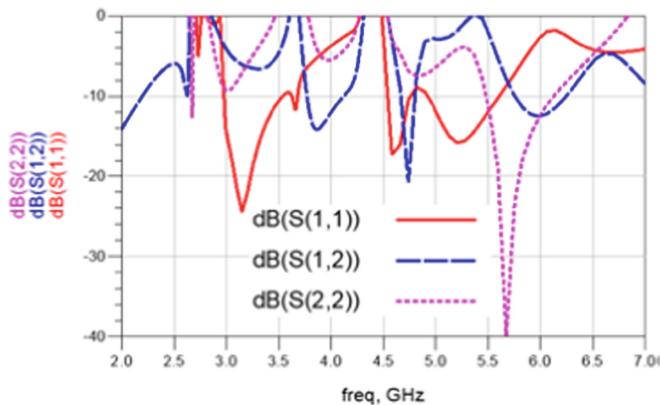


Fig. 2. Simulated S₁₁ for ant1 and ant2

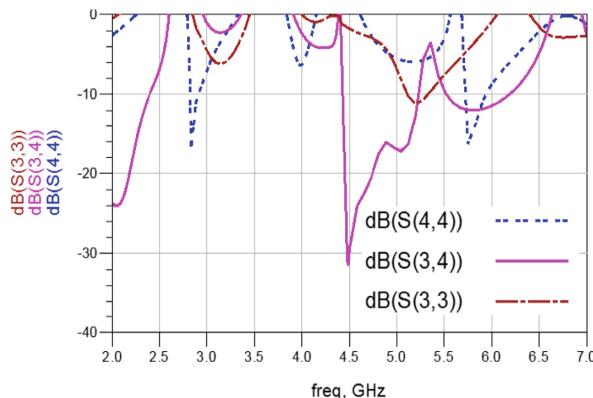


Fig. 3. Simulated S₁₁ for ant3 and ant4

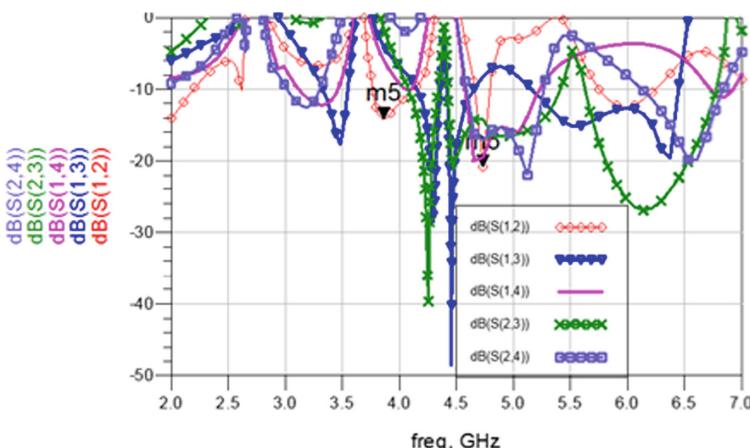


Fig. 4. Simulated mutual isolations of proposed antenna

3.2 Current Distribution

The performance of the proposed antenna is further analysed using surface current distribution. The current distributions of the antenna at WiMax frequency of 5.8 GHz is shown in Figs. 5 and 6. It shows that as any two element of the antenna is excited current distribution of the other element is reduced. The path of the current distribution is changed based on the dimensions of the circular patch. Other parameters also to change the current path, it would change the current path for another resonant frequency.

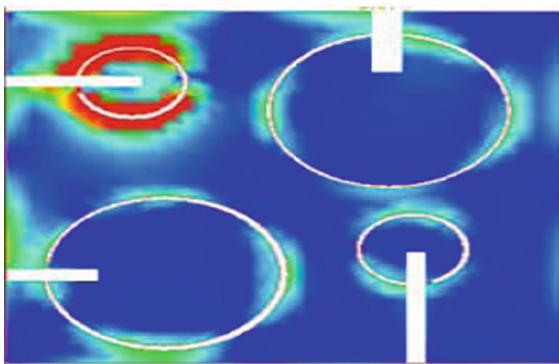


Fig. 5. Current distribution on ant2

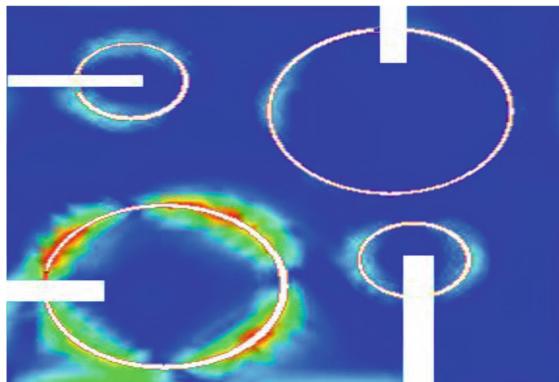


Fig. 6. Current distribution on ant1

3.3 Radiation Patterns, Gain and Efficiency

The radiation characteristics is simulated using commercial microwave simulation software of ADS Ver. 2011.

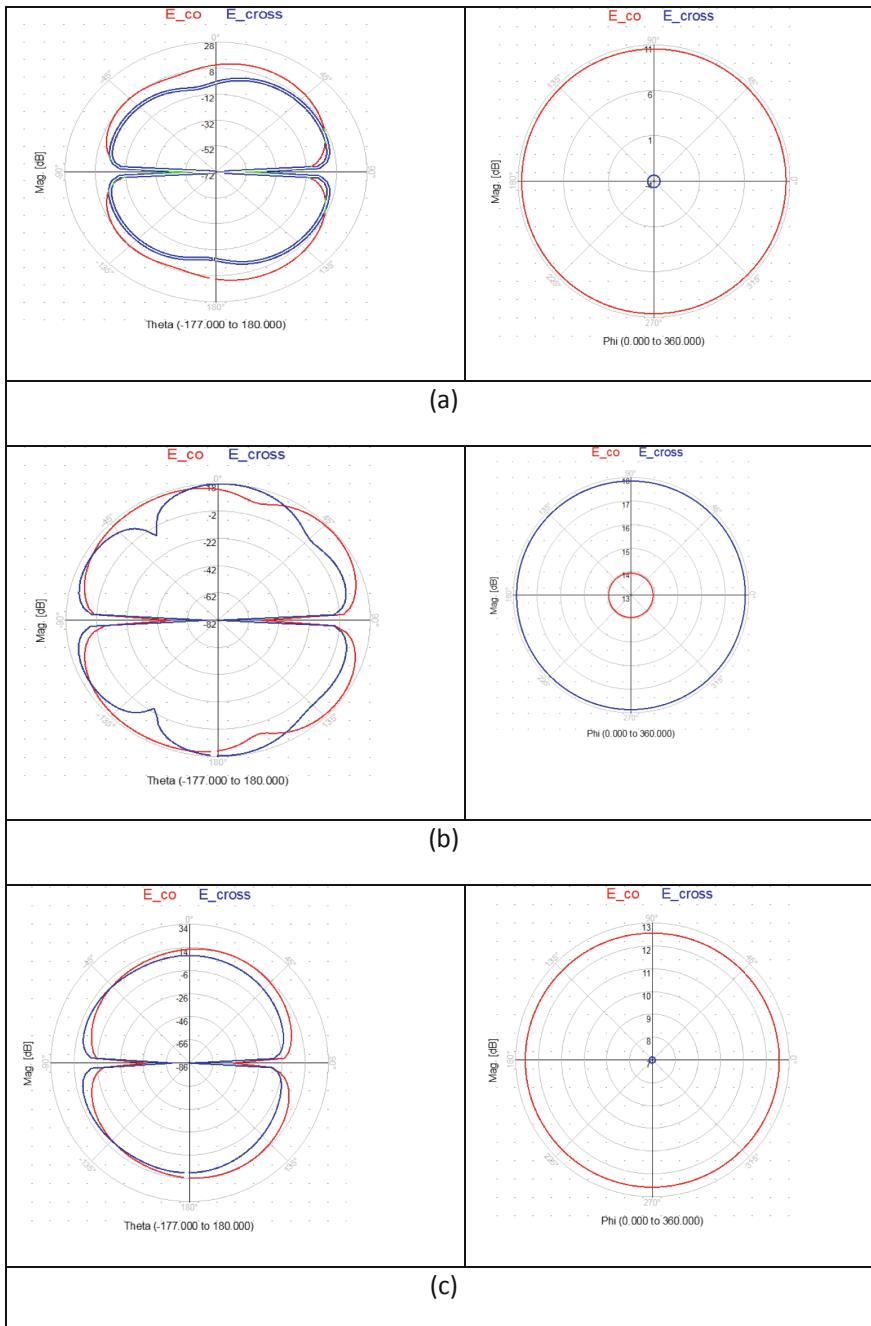


Fig. 7. 2D radiation pattern of E plane and H-plane (a) 3.2 GHz (b) 5.8 GHz (c) 4.5 GHz

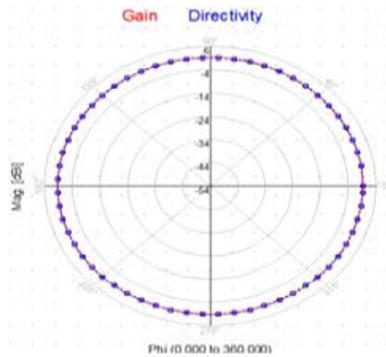


Fig. 8. Gain and directivity of the proposed antenna

The antenna parameters are analyzed. The simulated radiation pattern for co and cross polarizations for UWB frequencies are shown in Fig. 7. The simulated gain and efficiency of the antenna is shown in Fig. 8. The simulated efficiency is 99.996% with the corresponding gain and directivity of 6.51 dB and 6.52 dB it is higher than existing antenna.

4 Conclusion

The design of annular ring based circular slot MIMO antenna with a compact size of $51 \times 51 \times 0.8 \text{ mm}^3$ for ultra wide band applications has been successfully implemented. The circular slot on the patch and the dimensions of feed patch on the ground plane are generating a various frequency bands for UWB applications. These frequency bands can be independently controlled by using the slot gap. The antenna size is also reduced with enhanced isolation. The simulated outcome shows that the proposed antenna is suitable for Ultra wide band applications.

References

1. Gesbert, D., Shafi, M.: From theory to practice: an overview of MIMO space-time coded wireless systems. *IEEE J. Sel. Areas Commun.* (2005)
2. Deng, J.Y., Yao, J.: Ten-element MIMO antenna for 5G terminals. *Microw. Opt. Technol. Lett.* **60**(12), 3054–3059 (2018)
3. Khan, M.U., Sharawi, M.S.: A dual-band microstrip annular slot-based MIMO antenna system. *IET Microw. Antennas Propag.* **12**(6), 972–976 (2018)
4. Marzudi, W.N.N.W., Abidin, Z.Z.: A compact orthogonal wideband printed MIMO antenna for WIFI/WLAN/LTE applications. *Microw. Opt. Technol. Lett.* **57**(7), 1733–1738 (2015)
5. Li, M.Y., Ban, Y.L.: 8-port orthogonally dual-polarized antenna array for 5G smartphone applications. *IEEE Trans. Antennas Propag.* **64**(9), 3820–3830 (2016)
6. Kumar, J.: Compact MIMO antenna. *Microw. Opt. Technol. Lett.* (2016)

7. He, Y., Ma, K., Yan, N.: Dual-band monopole antenna using substrate-integrated suspended line technology for WLAN application. *IEEE Antennas Wirel. Propag. Lett.* **16**, 2776–2779 (2017)
8. Abutarboush, H.F., Nasif, H., Nilavalan, R.: Multiband and wideband monopole antenna for GSM900 and other wireless applications. *IEEE Antennas Wirel. Propag. Lett.* **11**, 539–542 (2012)
9. Cai, Y.Z., Yang, H.C., Cai, L.Y.: Wideband monopole antenna with three band-notched characteristics. *IEEE Antennas Wirel. Propag. Lett.* **13**, 607–610 (2014)



An Effective Logic Obfuscation Technique with AES Encryption Module for Design Protection

Binu P. Kumar^(✉) and M. Nirmala Devi

Department of Electronics and Communication Engineering,
Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India
binupkumar1993@gmail.com, m_nirmala@cb.amrita.edu

Abstract. The integration of Globalization in the semiconductor industry has resulted in the outsourcing of IC's by many companies. A person with a malicious intent in an untrusted foundry can pirate the IC's, overbuild the IC's and sell it illegally in the black market, reverse engineer the IC to obtain useful information about the IP, insert hardware trojans to disrupt the functionality of the IC or to leak sensitive information. Logic Encryption has become essential in order to protect the rights of the IP's owner and to save the IC design company from potential loss of money. It involves modifying the netlist to obfuscate the functionality of the design such that only on application with the correct key can unlock the design. We propose an efficient technique to controllably corrupt the design such that hamming difference of 50% is obtained between the correct and wrong outputs. The selected nets are encrypted using AES-128 block. The proposed encryption technique provides high security compared to the conventional encryption techniques using XOR's or multiplexers as it is insensitive to key sensitization attacks.

Keywords: Logic encryption · Hardware security · SCOAP measures · Hamming difference

1 Introduction

The number of IC design companies has increased due to the ever increasing need of semiconductor design technology. Most of these companies do not have a fabrication unit as it incurs heavy investment cost and hence they depend on third party fabrication unit. It leads to several threats like IC pirating, reverse engineering of IC to obtain information about the IP and selling the information to a rival company, insertion of hardware trojans to disrupt the functionality of the IC or to leak any sensitive information. To overcome these problems, logic encryption technique is used. Logic encryption technique is used to protect the IC's from attacks happening in untrusted Foundries. Logic encryption locks the IC with a secret key such that only on application with the correct key, the IC will be unlocked. It provides maximum security when there is an average hamming difference of 50% between the correct and obfuscated outputs. The proposed technique uses an algorithm based on combinational observability and number of fan out of each net in order to find nets which are suitable

for encryption such that an average hamming difference of 50% is obtained between the correct and obfuscated outputs. The technique is suitable for complex designs, which requires a comparatively high level of security. The encryption block uses a 128 bit key, which is practically not feasible to obtain the key through brute force attack. The proposed method is different from the conventional key based encryption techniques where key gates are inserted corresponding to each key bit. It provides high security as it is resistant to the key sensitization attacks. The key based encryption involves inserting key gates corresponding to every net, which is intended to remain encrypted. Each bit can be controllably corrupted by changing the key bit to the wrong logic value. The key gate based encryption is susceptible to key sensitization attacks [1]. The attacker is able to propagate the key bit to the output as each key bit influences only a single bit. The proposed technique encrypts the selected nets by using the AES encryption technique. For every single key bit change, multiple number of bits are corrupted. Hence, it becomes difficult for the attacker to isolate a particular key bit and propagate it to the primary outputs.

Section 2 describes the overview of the related works. Section 3 discusses the proposed technique. Section 4 illustrates the results of the work done. Section 5 gives the conclusion of the work done.

2 Overview

Logic obfuscation based on modification of gate level netlist is proposed in [2]. The nets to be modified are selected based on an iterative node selection algorithm considering the fan out and fan in cones. A technique based on fault impact to identify the insertion sites is proposed in [3]. The fault impact is calculated based on the number of test patterns that can propagate a ‘s-a-0’/‘s-a-1’ of a particular net to the primary outputs and the number of primary outputs which will be influenced by the ‘s-a-0’/‘s-a-1’ fault at a particular net. The nets which are having high fault impact are encrypted using XOR/XNOR gates or MUX’s. This kind of encryption technique is susceptible to key sensitization attacks. Several Key sensitization attacks are proposed in [1]. If the attacker has a functional IC and the obfuscated netlist, attacker can obtain the key bit by finding a suitable input pattern that can sensitize the key bit to primary output. A technique to overcome illegal overproduction and insertion of Hardware Trojan by minimizing the rare value nodes in the circuit is presented in [4]. The technique involves encrypting the circuit in order to reduce the number of rare nodes in the design. A technique to modify the inbuilt testing architecture to corrupt the functionality of the design when operated in obfuscated mode is proposed in [5]. The correct key will disable the test points and operate the design in transparent mode. An encryption technique using obfuscation cell (OC) which is composed of an inverter and a multiplexer is discussed in [6]. A SAT solver based attack algorithm to decipher the secret key is presented in [7]. A survey on various logic testing techniques that prevents Hardware Trojan insertion and the challenges faced is presented in [8]. A survey on different threat models, the techniques to overcome each attack and the metrics to

evaluate the strength of the defence is discussed in [9]. An analyses on the strength of the logic encryption based on fault impact and connectivity is presented in [10]. A technique to identify hardware Trojans based on Gate level characterization by considering leakage power is proposed in [11]. A detailed explanation of testability measures are given in [12] and [13]. An FPGA implementation of AES-128 with and without obfuscation in order to evaluate its security is proposed in [14]. The advantages and comparison of AES encryption with other encryption techniques are given in [15].

3 Proposed Methodology

The proposed methodology is explained with the help of a flowchart (Fig. 1). The first step is the computation of SCOAP measure and number of fan-outs corresponding to each net of the circuit. A set of 150 highly observable nets other than the primary outputs are considered. A set of 128 nets having high number of fan-outs is selected from the previous set. The selected nets are encrypted using AES-128 Encryption Block with a unique key. Section 3.1 explains the computation of SCOAP measures and number of fan-outs corresponding to each net. Section 3.2 explains the AES Encryption Block design Flow.

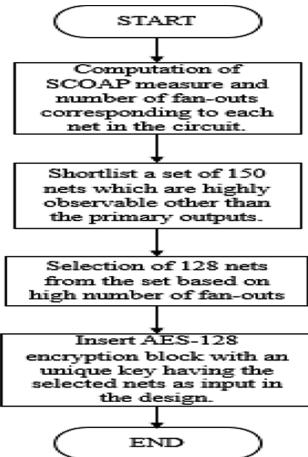


Fig. 1. Proposed methodology flowchart

3.1 A SCOAP Measure and Fan-Out Computation

The nets to be encrypted are selected based on SCOAP measures such as controllability and observability. The analysis is done on ISCAS'85 benchmark circuit. Controllability (0/1) of a net is the measure of how easy or difficult it is to force the net to logic (0/1).

Low values for controllability imply easy to control. High values for controllability imply difficult to control. Observability of a net is the measure of how easy or difficult it is to propagate the logic value of the net to the principle output. Low values of observability imply highly observable. High values of observability imply that it is very difficult to observe. Equations for computing combinational controllability and observability for various gates are mentioned in [12].

The algorithm for the computation of SCOAP measure and the number of fan-outs corresponding to each net in the design is given by (Fig. 2). The algorithm is implemented in python. The Verilog code of the design is converted into a readable form using Synopsys tetramax tool. The netlist is stored in a database with ‘xlsx’ extension. The contents of the netlist is converted into lists using ‘xlrd’ package of python.

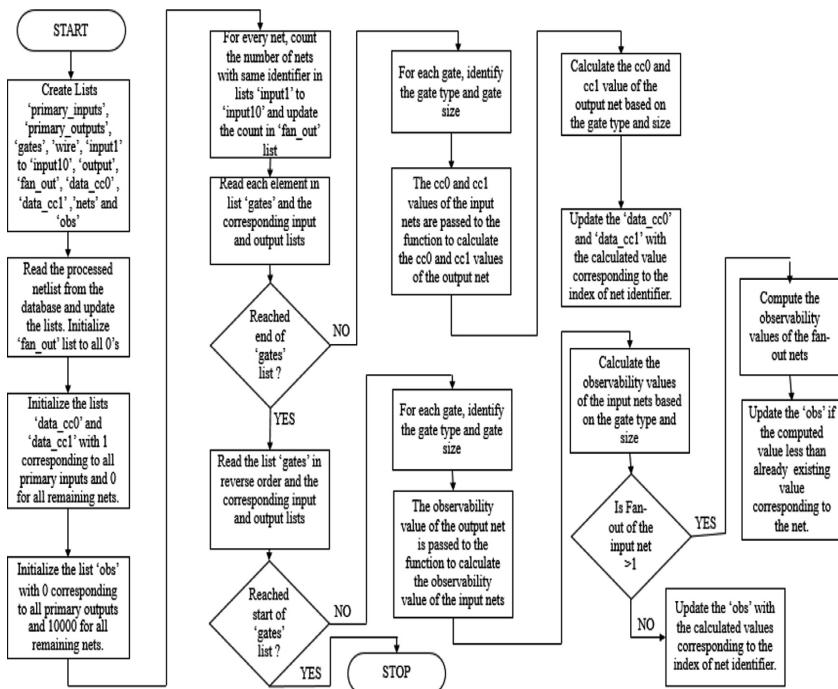


Fig. 2. SCOAP and fan out computation flowchart

3.2 Design of AES-128 Encryption Block

AES-128 Encryption Block encrypts plain text of size 128 bits with 128 bit cipher key. The encryption block is designed in such a way that only on application of correct key, the correct outputs are produced. In all the other cases, AES encrypted cipher text will

come as the output of the Encryption Block. The encryption consists of 10 rounds plus an initial key mixing stage. The cipher key is processed in each round to obtain sub keys. A key schedule algorithm is implemented in order to obtain the keys for different rounds. The AES Encryption Block Design flow is given by (Fig. 3). All the rounds are identical except the last round. Each round of operation consists of Byte Substitution stage, Shift Row stage, Mix column stage and round key mixing stage. The last stage consists of only Byte substitution, Shift Row stage and Round key mixing. The Byte substitution step reduces the bit level correlations of each byte. Each byte undergoes transformation by taking its multiplicative inverse in GF (2⁸) and affine mapping. It is implemented using a 16 × 16 lookup table. The byte is replaced by the byte obtained from the lookup table. The input byte is divided into two nibbles, the first nibble corresponds to the row index of the look up table and the second nibble corresponds to the column index of the look up table. The input byte is replaced by the byte obtained from the intersection of row index and column index in the look up table. The shift row operation involves 4 steps. The first row remains unchanged. The second row undergoes left circular shift by 1 byte, the third row by 2 bytes, and the fourth row by 3 bytes. The mix column step makes each byte of a column dependent on all the other bytes. The initial stage before the start of rounds mixes the plain text input with the cipher key. AES is an iterative block cipher. The same process is repeated for 10 rounds but with different sub keys. The key schedule algorithm transforms the 128 bit key to ten 128 bit sub keys. The key mixing stage involves the bitwise XOR operation of the input of the stage with the sub key generated by the key expansion algorithm. Each round, the keys are divided into 4 words W₀, W₁, W₂, W₃. Let W_{0,i}, W_{1,i}, W_{2,i}, W_{3,i} be the key of ith round. The key of (i + 1)th round is given by the Eqs. 1, 2, 3 and 4. The shift function performs byte wise circular left shift operation of the word. The byte substitution function replaces each byte of the 32 bit word with the corresponding byte from the S-Box. The round constant is 1 for the 1st round. The round constant for the rounds are given by the Eq. (5).

$$W_{0,i+1} = \text{byte substitution} (\text{shift}(W_{3,i})) \wedge \{\text{round_constant}, 24'd0\} \wedge W_{0,i} \quad (1)$$

$$W_{1,i+1} = W_{0,i+1} \wedge W_{1,i} \quad (2)$$

$$W_{2,i+1} = W_{1,i+1} \wedge W_{2,i} \quad (3)$$

$$W_{3,i+1} = W_{2,i+1} \wedge W_{3,i} \quad (4)$$

$$\text{round_constant}_{i+1} = \text{round_constant}_i * 8'h01 \quad (5)$$

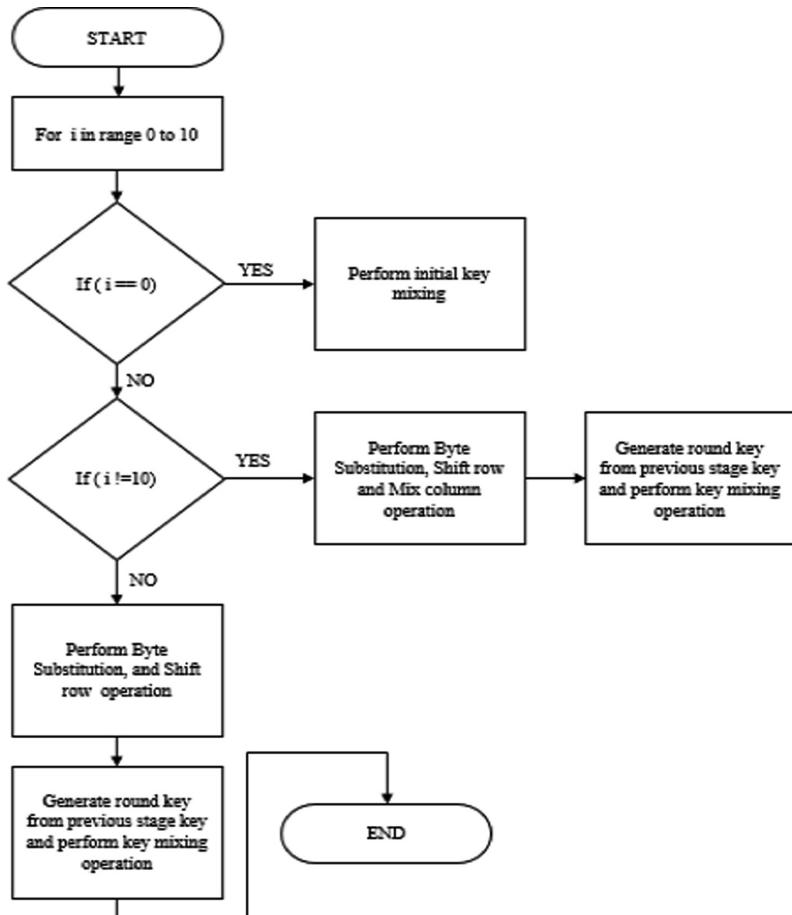


Fig. 3. AES design flow

4 Results and Discussions

The simulations of the Encryption block is done in Altera Model Sim. An AES Decryption Block is designed to verify the cipher text. The AES Encryption Block is designed such that only on application with the correct key, the output becomes the plain text. In all other cases, the output is the AES Encrypted cipher text. In order to verify the functional correctness of the encrypted cipher text, the output of the encryption block is passed through an AES-128 Decryption Block. The cipher text is decrypted using the same key used for encryption. The cipher text is correct if the decrypted output of the AES-128 decryption block matches the plain text.

Table 1. Encryption block results

Plain text	Key	Cipher text
0011-2233-4455-6677-8899-aabb-ccdd-eeff	1234-4321-1234-4321-1234-4321-1234-4321	eb7c-802f-fd7b-3376-8337-79d8-f97e-125e
0000-1111-2222-3333-4444-5555-6666-7777	1234-4321-1234-4321-1234-4321-1234-4321	488d-9872-731a-b528-9216-f1ed-ea64-2a78

Table 2. Decryption block results

Cipher text	Key	Plain text
eb7c-802f-fd7b-3376-8337-79d8-f97e-125e	1234-4321-1234-4321-1234-4321-1234-4321	0011-2233-4455-6677-8899-aabb-ccdd-eeff
488d-9872-731a-b528-9216-f1ed-ea64-2a78	1234-4321-1234-4321-1234-4321-1234-4321	0000-1111-2222-3333-4444-5555-6666-7777

Tables 1 and 2 shows the functional correctness of the AES-128 encryption block obtained through simulation in Modelsim. On applying the same key used for encryption in the AES-128 decryption block, the plain text is uncovered. Here the decryption block is designed in order to check whether the AES-128 encryption block is functionally correct.

Table 3. Round key generation.

Round	Sub keys (128 bit hexadecimal)
1	0b2e-bee8-191a-fdc9-0b2e-bee8-191a-fdc9
2	ab7a-633c-b260-9ef5-b94e-201d-a054-ddd4
3	8fb9-2bdc-3ddb-b529-8495-9534-24c1-48e0
4	ffe9-caea-c232-7fc3-46a7-eaf7-6266-a217
5	dcd3-3a40-1ee1-4583-5846-af74-3a20-0d63
6	4b04-c1c0-55e5-8443-0da3-2b37-3783-2654
7	e7f3-e15a-b216-6519-bfb5-4e2e-8836-687a
8	62b6-3b9e-d0a0-5e87-6515-10a9-e723-78d3
9	5f0a-5d0a-8faa-038d-e0bf-1324-079c-6bf7
10	b775-35cf-38df-3642-d860-2566-dffc-4e91

Table 3 shows the keys generated by the key generation block for various rounds of the encryption algorithm. The results shows the keys generated from a 128 bit input cipher key of value 12344321123443211234432112344321 in hexadecimal for every round.

Table 4. Cipher text generated by AES encryption

Plain text	Cipher key	Cipher text
0011-2233-4455-6677-8899-aabb-cddd-efff	4321-1234-4321-1234-4321-1234-4321-1234	e772-2d83-b242-7b4e-67d2-11ba-d0b6-d306
0011-2233-4455-6677-8899-aabb-cddd-efff	1234-5678-8765-4321-1234-5678-8765-4321	ac48-c315-dea5-eda7-5352-fedb-5a1f-b0db
0011-2233-4455-6677-8899-aabb-cddd-efff	1111-2222-3333-4444-5555-6666-7777-8888	428c-34ba-f97d-5a61-692b-dc3a-6863-237a
0011-2233-4455-6677-8899-aabb-cddd-efff	8888-1111-2222-7777-5555-4444-6666-3333	ede9-8404-f4c2-28c1-8147-8826-3d8b-ddee
0011-2233-4455-6677-8899-aabb-cddd-efff	1234-4321-1234-4321-1234-4321-1234-4321	0011-2233-4455-6677-8899-aabb-cddd-efff
0011-2233-4455-6677-8899-aabb-cddd-efff	1111-1111-9999-9999-6666-6666-ffff-ffff	ec31-f7ff-16fb-78b5-d43ab18-a743-2fed
0011-2233-4455-6677-8899-aabb-cddd-efff	aaaa-aaaa-bbbb-bbbb-ffff-ffff-9999-9999	906d-c530-4e60-e6ce-56af-0836-54f3-a22c
0011-2233-4455-6677-8899-aabb-cddd-efff	0123-4567-89ab-cdef-fedc-ba98-7654-3210	7eee-aae8-3552-ed18-e275-577f-d2eb-09d3
0011-2233-4455-6677-8899-aabb-cddd-efff	8281-8097-9781-8102-7000-9633-3979-2116	f751-5cc8-24e3-5a92-3cd7-8d33-5a03-9d54

Table 4 show that only on application with the correct key, the plain text is uncovered. In all the remaining cases, the output of the encryption block is AES-128 encrypted cipher text. In the above result, when the correct key of value 1234432112 3443211234432112344321 in hexadecimal is applied, the cipher text becomes equal to the plain text.

ISCAS-85 Benchmark circuit C6288 is taken into consideration for encryption. It has 32 primary inputs, 32 primary outputs, 2416 gates and 2448 nets. The proposed methodology is applied on c6288 circuit. 150 nets other than primary outputs which has high observability values are taken into consideration. From the 150 nets, only 128 nets having high number of fan-outs are chosen for encryption.

Table 5. Comparison of expected and encrypted output for c6288

Input	Expected output	Encrypted output	Hamming difference (%)
1010111010001011001111111010000	00110100011011000111001110010000	00000000000000000000111101000111000	37.5
0110010111111010101010100101101	00111000011111111110011100010	1000000011000001000111101001000	68.75
11101000001011001111000100000101	10011011000111101101010100000100	00000000000000000001110000000111000	53.125
01110010001101111100101000010101	0101001010110011111101011011010	0000000110101010000000110110101000	53.125
1000010000110001011010001001001	01101011110011111000100001110101	000000000000000000011011010010000	59.375
0101011100101100000100111110101	00000101100111011001001000100100	10000000000000100010001111101000	53.125
110000011100110000110001100110000	01001010111110111010001010000000	000000000000000000010111101000000	50
010010000001001100010110000001	000100011011110001011010100100101	100000001000000010010011110100000	56.25
11010101111010011111100111010101	10101100010110101101011010010101	0000000000000000000110011001000000	56.25
10101110010001001000001111010000	1010110010000001010100110000000	000000000000000000011001011011000	37.5

The selected 128 bits are encrypted using the AES-128 encryption Block. Table 5 shows the results on application of 10 random patterns. The columns shows the expected output, the outputs obtained after the encryption and the hamming difference between it. The average hamming difference percentage obtained between the expected and encrypted output is 52.5. For some input combination, the hamming difference goes above 50% as well as for some, it goes below 50%. However, it is able to achieve an average hamming difference close to 50%.

Table 6. Average H.D. for ISCAS-85 circuits

Circuit	Avg. hamming difference (%)
c1355	47.14
c1908	53.12
c2670	49.71
c3540	48.13
c5315	52.30
c6288	46.71
c7552	50.80

The Average Hamming difference between the outputs produced by the original design and the outputs produced by the encrypted design is calculated for 10,000 random inputs. The random inputs are generated using random package of python. The 10,000 random inputs from the text file are applied to the original design and the encrypted design. The outputs of the original design and the encrypted design are stored in separate text files, which are then used for the computation of average hamming difference. A verilog code is created for the computation of average hamming difference. Table 6 shows the achieved average hamming difference percentage for various ISCAS-85 benchmark circuits. All the circuits are able to achieve average hamming difference percentage close to 50%.

Table 7. Comparison of XOR and AES based encryption outputs for single key bit change

Key (one bit change)	XOR encryption	AES-128 encryption
0234-4321-1234-4321-1234-4321-1234-4321	1011-2233-4455-6677-8899-aabb-ccdd-eeff	cfbdfea2-6683-b9e0-5683-fcc4-90be-6ddc
1034-4321-1234-4321-1234-4321-1234-4321	0211-2233-4455-6677-8899-aabb-ccdd-eeff	3e1b-cb9a-281e-d50d-7f94-6b6b-0f2d-cfa8
1214-4321-1234-4321-1234-4321-1234-4321	0031-2233-4455-6677-8899-aabb-ccdd-eeff	4e52-2831-87c6-5389-8939-c23d-22d1-e982
1224-4321-1234-4321-1234-4321-1234-4321	0001-2233-4455-6677-8899-aabb-ccdd-eeff	3526-2532-0ac1-78a5-94f9-ac1-3ffe-257f
1230-4321-1234-4321-1234-4321-1234-4321	0015-2233-4455-6677-8899-aabb-ccdd-eeff	6366-c987-6e6f-2c61-454d-420a-1a7d-fd9e

The previous techniques using fault impact selection technique followed by key gate insertion also provided average hamming difference of 50%. However the conventional encryption techniques can be compromised if the attacker knows the net selection flow. In key gate based insertion, key gates are inserted corresponding to every key bit. The key bit changes/encrypts the logic value of a single bit. This makes it easy to sensitize the key bits to the primary outputs. These kind of techniques are susceptible to key sensitization attacks. Therefore additional steps have to be done to ensure that the key gate arrangement is strong [4]. In AES-128 encryption technique, each key bit affect the logic value of multiple nets. Table 7 shows the effect of inverting a single key bit on the selected net for XOR based encryption and AES based encryption for data 00112233445566778899aabccddeeff and key 12344321123443211234432112344321 in hexadecimal. Table 5 clearly shows that multiple bits of the encrypted output is affected by flipping a single key bit in encryption using AES Block. It is difficult to isolate a single key bit as the plain text undergoes a series of bit level and byte level transformations. The non-linear byte substitution further increases the complexity of encryption technique as it removes the bit level and byte level correlations.

5 Conclusion

An efficient technique for selecting the nets to be encrypted is proposed with the help of testability metric-combinational observability and number of fanout nets corresponding to each net. The selected nets are encrypted using AES-128 block cipher. It is practically infeasible to obtain the secret key using brute force attack as the number of key bits are very high. Unlike the previous encryption techniques using XOR's or MUX's, the encryption using AES-128 is not sensitive to key sensitization attacks. Overall the AES-128 based encryption technique provides high security compared to the conventional encryption techniques. The proposed technique is suited for complex designs which require high level of security. The application of the technique on sequential circuits is the future work.

References

1. Rajendran, J., et al.: Security analysis of logic obfuscation. In: Proceedings of the 49th Annual Design Automation Conference, pp. 83–89. ACM (2012)
2. Chakraborty, R.S., Bhunia, S.: Hardware protection and authentication through netlist level obfuscation. In: Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design, pp. 674–677. IEEE Press (2008)
3. Rajendran, J., et al.: Fault analysis-based logic encryption. IEEE Trans. Comput. **64**(2), 410–424 (2015)
4. Dupuis, S., et al.: A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans. In: 2014 IEEE 20th International On-Line Testing Symposium (IOLTS), pp. 49–54. IEEE (2014)
5. Chen, M., et al.: Hardware protection via logic locking test points. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **37**(12), 3020–3030 (2018)

6. Zhang, J.: A practical logic obfuscation technique for hardware security. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **24**(3), 1193–1197 (2016)
7. Subramanyan, P., Ray, S., Malik, S.: Evaluating the security of logic encryption algorithms. In: 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 137–143. IEEE (2015)
8. Dupuis, S., et al.: Protection against hardware trojans with logic testing: proposed solutions and challenges ahead. *IEEE Des. Test* **35**(2), 73–90 (2018)
9. Rostami, M., Koushanfar, F., Karri, R.: A primer on hardware security: models, methods, and metrics. *Proc. IEEE* **102**(8), 1283–1295 (2014)
10. Chandini, B., Devi, M.N.: Analysis of circuits for security using logic encryption. In: International Symposium on Security in Computing and Communication, pp. 520–528. Springer, Singapore (2018)
11. Karunakaran, D.K., Mohankumar, N.: Malicious combinational hardware trojan detection by gate level characterization in 90 nm technology. In: Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1–7. IEEE (2014)
12. Goldstein, L.H., Thigpen, E.L.: SCOAP: Sandia controllability/observability analysis program. In: 17th Design Automation Conference, pp. 190–196. IEEE (1980)
13. Bushnell, M., Agarwal, V.D.: Essentials of Electronic Testing for Digital, Memory and Mixed-Signal VLSI Circuits. Springer, Boston (2002)
14. Chhabra, S., Lata, K.: Enhancing data security using obfuscated 128-bit AES algorithm - an active hardware obfuscation approach at RTL level. In: 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 401–406. IEEE (2018)
15. Daemen, J., Rijmen, V.: The first 10 years of advanced encryption. *IEEE Secur. Priv.* **8**(6), 72–74 (2010)



Unequal Energy Aware Secure Clustering Technique for Wireless Sensor Network

Simran R. Khiani^{1,2(✉)}, C. G. Dethé³, and V. M. Thakare¹

¹ SGBAU, Amravati, India

simran.khiani@raisoni.net

² GHRCM, Pune, India

³ UGC Academic Staff College, Nagpur, India

Abstract. As wireless sensor network has limited resources in terms of battery power, computation capacity and memory, therefore a dynamic clustering approach is proposed in order to reduce the energy consumption of the network. The algorithm works on various parameters such as residual energy, distance to the base station, intra cluster distance and number of neighboring nodes to elect a Cluster Head. The Cluster Head aggregates the data from all the cluster members and uses chaining method to send data to the Base Station. The proposed system helps in reducing the energy consumption and increases the life time of the network as compared to the existing systems.

Keywords: Dynamic clustering · Wireless sensor network · Fuzzy logic · Cluster head · Aggregation

1 Introduction

Wireless Sensor networks have a large number of tiny sensor nodes scattered in a huge area. These nodes can sense parameters such as soil moisture, temperature, pressure etc. There are many applications such as monitoring of environment, defense work, tracking of objects etc. But since the wireless sensor network has limited power, less memory and little computation capability, it is difficult to develop applications based on WSNs.

The major difficulty in designing WSN network is the energy of the battery. The battery of sensor nodes cannot be changed after the deployment, so battery power should be less consumed in order to enhance the lifetime of the network. There are many algorithms developed in order to reduce the energy consumed by the network. Clustering [1] technique is one of the most commonly used methods for this purpose. In the Clustering method, the network is divided into various groups based on certain attributes. In the first phase, the network is formed and depending upon the energy of the nodes, the node with the highest energy is selected as the Cluster Head. After the cluster head is selected, the member nodes nearby the cluster head will join the network. The member nodes will sense the environment parameters and transmit the data to the Cluster Head and will go to idle state. The responsibility of the cluster head is to aggregate all the data and send it to the base station. The advantage of this method is that the Cluster head is only transmitting the data hence energy will be less consumed.

1.1 Routing Protocols

Routing is also an important criteria in transmitting data from one node to the other node. It is basically used to select the best available path from source to destination. Each node will initially send its information such as node id, energy, and distance to the base station. This concept work similar as in computer network. The routing data available at the base station will be used to select the best available path out of many paths. The selected path will be used to send data to the base station. Routing protocols in Wireless sensor network are divided based on operation of the protocol, structure of network.

In flat routing, all the sensor nodes have the same energy and sensing capability whereas in hierarchical routing, nodes are divided based on the energy level and each node is assigned a different task. The low level nodes perform sensing and the nodes at the higher level perform the task of collecting and transmitting the data to the base station (Fig. 1).

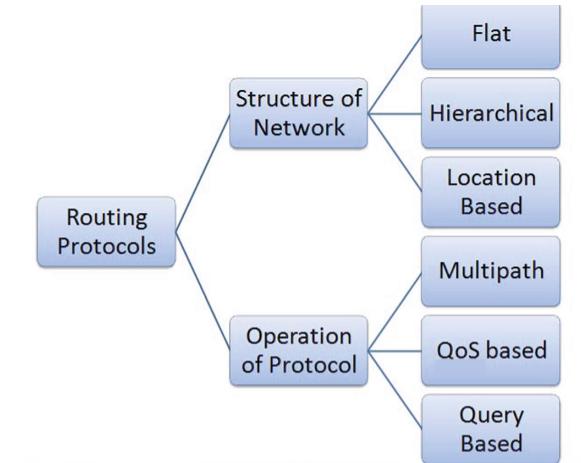


Fig. 1. Routing protocols

1.2 Clustering

Clustering has lot of advantages such as load balancing, reduced collisions, low delay etc. The responsibility of cluster head is to aggregate and transmit the data to the base station so routing table is not required at every node. Hence it is easy to manage and extend the network to get the values of sensed parameters. Load balancing is done as only cluster head communicates with the base station. Collision and delay is also reduced as cluster members transmit data to the cluster head only.

Clustering is divided into three categories [2] i.e. centralized, decentralized and hybrid. As the name implies in centralized method, a central node will take care of path selection from source to the base station. In decentralized method, every node can

become cluster head and there is no need to store global information for all the nodes. The third method i.e. hybrid method contains the characteristics of above two method.

Clustering algorithms can also be classified based on the method they work i.e. proactive, reactive and hybrid. The route for transmitting the data is computed in advance in proactive method.

According to the manner in which the sensor nodes work, the clustering algorithms can be divided as Proactive, Reactive and hybrid. In Proactive method, the route to transmit the data is computed in advance before all the data transmission. In reactive method, the route is selected dynamically when data is to be transmitted. Hybrid method is combination of the above two methods.

Based on data transmission, clustering can also be divided into intra-cluster and inter-cluster method. Intra cluster is a method in which sensor nodes transmit data to the cluster head whereas in inter cluster technique cluster heads transmit data to the other cluster heads nearby. Both the methods can be single or multi hop method.

Clustering can also be divided into areas of operation like block based, chain based and grid based. The detailed information about various algorithms is shown below.

1.2.1 Block Based Algorithms

1.2.1.1. LEACH: LEACH i.e. Low energy adaptive clustering algorithm is the major algorithm in wireless sensor networks. It uses strength of the signal to elect a cluster head. CH then forwards the data to the BS. This algorithm selects CH randomly which is a major drawback (Fig. 2).

1.2.1.2. HEED: Hybrid energy efficient distributed algorithm is a multi hop algorithm. It selects CH based on energy and intra cluster communication cost. This algorithm is energy efficient but overhead is more as it broadcast control packets.

1.2.1.3. TEEN: Threshold sensitive Energy Efficient sensor Network protocol (TEEN) is very useful algorithm for finding abrupt changes in serious situations. It works on threshold values. The major drawback of this algorithm is that if the value is below threshold, sensor will not transmit data.

1.2.1.4. Unequal Clustering Size (UCS) [3, 4] algorithm divides the network in the form of layers and in circular fashion. The cluster head works as a super node. The drawback of this method is that it requires CH node to be located at the center which is not possible in all cases so energy is not balanced in the network.

1.2.1.5. EECS: Energy Efficient Clustering Scheme (EECS) algorithm is a single hop algorithm. The selection of the CH is based on the energy. The node with highest energy is selected as CH. The drawback of this method is that if the CH is far away from BS then more energy will be consumed for transmitting data.

1.2.2 Grid Based Methods

1.2.2.1. GAF [5]: Geographic Adaptive Fidelity is geographic location based energy efficient algorithm for mobile adhoc network. The cells present in the cluster manage active and inactive time slots. One cell in each cluster is always active. The drawbacks of this algorithm are delay and large traffic.

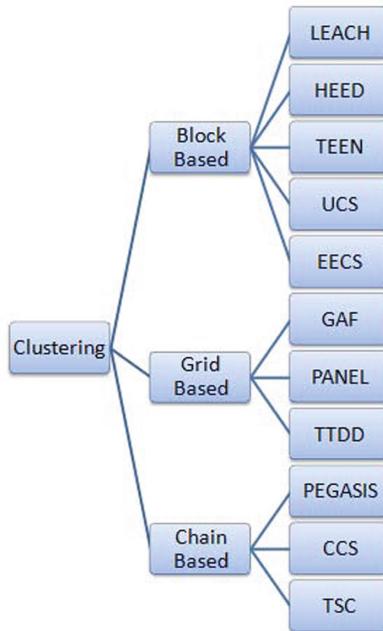


Fig. 2. Clustering algorithms

1.2.2.2. **PANEL:** Position based Aggregator Node Election method is used in database storage applications. Inter-cluster communication is used for selecting CH. The algorithm balances load and increases network life but the major problem is that at the time of deployment clusters are formed. So it is not applicable for real life applications.

1.2.2.3. **TTDD:** The Two Tier Dissemination is a reliable and extendable method which transmits data from multiple sources to multiple mobile sink nodes. This algorithm does not make use of shortest path technique hence the algorithm suffers from large latency.

1.2.3 Chain Based Clustering Algorithms

1.2.3.1. **PEGASIS [6]:** In Power Efficient Gathering in Sensor Information System clustering algorithm, a chain is formed by all the nodes by themselves or with the help of sink node. This algorithm aggregates the data by removing duplicate data before transmitting the data. The drawback of this algorithm is that all the nodes should have knowledge about the network which is not possible.

1.2.3.2. **CCS:** In Concentric Clustering algorithm, the system is distributed into round tracks. A chain of sensor nodes is formed in each circle. The CH at a level communicates with the CH at next level which reduces distance of transmission and

energy consumption. The drawback of this method is that the routing is done based on location of the node not energy.

1.2.3.3. TSC: Track Sector Clustering method divides the network into tracks and sectors. Each level will have a CH. The problem with this method is that the distribution of nodes is not uniform in all the tracks and energy is not used for selecting CH.

2 Proposed System

There are three phases of the algorithm: Network formation, CH selection and Data transmission. In the first phase, the BS will send control signal to all the nodes. The nodes will then send their information such as energy, id and distance to the BS. The BS then applies fuzzy logic in the second phase to the elect CH and creates a CH list. The details of the CH are sent to all the nodes. The sensor nodes depending upon the distance select CH nearby and join that CH.

Fuzzy logic is used in the proposed method. Centralized algorithm is used by the Base Station for selecting CH as the base station has large memory space and more powerful than the sensor nodes. Many parameters are used for electing Cluster head such as remaining energy, distance from BS, node location, computing power etc. (Fig. 3).

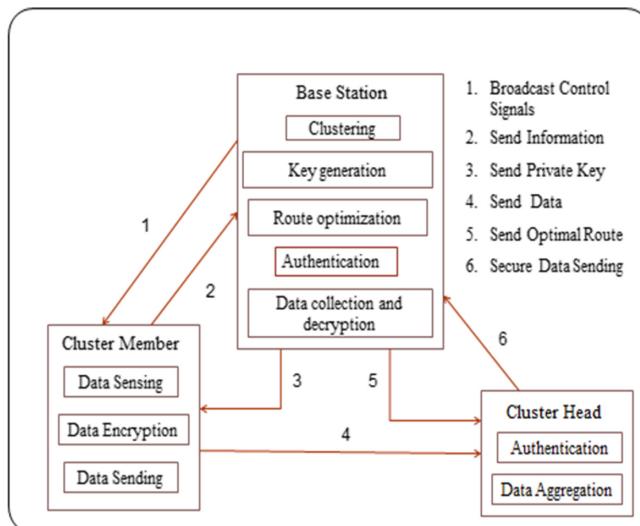


Fig. 3. System architecture

The third phase is data transmission. In this phase, the sensor nodes of a cluster send data to the CH and remain in idle state. The CH aggregates the data and forms a chain of CH and sends data to the BS through this chain. For providing security, BS will also apply a cryptography algorithm to generate public key and private keys of all

the nodes. The private key is transferred to all the nodes. After the CH aggregates [15] the data, it uses its private key to encrypt and send it to the other CH in chain. This process is continued till data reaches to the destination.

2.1 Parameters

As many parameters [7] such as energy of node, distance to the BS, neighboring nodes and intra cluster distance, latency, delay are available for selecting the cluster head. It is a difficult task to select parameters for choosing a CH.

The proposed work uses remaining energy of the node, distance to the BS, neighboring nodes and intra cluster distance for choosing a CH.

Energy of a node: Energy of a node [14] is a very important parameter. During data transmission and reception, energy of a node is consumed. Energy of a node ranges from 1 J to 3 J.

Distance to the BS: As all the data is to be transmitted to the BS, so the position of the BS is also important. The distance between the BS and a node is calculated using Euclidean distance. Distance and energy consumption during data transmission are directly proportional to each other i.e. if the distance is less, less energy will be consumed.

$$\text{EuclidianDist} = \sqrt{(X_i - X_c)^2 + (Y_i - Y_c)^2}$$

2.2 Intra-cluster Distance

It is the distance between the center and a node. It is calculated by taking the average of distance of all the nodes.

$$\text{Dist_IntraCluster} = \frac{1}{N} \sum_1^{\text{no_c}} \sum_1^{\text{no_s}} \|(\mathbf{S}_i - \mathbf{C}_i)\|^2$$

Where

no_c = No. of clusters

no_s = No. of sensors in a cluster

C_i = center of a cluster.

2.3 Inter-cluster Distance

It is the distance between the different CHs. According to the inter-cluster distance, chain of nodes is formed and data is transmitted through this chain to the BS.

For calculating the inter cluster dist., the formula used is as follows:

$$\text{Dist_IntraCluster} = (\|\mathbf{S}_i - \mathbf{S}_j\|)^2$$

Where $i = 1$ to $\text{no_c} - 1$ and $j = i + 1$ to no_c .

2.4 Fuzzy System

Type-2 Mamdani FLS (T2MFLS) [8–10] technique is used for electing a CH. Fuzzy system has various components such as inference engine, inference rules, fuzzy logic and de-fuzzification. The input parameters such as energy, intra-cluster distance [11], distance to the BS and no of neighbor nodes are given to the fuzzy system. All these parameters are denoted by certain levels for e.g. Energy [12] is denoted as low, medium and high. The fuzzy system applies fuzzy rules and output of the algorithm is the probability of a node to become CH [13].

2.5 Algorithm Cluster Head Selection

```

1: Control signal sent by BS to all the sensor nodes
2: Fuzzy Logic applied for CH selection
3: If node i is alive
4: [node i: probability] → [fuzzy_system (node i: energy, node i: neighbours; node
   i: distance to BS, node i: intra-cluster distance)
5: end if
6: sort ([node i: probability] in descending order)
7: for i = 1: i <= opt_cluster + 1: i++
8: for j = 1: j <= node_count: j++
9: if [node i: probability] < [node j: probability] then
10: node i ← member_node
11: end if
12: end

```

The Table 1 below shows the cluster head selection output which is in the form of probability of a node becoming cluster head.

Table 1. CH selection based on fuzzy logic method

Sr. no.	Node ID	Energy	Neighboring nodes	Dist. to BS	Dist. to CH	Probability of becoming CH	Remark
1	33	M	H	M	M	0.80	Member
2	17	M	L	M	H	0.60	Member
3	13	L	L	H	H	0.50	Member
4	34	M	M	L	L	0.90	Member
5	6	H	L	H	M	0.60	Member
6	2	L	L	M	H	0.60	Member
7	14	L	H	L	M	0.90	Member
8	32	H	M	M	M	0.70	Member
9	27	H	L	L	M	0.70	Member
10	5	H	M	L	L	0.90	CH

3 Results and Conclusion

The result below shows the clustering process. In this system four clusters are formed and based on fuzzy rules, CHs are selected (Figs. 4 and 5).

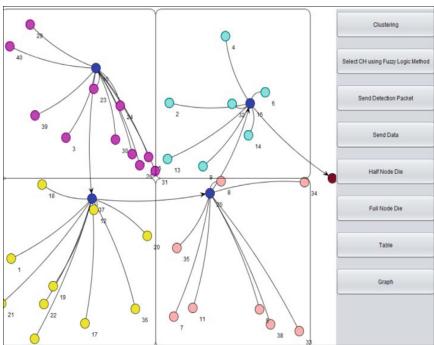


Fig. 4. CH selection and data transmission using fuzzy method

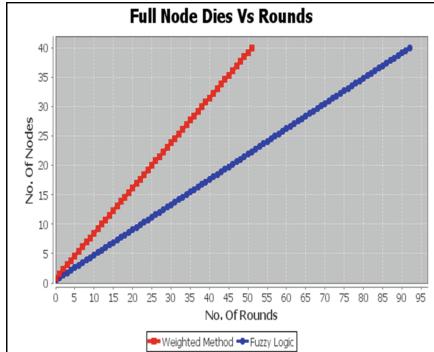


Fig. 5. Full Node Die (FND)

The results are compared with weighted algorithm. The result show that the full nodes of the system die in round 95 for the proposed system whereas all the nodes die in round 50 in the weighted method (Figs. 6 and 7).

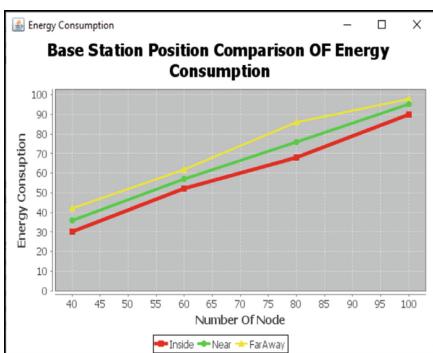


Fig. 6. Energy consumption

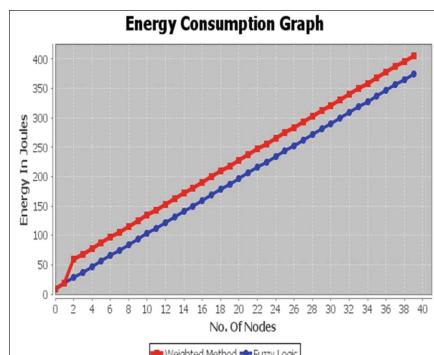


Fig. 7. Energy consumption based on position of base station

As shown in the above figure, the energy consumption is 8% less in fuzzy system as compared with the weighted method. The above figure shows the comparison of energy consumption based upon the location of base station. The base station was positioned near the network, far away from network and inside the network for an experimental purpose. It is clearly seen that when the BS is inside or near the network, the energy consumption of the network is less as compared to far away.

References

1. Misra, S.: A literature survey on various clustering approaches in wireless sensor network. In: IEEE 2nd International Conference on Communication, Control and Intelligent Systems (CCIS), pp. 18–22 (2016)
2. Liu, X.: Clustering routing algorithms in WSN. *KSII Trans. Internet Inf. Syst.* **6**(7), 1735–1755 (2012)
3. Wang, Y., Li, C., Duan, Y.: An energy-efficient and swarm intelligence-based routing protocol for next-generation sensor networks. *IEEE Intell. Syst.* **29**(5), 74–77 (2014)
4. Purkait, R.: Fuzzy based unequal energy aware clustering with multi-hop routing in wireless sensor network. In: 2015 IEEE Workshop on Computational Intelligence, pp. 1–10 (2015)
5. Dechene, D.J., El Jardali, A.: Survey of clustering algorithms for wireless sensor networks. In: Computer Communications. Butterworth-Heinemann, Newton (2007)
6. Boyinbode, O.: A survey on clustering routing algorithms. In: 2013 International Conference on Network Based on Information System, pp. 358–364 (2013)
7. Khan, A., Tamim, I., Ahmed, E., Awal, M.A.: Multiple parameter based clustering (MPC): prospective analysis for effective clustering in wireless sensor network (WSN) using k-means algorithm. *Wirel. Sens. Netw.* **4**, 18–24 (2012)
8. Zhang, Q.Y.: A clustering routing protocol for wireless sensor networks based on fuzzy logic and ACO. In: 2014 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 1060–1067 (2014)
9. Zhang, F.: ICTTSK: an improved clustering algorithm for WSN using a Takagi-Sugeno-Kang fuzzy logic system. In: 2013 IEEE Symposium on Wireless Technology and Applications (ISWTA), Kuching, 22–25 September 2013, pp. 153–158 (2013)
10. Zhang, Y.: Network energy efficient based on fuzzy interference system. In: IEEE 29th Chinese Control and Decision Conference (CCDC), pp. 2975–2980 (2017)
11. Riordan, D., Gupta, I., Sampalli, S.: Cluster-head election using fuzzy logic for wireless sensor networks. In: 3rd Annual Communication Networks and Services Research Conference (CNSR 2005), pp. 255–260 (2005)
12. Fazackerley, S., Paeth, A., Lawrence, R.: Cluster head selection using RF signal strength. In: 2009 IEEE Canadian Conference on Electrical and Computer Engineering, pp. 334–338 (2009)
13. Bajaber, F., Awan, I.: Centralized dynamic clustering for wireless sensor network. In: International Conference on Advanced Information Networking and Applications, pp. 193–198 (2009)
14. Bajaber, F., Awan, I.: Dynamic/static clustering protocol for wireless sensor network. In: Second UKSIM European Symposium on Computer Modeling and Simulation, pp. 524–529. IEEE (2008)
15. Sunanda, V.K., Jyothi, R.: Survey on dynamic clustering for energy efficient data aggregation technique using secure data encoding scheme for WSN. *Int. J. Eng. Res. Technol. (IJERT)* **3**(2) (2014). ISSN 2278-0181



Robust Smart Home Monitoring System Based on 802.11 Mesh Network

S. Loyola Samraj^(✉), Nisha V. Bhalke, A. Aarthi, R. Srinath,
and E. Prabhu

Department of Electronics and Communication Engineering,
Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India
loyola2308@gmail.com, nishavbhalke@gmail.com,
arthil998arthi@gmail.com, official.srinath@gmail.com,
e_prabhu@cb.amrita.edu

Abstract. Home automation is used to control and monitor home appliances, lighting, audio or video devices, etc. The demand for home monitoring systems to efficiently monitor the home appliances is constantly increasing and has a promising market trend in the near future. Present day home automation systems have limitations in programmability and customization. But when a functional block of home monitoring unit is made modular, it becomes versatile and can intelligently adapt to the required task assigned by the user. In this paper, we have built and implemented a system which would collect data from nodes that functions on a fault-proof Wi-Fi based self-stabilizing, ad-hoc mesh network based on painless Mesh. This has the potential to perform tasks like device status output, device control, and device automation. By establishing the client nodes in a mesh network, we will be able to connect the devices together and perform data acquisition through a server and transmit the data into a cloud platform through a gateway, and successfully notify the user through applets and a web-based GUI.

Keywords: IFTTT · MCU · IC · I2C · SCL · SDA · UART · MQTT · WMN · TTL

1 Introduction

The previous works on home automation is a system containing a central processing unit with various sensors attached to it. But the problem lies with how far the system remains flexible with the consumers' needs [2, 3, 8]. If in case, one doesn't need a sensor considering the environment, workplace and other such factors and if the customer wants to replace it with another sensor that would serve him with more utility, he must buy a whole new system with the desired sensors, which is generally not preferable. Another major drawback of the existing system is the need for an extra device to enable interoperability between two different systems.

Other limitations include high cost, the complexity of the system, which makes it too hard to use, and other forms of home automation system include lots of wiring,

complex installation process, difficulty in adding and fixing additional home appliances or monitoring systems, etc.

Thus, the aim of this paper is to build and implement a home monitoring system with the incorporation of the modularity concept, wherein adding an extra sensor or removing an additional sensor is made easier, with inter-node communication deployed over an ad-hoc, self-stabilizing network [1]. Thus, eliminating the fact that one should buy a whole new system if he/she wants to modify the existing system by adding or removing a sensor/a module. Furthermore, an early stage Field Programmable Gate Array design was discussed in [14].

2 Proposed Work

2.1 Wireless Mesh Technology

Wireless Mesh Networks mainly consist of multiple clients, the server and the gateway. Clients are the various sensor modules that intercommunicate with each other in a network. The server transfers the data packets from one network to another whereas Gateway is an electronic physical device that bridges the client network to the Internet [9]. The main advantage of the deployed WMN based on painless Mesh [13] is that it is easy to add or remove nodes without re-installing the system completely. WMN has plenty of applications which would enable us to monitor, notify and control systems in various fields like home appliances, defense, medicine, agriculture, etc. [12].

In the proposed work, we have used three sensor nodes for home security, ambiance monitoring, kitchen safety that are connected in a mesh topology, which utilizes I2C for modularity. Each node in the system works on master-slave configuration where sensors act as slave and NodeMCU act as the master. Each sensor has its own slave address which gets identified by NodeMCU. Through this process, NodeMCU can act accordingly based on the sensor to which it is connected. The collective data from the sensor nodes are sent to the gateway via the server which in turn transmits the data to Adafruit cloud. One can view the feeds and GUI by logging into the Adafruit cloud.

2.2 I2C Based Modularity

I2C is a multi-slave and multi-master, packet switched, single-ended serial computer bus. It is employed for connecting external peripherals working at low speed to computers, embedded systems, and other hardware. The I2C communication was basically formulated to facilitate both equipment manufacturers and system designers to increase the efficiency of hardware and to minimize the complexity of the circuit [4]. All the IC's that has I2C interface can directly communicate with each other through a basic two wired bus communication as these devices are incorporated with an on-chip interface. As I2C supports master-slave communication, the I2C integrated module that begins the data transfer is considered as master bus and the rest of the nodes are considered to be slave bus. All of these slave nodes have a unique 7-bit address corresponding to it. The availability of address space restricts the number of modules

that can be connected to the I2C interface. The transfer of information between the two lines SDA and SCL are segregated into eight bits along with the redundant bit. These redundant bits are used to notify the starting and end of the data packets.

One of the most remarkable advantages of using I2C is that the communication between modular boards can be easily implemented using the two-wire connection whereby reducing messy connections. The major reason to opt for an I2C communication protocol in this smart home automation paper is that it requires a comparatively limited number of data lines to connect many sensors together and offers modularity through address identification.

3 Output – Data Collection

3.1 Security Module

One of the nodes in our home monitoring system is a home security module, as shown in Fig. 1, which mainly comprises of a fingerprint sensor. This helps in securing one's source of the appliance with biometrics which facilitates storing fingerprint, detection, and verification [6, 10]. It performs image proffering, calculation, feature verifying, and searching. In addition, one can also enroll new fingerprints to be stored.

Thus, the main objective of the security module is to enroll fingerprints mapped to a specific ID and storing it onto the sensor's ROM and Validate as required.

Hardware Required and Features

The Fingerprint sensor module R307 is used in this proposed work. It processes imaging in <1 s and can store 172 fingerprints on its local memory.

Working

Fingerprint enrolling:

- (1) Prior to deploying the security node; the fingerprints of the authentic personnel are stored onto the ROM of the Fingerprint sensor.
- (2) This data is then validated during the deployment of the sensor into the mesh.

Fingerprint validation:

- (1) The node as stated on powering monitors its I2C and UART ports for the presence of any valid sensors.
- (2) If the Fingerprint sensor is present, the node is set into the “SECURITY” mode.
- (3) The UART pins of Node are connected to the Rx, Tx pins of the Fingerprint sensor and the outputs are stored in local variables.

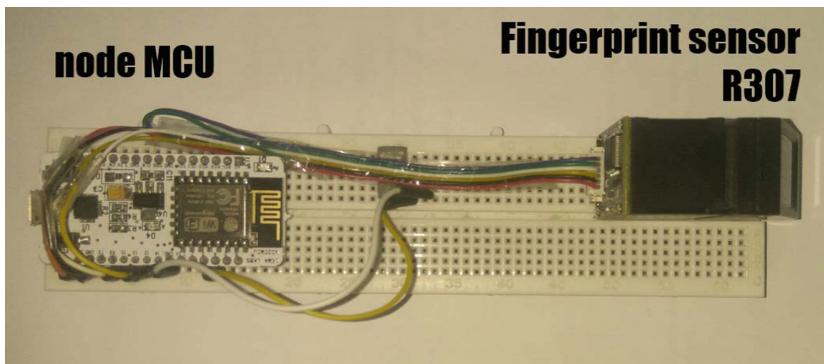


Fig. 1. The security module

3.2 Ambiance Module

This sensor node, as shown in Fig. 2, uses an Adafruit CCS811 sensor to monitor indoor air quality. When the sensor is connected using I2C to a NodeMCU which is incorporated with suitable code, it would produce an output of Total Volatile Organic Compounds (TVOC) [7] and carbon dioxide (CO_2) level in the air.

Thus, the main objective of ambiance module is to measure the quantity of TVOC concentration (in milligrams per meter cube) and CO_2 Concentration (in ppm).

Hardware Required and Features

Adafruit CCS811 air quality sensor is an ultra-low power module with onboard ADC converter and a microcontroller to provision I2C communication.

Measuring ranges of CO_2 is 400 to 8192 parts per million (ppm), and TVOC is 0 to 1187 parts per billion (ppb).

Working

- (1) The node as stated on powering monitors its I2C and UART ports for the presence of any valid sensors.
- (2) If the CCS811 sensor with I2C address of 0X5B (Hexadecimal number) is present, the node is set into the “AMBIANCE” mode.
- (3) The SDA, SCL pins of Node is connected to the SDA, SCL pins of the CCS811 sensor; and the outputs are stored in local variables.

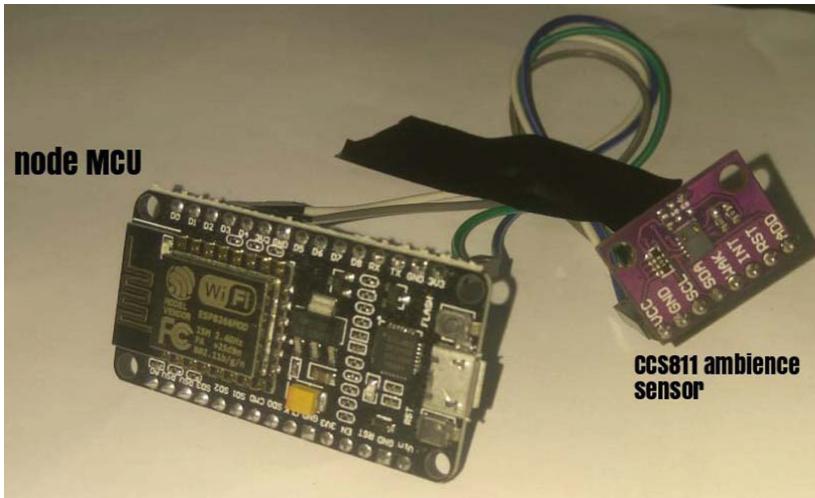


Fig. 2. The ambiance module

3.3 Kitchen Safety Module

In case when there is a gas leakage, extensive temperature or a burst of fire, it should be notified and addressed as soon as possible [12]. This node, as shown in Fig. 3, utilizes two sensors which would provide an output with information on temperature, pressure, humidity, and methane gas levels.

Thus, the major objective of kitchen safety module deals with measuring temperature (in Celsius), pressure (in millibars) and humidity (% relative humidity) and Methane (CH_4) concentration (in ppm).

Hardware Required and Features

- (1) Adafruit BME 280 temperature, pressure, humidity sensor.
- (2) MQ 5 methane gas sensor.

BME 280 sensor measures temperature, pressure, and humidity. It is suitable for all sorts of environmental detection. This sensor module is also interfaced with I2C which again supports the modularity concept of our home monitoring system. The measuring ranges for humidity are within $\pm 3\%$ accuracy, barometric pressure is within $\pm 1 \text{ hPa}$ accuracy and temperature is with $\pm 1.0 \text{ }^{\circ}\text{C}$ accuracy.

MQ 5 is a gas sensor for evaluating the quality of air and detects the presence of methane. It can also measure any kind of smoke, CO_2 , NH_3 , etc., One can use digital or analog pins as this sensor comes with both pin types. It has a broad detecting scope, fast response time, with extreme sensitivity which is vital for the working of the module.

Pre-setup

The Methane gas sensor, MQ5 is powered in room conditions and its values are noted. Based on this value, it is calibrated to scale the outputs measured henceforth. These equations and values are stored onto all the Nodes for calculations.

Working

- (1) The node as stated on powering monitors its I2C and UART ports for the presence of any valid sensors.
- (2) If the BME280 sensor – Temperature, Pressure, and Humidity sensor, with I2C address of 0X76 (Hexadecimal number), is present the node is set into the “KITCHEN” mode; the digital pin D5 is set in input mode for receiving data from the MQ-5 methane sensor.
- (3) The SDA, SCL pins of Node is connected to the SDA, SCL pins of the BME 280 sensor; and the outputs are stored in local variables.
- (4) The output from the D5 pin of Node is converted to ppm value of CH₄ and stored in a local variable.

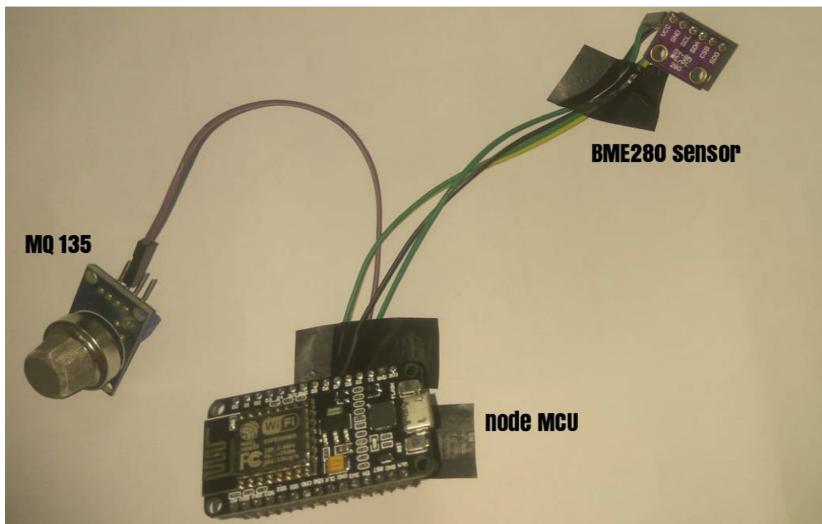


Fig. 3. The kitchen safety module

4 Output – Data Transmission

4.1 Across the Nodes

- (1) At every instance of powering up a node, the node broadcasts its Unique ID to its specific mesh ID along with the mesh password for authentication.
- (2) If the mesh is available; the connection is set up and the mesh sends periodic updates for stabilization.

- (3) If the mesh is unavailable, the node goes into a standalone working mode; periodically checking for presence for any valid node/mesh's presence.
- (4) If the node is powered down; updates are transferred across the mesh to stop acknowledging the presence of the node with its Unique ID anymore.
- (5) All the outputs stored in the local variables are converted into a JSON object, and along with the node's Unique ID is sent to the Server through the Mesh.

4.2 Server

Objective

Gathers JSON object from the nodes in the mesh either directly or indirectly. On receiving JSON object from the mesh, forwards it to the Gateway through physical UART, as shown in Fig. 4, for cloud-based monitoring [5].

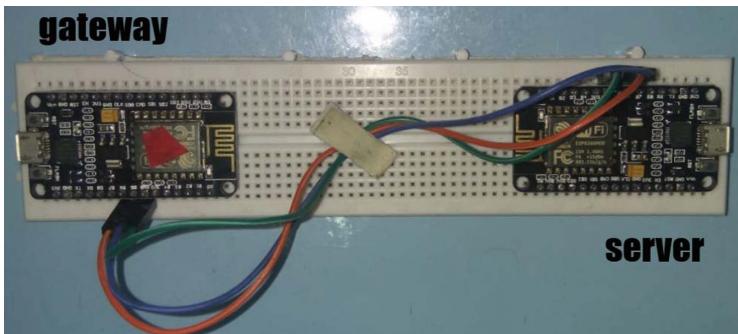


Fig. 4. The gateway and the server

Working

- (1) At every instance of powering up the Server, the Server broadcasts its Unique ID to its specific mesh ID along with the mesh password for authentication.
- (2) If the mesh is available; the connection is set up and the mesh sends periodic updates for stabilization.
- (3) If the mesh is unavailable, the server goes into a standalone working mode; periodically checking for presence for any valid node/mesh's presence.
- (4) If the server is powered down; updates are transferred across the mesh, to stop acknowledging the presence of the server with its Unique ID.
- (5) All the outputs of the nodes during the down period of the server are dropped.
- (6) Once the mesh stabilizes, the nodes send the data to the server either directly or indirectly (i.e., by making other nodes in its route to the server as repeaters) [1].
- (7) At every instance of receiving a valid JSON object from the mesh; the server forwards the JSON object through its physical UART to the Gateway.

4.3 Gateway

Objective

Acquire JSON objects periodically, as it arrives from the Server through physical UART, analyze and classify the data to identify the feed to transmit the values onto the Adafruit IO cloud platform, and transmit them by using MQTT protocol on WiFi communication [11].

Working

- (1) On powering up the gateway, as shown in Fig. 4, it scans for the specified Wi-Fi access point; and if available, it uses the credentials to access the Internet/cloud henceforth through that access point.
- (2) On acquiring the data packet from the server, the gateway analyzes the packet to understand which feed of data the values must be put on to.
- (3) The JSON object is broken into specific data sets and sent to specific feeds respectively; for data interpretation and user notification.
- (4) Data logging on cloud and notification:

It is possible to find out any potential problems in one or more nodes from the data that are fed into the server. In such a case, it doesn't affect the other nodes that make up the mesh and the system continues to perform its task. Even though the data from the faulty node doesn't reach the server and therefore is not fed into the monitoring process, the other nodes continue to feed the server with data; thus making up for a failure-proof monitoring system.

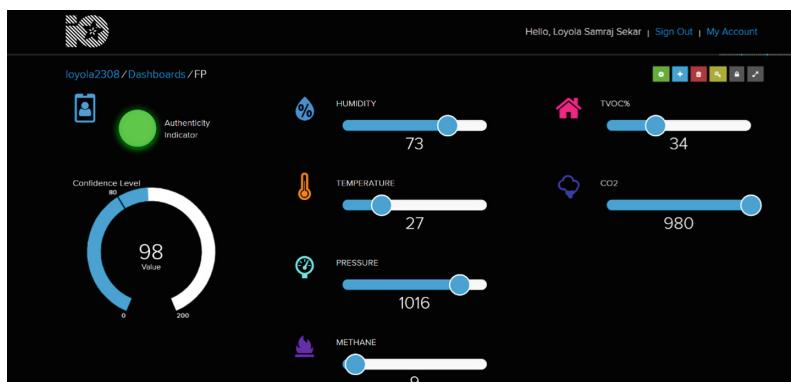


Fig. 5. Fully functional cloud service with value meters.

The data upon receiving at the gateway is processed and sent to the online cloud service based on MQTT protocol. Adafruit IO is the free cloud service that we make use of, which displays the real-time data in different formats on the dashboard [15]. As shown in Fig. 5, it creates an easy way to display and utilize the data feed sent to it. This data can be accessed through various forms of online platforms.

The proposed work uses IFTTT, which is a service that lets the user create miniature applets. IFTTT has Adafruit included as one of the online services that allow creating various different applets. The sensor value stream from Adafruit is patched to IFTTT in the applet and a threshold depending on the type of Sensor data and to the needs of the user is set. Based on the conditions, various methods of notification can be implemented.

As shown in Fig. 6, we notify the user through a push notification [10, 11] from the app or send a text message with detailed and precise information about what exactly happened with respect to the sensor values and set condition.

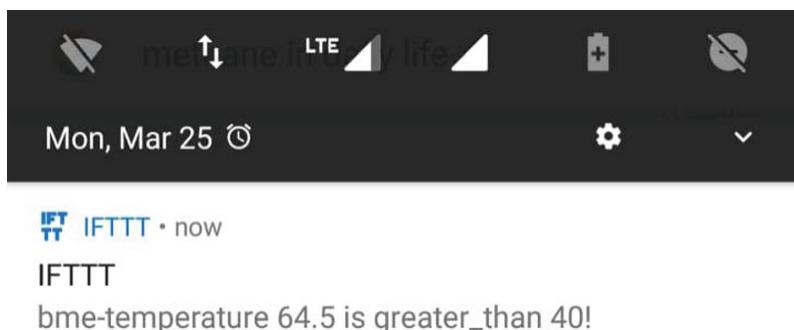


Fig. 6. Notification received by the user.

5 Conclusion

Thus a wireless smart home monitoring system comprising three modules namely Security, Ambient intelligence, and smart kitchen is built and implemented in an 802.11 mesh network, that would notify the user with the collected information. The implementation of modularity has made the system more flexible in order to help the user to add or remove any of the nodes in real-time. Using lightweight protocols and data structures like MQTT and JSON increases the performance and feasibility of the communication between the gateway and the Internet, and makes the entire system future-ready.

The future scope of this monitoring system is automation and FPGA design production for a standalone product. It can be developed into a Home Automation module where human interference is very minimal to make it possible by creating automation methods on all the devices. We can set thresholds for the sensor values and when the specified condition is met, we can automatically redirect the signal to an automated control system where it can automatically bring back any device to a desired functioning state.

References

1. Muhendra, R., Rinaldi, A., Budiman, M., Khairurrijal: Development of WiFi mesh infrastructure for internet of things applications. *Procedia Eng.* **170**, 332–337 (2017)
2. Noguchi, T.S.M.: Development of network management system in wireless home network. In: The 1st IEEE Global Conference on Consumer Electronics, pp. 737–740 (2012)
3. Manikasndan, J.: Design and evaluation of wireless home automation systems, Delhi (2016)
4. Thalmann, X.R.D.: Proposition of a modular I2C-based wearable architecture, Melecon, pp. 802–805 (2010)
5. Soratkal, R.K.K.S.: MQTT based home automation system using ESP8266 (2016)
6. Lu, S.Z.X.: Fingerprint identification and its applications in information security fields, Xi'an (2010)
7. Lasomsri, P., Yanbuaban, P., Ouypornkochagorn, O.K.T.: A development of low-cost devices for monitoring indoor air quality in a large-scale hospital, Thailand (2018)
8. Cheng, Y.Z.X.: Design of smart home remote monitoring system based on embedded system, Wuhan (2011)
9. Wang, W., Xia, W., Zhang, R., Shen, L.: Design and implementation of gateway and server in an indoor high-precision positioning system, Tokyo (2014)
10. Brundha, S.M., Santhanalakshmi, P.L.S.: Home automation in client-server approach with user notification along with efficient security alerting system, Bangalore (2017)
11. Dickey, N., Banks, D., Sukittanon, S.: Home automation using cloud network and mobile devices. In: 2012 Proceedings of IEEE SoutheastCon, Orlando, pp. 1–4 (2012)
12. Pavithra, D., Balakrishnan, R.: IoT based monitoring and control system for home automation. In: 2015 Global Conference on Communication Technologies (GCCT), Thuckalay, pp. 169–173 (2015)
13. GitLab repository for painlessMesh. <https://gitlab.com/painlessMesh>
14. Paleri, P.L., Ramesh, S.R.: Early stage FPGA architecture development by exploiting dependence on logic density. *Int. J. Appl. Eng. Res.* **10**(11), 28889–28902 (2015)
15. Varman, S.A.M., Baskaran, A.R., Aravindh, S., Prabhu, E.: Deep learning and IoT for smart agriculture using WSN. In: IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, pp. 1–6 (2017)



A Comprehensive Analysis of the Most Common Hard Clustering Algorithms

Aditya Vardhan^(✉), Priyanshu Sarmah, and Arunav Das

Odisha, India

{1605335, 1730106, 1605182}@kiit.ac.in

Abstract. From past decades, Clustering is the process of observation that set assignment into subsets called clusters. It is an unsupervised method and can be grouped as hard and soft clustering. Hard clustering methods assign the sample point to a specific cluster whereas soft clustering methods give a probability of assignment to all clusters. In this paper, we have tried to give intuition to some of the popular hard clustering methods with their associated algorithms.

Keywords: Unsupervised machine learning · K-means clustering algorithm · DBSCAN · Mean Shift Algorithm · Hierarchical Clustering · Cluster dissimilarities

1 Introduction

This paper gives a summarized intuition into the popular clustering methods and their algorithms. The primary aim is to facilitate the learning process of clustering algorithms and provide an overall review of the same. A number of clustering methods are discussed along with their algorithms, optimizations, applications and efficiency of some algorithms concerning the others. Hard clustering methods assign the sample point to a specific cluster whereas the soft clustering methods give a probability of assignment to all clusters.

2 K-Means Clustering

From [1], the first step of this fundamental and straightforward method of K-Means Clustering is to select k random points from the whole dataset. These points are the representation of the initial centroids. The centroid which is closest to each of the points in the dataset is assigned to it. The next step is the recalculation of the coordinates of the centroids. All points are averaged and then assigned to the respective cluster, the new points are the new coordinates of the specific centroid. This iteration process continues until an optimum cost function converges without the surety that it is the global one. Hence, it is a crucial step to select the initial centroids during the initialization process to fetch the best possible set of centroids. When using large datasets, the cluster analyses using K-means is heavily dependent centroid initialization methods which are adapted by the distributed datasets across several machines.

From [3], K-Means can be written as follows:

```

Input:
-K (number of clusters)
-Training set {x(1), x(2), ..., x(m)}
Initialize K cluster centroids randomly as  $\mu_1, \mu_2, \dots, \mu_K \in \mathbb{R}^n$ 
Repeat {
    for i=1 to m
        c(i) = index (from 1 to K) of the closest cluster centroid to x(i).
        (Cluster Assignment step)
    for k=1 to K
         $\mu_k$  = average (mean) of the points assigned to cluster k. (Move Centroid step)
}

```

The function J , known as the cost function or the distortion function is that value that the algorithm strives to minimize. It consists of the parameters $c^{(1)}$ through $c^{(m)}$ and μ_1 through μ_K that is being varied as the algorithm runs.

The K-Means Optimization objective is given by:

$$\begin{aligned}
J(c(1), \dots, c(m), \mu_1, \dots, \mu_K) &= 1/m \\
\text{Min } J\left(c^{(1)}, \dots, c^{(m)}, \mu_1, \dots, \mu_K\right) \\
c^{(1)}, \dots, c^{(m)} \\
\mu_1, \dots, \mu_K
\end{aligned}$$

The cluster assignment step requires us to minimize J with respect to the variables $c^{(1)}, c^{(2)}$ and so on, up to $c^{(m)}$ and simultaneously hold to the closest fixed centroids, μ_1 up to μ_K . So, the first assignment selects the exact values of $c^{(1)}, c^{(2)}$ up to $c^{(m)}$, while minimizing the cost function J .

The second step, known as the move centroid step, requires us to choose the values of μ that minimizes J with respect to the location of the cluster centroids μ_1 through μ_K continuing with further iterations. The partition of the two sets of variables into two halves first minimizes J with respect to C and then J with respect to the variables μ and the iteration proceeds further.

Random Initialization is the step of introduction of the cluster centroids at random locations When K-Means is being executed, it is advisable to have k number of cluster centroids which is to be set less than the number of training examples M .

Let us take an example (Fig. 1).

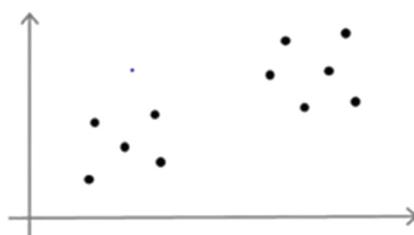


Fig. 1. A random dataset [Source: Andrew Ng (Coursera)]

We can randomly choose K training examples and equate μ_1 , up to μ_K to these K examples.

We choose a pair of examples and set the cluster centroids on top of those examples as shown below (Fig. 2).

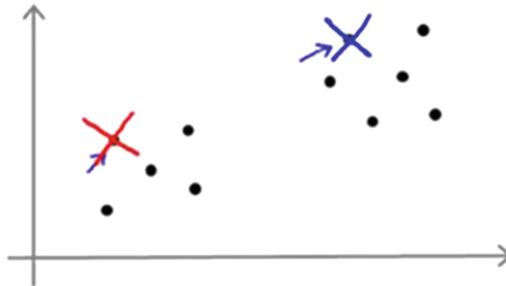


Fig. 2. A case of Random Initialization. [Source: Andrew Ng (Coursera)]

So, during initialization, the cluster centroid μ_1 that comes up first will be equal to $x(i)$ for some random value i , μ_2 equates to $x(j)$ for some random value of j and so on if there are several clusters and cluster centroids.

As suggested, there is a high possibility that we might end up converging to different solutions which depend on cluster initial initialization. Random initialization can let K-Means reach different solutions. And, particularly, K-Means can potentially end up reaching the local optima. The local optima refer to the one belonging to the cost function J .

If we are given a dataset as shown in Fig. 3,

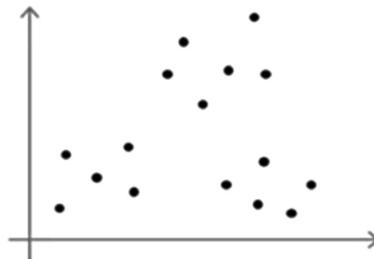


Fig. 3. Dataset [Source: Andrew Ng (Coursera)]

We might obtain the following clusters if K-Means ends up at a favourable local optimum (Fig. 4).

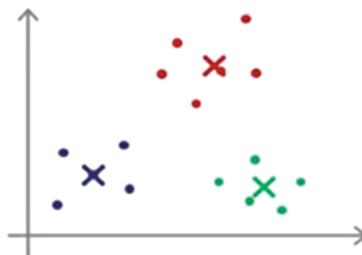


Fig. 4. A favourable condition of Random initialization. [Source: Andrew Ng (Coursera)]

But, an unfortunate random initialization, will lead to K-Means getting stuck at another local optima.

So, both of these examples correspond to different local optima of K-Means which forms unsuitable and inefficient clusters. When k means get stuck at local minima and is not able to minimize distortion function J efficiently, we increase the odds k value finding and hence finding the best possible clustering which can be achieved by multiple random initializations. We pick the random initialization that gives us the lowest distortion. Another crucial step of the K-Means Algorithm is choosing the number of clusters. We cannot describe a single best way to decide how many clusters we need or in fact automate it. The most common way it is done is still choosing it manually. One of the common methods to choose the number of clusters is the Elbow Method which has its advantages and shortcomings. K-Means is run for a different number of clusters and the cost function J is plotted. We end up with a curve showing how the distortion varies with a number of clusters as shown in the diagram below (Fig. 5).

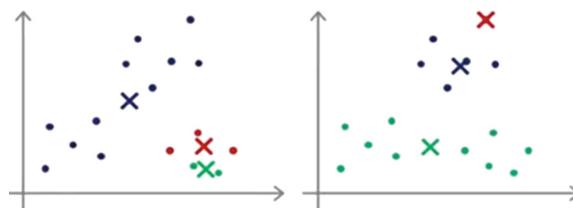


Fig. 5. The variability of Distortion Function with several clusters [Source: Andrew Ng (Coursera)]

We pick the elbow point where the distortion slows down after a rapid decrease. Here, in this case, the distortion goes down rapidly until K equals 3 and then there is a steady decrease. This is one of the reasonable methods for selecting the number of clusters. A disadvantage of this Elbow Method is that often we end up with a curve that looks ambiguous which does not show a clear cut elbow and instead distortion continuously decreases. There is no ready location where the Elbow lies. So, the Elbow method is not necessarily the best method for identifying the number of clusters.

Hence, the best way to choose the number of clusters is still by human insights. The number of clusters to be chosen depends on the later purpose that K-Means is run for.

The shortcomings of the K-Means Algorithm:

From [4] we infer,

- The distance calculation from data objects to the cluster center and then finding the smallest cluster distance, over several iterations it takes up longer execution time, thereby decreasing the efficiency the algorithm
- The efficiency of K-Means in the case of data is minimal.
- The final result is deeply impacted by the initial seeds.
- Sensitive to scaling: Rescaling the dataset (Normalization and Standardization) completely changes the results.

3 DBSCAN (Density-Based Spatial Clustering of Applications with Noise) Clustering

Noise based Density-Based Spatial Clustering is one of the most used density-based clustering algorithms. From [5], the central idea that DBSCAN is based on is to find regions of low density and high density, where high-density regions are separated from low-density regions. DBSCAN can discover clusters of arbitrary shape and distinguish noise. With the use of spatial access methods, it can efficiently cluster large spatial databases like GMeans.

To understand DBSCAN, we need to refer to a few related definitions. From [6], the detailed introduction of DBSCAN Algorithm is as follows:

'Eps - neighborhood of a point': It is the circular zone with p as Eps and centre as the radius. The points included in the set of the Eps-Neighborhood is denoted by $NEps(p) = \{q \in D \mid dist(p, q) \leq Eps\}$.

'Density of a point': The number of points within Eps-Neighborhood of a point p, where p is contained in the Dataset D.

'Core Point': The point where the density is greater than or equal to MinPts where MinPts is the threshold as the user specifies.

'Noise Point': Noise Point are those points which are neither core point nor border point.

'Directly Density-Reachable': Let us assume point q to be core point. A point 'p' is termed as directly density-reachable from a point q if point p belongs to the Eps-neighborhood of point q, as denoted by $p \in NEps(q)$, $|NEps(q)| \geq MinPts$.

'Density Reachable': Consider the point q, if there is a chain of points $q_1, q_2 \dots q_n$, $q_1 = v$, $q_n = q$, $p_i \in D$, $1 \leq i \leq n$, then p is density reachable from q, such that p_{i+1} is directly density-reachable from p_i .

'Density-Connected': For the given Eps, point p is referred as 'density-connected to point MinPts and q' if there exists a point O such that for the given Eps and MinPts, both of these points q and p are density-reachable from O.

The central theme of DBSCAN Algorithm follows a few general steps. It primarily begins with the cluster discovering step by finding a point p from the dataset D and

checking it. P is a core point if the number of points in the Eps-Neighborhood of a point p is larger than or equal to MinPts, Eps-Neighborhood points of p is sequentially checked as the seed points during the following process. Specifically, query the seed points continuously, put points in Eps-Neighborhood into seed set if current seed point is also a core point. In this manner, continuous extension of the class current data point takes place until a full class has been located, finally, the cluster relative to Eps and MinPts is determined. If p is a border point, the number of points in Eps-Neighborhood of a point p is less than MinPts, hence the algorithm would choose the next point of the dataset D to check. The remainder of the points which are not split into any clusters would be labelled as noise points.

The sequential execution of region query and determination acquire the points present in Eps-Neighborhood of a point p.

From [7], the pseudo-code of the DBSCAN algorithm can be written as:

“Input: Radius Eps, Data object D, Density threshold MinPts Output Clustered C

1. Data file analysis sample;
2. Computation of Euclidean distance between each point and all the subsequent other points;
3. K-distance values calculation and the k-distance set of all the points ascending order sorted along with the k-distance values sorting;
4. Scatter plots show the K-distance variation and Excel sheets are used to display them;
5. The radius value Eps is determined in accordance with the scatter plot;
6. Given, MinPts = 4 and Eps radius value, computation of the entire core points is done and the core points are mapped lesser between than the established radius Eps;
7. Calculation of all core points and Eps radius is done in accordance with the set and then the outliers are acquired;
8. Core points are connected and a cluster is formed with the distance from the radius Eps to the point larger than the core points;
9. Different radius Eps are selected, DBSCAN clustering algorithms are used to obtain a group of clusters and the clustering results are estimated with their outliers and scatter graph;”

The DBSCAN Algorithm comes with a few setbacks. These are as follows:

- DBSCAN has a high time complexity of $O(n^2)$.
- All the data should be kept in the memory which requires large memory and large I/O consumption.
- It is required for us to know the suitable parameters MinPts and Eps of each cluster and a minimum of one point from the cluster concerned. If the above parameters are fulfilled, only then all density-reachable from a given point can be retrieved. But, there lies no effortless method to get this information beforehand for each of the clusters in the database.

4 Mean Shift Clustering

Originally presented in 1975 by Fukunaga and Hostetler, the Mean Shift Algorithm can define clusters by assuming that all the data points are the sample of probability density functions and through these clusters can be defined. This is a method of finding the maxima or modes of a density function whose discrete data samples of the function are given.

Basic Mean Shift: Naïve estimator, kernel estimator, histograms are some of the non-parametric methods used to determine the density estimation. Due to its advantages over the other two, Kernel estimator is used mostly. Kernel estimator is given by the formula:

$$\hat{f}(x) = \frac{1}{nh^d} \sum_{i=1}^n K\left(\frac{x - x_i}{h}\right)$$

Where a given set x_i $i = 1..n$ points in the dimensional space R^d , $K(x)$ is the kernel with window radius (also known as bandwidth) h computed for point x .

Mean shift is based on the density contour of the Gradient ascent. The gradient ascent can be generically formulated as,

$$x_1 = x_0 + \eta f'(x_0)$$

On application to the Kernel Density estimator,

$$\hat{f}(x) = \frac{1}{nh^d} \sum_{i=1}^n K\left(\frac{x - x_i}{h}\right)$$

$$\nabla \hat{f}(x) = \frac{1}{nh^d} \sum_{i=1}^n K'\left(\frac{x - x_i}{h}\right)$$

Equating to 0 we get,

$$\sum_{i=1}^n K'\left(\frac{x - x_i}{h}\right) \vec{x} = \sum_{i=1}^n K'\left(\frac{x - x_i}{h}\right) \vec{x}_i$$

Finally,

$$\vec{x} = \frac{\sum_{i=1}^n K'\left(\frac{x - x_i}{h}\right) \vec{x}_i}{\sum_{i=1}^n K'\left(\frac{x - x_i}{h}\right)}$$

In mean shift, the feature space points are treated as a probability density function. Dense regions in the feature space defines the local maxima or modes. So we perform gradient ascent on the local estimated density for each data point until convergence. Density function modes are represented through gradient ascent. The same cluster includes all points associated with the same stationary point.

Assuming $g(x) = -K'(x)$, we have

$$m(x) = \frac{\sum_{i=1}^n g\left(\frac{x-x_i}{h}\right)x_i}{\sum_{i=1}^n g\left(\frac{x-x_i}{h}\right)} - x$$

$m(x)$ is termed as the mean shift. So the summary of the mean shift procedure is as following:

- ‘For all of the points x_i
- “1. Compute mean shift vector $m(x_i^t)$ ”
- “2. Shift the density estimated window by $m(x_i^t)$ ”
- 3. Repeat until it is converged.’

Application: The mean shift algorithm has been extensively used and studied in the area of image processing. The success of this algorithm in one area encourages its use in another area. As mentioned before, processing biological data is challenging due to its size. It would be interesting to use the mean shift algorithm on large biological data. A very recent work by Barash and Comaniciu showed that the mean shift algorithm can be used for the analysis of biological data. An algorithm based on quantum mechanics, called quantum clustering, was developed by Horn and Gottlieb and was applied on a data derived from microarray experiment by Horn and Axel. Barash and Comaniciu showed that the mean shift algorithm highly resembles the quantum clustering. They also mentioned that since quantum clustering has been successfully applied to microarray data even mean shift algorithm can be used on biological data. Inspired by the robustness of the mean shift algorithm and its potential for efficient performance on large biological data, the generalised mean shift algorithm by Cheng has been applied to a 0–1 matrix representing biological data and the results are studied. In the next chapter, some background in biology will be given to understand what data the 0–1 matrix hold.

5 Hierarchical Clustering

Hierarchical clustering is the method of building and analysis of clusters by building a hierarchy tree. [9] Data is grouped with a sequence of partition whereas partition clustering divides the data in a prescribed no of clusters without any levered structure. [9] It is specifically very useful for implementation in datasets when real hierarchical or levered relations exists in the dataset, example, organism evolutionary data, the article will focus on Agglomerative Hierarchical clustering which Is a widely used Clustering Algorithm, [8] splits and merges are decided in a greedy manner and the outcomes of the same are represented via Dendrogram. Agglomerative follows a “bottom-up” approach. Opposite to this is the Divisive Clustering, following a “top-down” approach.

The complexity of Agglomerative Clustering is $O(n^3)$ while it requires a memory of order $O(n^2)$ leading to slower process time, and also making it costly for even small datasets. [8] The complexity of divisive clustering is even worse being $O(2^n)$.

Divisive clustering is therefore rarely used in specific datasets, requiring specific need for the same. [9] Divisive Clustering further can be implemented through DIANA and MONA algorithms.

The general agglomerative clustering algorithm can be described as

- (1) Start with n -points.
- (2) Calculate the proximity matrix for the points.
- (3) Search the minimum distance.
- (4) Form a cluster of the closest proximity point.
- (5) Update the proximity matrix with respect to the new cluster.
- (6) Repeat Steps 2–3 until a single cluster is achieved once a single cluster is obtained it is further modifies according to need (i.e. slicing the dendrogram), for example identifying categories.

6 Cluster Dissimilarities

The algorithm and methods that are used to build up clusters, determine the efficiency and reliability of the Clustering model.

The clusters are made via a proximity matrix (distance matrix). The hierarchical relations are then depicted using a dendrogram. A measure of dissimilarity is required in order to decide the shape of the clusters and where they should be split. This is achieved by the use of metrics and a linkage criterion. Hence two of the aspects of the clustering process that influence the shape and the identity of the clusters are

1. Metric

It is the measure of the distance between the individual points or between the clusters. The distance between clusters can be the distance between the closest or the farthest points of the clusters, the distance between the centroid of the cluster or simply the average distance between each pair of points. The metric system used provides a definite shape to the cluster and divisibility to the dataset.

[8] Some of the commonly used metrics for hierarchical clustering are

- “Euclidean distance”
- “Squared Euclidean distance”
- “Manhattan distance”
- “Maximum distance”
- “Mahalanobis distance”

Formula

$$\|a - b\|_2 = \sqrt{\sum_i (a_i - b_i)^2}$$

$$\|a - b\|_2^2 = \sum_i (a_i - b_i)^2$$

$$\|a - b\|_1 = \sum_i |a_i - b_i|$$

$$\|a - b\|_\infty = \max_i |a_i - b_i|$$

$$\sqrt{(a - b)^\top S^{-1}(a - b)} \text{ where } S \text{ is the Covariance matrix}$$

2. Linkage Criterion

The distance between the sets of points or between the clusters using the metric is determined by the Linkage Criterion.

The prominent methods are

“Maximum or Complete Linkage”

“Minimum or Single Linkage”

“Mean or Average Linkage”

“Centroid linkage or UPGMC”

“Minimum Energy Clustering”

Formula

$$\max\{d(a, b) : a \in A, b \in B\}.$$

$$\min\{d(a, b) : a \in A, b \in B\}.$$

$$\frac{1}{|A| \cdot |B|} \sum_{a \in A} \sum_{b \in B} d(a, b).$$

$$\|c_s - c_t\| \text{ where } c_s \text{ and } c_t \text{ are the centroids of clusters } s \text{ and } t, \text{ respectively.}$$

$$\frac{2}{nm} \sum_{i,j=1}^{n,m} \|a_i - b_j\|_2 - \frac{1}{n^2} \sum_{i,j=1}^n \|a_i - a_j\|_2 - \frac{1}{m^2} \sum_{i,j=1}^m \|b_i - b_j\|_2$$

Efficiency: K-means algorithm is linear with respect to the number of data points i.e. O(n), n being the number of data points. The time complexity is quadratic for most of the hierarchical clustering algorithms. i.e. $(n^2)O(n^2)$ [Clustering]. Therefore, for the same dataset, hierarchical clustering will take a quadratic amount of time compared to the K-means Algorithm. Hence it has a very target use.

7 Conclusion

On reviewing various hard clustering methods, we found that most of the clustering methods compute a criterion, which is used as a basis for cluster assignment. The criterion differs from algorithm to algorithm and gives various results in various sample sets. Algorithms were discussed for K-Means, DBSCAN, Mean Shift and Hierarchical Clustering methods. We found that K-Means uses k no of nearest point(s), Mean Shift implements a non-parametric method, preferably Kernel Estimator, DBSCAN uses a

spatial density method and Hierarchical Clustering uses a hierarchy tree for cluster assignment. Further, optimizations and efficiency of some algorithms were discussed. Finally, Metrics and Linkage criteria were discussed which give the method to find the distance between individual Clusters.

References

1. Esteves, R.M., Hacker, T., Rong, C.: Competitive K-Means, a new accurate and distributed K-Means algorithm for large datasets. In: 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, pp. 17–24 (2013). <https://doi.org/10.1109/cloudcom.2013.89>
2. Shi, N., Liu, X., Guan, Y.: Research on k-means clustering algorithm: an improved k-means clustering algorithm. In: 2010 Third International Symposium on Intelligent Information Technology and Security Informatics, Jinggangshan, pp. 63–67 (2010)
3. <https://www.coursera.org/learn/machine-learning>
4. Advantages & Disadvantages of k-Means and Hierarchical Clustering (Unsupervised Learning). Machine Learning for Language Technology ML4LT (2016). Marina San, Department of Linguistics and Philology, Uppsala University
5. Smiti, A., Elouedi, Z.: Dynamic DBSCAN-GM clustering algorithm. In: 2015 16th IEEE International Symposium on Computational Intelligence and Informatics (CINTI), pp. 311–316 (2015)
6. Bansal, K., Bansal, M.: Dynamic data clustering and visualization using FDClust algorithm. In: 2017 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–5 (2017)
7. Zhang, L., Deng, S., Li, S.: Analysis of power consumer behaviour based on the complementation of K-means and DBSCAN. In: 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, pp. 1–5 (2017). <https://doi.org/10.1109/ei2.2017.8245490>
8. Ghuman, S.S.: Clustering techniques - a review. Int. J. Comput. Sci. Mob. Comput. **5**, 524–530 (2016)
9. Xu, R., Wunsch II, D.: Survey of clustering algorithms (2005)
10. Wang, L., Li, M., Han, X., Zheng, K.: An improved density-based spatial clustering of application with noise. Int. J. Comput. Appl. (2018)
11. Yu, Y., Zhao, J., Wang, X., Wang, Q., Zhang, Y.: Cludoop: an efficient distributed density-based clustering for big data using hadoop. Int. J. Distrib. Sens. Netw. **11**, 579391 (2015)
12. Smiti, A., Elouedi, Z.: DBSCAN-GM: an improved clustering method based on Gaussian Means and DBSCAN techniques. In: 2012 IEEE 16th International Conference on Intelligent Engineering Systems (INES) (2012)
13. Jain, A.K., Narasimha Murty, M., Flynn, P.J.: Data clustering: a review. ACM Comput. Surv. (CSUR) **31**(3), 264–323 (1999)
14. Steinbach, M., Karypis, G., Kumar, V.: A comparison of document clustering techniques. In: KDD Workshop on Text Mining, vol. 400, no. 1 (2000)



Development and Validation of Engine Start/Stop Strategy for P2 Hybrid Electric Vehicle

MeghRaj V. Palwe^(✉) and Pramod Kanjalkar

Department of Instrumentation, Vishwakarma Institute of Technology,
Pune 411037, India
{meghraj.palwe17, pramod.kanjalkar}@vit.edu

Abstract. Today we live in an era where environmental awareness is increasing day by day, at the same time the gradual increase of gasoline prices is also a major issue [2]. Automobile industries are making efforts to address this problem and they are trying to find new methods to increase the mileage of vehicles and reduce environmental pollution caused by vehicles. Hybrid Electric Vehicles (HEV) are one of the ways by which this goal can be achieved. This paper proposes a Start/Stop strategy for a vehicle consisting of P2 hybrid electric powertrain. In the vehicle with P2 hybrid electric powertrain, the clutch is present in between the engine and motor/generator. S/S strategy automatically turn off the engine when the vehicle is at rest and eliminate idle emissions. When the driver presses the clutch to select the 1st gear, S/S strategy restarts the engine automatically. In this system when a vehicle stops at a particular place for more than 10 s the vehicle will stop automatically and it will start as soon as the clutch is pressed. This strategy can be implemented in normal vehicles by converting them into P2 hybrid electric powertrain by means of very minor modifications. We have used LSM Amesim software to develop the P2 vehicle model and MATLAB Simulink to implement the Start/Stop control strategy. From experimentation, it is found that the fuel economy has improved by 5%–6% with limitation of start/stop frequency of 2 stops/km [9].

Keywords: P2 hybrid electric powertrain · Hybrid Electric Vehicles · Start/Stop strategy

1 Introduction

Today, the world is in need of alternative fuel resources in order to replace the non-renewable energy sources such as petrol, diesel, CNG, LPG etc. Scientists are looking for alternative fuel resources such as solar power, bio diesel, electricity, hydrogen, methanol, and ethanol etc. A HEV is a vehicle that use an electric engine as well as conventional internal combustion engine [8]. HEV uses an electric generator as one propulsion system and an IC engine that uses diesel, gasoline or any type of alternative fuel as the second [2]. HEV'S are considered to have a decent performance and mileage as compared to that of conventional vehicle. So HEV'S can be a good alternative which can replace conventional vehicles and will contribute to reduce environmental pollution

as they provide us the flexibility to implement Start/Stop, E-assist, E-launch, regenerative braking etc.

2 P2 Hybrid Electric Vehicle

A battery pack is used to stock or provide extra energy. Which offers two advantages.

- No reduction in regenerative braking due to engine friction.
- With the support of transmission, the motor/generator can rotate at greater speed to recuperate more energy.

A P2 configuration must be able to maintain a decent drive quality because the clutch engage and disengage the engine during operation.

New methods are developed to meet the demands of fuel economy and emissions regulations imposed by government (Fig. 1).

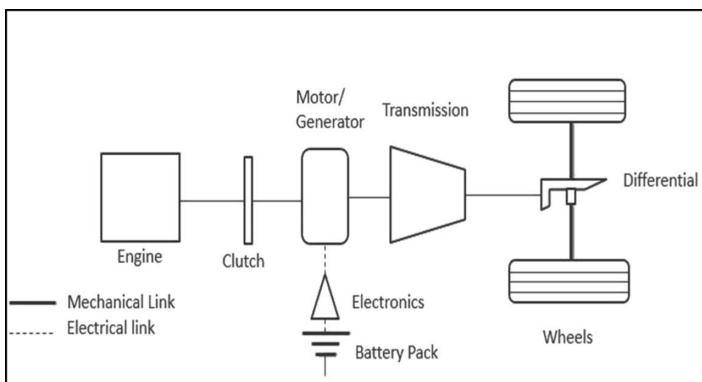


Fig. 1. P2 parallel hybrid electric vehicle.

These methods are as follows [6].

- Reduction of Weight
- Improvement of aerodynamic
- Reduction of rolling resistance
- Fuel cell hybrid systems
- Engine start stop systems
- Driveline and transmission efficiency Improvements

As compared to above methods the S/S can be easily implemented into a P2 type production vehicles and it can improve mileage of vehicle with minimum cost or effect on vehicle performance.

3 Proposed Start Stop Strategy

The idea of the S/S strategy is that it automatically turn off the engine when the vehicle is at rest and eliminate idle emissions. When the driver press the clutch to select the 1st gear, S/S strategy restarts the engine automatically to move the vehicle again. In this system when a vehicle stops at a particular place for more than 10 s the vehicle will stop automatically and it will start as soon as the clutch is pressed.

The following are the triggering conditions for Engine Start/Stop.

(A) Trigger conditions of engine start:

- Clutch pedal is pressed
- Vehicle is in gear
- Clutch pedal is released and accelerator pedal is pressed
- Vehicle velocity monitoring is ON (Fig. 2).

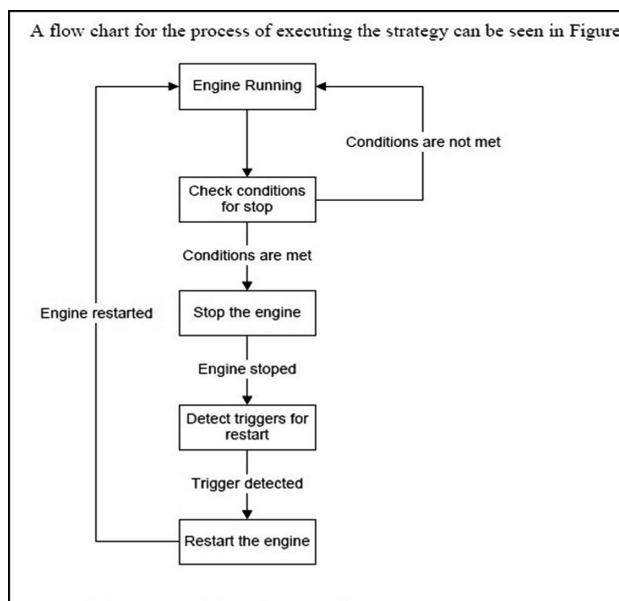


Fig. 2. Flow chart of start/stop strategy.

(B) Trigger for stopping the engine stop:

- Vehicle velocity is below the threshold value.
- Accelerator pedal position is pressed less than 5%.
- Vehicle is in stand still condition for more than 10 s.

If all the above conditions are met then vehicle will stop.

4 Overall System Requirement

The following parameters are considered and measured for implementation of Start/Stop strategy [5].

- **Clutch pedal position signal:** If the clutch pedal is pressed it is going to act as a trigger to start the engine.
- **Accelerator pedal position signal:** For implementation of S/S (Start/Stop) the accelerator pedal position should be monitored as it is going to be one of the triggers for engine stop as well as engine start condition. Here a 100% pressing of accelerator pedal will indicate that accelerator pedal is fully pressed and 0% pressing will indicate released position of accelerator pedal. A threshold value X will be given so that if the accelerator pedal is pressed below the threshold value the ECU (Engine control Unit) will get the signal to stop the engine and if the accelerator pedal is pressed above threshold value then it will trigger vehicle start signal to ECU.
- **Brake pedal Position Signal:** If S/S is performed at a traffic signal, where applying the brake is trigger for engine stop, the release of the parking brake would be a simple and obvious indication of that the driver intends to take off.
- **Gear position Indicator:** Signal the position of the gear is necessary so as the ECU will know that the vehicle is in gear. It will be analogue switch which will give 0 output when the vehicle is in neutral and 1 output when vehicle is in gear.
- **Vehicle speed indicator signal:** The speed of the vehicle should be monitored as it going to be as one of the triggering signal for vehicle stop condition.
- **Battery SOC (State of Charge) indicator:** The battery SOC must be above the given threshold value for working for S/S strategy and battery should be able to provide sufficient electrical power to both start the engine with the generator and accelerate the vehicle with the propulsion motor so continuous monitoring is necessary (Fig. 3).

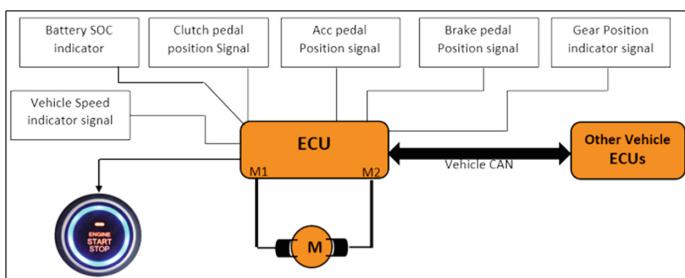


Fig. 3. System interface

For working of Start/Stop strategy the battery SOC should always be above the threshold value (Tables 1 and 2).

Table 1. Input signals to controller

Sr. no.	Inputs	Type of sensor-signal	Signal type	Range
1	Clutch pedal position	Analogue switch	Binary voltage	0/1
2	Acc pedal position	Analogue potentiometer	Voltage	0–5
3	Gear number	Analogue switch	Binary voltage	0/1
4	Vehicle speed	Digital from ECU	Digital	
5	Battery SOC signal	Digital from BMS	Digital	

Table 2. Output signal from controller

Sr. no.	Inputs	Type of sensor-signal	Signal type	Range
1	Engine start stop signal	Analogue	Binary voltage	0/1
2	Engine keep ON OFF signal	Analogue	Binary voltage	0/1

4.1 LSM Amesim

For this paper LSM Amesim is used to build the plant model of vehicle as LSM Amesim provides an easy to use interface. Different subsystems can be build inside the plant model and can be parameterized based on the requirement of project. Amesim used a set of given formula and code to simulate the entire plant model. For this project P2 configured parallel hybrid vehicle model was established with an objective to improve fuel economy as compared to baseline vehicles.

4.2 MATLAB Simulink

Although LSM Amesim helps a lot in developing the plant model for the entire vehicle. It does not provide the vast flexibility in designing a controller as Simulink does. A supervisory controller was developed in Simulink where logic of start stop strategy was developed.

5 Experimentation and Simulation Results

The model of P2 HEV was made in LSM Amesim and the control strategy was developed in MATLAB Simulink.

After carrying out the co-simulation between LSM Amesim and MATLAB Simulink following results are obtained. The driving cycle which was selected for obtaining the results of above control strategy was MIDC cycle. The duration of the cycle is 1180 s. After completion of simulation we found that the fuel economy was improved after implementation of start/stop strategy was around 7% (Figs. 4 and 5).

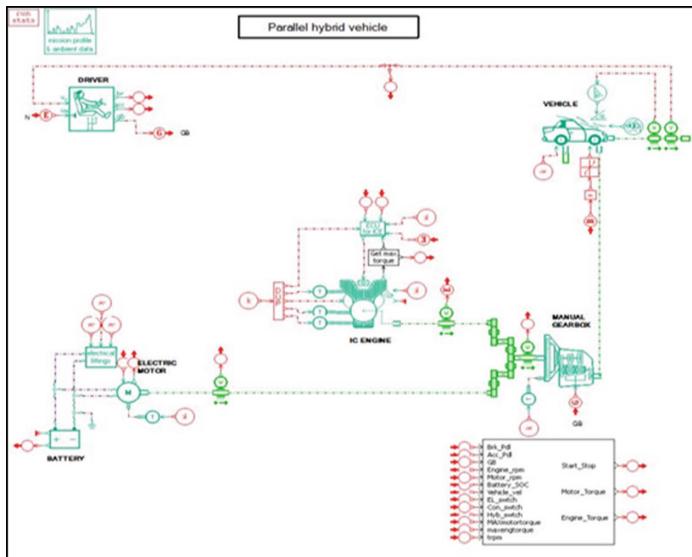


Fig. 4. Vehicle with start/stop strategy.

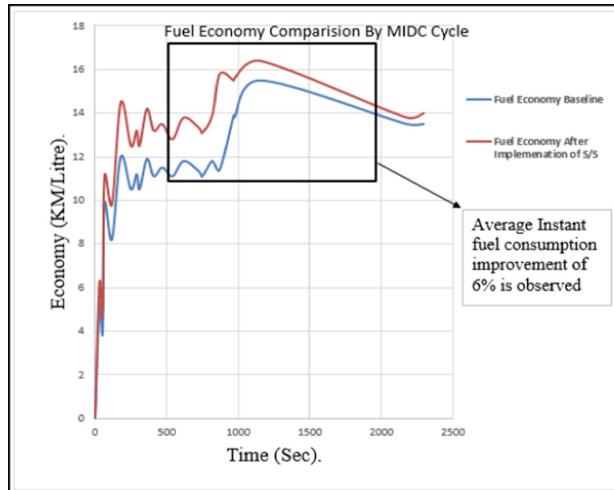


Fig. 5. Fuel economy comparison in MIDC cycle

The driving cycle which was selected for obtaining the results of above control strategy was MIDC (Modified Indian Driving Cycle) cycle. The duration of the cycle is 1180 s. After completion of simulation we found that the fuel economy was improved after implementation of start/stop strategy was around 6% (Fig. 6).

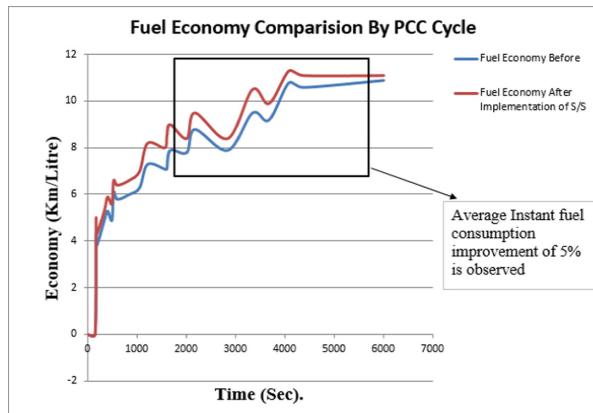


Fig. 6. Fuel economy comparison in PCC cycle

The second graph shows the results according to the PCC (Pune City Cycle). PCC was developed especially for Pune city. This cycle has a duration of 2150 s. After completion of the simulation we found that the fuel economy was improved by 5% (Table 3).

Table 3. Results

Sr. no.	Driving cycle	Operating mode	Fuel economy	% change in economy with Start/Stop
1	MIDC	Without S/S	15.2475	–
2	MIDC	With S/S ON	16.16235	6%
3	PCC	Without S/S	10.8125	–
4	PCC	With S/S ON	11.3531	5%

6 Conclusion

From the simulation results we conclude the following results.

- The P2 hybrid electric vehicle equipped with S/S control strategy automatically shut off the engine when all the necessary stop trigger conditions are met.
- Similarly the vehicle also starts when all the necessary stop trigger conditions are met.
- Similarly we also conclude from the graph obtained after simulation that the fuel consumption is reduced by 6% in MIDC cycle and 5% in PCC cycle.
- By the above mentioned results we can also conclude that there is considerable amount of reduction the emissions in the environment.

References

1. Wang, H., Qiao, Y., Yang, Y., Li, Z., Yuwen, Z.: Study on engine start-stop strategy for series-parallel hybrid vehicle. In: IEEE International Conference on Mechatronics and Automation, Beijing, 2–5 August 2015, pp. 1978–1982 (2015)
2. Rizoulis, D., Burl, J., Beard, J.: Control strategies for a series-parallel hybrid electric vehicle. In: SAE International, University of British Columbia, Vancouver, 31 July 2018
3. Lu, Z., Cheng, X., Feng, W.: Coordinated control study in engine starting process of hybrid vehicle, p. 2111. IEEE, Harbin (2010)
4. Rizzoni, G., Pisù, P., Calò, E.: Control strategies for parallel hybrid electric vehicles. SAE Technical Paper Series, 5–8 March 2001
5. Zhang, B., Li, J., Yang, S.C., Gao, Y.: Control strategy for engine start-stop in hybrid electric vehicle. In: College of Automotive Engineering, Jilin University, Changchun, March 2009
6. Chen, H., Zuo, C., Yuan, Y.: Control strategy research of engine smart start/stop system for a micro car. In: SAE Technical Papers 2 (2013). <https://doi.org/10.4271/2013-01-0585>
7. Bishop, J., Nedungadi, A., Ostrowski, G., Surampudi, B., et al.: An engine start/stop system for improved fuel economy. In: SAE Technical Paper 2007-01-1777 (2007). <https://doi.org/10.4271/2007-01-1777>
8. Xu, X., Zhao, S., Dong, P.: Engine-start control strategy of P2 parallel hybrid electric vehicle. In: School of Transportation Science and Engineering, Beihang University, Beijing (2017)
9. Rocstrom, R.: An engine start/stop strategy for city bus. Master of Science thesis MMK2009:64 MDA 342 KTH industrial engineering and management machine design, Stockholm
10. Athani, G., Gavaraju, S., Kulkarni, S., Koduru, R., et al.: Implementation of design thinking, to improvise the engine stop/start system for enhanced benefits in real time driving conditions in India. In: SAE Technical Paper 2015-01-0142 (2015). <https://doi.org/10.4271/2015-01-0142>
11. McGeoch, D.J., Deutsch, P.: Control of automated engine stop/start for vehicles with an automatic transmission. In: UKACC International Conference on Control, 7–10 September 2010, pp. 1–6 (2010). <https://doi.org/10.1049/ic.2010.0364>
12. Qiao, S., Yang, Y., Li, Y., Yue, Z., Wang, Z., Zhu, X., Zhou, X.: Application of engine intelligent start-stop system in technology of vehicle fuel saving. In: 2014 Sixth International Conference Measuring Technology and Mechatronics Automation (ICMTMA), 10–11 January 2014, pp. 128–131 (2014). <https://doi.org/10.1109/icmtma.2014.35>
13. Decker, H., Stock, R.: BOSCH-ABS - designed for the user. In: SAE Technical Paper 861977 (1986). <https://doi.org/10.4271/861977>
14. Kaasinen, E., Roto, V., Hakulinen, J., Heimonen, T., et al.: Defining user experience goals to guide the design of industrial systems. Behav. Inf. Technol. (2015). <https://doi.org/10.1080/0144929X.2015.1035335>



Security Landscape for Private Cloud

Sheeja Shaji Manakattu^(✉), Shivakumar Murugesh,
and Rajashekhar Ningappa Hirekurabar

Central Research Laboratory, Bharat Electronics Limited, Bangalore, India
{sheejasmanakattu, shivakumarm, rajashekharh}@bel.co.in

Abstract. Cloud computing is gaining momentum due to its features like scalability, pay-per-use model, dynamic resource allocation etc. Since many applications and platforms of different organizations or departments are running on the same infrastructure, security is of utmost importance in the cloud. Cloud computing faces common security issues like data loss, malware attacks, phishing attacks, man in the middle attack etc., if proper care is not taken in hosting of applications and services. The technologies that make cloud computing possible like multi-tenancy, virtualization etc. itself can be exploited. Organizations often move to private cloud infrastructure in order to have better control over the data, infrastructure and security policies compared to the public cloud. Moving to a private cloud will not make the cloud more secured in nature. Security measures must be taken to make sure that the private cloud is secured. This paper discusses the security issues that can occur in a private cloud and its possible solutions.

Keywords: Cloud computing · Cloud security · Data security · Virtualization security · Application security

1 Introduction

Cloud computing provides scalable, on demand, convenient and shared pool of computing, storage and networking resources. The resources can be provisioned and released with minimal effort. The cloud model is composed of five essential characteristics namely: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [1, 2]. These five characteristics must be available in a computing capability to be qualified as a “cloud service” [1, 2]. The delivery of the five cloud characteristics are enabled using cloud service models namely Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). The service models are dependent on each other, but they can be implemented independently. The service models of cloud computing are known as SPI (SaaS, PaaS, IaaS) model, which is built on top of one another. It provides flexibility in managing computing, storage and network resources. The way the cloud is operated and who has access to the cloud service resources [1, 2] is defined using Cloud Computing Deployment Models namely; Private cloud, Community cloud, Public cloud and Hybrid cloud.

2 Security Issues in Private Cloud

Organizations often move to private cloud to have better control over the data, infrastructure, security, policies etc. But moving to private cloud infrastructure alone does not ensure complete security. Proper security measures and policies must be implemented to make sure the data and infrastructure is secure. The security measures start from the selection of cloud infrastructure management platform to securing applications and services hosted on the cloud. It is required to be aware of the security concerns to ensure that the private cloud is secure. This paper lists the security issues that are encountered in a private cloud infrastructure and the available solutions for them. The paper presents a security landscape of the security issues and solutions. Figure 1 shows the security issues in a private cloud.

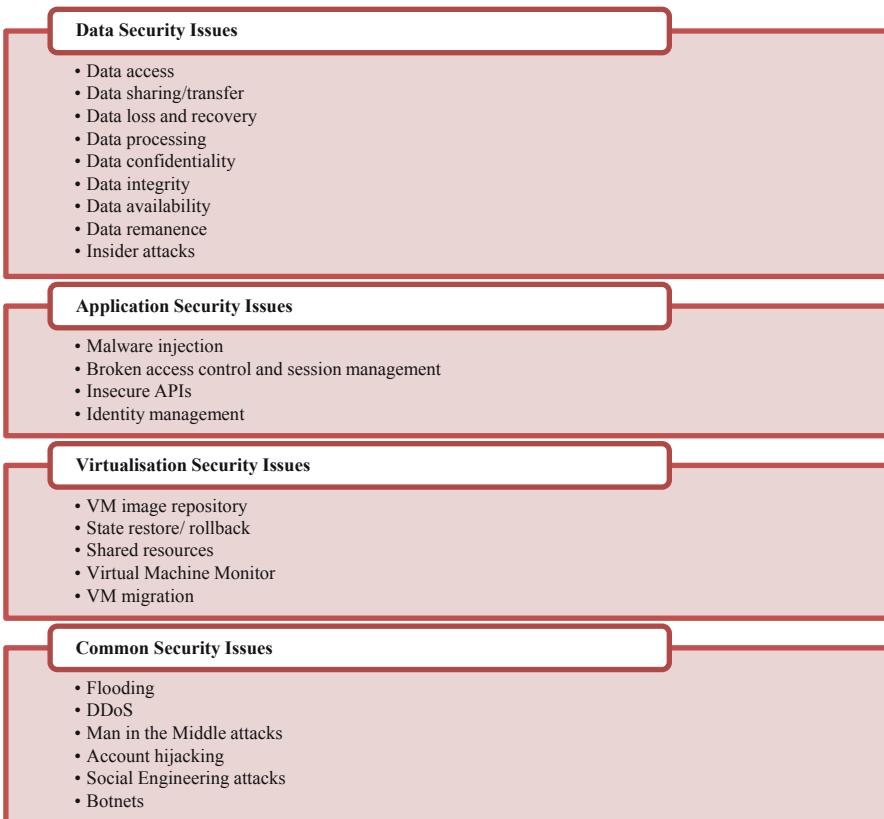


Fig. 1. Cloud security issues

2.1 Data Security Issues

In a Private cloud, data is stored inside the organization or a third-party vendor that hosts the cloud. Any data breach can cause serious threats to the organization depending on the data that is lost in the breach. The data security issues are:

- (1) **Data access:** Unauthorized users or entities accessing the data may lead to deletion or modification of data, unavailability of data etc.
- (2) **Data sharing/transfer:** When data is transmitted from creation site to the processing site, attackers can extract data if it is not protected.
- (3) **Data loss and recovery:** Data should neither be deleted by unauthorized users or entities nor be locked out for the authorized users.
- (4) **Data processing:** Attackers can access the plain form of data while data is being processed in the cloud.
- (5) **Data confidentiality:** Data should get disclosed only to authorized users and entities.
- (6) **Data integrity:** Data should be kept in its actual form without any modification.
- (7) **Data availability:** Data should be available for access for authorized entities or users at any time without any delay.
- (8) **Data remanence:** The residual data that lies in the disk even after deletion may be used to retrieve the actual data [7].
- (9) **Insider attacks:** The weakness in the data security model maybe exploited to access the sensitive data stored in the cloud [8].

2.2 Application Security Issues

The applications and services hosted on cloud is susceptible to attacks that exploits the vulnerabilities in the applications. Common attacks are:

- (1) **Malware injection:** Cross Site Scripting, SQL Injection, OS Injection and Command Injections are the common types of Malware Injection. In a cloud environment, injection of malicious services and VMs can be termed as malware injection [15].
- (2) **Broken access control and session management:** Incorrect implementation of session management and access control can lead to weak account management, exposure of session IDs, compromised passwords, user credentials, session tokens, loss of sensitive data etc. [6].
- (3) **Insecure APIs:** Weak authentication and authorization mechanisms, insufficient input data validation, weak credentials etc. [10] can cause the APIs to be less secure.
- (4) **Identity management:** Denial of services, insufficient authorization checks, insufficient logging and monitoring etc. [10] can occur in applications hosted on cloud due to weak identity management mechanisms.

2.3 Virtualisation Security Issues

The technologies like virtualization that enable cloud computing can be exploited and the common issues are:

- (1) **VM image repository:** VM images uploaded in the common repository may contain malicious code added by attackers which can be exploited to create an attack scenario in cloud.
- (2) **State restore/rollback** feature of virtualization can be misused by attackers to add or remove any previously enabled accounts and passwords or to nullify the security patches applied in the current state [10, 12].
- (3) **Shared resources:** In a cloud, the resources are pooled together to provide a common infrastructure. Sharing of the infrastructure can be exploited to create security issues like data leakage. Malicious VMs try to infer information about other VMs on the host through shared memory or other shared resources which is then used to attack the VMs. Also, due to the shared resources VMs try to communicate through covert channels by bypassing rules set by VMM [12].
 - a. *Multi-tenancy*: In a private cloud, even though the infrastructure is within the company itself, different departments in the company may require complete data and services' isolation.
 - b. *Side Channel Attacks*: The attacker places a VM on the same host as the target VM and tries to extract information from the target VM [20, 21].
 - c. *Virtual Networks*: Virtual networks are used to interconnect different VMs in the cloud. A malicious VM can do sniffing in the entire virtual network and obtain information about the different VMs hosted on the same virtual network.
- (4) **VMM:** Virtual Machine Monitor (VMM) or hypervisor is a software that provides isolation among VMs. As VMM itself is a software, any vulnerability in the VMM code can be exploited. Attackers can use a compromised VMM to compromise its migration module to perform malicious VM migration. VM escape is a form of attack on the VMM which can be used to bring down a VMM and thus the attacker gets full control of the storage and computing resources [10].
- (5) **VM migration:** Migration of VM is allowed to provide load balancing, fault tolerance and maintenance [10, 12]. This feature is exploited to migrate a target VM on a malicious host or a malicious VM to a target host. While migrating a VM, the entire contents of VM is exposed on the network which compromises data integrity, confidentiality and privacy.

2.4 Common Security Issues

Attackers can use vulnerabilities and weaknesses in the applications and network security configurations to cause breach in the system [8]. Flooding, DoS/DDoS, Man in the Middle attacks, Account Hijacking are the common network security issues. Social engineering attacks, Botnets, OS vulnerabilities, Platform and Middleware vulnerabilities and Key Management are some of the common issues that are applicable to cloud also. In cloud environment, botnets can cause DDoS attacks, data loss etc.

3 Security Solutions in Private Cloud

In a private cloud, protection of data, applications and infrastructure is of prime importance. Various methods like authentication, authorization, encryption, access control, identity and access management, security policies and audits and logs as listed in Figs. 2, 3 and 4 are used to protect a private cloud.

3.1 Data Security Solutions

The data needs to be protected at any stage in data's life cycle so as to avoid unauthorized access, data leakage and to ensure confidentiality, integrity, availability of data.

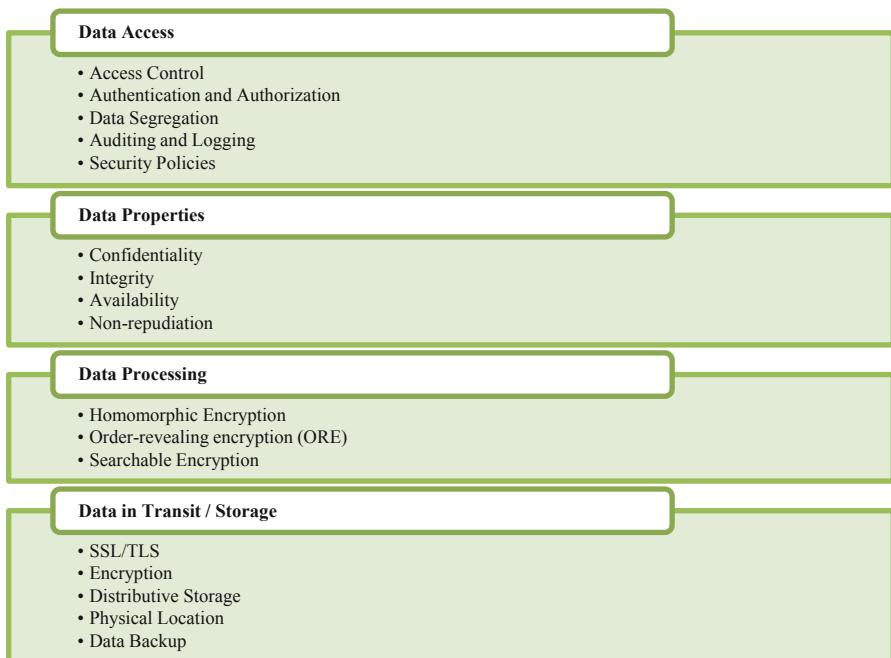


Fig. 2. Data security solutions

- (1) **Data Access:** The following methods are used to provide data access security.
 - a. *Access Control:* Access Control can be achieved using traditional methods like Access Control Lists (ACL), Role Based Access Control (RBAC), Mandatory Access Control (MAC), Discretionary Access Control (DAC) and cloud based methods like Attribute-based Access Control (ABAC), dRBAC (distributed RBAC) and coRBAC (Cloud optimized RBAC) [17, 18]. ABAC is a secure, scalable and flexible access control method in which users are assigned attributes and the access on the data is determined based on the attribute of the user. dRBAC is a distributed Role based Access Control systems suitable for cloud like environments.

- b. *Authentication and Authorization* checks should be made mandatory for users and services accessing any data on cloud.
 - c. *Data segregation* or data classification techniques allow to segregate data into different categories so that different data access policies can be applied based on the sensitivity of data. It can also help in identifying the type of storage and replication the data should undergo.
 - d. *Security policies:* Common methods used to avoid insider attacks are security policies and data segregation. Removal and addition of users and entities as they leave or enter the system should be done in a fast pace so as to avoid unauthorized access of data. A process should be defined to detect any data breach and to notify the authorities about the breach [9].
- (2) **Data Properties:** *Confidentiality* can be ensured by encrypting the data so that only authorized users, i.e. the user with the matching key can decrypt the data and use it. *Integrity* of data can be ensured using MAC (Message Authentication Code), Hashing, Signature etc. When using Signature, authenticity of the data can also be ensured along with integrity [9]. Integrity checks should be performed on the data that was transmitted from one service to another or from one location to another. Integrity checks should also be performed periodically on the data stored in the cloud to ensure data is not tampered while in storage. High *availability* of data in cloud can be provided using methods like replication or redundancy, backup of data in different geographical locations or RAID, defined policies for storage failure etc. *Nonrepudiation* is the assurance that an authenticated user cannot deny after performing a job [6]. It can be achieved by using signatures, digital confirmation acknowledgements and timestamps.
- (3) **Data Processing:** In order to avoid decrypting of data for processing, methods like homomorphic encryption, encrypted search is used. *Homomorphic Encryption* allows processing on encrypted data itself and only the users with the appropriate key can access the final processed output [12, 19]. It requires huge processing power and the operations possible are also limited. *Order-revealing encryption* (ORE) is capable of comparing cipher texts and returns the order of the original plaintexts [11]. *Searchable Encryption* process makes it possible to search for keywords in documents without decrypting the entire document.
- (4) **Data in Transit/Storage:** While data is getting transmitted from one service to another or from one location to another or from cloud service consumer to cloud service, attackers may try to capture the data. To protect data in transit, *SSL/TLS* can be used. This will help in preventing Man in the Middle attacks, provided SSL is configured properly. *Encryption* can be used to secure data at rest and in transit. *Distributive Storage* method can be used in which the data is divided into smaller chunks and then encrypted and stored in different locations in cloud thereby increasing the security of data stored in cloud [16]. The *physical security* of the cloud storage area should be ensured. Geographical location that is prone to natural disasters should be given least priority to host cloud storage. Data retrieval mechanism in case of disasters also needs to be defined. A *regular data backup* mechanism is needed to ensure availability and recoverability of data [10]. Protection of backup data using methods like encryption is also required.

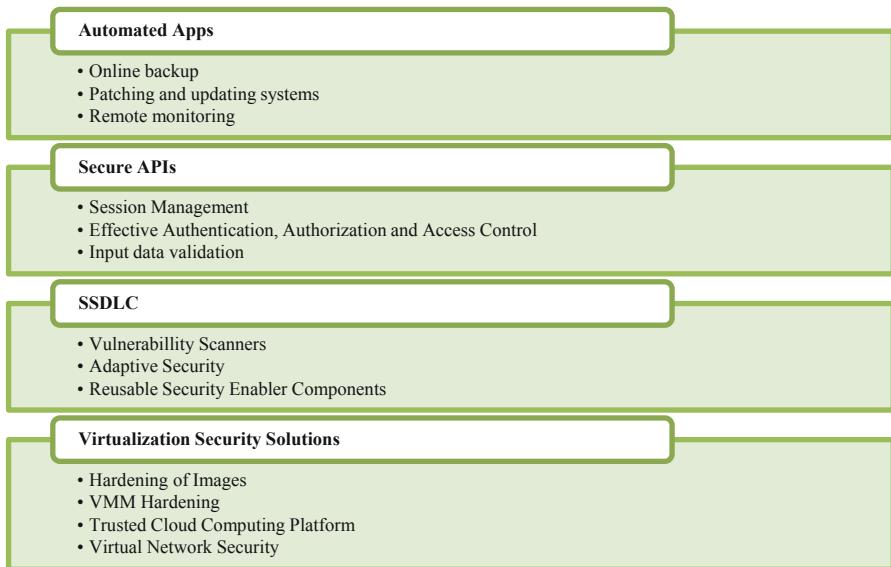


Fig. 3. Application and virtualisation security solutions

3.2 Application Security Solutions

Vulnerabilities in the applications can create serious security threats in cloud. Few commonly used methods to improve application security are:

- (1) **Secure APIs:** Since APIs act as the point of intersection for cloud services and cloud applications, the APIs exposed by the services has to be made secure. All *input data should be validated* before being used by the service inorder to prevent issues like buffer overflow attacks, data loss, etc. *Authorization and authentication* of each service request has to be checked to grant access. Methods like OAuth (Open Authorization), Single Sign On (SSO) can be used by the services for effective authorization. The APIs should have strong access control mechanisms to avoid unauthorized usage. Shorter sessions and session termination policies should be applied to provide better *session management* in cloud applications and services. Usage of cookie security parameters like secure flag, HTTPOnly flag, domain flag etc. [3] is recommended to improve security of web application.
- (2) **Automated Apps:** To ensure better security and availability of applications, automated applications can be used to perform online backup, patching and monitoring of the applications. The state of the applications or the whole applications can be periodically backed up to ensure higher availability. Also continuous monitoring of the resources used by the applications can help in identifying any flaws in the applications that may be exploited by the attackers.
- (3) **Secure Software Development Life Cycle (SSDLC):** The application development life cycle should use tools to enable development of secure applications. Reusable security enabling components [10, 13] should be included for

developing secure cloud applications. Applications should support adaptive security [13] so as to support various security requirements. Also before hosting the applications on cloud, it is recommended to perform web application vulnerability scanning [12], penetration testing and session management tests [10] to identify any common vulnerabilities.

3.3 Virtualisation Security Solutions

- (1) **Hardening of Images:** The VM image repository should be patched, hardened and updated with the latest security releases before uploading in cloud. Regular checking of these images for security updates is also recommended. The authenticity and the correctness of the images needs to be validated before uploading to the common repository.
- (2) **VMM hardening:** Since VMM is also a software, it is advised to keep VMM code simple and small in order to reduce the risk of exploits and to fix vulnerabilities if any.
- (3) **Trusted Cloud Computing Platform (TCCP)** allows users to determine whether the environment is secure to launch VMs. This will provide secure migration of VMs also [12].
- (4) **Security of the virtual network** is also required so as to establish a secure private cloud computing platform.

3.4 Common Security Solutions

Authentication, Authorization, Access Control, Identity Management, Audits, Logs, Performance monitors and network security solutions are the common solutions used for securing data, processes, machines, services and applications on cloud.

- (1) **Network security solutions:** In a private cloud, DoS attacks maybe created by malicious VMs or malicious users in the system. Provisions should be made to identify and screen automated requests [14] for a service. Providing a *Firewall* at the perimeter or boundary of the cloud is recommended. Spurious requests and some attacks can be prevented to an extent with the help of firewalls. *IDS* on a cloud is also recommended to prevent any intrusions to the cloud. *Monitoring of traffic* can be used to identify possible DDoS attacks, botnets, etc. The OS and system applications needs to be *patched regularly* for any security updates.
- (2) **Access Management and Authentication:** Use passwords, OTP, RSA tokens, smartcard/PKI, biometric etc. based on the feasibility in the system to provide strong authentication in cloud. Authentication should be performed not only on users but also on machines and services. Automated applications like patch management, backup, monitoring systems etc. should have access management and authentication. Using passwords alone for authentication is not recommended since insider attacks, social engineering attacks, brute force attack etc. can be used to obtain the password of a user. Hence *multi factor authentication* is recommended to improve security of the system.

When a request is made to change the password of the user, the user's identity should be verified. Authentication of the user should be made mandatory. Also users should not be allowed to keep default passwords set by system or network administrators. It should be changed on the first access itself. User credentials should be removed as early as possible if any users are leaving the system. Access permission modification on role change of any user also should be done with care.

- (3) **Identity Management:** Any secure system must have an identity management system to keep track of all users, services, applications, and servers that access the system. It helps to prevent unauthorized access of data and services, maintain integrity of data, keep track of users, services and other entities in the system. Account from which malicious activities are noticed can be locked out for a period of time to stop the attempts by the attacker. This can be used to prevent login attempts, usage of stolen user credentials etc.

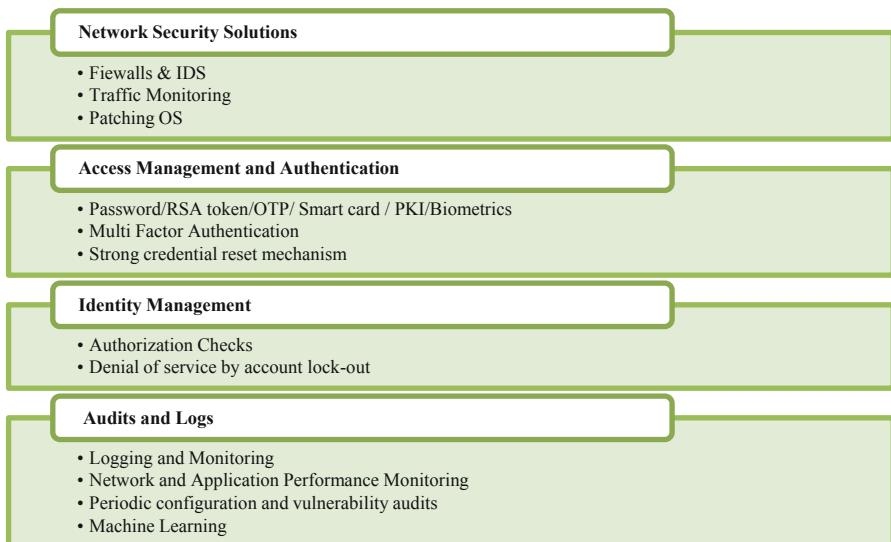


Fig. 4. Common security solutions

- (4) **Audits and Logs:** Creation of logs on any activity on the cloud is a mandatory requirement. Logs can be audited to find out if any unauthorized or malicious activity is going on in cloud. Logs should be created with timestamp, user details, type of access etc. Logs can also be generated on where the data is stored, who accessed the data, which machines are accessing the data etc. to identify data breaches [4]. Logging of VM creation and removal from cloud will help in identifying any malicious activity on the host [21]. Logs are used to perform forensics on the security breach event and to optimize the services and applications [4]. Monitoring of the incoming traffic and application is also required for ensuring security of the cloud. Monitoring can help in identifying attacks like

DoS, social engineering attacks etc. NPM (Network Performance Monitoring), APM (Application Performance Monitoring), Machine Learning and Periodic configuration and vulnerability audits are some of the methods used for auditing.

4 Security Landscape Model

The security issues that are common in a cloud are listed in Sect. 2. Some of the security issues exists only in one layer of SPI model, whereas some are common to all layers. As PaaS and SaaS are hosted on IaaS, any exploitation in IaaS level can cause breach in SaaS and PaaS. Similarly, vulnerability in SaaS can impact the security of underlying PaaS and IaaS layers. Thus, a security breach in any layer can impact the other two layers also [5]. A landscape of issues pertaining to SPI model can be drawn as shown in Fig. 5.

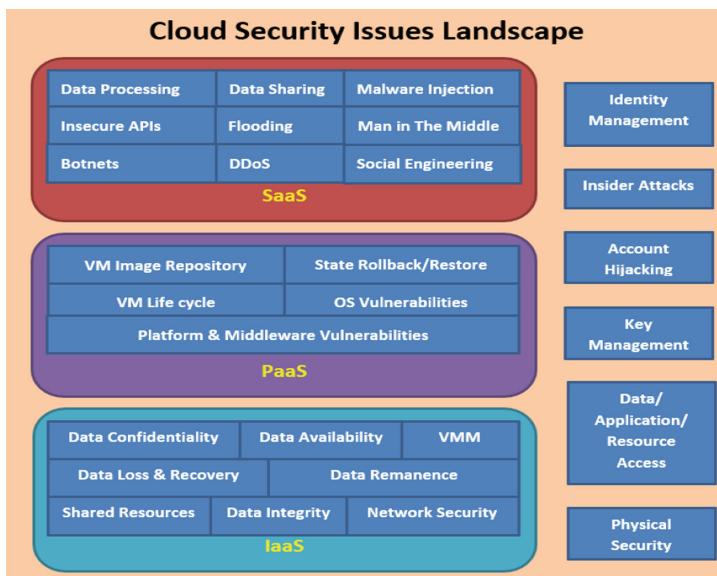


Fig. 5. Security issues classification in SPI model

The solutions to the security issues that are common in a cloud are already seen in Sect. 3. Some of the security issues can be solved by solutions pertaining to one layer, while some require solutions spanning all layers of SPI model. A model of security solutions' classifications can be drawn as shown in Fig. 6. The SPI model classification allows to identify and classify issues in different layers of cloud and also find suitable solutions. The security landscape can be used to clearly check for issues and provide solutions in a private cloud configuration.

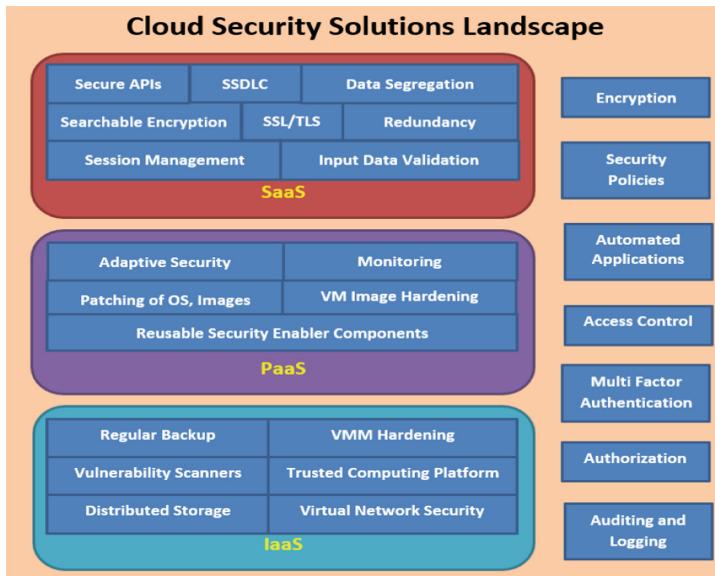


Fig. 6. Security classification in SPI model

5 Conclusion

Having a private cloud improves security as the services, applications and data are owned and maintained by the organization. The infrastructure if maintained within the perimeter of the organization and also on the internal network increases security and reduces attack scenarios. But attacks that exploit features like multi tenancy, virtualization attacks, attacks on application and services etc. may still exist. Patch management, policy updates, technology adaptations may introduce new attack vectors on the cloud. So, the organization that owns private cloud needs to employ security experts to continuously monitor and update the private cloud. Continuous testing of the security of the infrastructure and services is required to maintain a secure cloud. Also, proper planning and mitigation techniques are required to maintain security of the cloud. To manage the infrastructure and the services, a security model is required that can control the overall security of the cloud infrastructure. This can be achieved better in a private cloud deployment model as the cloud is owned, managed and operated by a single organization for its own use.

References

1. Mell, P., Grance, T.: The NIST definition of cloud computing, September 2011
2. Simmon, E.: DRAFT - evaluation of cloud computing services based on NIST 800-145. NIST

3. Ramesh Babu, G., Venkataramana, K.: Client centric model for secure session management for SaaS in cloud environment. *Int. J. Comput. Commun. Data Eng.* **01**(04) (2018)
4. Chavan, P., Patil, P., Kulkarni, G., Sutar, R., Belsare, S.: IaaS cloud security. In: 2013 International Conference on Machine Intelligence Research and Advancement (2013)
5. Walden, J.: Cloud Computing Security. Cincinnati Chapter Meeting, Northern Kentucky University, OWASP, 22 February 2011 (2011)
6. Ravi Kumar, P., Herbert Raj, P., Jelciana, P.: Exploring data security issues and solutions in cloud computing. In: 6th International Conference on Smart Computing and Communications (2017)
7. A guide to understanding data remanence in automated information systems, September 1991
8. Chowdhury, R.R.: Security in cloud computing. *Int. J. Comput. Appl.* **96**(15) (2014)
9. Aldossary, S., Allen, W.: Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *Int. J. Adv. Comput. Sci. Appl.* **7**(4), 485–498 (2016)
10. Ali, M., Khan, S.U., Vasilakos, A.V.: Security in cloud computing: opportunities and challenges. *Inf. Sci.* **305**, 357–383 (2015)
11. Alves, P.G.M.R., Aranha, D.F.: A framework for searching encrypted databases. *J. Internet Serv. Appl.* **9**, 1 (2018)
12. Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. *J. Internet Serv. Appl.* **4**, 5 (2013)
13. Al Morsy, M., Grundy, J., Müller, I.: An analysis of the cloud computing security problem (2016)
14. Christina, A.: Proactive measures on account hijacking in cloud computing network. *Asian J. Comput. Sci. Technol.* **4**(2), 31–34 (2015)
15. Rao, R.K., Vasudha, Bhat, S.: A review on malware injection in cloud computing. *Int. J. Innov. Res. Comput. Commun. Eng.* **6**(4) (2018)
16. Sun, Y., Zhang, J., Xiong, Y., Zhu, G.: Data security and privacy in cloud computing. *Int. J. Distrib. Sens. Netw.* **10**, 190903 (2014)
17. Punithasurya, K., Jeba Priya, S.: Analysis of different access control mechanism in cloud. *Int. J. Appl. Inf.* **4**(2), 34–39 (2012)
18. Mulimani, M., Rachh, R.: Analysis of access control methods in cloud computing. *Int. J. Educ. Manag. Eng.* **3**, 15–24 (2017). <https://doi.org/10.5815/ijeme.2017.03.02>. Published online May 2017 in MECS
19. Schoo, P., Fusenig, V., Souza, V., Melo, M., Murray, P., Debar, H., Medhioub, H., Zeghlache, D.: Challenges for cloud networking security (2010)
20. Bryk, A.: Cloud computing: a new vector for cyber attacks. Dev Blog, 26 February 2018. <https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks>
21. Cloud computing: attack vectors and counter measures posted in cloud computing, 30 December 2015. <https://resources.infosecinstitute.com/cloud-computing-attacks-vectors-and-counter-measures/>



An Efficient Medium Access Control Mechanism Using Multiple Data Rates in Ad Hoc Networks

Arundhati Arjaria¹(✉), Priyanka Dixit¹, Shivendra Dubey²,
and Uday Chourasiya¹

¹ Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, India
arundhatiarjaria07@gmail.com,
priyanka.dixit@yahoo.com,
uday_chourasia@rediffmail.com

² Sagar Institute of Research Technology & Science, Bhopal, India
shivendra.dubey5@gmail.com

Abstract. Specially appointed remote systems made of versatile stations that transmit information over a typical remote channel, along these lines are shaping an all-remote correspondence arrangement. In contrast to cell/wired systems, the portable stations are not upheld by a pre conveyed foundation. For example, base stations, a wired spine, a focal system station, and so forth. Subsequently, the foundation of the system structure and its operational execution must be only over the remote medium, and in a dispersed and decentralized way. With the conspicuous innovative difficulties, these systems have pulled in noteworthy research enthusiasm for ongoing years, as they are very appropriate for some trying settings, for example, in pursuit and salvage tasks, detecting applications, work systems, vehicular interchanges, and so forth. Here in this paper, we present the idea of remote impromptu systems; we talk about their points of interest and the reasons which debase the execution of specially appointed systems and significantly diminish the throughput of the system and increment the crash and postponement of the systems in particular “Hidden” and “Exposed” station issue. We have employed a twofold busy tone build Medium Access Control methodology to totally alleviate these problems. Reenactment results demonstrate the exactness of our proposed plan as far as higher throughput and lesser crash rate.

Keywords: Wireless ad hoc networks · Medium Access Control · Busy tone · Hidden · Exposed stations

1 Introduction

Remote frameworks are collections of compact stations furnished with remote handsets and act absolutely over a standard remote channel. The character of the remote channel, each station will only examine genuinely with someone of a kind station lying in its neighborhood. Unexpectedly hand, the traffic necessities of the framework are resolved evacuated stations may need to exchange information. Thusly, the stations focus such act sets can need to hand-off the data in an exceedingly multihop fashion.

In remote extraordinarily selected frameworks, the remarkable Hidden Station and Exposed-Station issues may spoil the execution of the framework to the extent unfairness and different issues. The primary mean to plan MAC convention is to expand the channel usage. Where numerous fighting stations are there to get to a similar channel, MAC convention is utilized to arrange the channel access among every one of the stations. To accomplish this objective MAC conspire needs to limit the odds of crashes and in the meantime expand the spatial reuse.

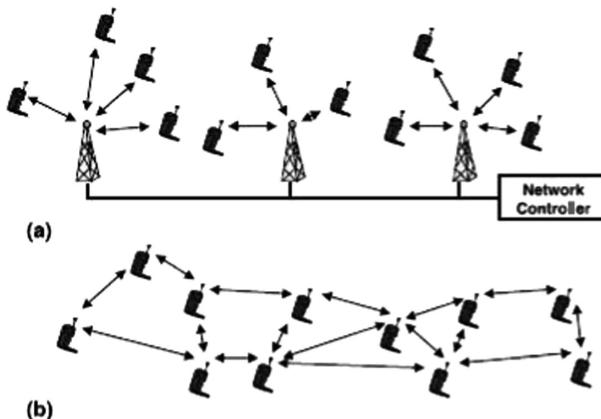


Fig. 1. (a) An abnormal state deliberation of a cell organize, (b) An abnormal state abstraction of a remote specially appointed system.

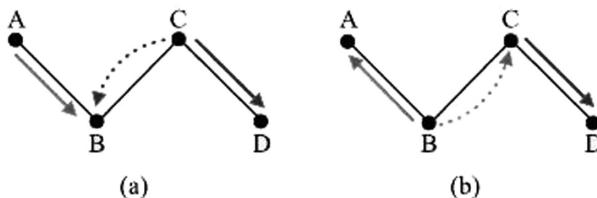


Fig. 2. (a) The concealed node problem: Node A is currently communicating to Node B. Node C can't hear the communication, and if C communicates to node D, will cause an effect at node B. (b) The revealed node problem: Station B is communicating with station A, and node C has data for station D. Station C won't send to D, notwithstanding the way that in case it did, it would not cause an effect.

1.1 Medium Access Control

At the point when a station is imparting over a remote medium, the flag comes at the proposed recipient, yet additionally at all different collectors in the area territory. So as to maintain a strategic distance from the impact of signs at recipients and their common devastation, it is vital that stations facilitate, so concurrent transmissions are not all that nearby in order to meddle with one another at their intended beneficiaries. (Clearly, the

greatest satisfactory dimensions of obstruction will rely upon the specific physical layer utilized, yet such an exchange is past our degree.) Then again, it is also imperative that continuous communication is full as adjacent as could sensibly be normal, so the exchange speed isn't wasted, and correspondence rates between customers are increased. Give us initial a chance to look at the concealed terminal issue.

2 Problem Statement

This area portrays the issues in multi-bounce specially appointed systems when the IEEE 802.11 Medium Access Control convention is executed. The covered up and uncovered station issues are two surely understood issues.

Here, in this segment, the covered up and uncovered Station issues are characterized properly.

(1) Hidden Station Problem

The covered up and uncovered Station issues are two surely understood issues. For test example, in Fig. 1, it demonstrates that station A is in the transmission extend on station B and station C in additionally in the station B's transmission run. A concealed station issue happens for this situation so it must be significant that the transmission range and detecting extent ought to appear as something else.

(2) Exposed Station Problem

As shown in Fig. 2, where node C is in the communication area of node B which is the transmitter and station D is in the communication range of station C, so in this case, station C has to wait until station B completes its transmission, in this station B and station C, are exposed to each other.

3 Proposed Protocol

In our method, a medium is a piece of two sub-mediums: an information vehicle for information follows and a control mechanism for control plots to resolve Hidden and exposed mobile nodes problem. Double tones proliferations included tone (BTT) and gets the included tone (BTr), are assigned dual random solitary frequencies of control medium. Here, we have considered various data rate condition to deal with all of these issues. In a general sense IEEE 802.11 standard sponsorships four sorts of data rates that are 1, 2, 5.5 and 11 Mbps. It depends upon the Bit Error Rate of the correspondence channel what data rate is maintained by the framework. If the Bit error rate is higher than lower data rate is supported (1 Mbps and 2 Mbps) and if the bit error rate is lower than higher data rate is maintained (5.5 Mbps and 11 Mbps). We decided the Bit Error Rate of the channels and kept an eye on these entire issues on the diverse data rates.

4 Operation Procedure

The convention works as pursues:

When a transmitter requires sending the packet, it initially distinguishes channel for BTr to ensure that arranged beneficiary isn't at present getting data from another "disguised" station. In the occasion that arranging recipient isn't getting from another source, the transmitter sends the Request to Send packaging to the concerned receiver. In the wake of getting this RTS diagram, the recipient resources for BTT to guarantee that the information it is depended upon to get won't collide with another advancing data transmission close-by. We have used four sorts of information rates to decide the concealed and revealed terminal issue that is 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps. in addition, consequent to reproducing the framework in various data rate condition it has shown that our arrangement is working in a wide scope of data rate condition.

5 Performance Evaluation

5.1 Simulation Background

The reenactments are done in NCTUns 5.0 test framework. The NCTUns orchestrate simulator and emulator (NCTUns) is a committed framework for reenacting various contraptions and shows used in both wired and remote frameworks. The data transmission broaden is 250 m, data hindrance run is 550 m, RTS edge regard is 300 bytes, crucial rate (RTS/CTS) transmission is 2 Mbps.

In our proposed method, the association information exchange limit moves as demonstrated by the reenactment and it contrasts from 11 Mbps to 5.5 Mbps, 1 Mbps, and 2 Mbps.

5.2 Results and Discussions

We assess the presentation of the system under different topologies. The framework execution is assessed under some particular topologies right off the bat as appeared in Fig. 3. At that point, irregular topologies are mimicked for a progressively thorough assessment.

Here in NCTUns window, the stations are there representing by their station id. Simulation of the network is shown in the running condition, where data is transmitted from one station to another.

In Figs. 3 and 4 three mobile nodes/stations are representing the transfer between them which results in the performance procedure in a simulated environment.

In the same way, we have simulated the results for hidden and exposed nodes on various data rates and generated the results in the form of presented graphs.

It has been seen by simulations that are not a fully connected scenario the RTS collision probability of IEEE 802.11e is much greater than in a completely associated system. Here, the RTS collision probability is less is a fully connected network as well as a nonfully connected network.

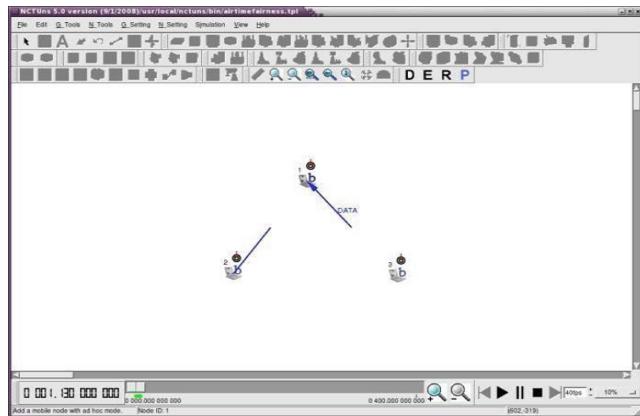


Fig. 3. NCTUns Window (1) with three mobile stations

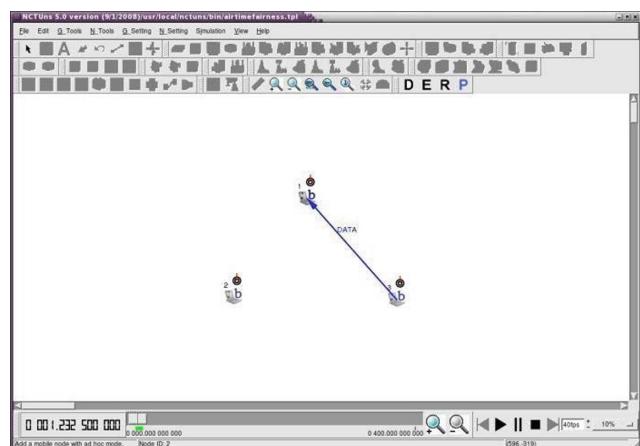


Fig. 4. NCTUns Window (2) with mobile stations

Figure 5 shows the NCTUns Window with 9 mobile stations, in which station 2 is the receiver station and rest of the stations (1, 3, 4, 5, 6, 7, 8, 9) are the sender stations which transmits the data frame to the station 2.

An access delay framework incorporates defensive power protects, aloof obstructions, and dispensable hindrances to expand the likelihood that an enemy will be hindered previously achieving his target.

Results show that the suggested plan has better results than IEEE 802.11e in parameters as lesser access delay, lesser packet drop ratio and higher throughput ratio.

Figures 6 and 7 represent the total access delay ratio and packet drop ratio of the network in various data rates.

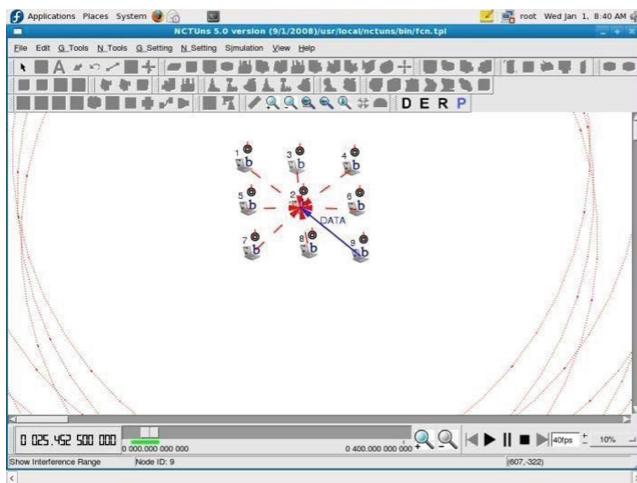


Fig. 5. NCTUns Window with 9 mobile stations

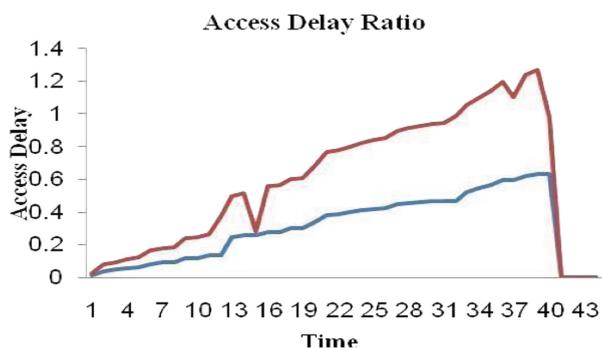


Fig. 6. Time vs. access delay

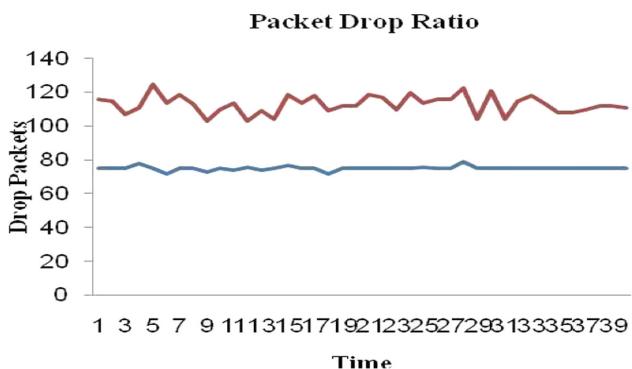


Fig. 7. Time vs. packet drop ratio

Throughput is the rate of successful transmission of messages conveyance over a channel and Packet delivery proportion is the proportion of received bundle over sent the data packets in the system.

Figure 7 represents the Time vs Packet delay ratio over a transmission channel and Fig. 8 speaks to throughput proportion of our proposed plan and past plan, in the wake of reenacting the system we have found in our proposed plan that the estimation of access postpone parcel drop and throughput proportion in our plan gives the better outcomes. All the determined outcomes demonstrate that our plan has settled the covered up and uncovered station issue.

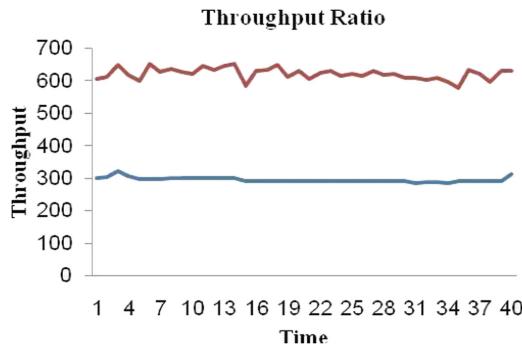


Fig. 8. Time vs. throughput ratio

6 Conclusion

In the remote extraordinarily selected frameworks, the remarkable shrouded terminal and uncovered terminal issues may degenerate the execution of the framework to the extent lesser throughput and despicableness issues. Various instruments have been proposed in the present writing to decrease genuine accidents of DATA bundles at the MAC framework. Here, we identified the concealed & uncovered terminals are the issues that are the essential driver of hair-raising execution degradation of the IEEE 802.11 MAC in impromptu frameworks. To facilitate these problems, we proposed another MAC show which used dual mediums: one for control and Data bundles. Our component diminishes the concealed similarly as uncovered terminal issue and manufactures the throughput of the framework with decreasing the effect rate by reducing the pack drop extent and the total access deferral of the framework in various information rate condition as stand out from IEEE 802.11e MAC plot. Our instrument and diversions exhibit that the proposed instrument can overcome the issues and manufactures the execution of the framework and gets rid of the accident probability.

References

1. Choudhury, R.R., Vaidya, N.: Deafness: a MAC problem in ad hoc networks when using directional antennas. In: Proceedings of IEEE ICNP, Berlin, October 2004
2. Cesana, M., Maniezzo, D., Bergamo, P., Gerla, M.: Interference-Aware (IA) MAC: an enhancement to IEEE 802.11b DCF. In: Proceedings of IEEE Vehicular Technology Conference, Orlando, Florida, USA, October 2003
3. Ye, F., Yi, S., Sikdar, B.: Improving spatial reuse of IEEE 802.11 based on ad hoc networks. In: Proceedings of GLOBECOM 2003, San Francisco, CA, December 2003
4. Tobagi, F.A., Kleinrock, L.: Packet switching in radio channels: Part II—the hidden terminal problem in carrier sense multiple-access and the busy-tone solution. *IEEE Trans. Commun.* **23**(12), 1417–1433 (1975)
5. Xu, K., Gerla, M., Bae, S.: Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks. *J. Ad Hoc Netw.* **1**, 107–123 (2003)
6. He, Q., Cai, L., Shen, X., Ho, P.-H.: Improving TCP performance over wireless ad hoc networks with busy tone assisted scheme. *EURASIP J. Wirel. Commun. Netw.* **11**, Article ID 51610 (2006)
7. Jurdak, R., Lopes, C.V., Baldi, P.: A survey, classification and comparative analysis of medium access control protocols for ad hoc networks. *IEEE Commun. Surv. Tutor.* **6**(1), 2–16 (2004)
8. IEEE Standards Department: ANSI/IEEE Standard 802.11. IEEE Press (1999)
9. Li, J., Blake, C., De Couto, D.S.J., Lee, H.I., Morris, R.: Capacity of ad hoc wireless networks. In: 7th ACM International Conference on Mobile Computing and Networking, Rome, Italy, July 2001
10. Gupta, P., Kumar, P.R.: The capacity of wireless networks. *IEEE Trans. Inf. Theory* **46**(2), 388–404 (2000)
11. Chow, C.C., Leung, V.C.M.: Performance of IEEE 802.11 medium access control protocol over a wireless local area network with distributed radio bridges. In: WCNC 1999, New Orleans, LA, USA, September 1999
12. He, J., Kaleshi, D., Munro, A., Wang, Y., Doufexi, A., McGeehan, J.: Performance investigation of IEEE 802.11 MAC in multihop wireless networks. In: Proceedings of the 8th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, Montreal, QC, Canada, October 2005
13. Haas, Z.J., Deng, J.: Dual Busy Tone Multiple Access (DBTMA): a multiple access control scheme for ad hoc networks. *IEEE Trans. Commun.* **50**(6), 975–985 (2002)
14. Karn, P.: MACA—a new channel access method for packet radio. In: RRL/CRRRL Amateur Radio 9th Computer Networking Conference, pp. 134–140 (1990)
15. Bharghavan, V., Demers, A., Shenker, S., Zhang, L.: MACAW: a media access protocol for wireless LAN's. In: Proceedings of ACM SIGCOMM (1994)
16. Fullmer, C.L., Garcia-Luna-Aceves, J.J.: Solutions to hidden terminal problems in wireless networks. In: Proceedings of ACM SIGCOMM 1997, September 1997
17. Xu, S., Safadawi, T.: Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks? *IEEE Commun. Mag.* **39**, 130–137 (2001)



Ranked Keyword Search Result Verification to Detect Misbehaving Cloud Servers

L. Ashwini^(✉) and N. R. Sunitha

Department of CSE, SIT, Tumkur, India
ashwinilashu95@gmail.com, nrsunithasit@gmail.com

Abstract. Nowadays, so many people outward their delicate information to the cloud in an encrypted format to maintain its privacy. On this basis, financial cloud computing becomes more efficient and useful. Protected keyword go through encrypted cloud information has fascinated many scholars for performing an effective data utilization. Current research is based on the impression that a cloud server is curious but truthful and therefore the search outcomes are not proved. But in real-world, sometimes cloud server might compromise and behave untruthfully. To maintain the reliability and secrecy, the outsourced delicate information should remain in the encrypted form. It is a task to go through the encoded data. There is a search facility to deliberate a ranked keyword search and there will be various data users and important files imported into the cloud. Hence, we propose a Ranked keyword search result verification for the detection of misbehaving cloud servers. We demonstrate two misbehaving scenarios of cloud server that will be detected by data user by using the relevance score of each file. In the whole process cloud server operates on the encrypted data.

Keywords: Cloud-computing · RSA · CP-ABE · Ranked keyword

1 Introduction

Cloud environment provides the enumerated facilities over the internet. Cloud environment is a computing template in huge number of systems that are linked in social or private networks [1]. The cloud computing template allows any individual user to access data and computer properties from anywhere across the globe.

The cloud architecture spread widely in the form of public clouds and it is available to all the users. Authorized user can access the server to run an application, to store the important data or to make any other computing task. Nowadays, many people use the cloud services. As the usage of cloud service is growing more delicate data are uploaded into the cloud such as private photos and videos, email and personal files etc. [2, 3]. To protect data from the attackers the delicate information should be encoded early it is outwarded to the cloud that is shared with the large number of users. To find any data file, one of the popular search methods is keyword-based search. Users, generally need to collect some certain specific files of user required through a particular period. Unfortunately, conventional text search process fails for encoded data in the cloud. So, many researchers focus on ranked single-keyword search and multi-keyword

search [4, 5]. Ranked single-keyword search greatly increases the system utility by providing a corresponding file in a ranked order with reference to specific relevance score. Multi-keyword ranked search uses the privacy preserving multi-keyword ranked search (MRSE) depending on the indexing and ranking. Indexing will provide a fast access to file search and ranking will arrange the list according to the priority. Multi-keyword ranked search improves the search accuracy. Many existing schemes believe that cloud server is curious but truthful. In real-world cloud server may compromise and act unfairly. So, here we recognize the ranked keyword search results to detect misbehaving cloud servers.

The following are the important objectives of this paper:

1. Ranked keyword search result verification for the detection of misbehaving cloud servers.
2. We demonstrate the two misbehaving scenarios of cloud server and which will be detected by data user using the relevance scoring of each file.
3. During the whole process cloud server must operate on encoded data.

2 Literature Survey

In [6] authors describe and resolve the issue of efficient yet protected ranked keyword go through the encrypted cloud data. Searchable Symmetric encryption (SSE) provide data owner to outward his information in the encrypted method although keeping the search ability over encoded data.

In [7] authors propose a multi keyword fuzzy search system which is a helpful technique to outward a various file. A data owner constructs a protected searchable index for the document set and then transfer the encrypted documents.

In [8] authors propose a useful method that considers encrypted data allows user to go through a rank keyword firmly and recover the file of interest. Searchable encryption outlines can be built by rank key based cryptography or public key based cryptography.

In [9] authorized keyword search is proposed. The authors use the cipher text policy attribute-based encryption method to accomplish accessible small-grained legal keyword search over encoded data which supports different data users and owners.

In [10] and [11] authors have proposed a multi keyword search that considers a keyword relevance and used a multi-dimensional tree method to attain effective search request. They have developed searchable encryption by seeing the huge amount of outward records stored in the cloud by using the relevance score and k-nearest neighbor methods and have developed an effective ranked keyword search system that will recover to ordered results relying on the correctness.

All these methods are depending on the impression that cloud server is “interested but truthful” where the search results are not confirmed, but, in practical cloud server may compromise and provide the false search results.

To overwhelm this problem, we propose a ranked keyword search result verification to detect misbehaving cloud servers where different data owners and data users are involved.

3 Proposed System

Proposed scheme considers a system, in which cloud server would maybe behave untruthfully. Based on this, we propose a ranked keyword search result verification to detect misbehaving cloud servers. The outline of the proposed scheme is as shown in the Fig. 1. The proposed system contains the following characters namely: Data owners, Data users and Cloud server.

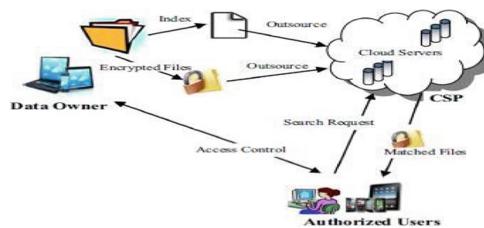


Fig. 1. Overview of the proposed system

Data owner: The data owner who outward his files to the cloud and that can be retrieved by valid search users securely and properly. Before out warding the data, he will extract the keyword from the file and that will be stored in the index document then he will encrypt the file to be uploaded. He also distributes the symmetric key with the authorized users who needs for the files to be downloaded. The access control technique is used to handle decryption abilities provided to users.

Data users: The authorized user sends search requests to the cloud server, trapdoor (Encrypted keyword) will be generated for those keywords based on the trapdoors cloud server retrieve the matched files. The data user can send multiple keywords so that cloud server can provide more matching documents to the search query.

Cloud server: The cloud server provides the space for information loading and we can also retrieve the files of interest. Sometimes we cannot trust the cloud server completely hence data owner will upload his file in the encrypted format.

4 Discussion of Proposed Work

We propose efficient ranked keyword search result verification scheme to detect misbehaving cloud servers. Different from previous schemes we demonstrate how the cloud server misbehaves while providing search results to the data user and how that will be detected by data user.

Data owner registers to the cloud and logins to the cloud then set of documents have to be uploaded to the cloud server by the data owner. If he is a registered owner, then he will get an access policy key (which means only valid users are accessing the services and resources). Initially data owner creates the public and private key pair. He relies index from many different keywords (We assume that a keyword is a word that will repeat more than 10 times in a file) which are extracted from his file. He counts the

relevance score, which is defined by calculating the relevant keywords in each and every file. The relevance score is added to index list. To provide confidentiality for file and index, the data owner encodes both the file and index with his public key. RSA Homomorphic encryption is used here. Finally, the data owner outwards his encrypted index and files to the cloud server. Data owner permits authorized users to make use of his files and therefore shares the trapdoor information with the valid data users.

If a valid data user needs to do search operation, data user creates the trapdoor (trapdoor means encrypted form of keywords) for a set of keywords, then send a search appeal to the cloud. Upon getting the search appeal the cloud server looks for relevant documents and their matching relevance scores depending on the trapdoor. If keywords matched with the index then the server retrieved the ranked files depending on matching of keywords in every file depend on the relevance scores and send a file to the user. If the valid user wants to download a file then he should enter the access policy to decrypt the file.

In this paper, we consider the dishonest cloud wherein we consider two misbehaving scenarios.

Misbehaving scenario 1: When the valid data user enters the keywords and transmit search request to the cloud server then it retrieves the unranked search results (For this we use an SQL query to show the misbehaving by cloud server). When the user gets the search results, if the user is not satisfied with the search result then he can go to the misbehave detection feature. The data user logins and enters the same keywords as a search request, trapdoor will be generated for those keywords, then he will get the files in which those keywords are present and also relevance score of each file. By obtaining this, data user will detect the cloud server misbehavior.

Misbehaving scenario 2: When the data user enters the keywords and transmit search request to the cloud server, then it does not return relevant files though keyword is available in that file. So, if the user does not get a file which he wants to download then he will go to the misbehave detection. As mentioned above the detection scheme will be same for both the misbehaving scenarios.

5 Implementation Details

The following techniques are used for the implementation:

RSA (Rivest-Shamir-Adleman) [12, 13] and CP-ABE (cipher-text policy-Attribute based encryption) [14, 15]: These techniques are employed for encrypting the file before uploading and decrypting while downloading.

- RSA algorithm is an asymmetric key cryptosystem, which means key pair will be generated, a private key and a public key. Public key can be shared with the authorized users and private key will kept secret.
- CP-ABE is a kind of public key encryption in that a user's secret key is connected to a set of features and a ciphertext requires an access policy. In that method, the decryption of a ciphertext is able only if the set of features of the authorized user key matching the features of the cipher text.

6 Screen Shots

6.1 Data Owner Side Operation

When data owner wishes to upload his document to the cloud, he will get an access policy to the file through email as shown in Fig. 2.



Fig. 2. Figure shows the access policy generation for a file.



Fig. 3. Data owner operation while uploading file.

If he wishes to upload his file to the cloud, data owner specifies the file, extracts keyword, generates the public and private keys, encrypts and uploads the file to the cloud as shown in Fig. 3.

6.2 Cloud Server-Side Operation

When the cloud server gets the search appeal from the valid user. Upon getting the search appeal the cloud searches for matched files and their related relevance scores based on the trapdoor as shown in Fig. 6 (Figs. 4 and 5).



Fig. 4. When a valid user enters the different keyword to search, cloud different keyword to search, cloud server misbehaves by providing unranked search results.



Fig. 5. Valid data user enters the keyword to search, cloud server does not provide the file even though those keywords are available in that file.

filename	location
cess.m4	0.200570380
dist.m4	0.097433928
Data Governance Through Bigdata.pdf	0.097433924
m3.pdf	0.0118453875
mm3.pdf	0.012469911
mm4.pdf	0.012469910
ft.pdf	0.013817105
ft4.pdf	0.013817106
13.pdf	0.015394015
dist.pdf	0.021926043
dist1.pdf	0.021926049
Algorithmic Tax Scheduling Algorithm in Cloud.pdf	0.023458233
Big Data Set Privacy Preserving through Sensitive.pdf	0.023458239
Designing and Developing Data in Cloud.pdf	0.025489448
mm3.pdf	0.027377678
2.pdf	0.027377679
pmc2018.pdf	0.027734499
jsf_hibernate.pdf	0.027734500
1.pdf	0.028391158
4.pdf	0.028391159
ml.pdf	0.030834925
ml4.pdf	0.030834926
01_Tutorial.pdf	0.037760527
02.pdf	0.037760528
face_recognition.pdf	0.047337445
algorithms.pdf	0.048405018
A Survey on Dynamic Multi-keyword Ranked Search Scheme over.pdf	0.053154543
parentheses.html	0.053154544
new.pdf	0.053154545
v2.pdf	0.10089055
Privacy_Preserving_and_Dynamic.pdf	0.10089056
ASD1.pdf	0.1175787
alarm system using image processing.pdf	0.1175788
Macromedia PDF File Access Available.pdf	0.12685728
1.pdf	0.3517851

Fig. 6. Filename and scoring.

6.3 Data User Side Operation

See Fig. 7.



Fig. 7. For detecting the misbehavior of the cloud server, data user/data owner enters the same keywords, trapdoor will be generated for those keywords.

7 Conclusion

We have designed a Ranked Keyword Search Results Verification to Detect Misbehaving Cloud Servers to enable the user to perform keyword search. Sometimes cloud server provides an unranked search results or does not return relevant files though keyword is available in that file, so here we consider the dishonest cloud server. To detect how the cloud server misbehaves while providing search results, the data user enters the same keywords to create trapdoor for those keywords. The cloud server searches for relevant documents and its related relevance score depends on the trapdoor.

References

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. *Commun. ACM* **53**(4), 50–58 (2010)
2. Zhu, C., Leung, V., Hu, X., Shu, L., Yang, L.T.: A review of key issues that concern the feasibility of mobile cloud computing. In: Proceedings of IEEE International Conference on IEEE Cyber Physical and Social Computing, and Green Computing and Communications, and IEEE Internet of Things, pp. 769–776 (2013)
3. Ritz, Vulnerable icloud may be the reason to celebrity photo leak (2014). <http://marcritz.com/icloud-flaw-leak/>
4. Hore, B., Chang, E.C., Diallo, M.H., Mehrotra, S.: Indexing encrypted documents for supporting efficient keyword search. In: Proceedings of Secure Data Manage, Istanbul, Turkey, August 2012, pp. 93–110 (2012)
5. Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: Cachin, C., Camenisch, J.L. (eds.) *Advances in Cryptology - EUROCRYPT 2004*, pp. 506–522. Springer, Heidelberg (2004)
6. Wang, C., Cao, N., Li, J., Ren, K., Lou, W.: Secure ranked keyword search over encrypted cloud data. In: Proceedings of IEEE Distributed Computing Systems, Genoa, Italy, June 2010, pp. 253–262 (2010)
7. Wang, B., Yu, S., Lou, W., Hou, Y.T.: Privacy preserving multi keyword fuzzy search over encrypted data in the cloud. In: Proceedings of IEEE INFOCOM, Tornoto, Canada, May 2014, pp. 2112–2120 (2014)
8. Chang, Y.-C., Mitzenmacher, M.: Privacy preserving keyword searches on remote encrypted data. In: Proceedings of the Third International Conference on Applied Cryptography and Network Security, pp. 442–455. Springer (2005)
9. Sun, W., Yu, S., Lou, W., Hou, Y.T., Li, H.: Protecting your right: attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In: Proceedings of IEEE INFOCOM, Tornoto, Canada, May 2014, pp. 226–234 (2014)
10. Jung, T., Mao, X., Li, X., Tang, S.-J., Gong, W., Zhang, L.: Privacy preserving data aggregation without secure channel: multivariate polynomial evaluation. In Proceedings of INFOCOM, pp. 2634–2642. IEEE (2013)
11. Yang, Y., Li, H., Liu, W., Yang, H., Wen, M.: Secure dynamic searchable symmetric encryption with constant document update cost. In: Proceedings of GLOBECOM. IEEE (2014, to appear)
12. Boldyreva, A., Chenette, N., Lee, Y., O'Neill, A.: Order-preserving symmetric encryption. In: *Advances in Cryptology - EUROCRYPT*, pp. 224–241. Springer (2009)
13. Yu, J., Lu, P., Zhu, Y., Xue, G., Li, M.: Towards secure multi keyword top-k retrieval over encrypted cloud data. *IEEE Trans. Dependable Sec. Comput.* **10**(4), 239–250 (2013)
14. Li, R., Xu, Z., Kang, W., Yow, K.C., Xu, C.-Z.: Efficient multi keyword ranked query over encrypted data in cloud computing. *Future Gener. Comput. Syst.* **30**, 179–190 (2014)
15. Li, H., Liu, D., Dai, Y., Luan, T.H., Shen, X.: Enabling efficient multi keyword ranked search over encrypted cloud data through blind storage. *IEEE Trans. Emerg. Top. Comput.* (2014). <https://doi.org/10.1109/tetc.2014.2371239>



Miniaturized Device for SHM Using Electromechanical Impedance Technique

Ashutosh K. Kedare^(✉) and Kapil Mundada

Instrumentation Engineering Department,
BRACT's Vishwakarma Institute of Technology, Pune, India
 {ashutosh.kedare17,kapil.mundada}@vit.edu

Abstract. Accidents due to the failure of the critical components in automobiles are always common. Generally, cyclic loading and mechanical impact is responsible for the deterioration of their structural integrity. So it is important to monitor the health of the component and damage occurred to automobile components on timely basis to avoid accidents. Various Global and Local techniques are used for structural health monitoring (SHM). This paper deals with the EMI Technique due to its advantages over the other local techniques for SHM. Most importantly, EMI Technique is used in real time. PZT patch is bounded to the component in this technique and a data containing information about the structural integrity is acquired in the form of the Admittance i.e. Conductance and Susceptance by the Impedance Analyser which is highly precise equipment by HIOKI. In this paper piezoelectric material EMI technique is discussed in detailed. Study of data acquiring using AD5933 board. Comparison of data acquired by AD5933 and IM3570 is done which are nearly matched, hence in proposed system hardware reduction and cost cutting is done.

Keywords: Non-Destructive Evaluation (NDE) · Conductance · Structural health monitoring (SHM) · Electromechanical impedance (EMI) · PZT patch · Impedance · Admittance · Susceptance · AD5933

1 Introduction

The advent of the smart materials in 21st century gave rise to the many technological marvels. The Piezoelectric material is one of the earliest discovered and fascinating smart material. The word “piezo” is the Greek word which is synonymous to pressure. The Piezoelectric material works on the principle of Piezoelectricity which was discovered by Pierre and Paul Curie in 1880. The most widely used piezo-ceramic today is Lead (Pb) Zirconate Titanate (PZT) which is stiff and brittle in nature. On the other hand piezo polymers are very flexible in nature example polyvinylidene fluoride (PVDF). Piezoelectric materials are basically used in accelerometers, strain sensors, vibration sensors, pressure transducers, actuators. They are increasingly deployed in turbo machinery, vibration dampers and for active vibration control of the structure over last two decades [1]. They are used as a dynamic strain sensors and as an impedance sensors in the field of SHM [2].

Structural Health Monitoring is a field in which the structure is inspected continuously against occurrence of the damage i.e. the structural integrity of the structure is checked and if any deterioration in the structure has occurred due to cyclic loading or mechanical impact it is repaired or replaced to avoid accidents due to breakdown of the structure. The damage to the structure affects its operation, serviceability, safety or reliability. Previously SHM has been used in Aerospace industry SHM of the aeroplane's wing has done [9, 10, 14] and their structural integrity is monitored to avoid accidents and SHM of civil infrastructures like bridges had been done [3, 15]. SHM provides continuous monitoring, acquisition, validation and analysis of the technical data to take safety actions against failures. Various Global and Local techniques are used for implementing SHM. Specifically, Non-Destructive Evaluation (NDE) techniques are used for SHM because these techniques do not interfere with the structural integrity of the structure. NDE techniques such as Ultrasonic interrogation, Acoustic emission, Eddy currents, Impact echo testing, Magnetic field analysis, Penetrant dye testing and X-ray analysis are used. The recent technique among these local NDE techniques is the Electro-mechanical Impedance (EMI) technique. This technique employs excitation frequency in Kilo Hertz range. The aim of this paper is to summarize the SHM in automobiles using EMI technique and use of the miniaturized device for it. The remaining paper is organized as follows: Sect. 2 describes piezoelectric material and EMI technique for Structural health monitoring and suitability of EMI technique for SHM in Automobiles. Experimentation details of the EMI technique is discussed in Sect. 3. Section 4 gives details about experimental analysis and results where, the comparison of AD5933 data and IM3570 data is done. Conclusion is given in Sect. 5 with acknowledgement and references at the end.

2 Piezoelectric Material and EMI Technique

PZT patches are used for structural health monitoring in EMI technique and same PZT patch is employed as sensor as well as actuator in EMI technique. Below are the Eqs. (1) and (2) of the piezoelectric material for actuator (converse effect) and sensor (direct effect) application of the PZT patch respectively.

$$D_3 = \bar{\epsilon}_{33}^T E_3 + d_{31} T_1 \quad (1)$$

$$s = ST + dE \quad (2)$$

Where, D_3 is surface charge density, T_1 is mechanical stress, E_3 is electric field, d_{31} is piezoelectric strain coefficient and $\bar{\epsilon}_{33}^T$ is complex electric permittivity at constant stress. The subscript 31 means that electric field is applied along 3rd direction and strain is measured along 1st direction. And Eq. 2 represents actuator application of piezo where, s is strain vector and S is compliance matrix.

The EMI Technique is invented by Liang, Rogers and coworkers and studied by many other prominent research groups in the world. EMI technique involves bonding a PZT patch on the surface of the structure to be monitored [4]. In Electro-mechanical Impedance (EMI) technique as the same piezo patch is used as an actuator and sensor

the cost of using multiple sensors is minimized. The thin PZT patches of size nearly 0.3 to 0.5 mm thickness are used for SHM purpose using EMI technique. The favourable frequency range to detect damage is from 30 kHz to 400 kHz and PZT patches 5 to 15 mm in size are best for EMI technique. The main advantage of using EMI technique for SHM in automobile is that this technique is highly sensitive to damage and can be used in real time compare to the other techniques mentioned above. The bonding of PZT patch to the structure is done by applying thin layer of Epoxy adhesive on it [6]. After bonding PZT patch, it is electrically excited over a high frequency range nearly (30 kHz – 400 kHz) and the characteristics admittance signature is acquired which is the baseline signature. This signature undergoes changes in it as the component which is to be monitored undergoes damage. Changes in the structural integrity can be detected by measuring stiffness in terms of the conductance signature change. By observation of the conductance and susceptance signatures the damage can be detected hence no need to use complicated algorithms. The hardware required in EMI technique is also less compared to other techniques. Hence, it is efficient to use EMI technique due to its advantages over the other NDE techniques (Fig. 1).

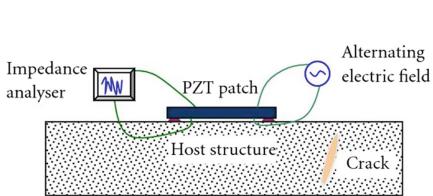


Fig. 1. Piezoelectric patch bounded to structure/component



Fig. 2. Functional Block Diagram of the EMI Technique

$$Y = 2\omega j \frac{wl}{h} \left[\epsilon_{33}^{-T} + \left(\frac{Z_a}{Z + Z_a} \right) d_{31}^2 \vec{Y}^E \left(\frac{\tan kl}{kl} \right) - d_{31}^2 \vec{Y}^E \right] \quad (3)$$

3 Detail Experimental Set-Up of EMI Technique

3.1 Practical Implementation of EMI Technique on Automobile Structures

- i. Bound the PZT patch on the smooth polished surface of the structure.
- ii. Excite the PZT patch electrically by Impedance analyser over high frequency range anywhere between 30–400 kHz. PZT vibrates and produces surface waves in the structure.

- iii. The waves are reflected by the surface of the component and edges. Acquire the Admittance signature with the help of Impedance analyser and LCR meter software as shown in Fig. 2.
- iv. The signature acquired is the baseline signature which represents the healthy component consisting of Conductance (G) and Susceptance (B) which are real and imaginary part respectively.
- v. The health of the component is checked after damage and cyclic loading to component and the acquired signature is compared with the healthy component signature. If the signature is not in the specified limits to that of the baseline signature then the component had undergone maximum damage and must be replaced.
- vi. The change in Conductance (G) gives the idea about the structural changes in the component i.e. damage to the structure, cracks etc. and the Susceptance (B) gives idea about the health of the PZT patch, its bonding to component which is used to acquire Admittance (Y) data. Figure 3 shows the sample conductance data acquired at various cycles.

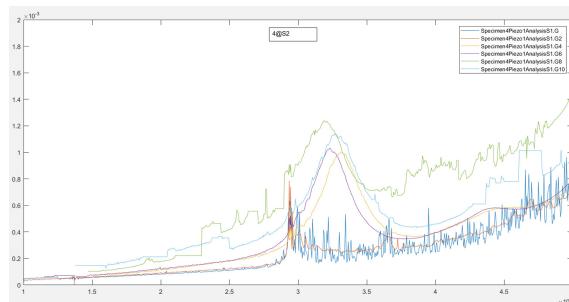


Fig. 3. Sample of Conductance Signature at different cycles for Mild Steel.

3.2 Problem of Using Impedance Analyser in Automobile

In EMI Technique the impedance analyser is used for acquiring the admittance data accurately. It acquires the data by taking DFT of the time series data over the specified number of points maximum up to 801 points. In automobile weight, space and power requirement are stringent design parameters. Due to large size, weight and power requirement of impedance analyser it can't be used practically in automobiles for SHM. To cope with this problem of impedance analyser Evaluation Board AD5933 is used which is an impedance converter circuit as shown in Fig. 4.

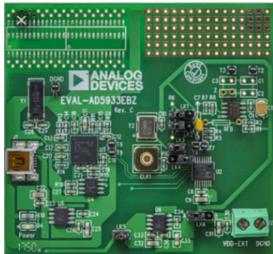


Fig. 4. Evaluation board AD5933

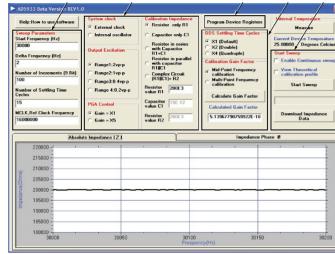


Fig. 5. AD5933 Evaluation board's GUI

The function of the impedance analyser can be performed by using this evaluation board AD5933. The board uses IC AD5933 which is impedance measurement IC [7]. The board has frequency generator which excites external impedance with known frequency range. Then ADC samples the response signal from the impedance, and a DSP engine calculates DFT at each excitation frequency. The impedance data is acquired which is then processed and admittance is calculated. The board uses AD5933 evaluation board software which provides GUI as shown in Fig. 5. As the evaluation board is small chip the space and power requirement is comparatively low than impedance analyser. Comparatively AD5933 board is somewhat less accurate than impedance analyser but this problem can be overcome by perfect calibration of the AD5933 evaluation board. The calibration process plays the main role in the accuracy of the evaluation board. Hence impedance analyser is satisfactorily replaced by Evaluation board AD5933 as all the problems are overcome.

3.3 Calibration Process of Evaluation Board AD5933

The Calibration process of AD5933 involves 2 methods Mid-point frequency and Multipoint frequency calibration. So for calibration either one of them is used for calibration. Here the mid-point frequency calibration process is used.

- i. Connect the AD5933 evaluation board to PC and load the AD5933 evaluation board software on PC, which is open source software.
- ii. Evaluation board has 2 inserting positions Z and RFB position. Z position is for the complex impedance connection and RFB is the position for the OP-Amp gain setting resistor.
- iii. Measure the impedance of the PZT patch on impedance analyser providing frequency sweep anywhere between 4 kHz to 100 kHz which is the frequency limit for Evaluation board AD5933. Observe the range of values of impedance and find out mid-point frequency value and note it.

If the Frequency Sweep chosen is 10 kHz to 90 kHz then

$$\text{Start Frequency} = 10 \text{ KHz}$$

$$\text{Stop Frequency} = \text{Start Frequency} + (\text{No. of increments} \times \text{Delta Frequency})$$

$$\text{Number of Increments} = 0 \text{ to } 511$$

Maximum value is 511 points for AD5933. Setting this for maximum value provides more detailed signature.

$$\text{Delta Frequency} = (\text{Stop Frequency} - \text{Start Frequency}) / (\text{Number of Increments})$$

- iv. Insert the fixed value resistor in Z position equal to the value of the impedance of PZT patch connected automotive component which is corresponding to mid-point frequency value. This is the calibration impedance.
- v. Place a same value through-hole resistor in the RFB position to keep the gain value 1. This is the feedback resistor. On the AD5933 software set all the parameters as per calculations and Program Device Registers.

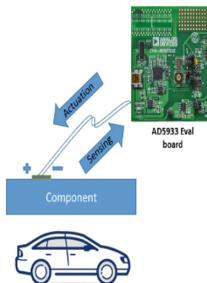


Fig. 6. Signature acquired through Eval Board AD5933 using AD5933 software

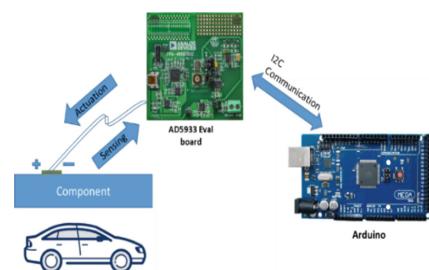


Fig. 7. Signature acquired through Evaluation board AD5933 interfaced to Arduino Mega 2560

- vi. Calculate Gain factor.

$$\text{Gain Factor} = \frac{1}{(\text{Impedance}) \times (\text{Magnitude})}$$

Where,

$$\text{Magnitude} = \sqrt{R^2 + I^2}$$

$$R = Z \times \cos\theta, \quad I = Z \times \sin\theta$$

This process calibrates the evaluation board to the selected frequency sweep.

3.4 Acquire Signature with AD5933

To acquire the Impedance data through AD5933 first step is to calibrate the device. The exact signature of the component corresponding to its stiffness change can be acquired by AD5933 evaluation board after it has been calibrated using calibration process

above. In this document the impedance signature acquired by AD5933 evaluation board is compared with that acquired by the Impedance Analyser IM3570. Same steps above as in calibration process are followed to acquire impedance data through AD5933 only instead of inserting fixed value resistor as in step iv of calibration process, insert the component under test attached with the PZT patch to acquire its admittance signature shown in Fig. 6.

Keeping program device registers unchanged start the sweep. Completion of the sweeps results the Impedance and Phase Data which can be observed and downloaded. To use the AD5933 in real life application example in automobile it can be interfaced with the microcontroller. The communication between AD5933 evaluation board and controller uses I2C protocol as shown in the Fig. 7.

4 Experimental Analysis and Results

The admittance signature is acquired at a healthy state of the component and stored in the memory which is also known as the baseline signature or healthy signature. After deterioration the signature is acquired again and it is compared with the baseline signature. The change in the characteristics of the signature from the baseline admittance signature denotes the change in the structure due to damage. The change in the real part of the Admittance(Y) i.e. Conductance (G) depends on the structural changes mainly in terms of stiffness, occurs due to cyclic loading and damage to the component. Similarly, imaginary part of Admittance signature i.e. Susceptance (B) denotes the damage to the Sensor which is PZT patch.

The baseline conductance signature is shown in Fig. 8(a) of a test specimen at 0 cyclic loading condition for the frequency sweep 100 kHz to 500 kHz. Similarly, Fig. 8(b) shows the 138455 cyclic loading signature data which is compared with the baseline signature, in which amplitude of the signature is slightly changed.

In Fig. 8(c) 267387 cycles signature data which is the signature where crack is generated in the automotive test Specimen which is compared with the signatures in Fig. 8(b) previous signatures. The signature in Fig. 8(c) denotes crack is generated in the component and maximum damage occurred to it. It should be changed as soon as possible to avoid accidents due to the component failure.

The experimentation is conducted on PZT patch of (5*5) mm in which its impedance data is acquired with the help of the Impedance analyser IM3570 and also with Evaluation board AD5933. The Impedance Signature data of PZT patch at free condition acquired with both of them is then plotted and compared as shown in Fig. 9(a).

As observed from Fig. 9(a) the Impedance data of AD5933 (shown in red colour) is exactly matched with the Impedance data acquired with Impedance analyser IM3570 (shown in blue coloured), the accuracy of AD5933 is nearly matched to that of the IM3570 Impedance Analyser.

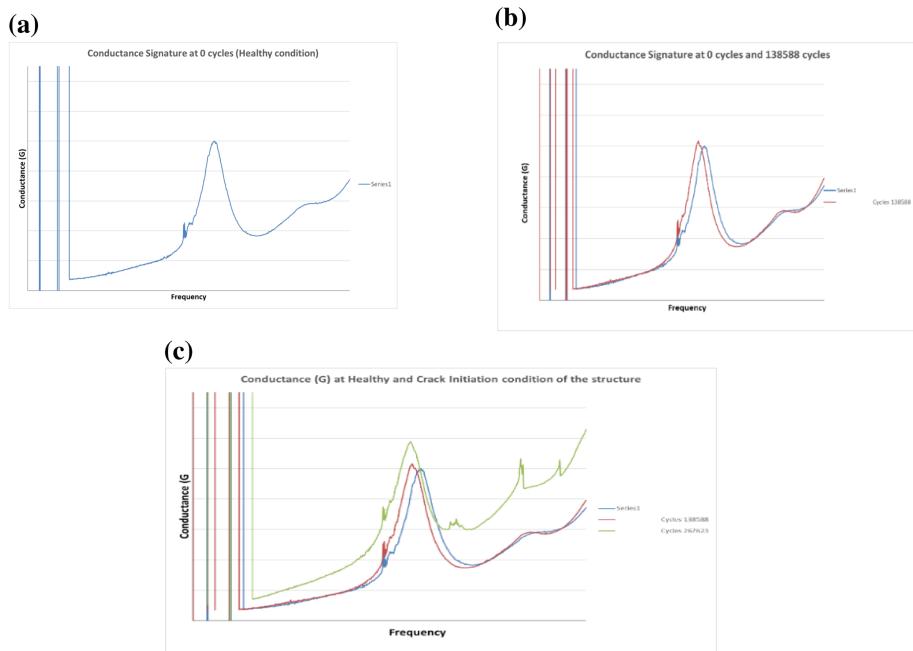


Fig. 8. (a) Baseline Conductance (G) Signature (b) Comparison Baselin signature and Signature at 138588 cycles (c) Specimen Crack Generation Conductance Signature Data (Green)

Admittance Signature data of Impedance Analyser IM3570 and AD5933 is compared in Fig. 9(b) for the frequency sweep 10 kHz to 90 kHz. The comparison shows the admittance signature of both the devices are nearly matched to each other hence the use of Impedance Analyser can be successfully replaced by AD5933 to acquire

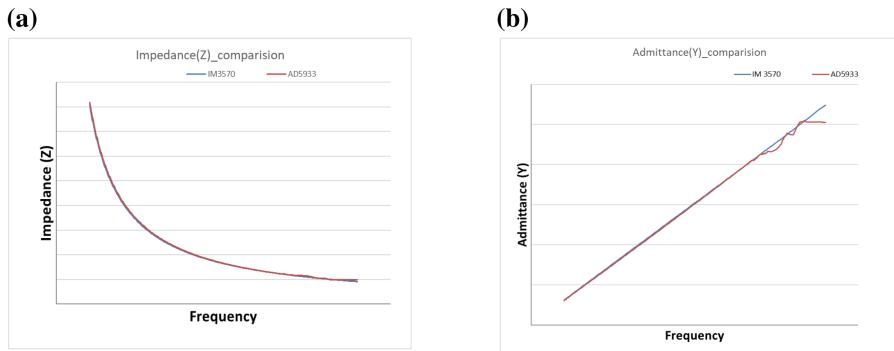


Fig. 9. (a) IM3570 and AD5933 Impedance data (b) IM3570 and AD5933 Admittance data

Table 1. Comparison IM3570 and AD5933

	Parameters	IM3570	AD5933 Eval board	Unit
1	Dimension	330 * 119 * 307	100 * 75 * 15	mm
2	Cost	9,995	150	\$
3	Weight	5.8	0.237	kg
4	Power supply voltage	90–230 AC	3.3–5.5 DC	V
5	Power consumption	150	0.05	W

Admittance signature data as the accuracy of both the devices is nearly same. And hence the light weight and low power design consideration can be successfully achieved in automobile along with its structural health monitoring using AD5933.

Table 1 shows a comparative analysis of proposed miniaturized device and conventional hardware device.

5 Conclusion

This paper talks about hardware development for Structural Health Monitoring in automobiles which is done using AD5933 evaluation board which can replace Impedance Analyser. As mentioned in Table 1 it can be clearly seen that there is a substantial reduction in space requirement, cost, power consumption and weight in the proposed system. So it is beneficial to use proposed miniaturized device over conventional device.

Acknowledgements. The research is being conducted in Automotive Research Association of India, Pune. I, sincerely thank Mr. M.R. Saraf (H.O.D- SDL, AML and TG, ARAI) and Mrs. Medha Jambhale (H.O.D ITM Dept. and Deputy Director - SDL) for giving me the opportunity to work as an Intern at SDL Dept. I thank my guide Mr. Virendra Kuwar for their constant guidance and Mr. Shivam Setia for his insights and all the members of SDL Dept. for their valuable contribution. The research conducted in ARAI is confidential hence the exact data is not shared in this paper.

References

1. Heganna, K.S., Joglekar, J.J.: Active vibration control of smart structure using PZT patches. *Procedia Comput. Sci.* **89**, 710–715 (2016)
2. Tianze, L., Xia, Z., Chuan, J.: Analysis of the characteristics of piezoelectric sensor and research of its application. In: 18th IEEE international Symposium on the applications of ferroelectrics (2009)
3. Fernandes, R.N.: The use of electromechanical impedance based structural health monitoring technique in concrete structure. Federal University of Uberlândia, Brazil
4. Giurgiutiu, V., Rogers, C.A.: Recent advancements in the electro-mechanical (E/M) impedance method for structural health monitoring and NDE. In: 5th Annual International Symposium on Smart Structures and Materials, San Diego (1998)

5. Budoya, D., de Castro, B., Campeiro, L.: Analysis of piezoelectric diaphragms in impedance based damage detection in large structures. In: 4th International Electronic Conference on Sensors and Applications (2017)
6. Mustapha, S., Ye, L.: PZT wafers for application in structural health monitoring - adhesive selection. *Res. Nondestruct. Eval.* **26**, 23–42 (2014)
7. Noveletto, F., Bertemes-Filho, P., Dutra, D.: Analog front-end for the integrated circuit AD5933 used in electrical bioimpedance measurements. In: II Latin American Conference on Bioimpedance, pp. 48–51 (2016)
8. Wandowski, T., Malinowski, P., Ostachowicz, W.: Calibration problem of AD5933 device for electromechanical impedance measurements. In: EWSHM – 7th European Workshop on Structural Health Monitoring, France (2014)
9. Diamanti, K., Soutis, C.: Structural health monitoring techniques for aircraft composites structures. *Science Direct Progress in Aerospace Sciences*, UK (2010)
10. Giurgiutiu, V., Zagrai, A., Bao, J.J.: Piezoelectric Wafer Embedded Active Sensors for Aging Aircraft Structural Health Monitoring, USA (2002)
11. Giurgiutiu, V.: Tuned Lamb wave excitation and detection with piezoelectric wafer active sensors for structural health monitoring. *J. Intell. Mater. Syst. Struct.* **16**, 291–305 (2005)
12. Spencer, B.F., Ruiz-Sandoval, M., Kurata, N.: Smart sensing technology for structural health monitoring. In: 13th World Conference on Earthquake Engineering, Canada (2004)
13. Kawiecki, G.: Modal Damping Measurement for damage detection. *Smart Materials and Structures*, USA (2001)
14. Eua-anant, N., Cai, X., Udupa, L., Chao, J., Elshafiey, I.: Crack detection in eddy current images of jet engine disks. In: AIP Conference Proceedings, USA (2000)
15. Otsuka, K., Takeda, M.: Detection of fine cracks by X-ray technique using contrast medium in concrete. In: Proceedings of JSCE, Japan (2003)
16. Budoya, D., Baptista, F.: Comparative study of impedance measurement techniques for structural health monitoring applications. *IEEE Trans. Instrum. Meas.* **67**, 912–924 (2018)



Malicious User Detection in Cooperative Sensing Environment Using Robust Distance

N. Swetha^(✉), D. L. Chaitanya, HimaBindu Valiveti, and B. Anil Kumar

GRIET, Hyderabad, India

swethakarima@gmail.com, chaiturohini@gmail.com, valiveti.bindu@gmail.com,
anilbudati@gmail.com

Abstract. In a Cooperative Spectrum Sensing environment, malicious secondary users (SU) degrade the overall performance of the radio network. The existing techniques need to assume an upper bound on the number of such users in a network, to identify them. In the present work, we use the robust distance based on minimum covariance determinant (MCD) to identify the malicious users in the network without assuming such an upper bound. Further, we validate the performance of the proposed RD method in random, always high and always low selfish attacks scenarios.

Keywords: Robust distance · Mahalanobis distance · Minimum Covariance Determinant · Entropy detection

1 Introduction

Cooperative sensing combines the observations from several SU's to improve the sensing reliability [1]. However, the detection performance severely degrades if the SU's report false data. The false data may be due to intentional malicious users or unintentional malfunctioning SU's [2]. The unintentional attack is known as a random attack, whereas the intentional attack is known as Byzantine or spectrum sensing data falsification (SSDF) attack [3, 4].

Outlier data are wrong data values that deviate from the actual distribution of data. Such malicious data cannot be separated visually. Many univariate and multivariate outlier detection techniques use arithmetic mean, covariance, and the correlation between data to identify malicious users [5]. A malicious detection scheme using spatial location information is proposed in [6]. It assigns an outlier factor to each SU. It is used as a measure to identify the malicious users in the network. Such users are suppressed by assuming the prior information about the PU activity and knowing the location information of SU's, which is practically not feasible. The different attack strategies of a single attacker are analyzed using an abnormality detection technique in [7]; however it fails to perform, when the number of attackers varies in a network. In practice, the number of attackers

is not always fixed. In [8], the authors detected SSDF attacks and isolated the malicious data using a local outlier factor. In [9], the attacks are neutralised by introducing probation and back off period.

A clustering-based malicious user detection scheme is presented in [10]. The maximum likelihood (ML) estimator is employed to estimate the distance between the PU and the respective cluster. The condition that limits the performance of the cluster based technique is that the number of malicious users must be less than the number of clusters, and there should be at least one cluster without malicious users. In contrary, a new defense strategy is incorporated in CSS [11]. The attack strength is estimated and applied to majority rule to obtain the optimum value that minimizes the Bayesian risk. However, it needs assumption of prior probabilities. Furthermore, the single and multiple untrustworthy malicious users were considered in [12]. Here, the historical reports from each SU were collected to determine the suspicious level and suppress the influence of malicious users. In [13], a reputation based scheme was proposed to thwart the intelligent malicious users. A moral hazard framework was designed to punish the rational and irrational malicious users. The main drawback observed in traditional schemes is that they require an upper bound on the number of malicious users [1]. In a practical scenario, a priori knowledge about the number of malicious users in a network is not feasible.

In the present work, we present a blind outlier detection scheme based on statistical distance measures, i.e., Mahalanobis and Robust distance to detect all the outliers in a network. The Mahalanobis distance (MD) uses mean, covariance and finds the similarity between the data samples. In the case of larger datasets, it is difficult to find a robust fit using MD measures. In the present work, we find the good data points first and then start finding the malicious ones, instead of searching for the bad data points. Such a dynamic multivariate regression technique is known as Robust distance using Minimum Covariance Determinant (MCD) [5]. In the MCD approximate, the covariance matrix that has least determinant is evaluated considering only a few samples (out of all). In this paper, all the SU's perform local sensing using entropy detection and the appropriate decision is taken using simple hard fusion rule. The average entropy of all SU's is fed to the proposed malicious user detection method to identify and remove all the malicious users. The random attack and two selfish attacks - 'always high' and 'always low' are sustained without degrading the performance [14]. The proposed method does not require any assumption regarding the number of malicious users in the network. The performance of RD technique is compared with MD, generalized extreme studentized deviate test (GESD) [1], Grubbs and Thompson Tau (TT) methods [3, 15]. The proposed RD scheme performs better in nullifying the attacks.

Section 2 presents the cooperative sensing model. Section 3 formulates the statistical distance metrics for outlier detection. Section 4 discusses the different types of attacks. The simulation results are detailed in Sect. 5, and finally, the conclusions are summarized in Sect. 6.

2 Cooperative Sensing Model

Let us consider, a typical CSS scenario with C channels in the spectrum of interest. Each channel is either occupied or unoccupied by PU signal. A set of SU's distributed in Q random locations continuously sense the channel. It is assumed that there are R number of SU's in each location. The SU's in each location are indexed as $SU_{11}, SU_{21}, \dots, SU_{R1}$ as shown in Fig. 1. The forward channels for transmission of data to the FC are assumed to have negligible interference. The SU's in each location sense the channels and transmit the entropy values (in frequency domain) to the FC [16]. Assume $E_r[z]$ represents the entropy at r^{th}

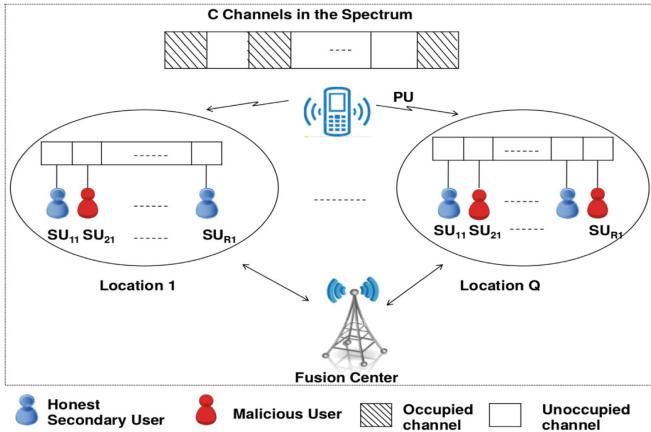


Fig. 1. Cooperative spectrum sensing network model with malicious users

SU in each location. The true hypothesis (H_1) and the null hypothesis (H_0) represent the presence and absence of the PU signal. The Shannon entropy at each SU can be evaluated by considering the teststatistics as [16]

$$E_r[z] = -\sum_{i=1}^L \frac{k_{ir}}{N} \log \frac{k_{ir}}{N} \quad \begin{matrix} H_1 \\ \geq \\ H_0 \end{matrix} \quad \lambda \quad (1)$$

$$r = 0, 1, 2, \dots, R-1$$

$$z = 0, 1, 2, \dots, N-1$$

where N denote the number of received signal samples, z denote the sample index, L is the bin length required for evaluating the entropy. k_{ir} represents the probability of data samples falling in i^{th} bin computed using histogram pdf [16]. λ is the detection threshold of r^{th} SU stated in [17].

Each SU reports its decision to the fusion center for detection. Since the focus of this work is to detect the malicious SU's and not to enhance the detection

probability, so a simple OR- rule is adopted at FC. The detection probability of cooperative sensing (C_d) using OR fusion rule is given as

$$C_{d,or} = 1 - \prod_{i=1}^R (1 - P_{d,i}) \quad (2)$$

where $P_{d,i}$ is the probability of detection of each SU.

3 Statistical Distance Metrics for Outlier Detection

In literature, there exist several approaches for outlier detection based on distribution, density, clustering, depth and distance [18]. The inter-relationships between data is measured using different distance-based methods. These are often used in clustering techniques.

3.1 Mahalanobis Distance

The entropies of several SU's is assumed to be a univariate data vector $\mathbf{E} = (E_1, E_2, \dots, E_R)^T$ of size $R \times 1$. The Mahalanobis distance identifies the similarities between unknown samples and normal samples whereas the Euclidean distance captures the correlations between samples. The MD is usually measured for a set of samples with a particular mean and covariance. The covariance matrix clearly differentiates two vectors possessing the same statistical distribution. The MD of each measure E_i at the FC is given as

$$MD(E_i) = \sqrt{(E_i - \hat{\mu})^T \hat{S}^{-1} (E_i - \hat{\mu})} \quad (3)$$

Here $\hat{\mu}$ and \hat{S} denote the arithmetic mean and covariance matrix. The $MD(E_i)$ corresponds to the relative distance of E_i from the mean. These distances suffer from a serious problem of masking effect, i.e., the larger outlier crowd influences the $\hat{\mu}$ and \hat{S} to obtain least $MD(E_i)$ making the outliers invisible. The cutoff values of MD method are evaluated using chi-square distribution, which cannot identify the outliers in a larger data. Hence, there is a need to study robust methods that are highly immune to malicious users.

3.2 Robust Distance

In cooperative spectrum sensing, the malicious attacks deviate the signal power to low or high increasing the probability of misdetection. Such type of attacks can be easily resolved using MCD shape and location estimates. The MCD method randomly choose k observations out of R ($k \leq R$) whose covariance matrix has low determinant [18]. The average of these k observations is the location estimate, and a multiple of the covariance matrix is the shape estimate of the MCD. Here, the optimum cutoff is determined using F-distribution to discover the malicious for various sample size. The univariate MCD is [18],

$$\begin{aligned} MCD &= (\hat{\mu}^*, S^*) \\ \hat{\mu}^* &= \frac{1}{k} \sum_{i \in G} E_i \end{aligned} \quad (4)$$

$$\hat{S}^* = \frac{1}{k} \sum_{i \in G} (E_i - \hat{\mu}^*)(E_i - \hat{\mu}^*)^T \quad (5)$$

$\hat{\mu}^*$ and \hat{S}^* represent robust estimates of mean and covariance matrix. The parameter G is the subset of R samples. The Robust distance of measure E_i is [18],

$$RD_i = \sqrt{(E_i - \hat{\mu}^*)^T \hat{S}^{*-1} (E_i - \hat{\mu}^*)} \quad (6)$$

The complete process of the proposed method is described in Algorithm 1. The computational overhead of the method is equal to $O(n)$, because the K_{new} can be computed in $O(n)$ operations without fully sorting distances $((d_{old})_k)$. The algorithm can be iterated until $\det(\hat{S}_{new}^*) = 0$ or $\det(\hat{S}_{old}^*) = \det(\hat{S}_{new}^*)$. The determinants obtained should converge in finite iterations subjected to k subsets.

Algorithm 1. Pseudo-code of the proposed Robust distance based malicious user detection

Initialize $E = E_1, \dots, E_n$ and let $K_{old} \subset 1, \dots, n$ be a subset of length k .

Step 1: Compute $\hat{\mu}_{old}^* = \frac{1}{k} \sum_{i \in K_{old}} E_i$ and $\hat{S}_{old}^* = \frac{1}{k} \sum_{i \in K_{old}} (E_i - \hat{\mu}_{old}^*)(E_i - \hat{\mu}_{old}^*)^T$ and determine the $\det(\hat{S}_{old}^*)$.

Step 2:

while $(\det(\hat{S}_{old}^*) \neq 0)$ **do**

Step 2.1: define the relative distances

$$d_{old}(i) = \sqrt{(E_i - \hat{\mu}_{old}^*)^T \hat{S}_{old}^{*-1} (E_i - \hat{\mu}_{old}^*)} \text{ where } i = 1, \dots, n$$

Step 2.2: Now, take new subset K_{new} such that $\{d_{old}(i), i \in K_{new}\} = \{(d_{old})_1, \dots, (d_{old})_k\}$ and sort them.

Step 2.3: Again compute new $\hat{\mu}_{new}^*$, \hat{S}_{new}^* and $\det(\hat{S}_{new}^*)$ using K_{new} .

Step 2.4:

if $(\det(\hat{S}_{new}^*) > \det(\hat{S}_{old}^*))$

Add another random observation and repeat from step 2.

else

go to step 3

endif

end while

Step 3: Claim that the most concentrated subset without malicious nodes is classified.

4 Attack Analysis

In this section, we consider three attacks for analyzing the detection performance of the proposed outlier detection scheme. The first one is the random attack where the malicious user arbitrarily reports incorrect data [14]. In the random attack, SU reports either high entropy or low entropy values to the FC. If the fusion center receives entropy greater than the maximum SNR detected regime, the probability of false alarm (p_{fa}) increases [19]. On the other hand, if it receives entropy less than the detection range, the probability of detection (p_d) decreases [19, 20].

The second type of attack is a selfish attack/Byzantine attack where the malicious user senses the spectrum and willingly reports relatively lower or higher entropy values compared to other SU's to the fusion center. We have considered 'always high' and 'always low' selfish attacks for analysis. In 'always high' scenario, the malicious user sends the entropy values higher than the SNR wall of detection, effecting the detection performance whereas in 'always low' scenario, it sends entropy value less than the SNR wall of detection that results in increasing the p_{fa} [19]. These abnormalities cause the interference levels to increase and create a confusion whether the abrupt increase/decrease in entropy is due to weak channels and fading or due to the presence of malicious users. Hence, a robust malicious detection scheme is required to find the mutual relationship between data samples and eliminate the suspicious ones in the presence of attacks.

Let γ_{wall} , γ_{low} , γ_{high} represent the SNR wall of detection, low and high signal powers of the entropy detection method. γ_{wall} is the minimum signal power of entropy detection technique below which the detection fails. The malicious users are generated by deviating the signal power to γ_{low} and γ_{high} . The corresponding entropies E_{low} and E_{high} , using Eq. (1) are

$$\begin{aligned} E_{low} &= E(\gamma_{low}) \\ E_{high} &= E(\gamma_{high}) \end{aligned} \tag{7}$$

For different attacks, the entropy of m^{th} malicious node is given by,

$$\begin{aligned} E_{m,random}[z] &\in (E_{low}, E_{high}) \quad \text{for } \gamma_m \rightarrow (\gamma_{low}, \gamma_{high}) \\ E_{m,alwayshigh}[z] &\in (E_{high}, E_{\gamma_{wall}}] \quad \text{for } \gamma_m < \gamma_{wall} \\ E_{m,alwayslow}[z] &\in [E_{\gamma_{wall}}, E_{low}) \quad \text{for } \gamma_m > \gamma_{wall} \end{aligned} \tag{8}$$

where γ_m and E_m denote the SNR and entropy of m^{th} malicious node respectively.

5 Simulation Results

Let us consider 40 SU nodes in the network in which 10% ($M = 4$) of them are malicious. We have considered the PU signal as a DVB-T signal with AWGN

channel. The DVB-T signal comprises of OFDM symbols with finite duration. The parameters of the signal include bandwidth, mode and length of cyclic prefix. The carrier frequency and bandwidth of the signal are set to 4.8 MHz and 6 MHz–8 MHz. The number of sub-carriers in OFDM modulation are decided by the two modes namely 2K and 8K modes. 2K-mode uses only 1705 sub-carriers and 8K-mode uses 6817 sub-carriers. A cyclic prefix is generally added to the data in OFDM to lower the adjacent channel interference. The cyclic prefix length used are 1/4, 1/8, 1/16, 1/32 [21]. In this work, 2K-mode is assumed to generate the DVB-T signal. At each SU, the entropy is computed using 256 samples ($N = 256$). 10000 Monte-Carlo simulations are carried out for evaluating p_d . The bin length for evaluating entropy is $L = 15$. The parameters p_d and p_{fa} are set to 0.9 and 0.1 respectively. The SNR of malicious users are varied by 0.5 to 1 dB below or above the SNR wall of detection ($\gamma_{wall} = -14$ dB) for incorporating the attacks.

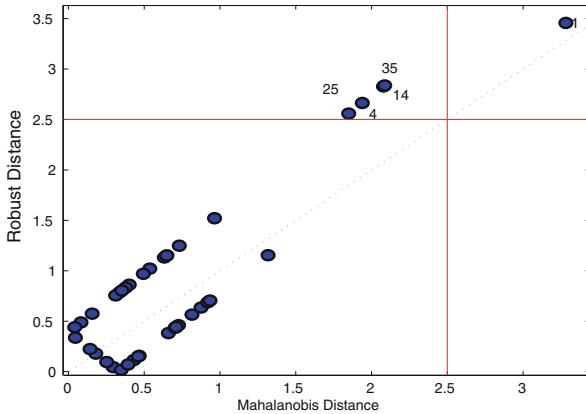


Fig. 2. Mahalanobis vs. Robust distance of cooperative nodes with malicious nodes

The robust and Mahalanobis distance between the SU's are computed using Eqs. (3) and (6) respectively. Further, Fig. 2 compares both the distances in a single plot. This plot shows that the node 1 is largely deviated from the remaining nodes, hence is identified by both the distances.

Further, the Receiver Operating Characteristics (ROC) curves of the random attack are depicted in Fig. 3. It compares the cooperative detection probability (C_d) of the proposed RD with MD, GESD, TT and Grubbs methods. The random attack can be handled easily using Grubbs test and TT as the entropies deviate and spread in a wide range. Hence, the detection probability of Grubbs test and TT is higher than the other methods.

The cooperative detection probability (C_d) of the ‘always high’ attack for varying the number of malicious users is depicted in Fig. 4. It is observed that the C_d decreases as the number of malicious user increases from $M = 1$ to 4.

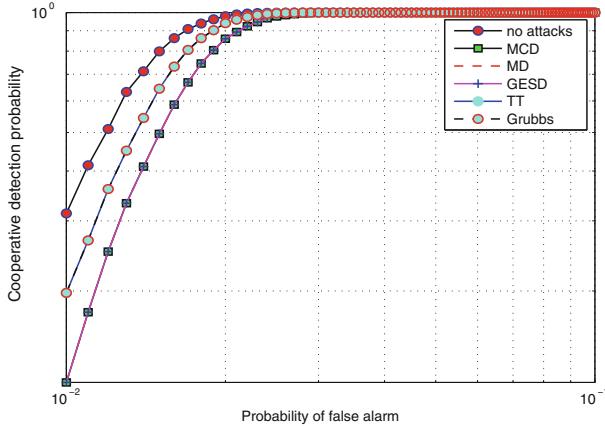


Fig. 3. Comparision of the receiver operating characteristics for random attack with 4 malicious users ($M = 4$)

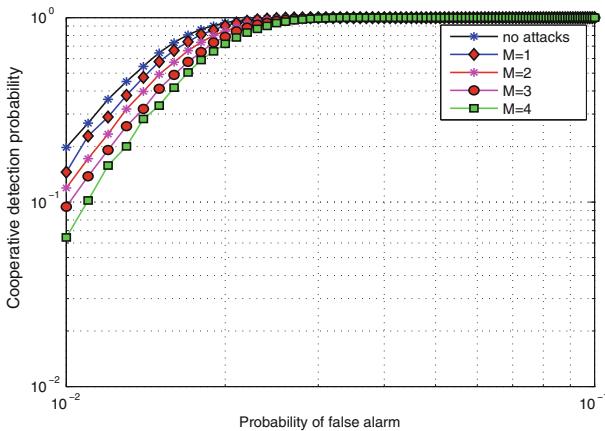


Fig. 4. Comparision of the receiver operating characteristics for ‘always high’ attack by varying the number of malicious users from $M = 1$ to 4

Next, the detection performance for $M = 2$, $M = 4$ is plotted in Figs. 5. The RD test detects the malicious users without any apriori knowledge of M . However, if the upper bound is specified as 4, GESD and TT erroneously nullifies four users out of which two are malicious users and two are not. The Grubbs and MD tests cannot identify them.

The cooperative detection probability (C_d) of the ‘always low’ attack using different test techniques for $M = 2$ as shown in Fig. 6. In ‘always low’ scenario, the interference increases due to low SNR (below SNR wall). It is evident from

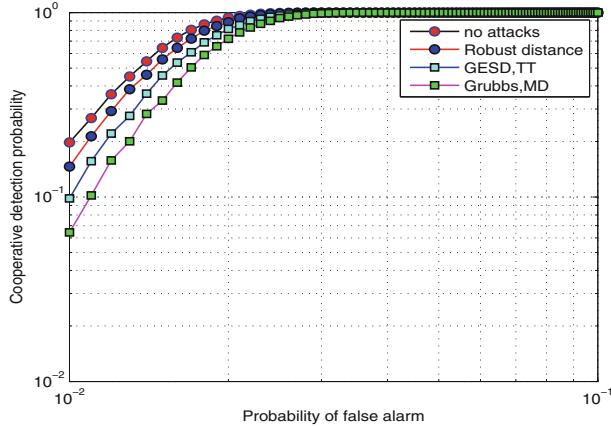


Fig. 5. Comparision of the receiver operating characteristics for ‘always high’ attack; $M = 2$

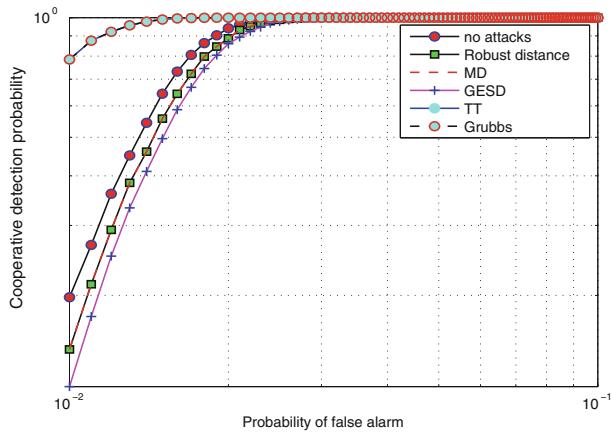


Fig. 6. Comparision of the receiver operating characteristics for ‘always low’ attack; $M = 2$

the figures that the C_d of the proposed RD method is higher than the MD and GESD techniques. On the other hand, the Grubbs and TT tests fail to identify the malicious users showing abnormal C_d (higher than no attacks) because of low entropy values.

Hence, the adverse effects of more than 10% malicious users are nullified using the proposed univariate MCD method.

6 Conclusion

A blind outlier detection scheme is proposed using robust distance based on MCD for efficient cooperative spectrum sensing. The current malicious detection techniques either require an upper bound or limited by the percentage of malicious users in the CR network. The proposed approach suppresses a significant number of malicious users by computing the robust distance between the samples having a minimum determinant. The performance of the scheme is tested for various types of SSDF attacks. The main advantages of the proposed RD method is that it does not require any upper bound on the number of malicious users in the network. This work can be extended by applying neural networks with quite a large sample set and observations.

References

1. Srinu, S., Sabat, S.L.: Cooperative wideband spectrum sensing in suspicious cognitive radio network. *IET Wirel. Sens. Syst.* **3**(2), 153–161 (2013)
2. Marinho, J., Granjal, J., Monteiro, E.: A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIP J. Inf. Secur.* **2015**(1), 1–14 (2015)
3. Zhang, L., Ding, G., Wu, Q., Zou, Y., Han, Z., Wang, J.: Byzantine attack and defense in cognitive radio networks: a survey. *IEEE Commun. Surv. Tutor.* **17**(3), 1342–1363 (2015)
4. Duggineni, C., Chari, K.M.: Mitigation strategy against ssdf attack for healthcare in cognitive radio networks. *Int. J. Biomed. Eng. Technol.* **27**(1–2), 33–49 (2018)
5. Hubert, M., Rousseeuw, P.J., Van Aelst, S.: Multivariate outlier detection and robustness. *Handb. Stat.* **23**, 263–302 (2005)
6. Kaligineedi, P., Khabbazian, M., Bhargava, V.K.: Malicious user detection in a cognitive radio cooperative sensing system. *IEEE Trans. Wirel. Commun.* **9**(8), 2488–2497 (2010)
7. Li, H., Han, Z.: Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks. *IEEE Trans. Wirel. Commun.* **9**(11), 3554–3565 (2010)
8. Bhattacharjee, S., Marchang, N.: Malicious user detection with local outlier factor during spectrum sensing in cognitive radio network. *IJAHC* **30**(4), 215–223 (2019)
9. Maric, S., Reisenfeld, S., Abbas, R.: Combating SSDFA reputation mining and reset attacks in cognitive radio networks. In: IEEE Region Ten Symposium (Ten-symp), pp. 40–44 (2018)
10. Ghaznavi, M., Jamshidi, A.: A reliable spectrum sensing method in the presence of malicious sensors in distributed cognitive radio network. *IEEE Sens. J.* **15**(3), 1810–1816 (2015)
11. Sharifi, A.A., Niya, M.J.M.: Defense against SSDF attack in cognitive radio networks: attack-aware collaborative spectrum sensing approach. *IEEE Commun. Lett.* **20**(1), 93–96 (2016)
12. Wang, W., Li, H., Sun, Y.L., Han, Z.: Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks. *EURASIP J. Adv. Signal Process.* **2010**(1), 1 (2009)

13. Wang, W., Chen, L., Shin, K.G., Duan, L.: Thwarting intelligent malicious behaviors in cooperative spectrum sensing. *IEEE Trans. Mob. Comput.* **14**(11), 2392–2405 (2015)
14. Sharma, R.K., Rawat, D.B.: Advances on security threats and countermeasures for cognitive radio networks: a survey. *IEEE Commun. Surv. Tutor.* **17**(2), 1023–1043 (2015)
15. Prasain, P., Choi, D.-Y.: Nullifying malicious users for cooperative spectrum sensing in cognitive radio networks using outlier detection methods. In: *Ubiquitous Computing Application and Wireless Sensor*, pp. 123–131. Springer (2015)
16. Zhang, Y.L., Zhang, Q.Y., Melodia, T.: A frequency-domain entropy-based detector for robust spectrum sensing in cognitive radio networks. *IEEE Commun. Lett.* **14**(6), 533–535 (2010)
17. Swetha, N., Sastry, P.N., Rao, Y.R., Sabat, S.L.: Parzen window entropy based spectrum sensing in cognitive radio. *Comput. Electr. Eng.* **52**, 379–389 (2016)
18. Cai, Q., He, H., Man, H.: Spatial outlier detection based on iterative self-organizing learning model. *Neurocomputing* **117**, 161–172 (2013)
19. Kalamkar, S.S., Banerjee, A., Roychowdhury, A.: Malicious user suppression for cooperative spectrum sensing in cognitive radio networks using Dixon’s outlier detection method. In: *National Conference on Communications (NCC)*, pp. 1–5. IEEE (2012)
20. Kalamkar, S.S., Singh, P.K., Banerjee, A.: Block outlier methods formalicious user detection in cooperative spectrum sensing. In: *IEEE79th Vehicular Technology Conference (VTC Spring)*, pp. 1–5. IEEE (2014)
21. EN ETSI: 300 744 v1. 6.1 2008–2009: European standard (telecommunications series) digital video broadcasting (DVB). Framing structure, channel coding and modulation for digital terrestrial television (2009)



Smart Irrigation Alert System Using Multihop Wireless Local Area Networks

C. V. N. S. Lalitha, M. Aditya, and Manoj Panda^(✉)

Department of Electronics and Communication Engineering,
Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India
cvnslalitha@gmail.com, adityamnair97@gmail.com,
mk_panda@cb.amrita.edu

Abstract. From past decades, India is an agriculture-based country where the majority of the population is heavily dependent on farming. However, energy management and resource conservation continues to be the major issues in agricultural domain. The main motivations of this research is to conserve water which is a fast depleting source, and also automates the process of watering in order to reduce human workload in remote areas. In this paper, a smart irrigation alert system is developed using NodeMCU boards, a soil moisture sensor and a servo motor. The sensor measures the volumetric content of water in the soil and data is uploaded to the cloud. The main challenge addressed in this research is to seamlessly connect multiple Node MCUs to a sink (or, gateway) node such that the data can be uploaded to the cloud. Two topologies are considered. The first one is the star topology which is efficient for a kitchen garden where each of the plants is in close proximity of the sink. The second one is the multi-hop topology which is necessary in a big agriculture field. The soil moisture is sensed using multiple FC-28 sensors and uploaded to the cloud. When the moisture content drops below the threshold value, an alert notification is sent to the subscriber by e-mail and automatic watering follows by actuating the servo motor. The user can monitor and control the status of watering anywhere through the Internet. The integration of sensors, cloud and the servo motor through multiple Node MCUs is the main novelty of this work.

Keywords: Internet of Things (IoT) · Node Micro Controller Unit (Node MCU) · Automatic irrigation system · Wireless sensor networks

1 Introduction

Farming has gone through much technological advancement in recent times. Internet of Things (IoT) has the potential to bring a shift from the traditional methods to modern agriculture. The data collected by the sensors such as climatic conditions, soil, moisture content, temperature, humidity help us to monitor the crop's progress [1]. It is also cost-efficient and helps in the reduction of wastage. If the efficiency of the system increases, labor work force is reduced. The data obtained can be used to decide the right crops for the climatic conditions present and increase the crop yield as well to boost productivity [2, 13].

Keeping the soil moisture values in focus, a predetermined value range for soil moisture is set according to soil type. The automatic irrigation system works without any human intervention. The major reason behind this “Smart Irrigation Alert System” with automatic watering is to make use of the emerging Internet of Things to reduce human labor of watering plants under strenuous conditions and to tackle the problem of water scarcity by making judicious use of this depleting resource [3, 6]. The connection of the Node MCUs is done first by a single hop and then expanded to multiple intermediate nodes that act as repeaters to transmit the data. Serial communication takes place among the Node MCUs.

2 Ease of Use

This experimental setup is applicable to both small-scale kitchen garden design as well as a big crop field used for farming. The initial budget will be moderately high but once the system is set up, it requires zero or very less maintenance. Day and night 24×7 monitoring of the farm can be done from any part of the world. This will reduce the human workload especially in remote areas. The statistics collected gives us updates at intervals about the status of the physical or soil condition [4]. Manual intervention is not required. Internet access and a Google mail account is a must for this setup [5].

3 Literature Survey

The monitoring of climatic conditions is done by collecting the data from various weather stations. This data can be used to match the climate conditions, select the right crops and do the necessary to increase production. Precision method is a major method for crop management. Data is collected by sensors to monitor the crop’s progress. Open Garden Shield for Arduino provides input-output connectors for agriculture purposes. It involves the usage of a radio frequency module with 433 MegaHertz frequency. To read soil moisture values, analog I/O, analogRead() and analogWrite() should be used. A common gardening water system which is used in houses uses one power supply, suitable for these water valves. A smart irrigation system consisting of a microcontroller Atmega 328 which is the heart of the system. The moisture and tempearture sensors are connected to the input pins of the microcontroller [14]. If the sensors diverge from the specific range, the controller turns on pump. The android application controls the water pump by GSM network which sends an SMS to the farmer’s mobile number. Water efficiency isn’t there in the previous irrigation methods. Quantity of water required is not specific in irrigation system [15].

4 Hardware System Components

The Node MCU runs on the ESP8266 System-On-Chip Wi-fi Module with Arduino core and its hardware is based on ESP 12 module. This is a microcontroller which is an open source IoT platform that helps to connect to the internet for IoT related projects.

The firmware uses the Lua scripting language. The Node MCU supports the Message Queuing Telemetry Transport (MQTT) protocol designed for subscribing and publishing messages to and from the Internet. It consists of a client communicating server where the client can be a subscriber or a publisher. The Node MCU has a memory of 128 KB and is powered by connecting to a computer system via a USB cable [7].

The FC-28 hygrometer sensor is used for measuring the moisture level in the soil. It consists of two flat conductors separated by air. The moisture is measured using the amount of resistance between the electrodes. If high moisture is present, then the resistance will be low. If moisture level is low, then the resistance will be high. Moisture value is depicted in percentage values from a minimum of 0 to a maximum of 1023 based on an internal algorithm [8, 11].

5 Software Used

The Arduino Integrated Development Environment is used to write and upload programs to the boards based on Arduino core. The libraries used for this project are “ESP8266.h” and “Servo.h” for Node MCU and the servo motor respectively. Arduino 1.8.2 has been used in the proposed system [9, 10].

If This Then That (IFTTT) is a web-based service to create ‘applets’ which are conditional statements. These statements are triggered to carry out a specified action such as sending mail alerts or app notifications when a condition is satisfied.

ThingSpeak is an open source IoT platform to store and retrieve data over the internet using HTTP (HyperText Transfer Protocol). It allows sensor logging application, location tracking application and data monitoring [12].

6 The Proposed System

The steps to be followed for collecting the data from a single sensor are as follows (Fig. 1):

- A sample plant was taken and a FC-28 soil moisture sensor was used to collect the data.
- During the initial phase, a single Node MCU was used to upload data to the cloud, [ThingSpeak.com](https://thingspeak.com).
- The code for the same was written in Arduino 1.8.2. To upload the data, a unique ThingSpeak API key was generated and used.
- The user ID and password of the hotspot to be used to connect the Node MCU to the Internet is also included in the code.
- The sensor readings are continuously displayed in the serial monitor as well as real time uploading in the cloud takes place.
- A servo motor was also connected to the controller and configured to open the pump when the moisture level went below a certain threshold and close it after a time interval.

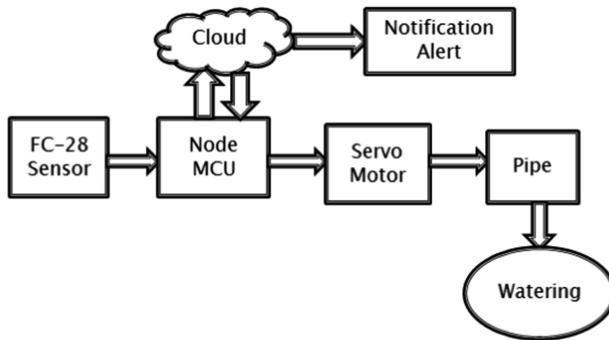


Fig. 1. Block diagram of the system.

As the project progressed, multiple Node MCUs were connected in a star topology. Multiple sensors were connected to multiple MCUs.

- These MCUs were configured as Station Points (Clients) to connect to a central node, the Access Point (Server) through which data will be uploaded to the cloud.
- A channel was created for data feed in [ThingSpeak.com](#).
- An applet was created in IFTTT, where conditions for the trigger were provided. The condition was: “If Maker event Moisture Alert then send yourself an email from xxxx@gmail.com”. A URL from ThingSpeak is taken into use in the applet for the data required for the trigger.
- A Web hook is provided to request for a web service which is to get the data from [ThingSpeak.com](#).

Once the entire system starts functioning, the applet becomes active and continuously sends mail alerts every time the condition is satisfied (Fig. 2).

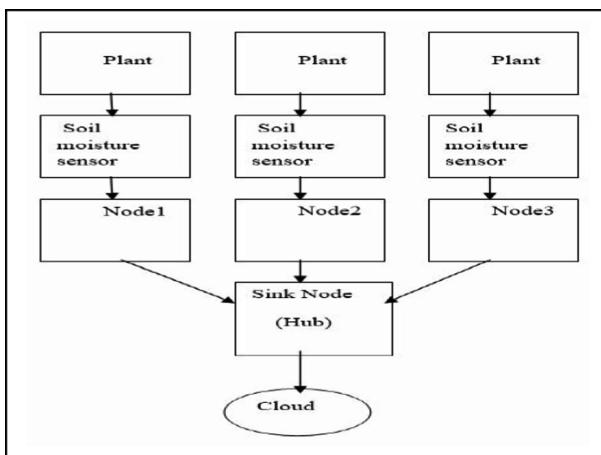


Fig. 2. Star topology system modules.

The multi- hopping arrangement was developed as follows:

- The sensor reading was sent to a Node MCU which sent it to another Node MCU. The nodes acted both as a client and as a server to receive it from one node and send it to another.
- The sensor reading is sent to the Node MCU which in turn gets connected to the closest Access Point and sends an HTTP request to its server with the data.
- The data is received by the middle Node MCU which is programmed to listen and receive the readings configuring the middle Node MCU to act as Access Point and Station Point at the same time.
- Each Node MCU was assigned a unique SSID (Service Set Identifier) that is used for naming the wireless networks. When multiple wireless networks overlap in a certain location, SSIDs make sure that data gets sent to the correct destination.
- After three hops, these hops can be modified based on the number of NodeMCUs being added. Then the final node (sink node) uploads the data to the cloud and the entire process of conditional checking and notification alert takes place. This step, in principle, can be repeated as many times as required.
- This topology will be able to cover maximum area of the field by using the Node MCU as signal repeaters.
- Finally, a servo motor SG-90 is connected to the root Node MCU connected to the sensor which will rotate as an indication of water flow (Fig. 3).

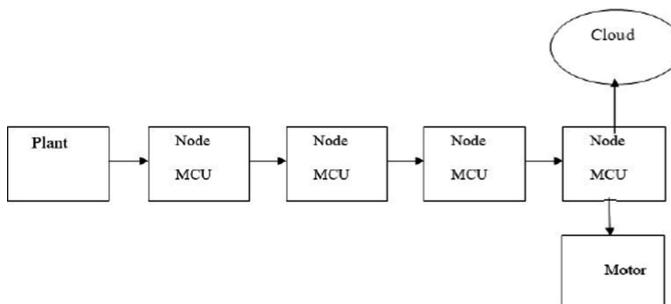


Fig. 3. Multihop topology system modules.

In multi-hop system each Node MCU is programmed to receive data, read the sensors and connect to the nearest Node MCU available. It can create Wireless Local Area network to which any wi-fi enabled device can make a connection. We can set SSID and password for AP mode which will be used to authenticate other devices while connecting to it. The continuous stream of bytes is transferred to the destination in packets. This will help us to know the availability and status of the database along with the sensor readings. In the end, the data gets uploaded into the ThingSpeak IoT platform through the internet router or it retains the data in memory until internet is available.

In the star topology for a kitchen garden system all the nodes are individually connected to one common node. We can cover upto seven individual nodes to the sink node. And by combining multihop along with star topology, a large area of land is covered. Even if one link fails, the system will work.

7 Experimental Results

The FC-28 soil moisture readings are collected in Arduino serial monitor and then uploaded to ThingSpeak cloud platform (Fig. 4).

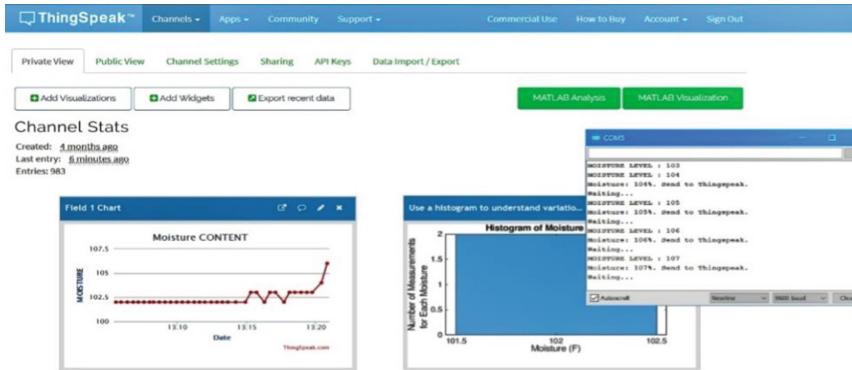


Fig. 4. Uploading of sensor value to cloud (single hop).

Multiple Node MCUs are taken and connected together. The receiving of bytes from the AccessPoint and to the Station point is seen in the serial monitor (Fig. 5).

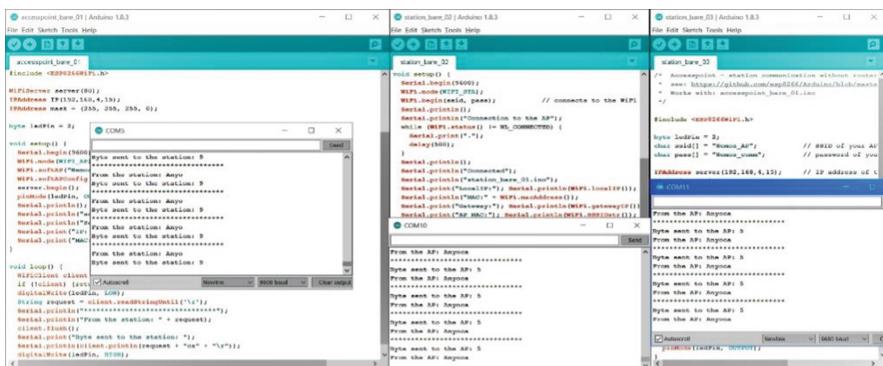


Fig. 5. Connection of node MCUs.

A notification alert is sent to the user when the moisture drops below a threshold level (Fig. 6).

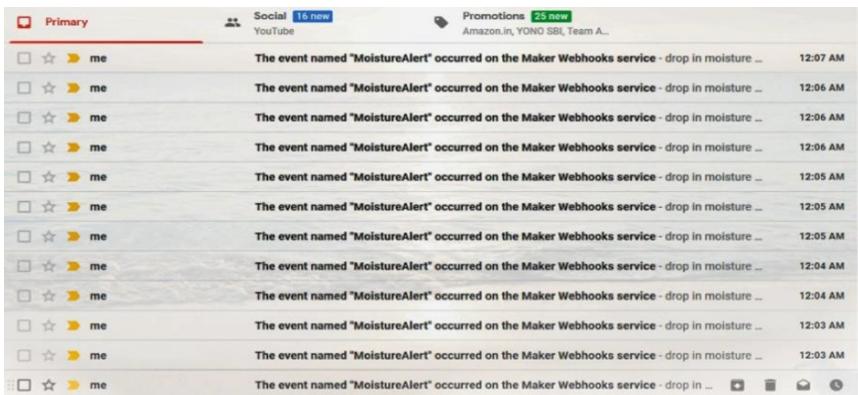


Fig. 6. Notification alert through google mail.

Uploading of the sensor values through Node MCUs is done and the final readings are updated in the cloud (Fig. 7).

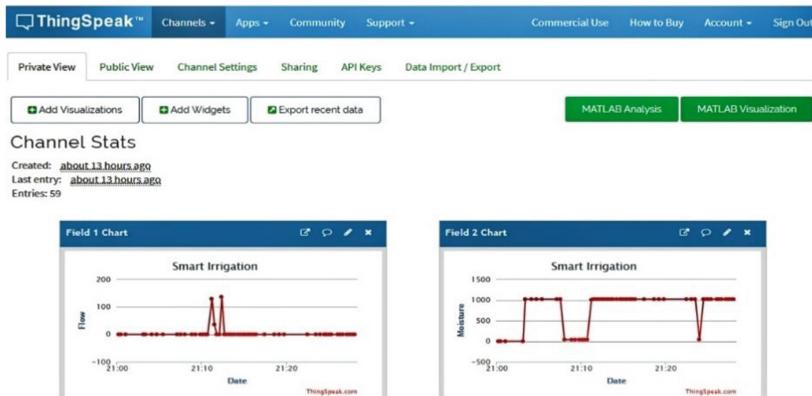


Fig. 7. Uploading of sensor values to cloud.

8 Conclusion

Agriculture, being majorly dependent on irrigation has been affected the most. The aim of the project was to develop an automatic watering system with the underlying was to make this irrigation system a helping hand for farms/gardens in rural areas. In such places where internet access and connectivity would be low, the concept of multi hopping was brought into the picture. Data will be forwarded between multiple Node

MCUs till the nearest internet access (the sink node) and will then be uploaded to the cloud. The system can be made better by measuring the water level in the tank also and notifying the farmer.

References

1. Joshi, A., Ali, L.: A detailed survey on auto irrigation system. In: IEEE Conference on Emerging Devices and Smart Systems (2017)
2. Rajkumar, N., Abinaya, S., Venkatesa Kumar, V.: Intelligent irrigation system- an IoT based approach. In: IEEE International Conference on Innovations in Green Energy and Healthcare Technologies
3. Shah, S.H., Yaqoob, I.: A survey: Internet of Things (IoT) technologies, applications and challenges. In: 4th IEEE International Conference on Smart Energy Grid Engineering (2016)
4. Giri, M., Wavhal, D.N.: Automated intelligent wireless drip irrigation using linear programming. *Int. J. Adv. Res. Comput. Eng. Technol.* **2**(1), 1–5 (2013)
5. Ramu, M., Rajendra Prasad, C.H.: Cost effective atomization of Indian agricultural system using 8051 microcontroller. *Int. J. Adv. Res. Comput. Commun. Eng.* **2**(7), 2563–2566 (2013)
6. Dinesh Kumar, N., Pramod, S., Sravani, Ch.: Intelligent irrigation system. *Int. J. Agric. Sci. Res.* **3**(3), 23–30 (2013)
7. Raut, J., Shere, V.B.: Automatic drip irrigation system using wireless sensor network and data mining algorithm. *Int. J. Electron. Commun. Comput. Eng.* **5**(07), 195–198 (2014)
8. Kavianand, G., Nivas, V.M., Kiruthika, R., Lalitha, S.: Smart drip irrigation system for sustainable agriculture. In: 2016 IEEE Technological Innovations in ICT for Agriculture and Rural Development (TIAR), pp. 19–22. IEEE (2016)
9. Rajalakshmi, P., Devi Mahalakshmi, S.: IOT based crop-field monitoring and irrigation automation. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–6. IEEE (2016)
10. Sales, N., Remýdios, O., Arsenio, A.: Wireless sensor and actuator system for smart irrigation on the cloud. In: IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 693–698 (2015)
11. Nilson, K., Sharmila, G., Praveen Kumar, P.: Intelligent auto irrigation system using ARM processor and GSM. In: International Conference on Innovative Trends in Electronics Communication and Applications 2015, pp. 36–40 (ICIECA 2015) (2015). ISBN 978-81-929742-6-2
12. Viswanathan, A., Shibu, N.S.B., Rao, S., Ramesh, M.V.: Security challenges in the integration of IoT with WSN for smart grid applications. In: 2017 IEEE International Conference on Computational Intelligence and Computing Research(ICCIC), Coimbatore (2017)
13. Varman, S.A., Baskaran, A.R., Aravindh, S., Prabhu, E.: Deep learning and IoT for smart agriculture using WSN. In: 2017 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2017 (2018)
14. Ramesh, S., Smys, S.: Performance analysis of heuristic clustered (HC) architecture in wireless networks. In: 2017 International Conference on Inventive Systems and Control (ICISC), pp. 1–4. IEEE (2017)
15. Smys, S., Bala, G.J., Raj, J.S.: Self-organizing hierarchical structure for wireless networks. In: 2010 International Conference on Advances in Computer Engineering (ACE), pp. 268–270. IEEE (2010)



Real Time Health Monitoring System Using IoT

Bhagyashree Behara^(✉) and Manisha Mhetre

Department of Instrumentation, Vishwakarma Institute of Technology,
Pune 411037, India
{bhagyashree.beharal7, manisha.mhetre}@vit.edu

Abstract. Timely health monitoring is essential to diagnose severe health condition at an early stage. With the recent technological advancements, we can obtain the recommendations of doctor from anywhere and at anytime. This is all possible with a wearable and remote monitoring system. In this paper we are implementing data acquisition system using Arduino Uno & RPi. Various health parameters like temperature, pulse and ECG, can be monitored. The acquired data is pre-processed and sent to server i.e. IoT cloud platform Thinspeak. The main aim of this research work is to develop a remote health monitor system, which can reduce the expenses made on frequent hospital visits.

Keywords: IoT · Thingspeak · ECG · Heart rate · RPi

1 Introduction

The health monitoring system is one of the best examples of IoT applications. Previously different technologies such as GSM, RFID, Zigbee, Arduino, etc. were used in a healthcare monitoring system. But in this project, we have used Raspberry Pi, a next-generation evolution in IoT, which has the outstanding processing and networking capability with less man-machine interferences. As the Medical treatment is getting more expensive day-by-day and with old age the mobility of patients get decreased. Having a routine check becomes as an essential component for a healthy life. The objective of this paper is to develop a low-cost health monitoring system using IOT. With a lot of design & development in biomedical field especially in remote health monitoring domain The wearable biomedical device has gained enough popularity over a year, with a lot of design & development in biomedical field especially in remote health monitoring domain. Internet-of-Things provide a platform for low power embedded devices to get connected to the internet. Internet access provides a capability for remote monitoring and data visualization, which is done using Thingspeak. This paper aims to find easy methods to determine ECG, Heart Rate and body-temperature. Moving away from traditional method to remote health monitoring system is an modern approach to reduce the time consumption in Hospital. Bio medical device is on trend to provide a better health care system. Various innovative technologies are being implemented to improve the health of a person with miniature sensor and equipment.

ECG measurement has been carried out by using electrode and AD8232 single lead heart rate sensor module. Heart Rate is calculated by monitoring the QRS complex waveform. Standard ECG time and amplitude are compared with patient data and supportive diagnosis has been implemented with the help of doctor guidelines. LM35 sensor is used for temperature measurement, which is an easy to use 3 pin IC. Also, pulse sensor for pulse measurement. The IoT device used is RPi. RPi does not have analog sensing capability so we are making use of Arduino Uno to connect an analog sensor. Then connecting arduino to Raspberry pi serially over USB. Further transmitting the data to Thingspeak using the Raspberry pi inbuilt Wi-Fi module.

2 Literature Survey

Thus zigbee is used to transmit and receive the data from PIC microcontroller, which connected directly with specified Human body sensors. In [4] 6lowpan node with biomedical sensor placed on the patient body area network for monitoring health parameter. The 6lowpan node has IP-address so it provides real-time feedback of patient to the service provider or doctor. In [5] healthcare system is designed using a microcontroller device and LCD module for monitoring heart rate and body temperature. These parameters are send over internet using a Wi-Fi module. Sudden changes in parameters are reported as alerts. An Arduino uno module interfaced with Wi-Fi module is used in [6] to monitor heart rate and body temperature.

3 Material and Method

3.1 Block Diagram

We are using Raspberry pi 3B+ as the central device in this project. The analog sensor is connected to Arduino Uno as Raspberry pi doesn't have an analog pin. This will also help to increase the number of input to RPi. The arduino is power up over USB. So no external supply is required to power Arduino. The sensor data is sent to raspberry pi serially. The arduino device location is obtained in raspberry pi and set to communicate serially. The temperature, pulse, and ECG sensor data are send Raspberry pi 3 B +. All the sensor are power from Arduinio Board. Also 16 × 2 LCD display is connected to arduino to locally visualise the data.

The Rpi is set over Wi-Fi for internet access using Rpi configuration setting. The data is then sent to Thingspeak for visualization. This data can be accessed from anywhere over the internet. The sensor is calibrated to give an accurate result (Fig. 1).

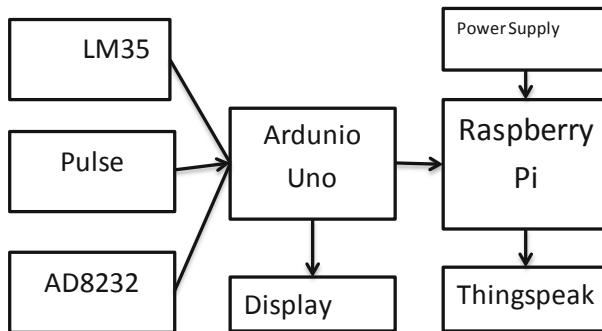


Fig. 1. Block diagram

3.2 Hardware

- LM 35-LM35 are precision temperature IC with an output voltage linearly proportional to the temperature in centigrade, over -55°C to 150°C Temperature Range. Having a linear scale factor of $+10 \text{ mV}/^{\circ}\text{C}$. The low-output impedance, linear output and precise inherent calibration of the LM35 device make interfacing to readout or control circuitry especially easy. Very suitable for remote applications.

Below Fig. 2 shows the actual system setup.

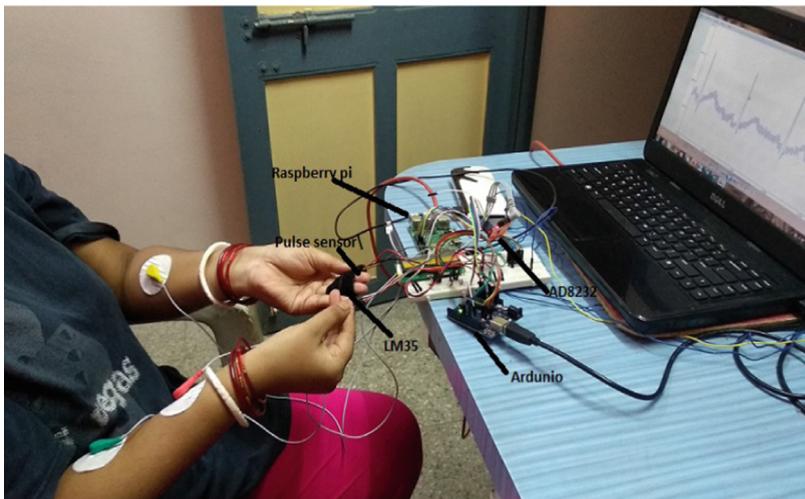


Fig. 2. Actual system setup

3.3 Software

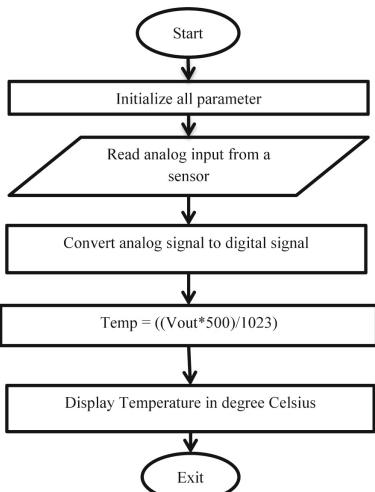
The Arduino Uno is programmed to sense analog parameter in Arduino IDE. To connect and start using RPi on laptop install Putty. For GUI for RPi install Xming.

Download and copy Raspbian OS onto 16 GB SD card. Insert the SD card into RPi and power using 5 V micro USB Charger. The following strategy is implemented in programming and respected flowchart can be found below.

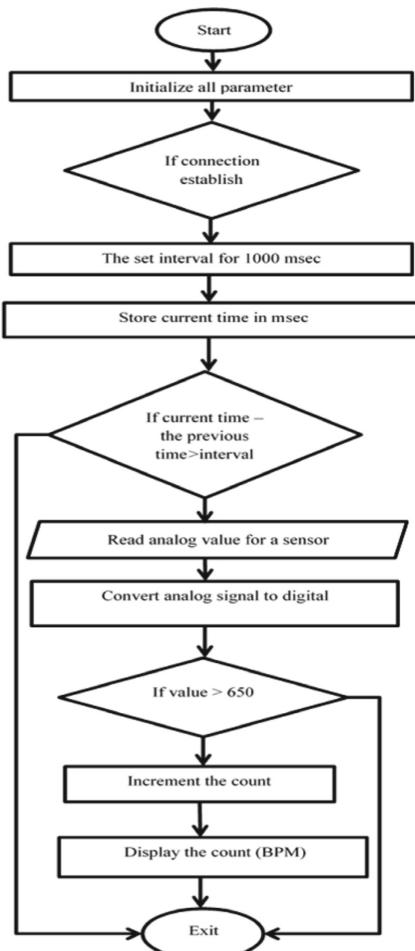
3.4 Flowchart

The temperature is measured by connecting the temperature sensor to analog pin which gives out analog value. The output is directly proportional to temperature in °C. The conversion from °C to °F is also done. The BPM is calculated by implementing following strategy.

1. Temperature measurement



2. The BPM measurement



4 Result

4.1 Temperature Reading

Body temperature for different persons. The normal body temperature range of persons is 97 to 99°F. The body temperature of different person is recorded and given in Table 1.

Table 1. Temperature reading

Patients	Actual reading (°F)	Recorded reading (°F)
A	93.8	91.82
B	94.8	92.70
C	92	90.24
D	95.7	93.58
E	90.3	89.18

4.2 Pulse Reading

Average Pulse rate of person is between 60 to 100 BPM. Pulse rate of different person is recorded and given in Table 2.

Table 2. Heart rate reading

Patients	Actual reading (BPM)	Recorded reading (BPM)
A	60	66
B	75	71
C	80	85
D	83	89
E	62	63

4.3 ECG Graph

Desired ECG signal is obtained and heart rate is calculated from PQRST waveform. The measured waveform can be either be displayed on serial plotter of arduino IDE or processing software can be used. Calculated BPM is send to thingspeak. Figure 3 shows the ECG graph of persons on Serial plotter.

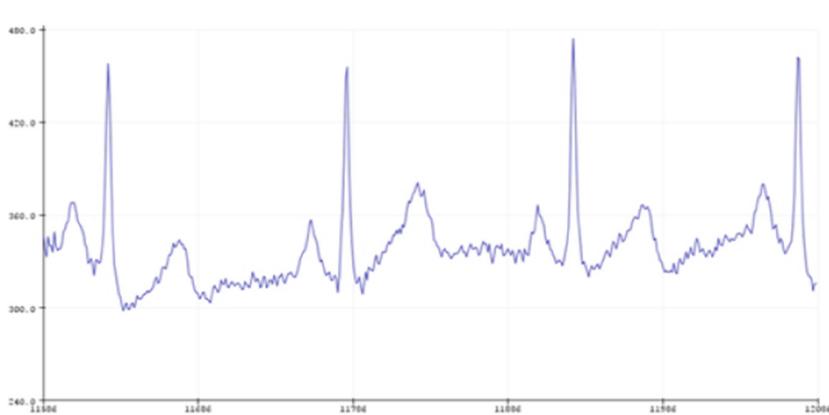


Fig. 3. ECG graph

4.4 Thingspeak Temperature Visualization Window

The data can be sent to server from IoT device having Internet connectivity capability. The connection is establish using RPi inbuilt Wi-Fi. The Wi-Fi is set to connect to router. This setting is done on RPi config windows. To send data we need to channel ID, write API key. That can be obtained once you sign in to thingspeak server. Figure 4 shows the visualizations window for temperature.

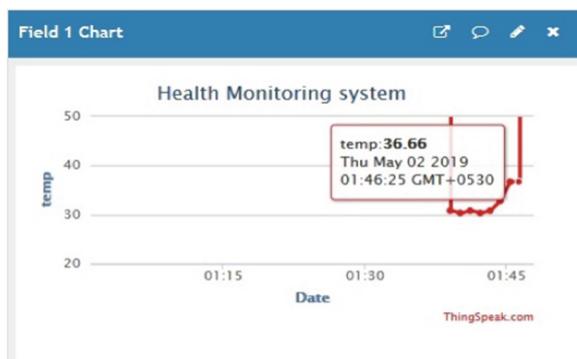


Fig. 4. Temperature visualization window

The BPM obtained is also send to thinspeaks server. Figure 5 shows the heart rate monitoring window for visualizations.

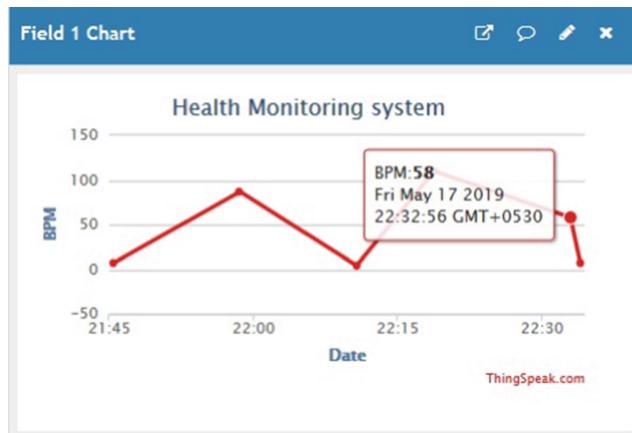


Fig. 5. BPM visualization window

4.5 Android Application on Mobile

Figure 6 Shows the real time data monitoring using android application ThingView-ThingSpeak viewer on mobile. This help in easy access of data. Download the application on to our mobile an use channel ID to access the data over Internet.

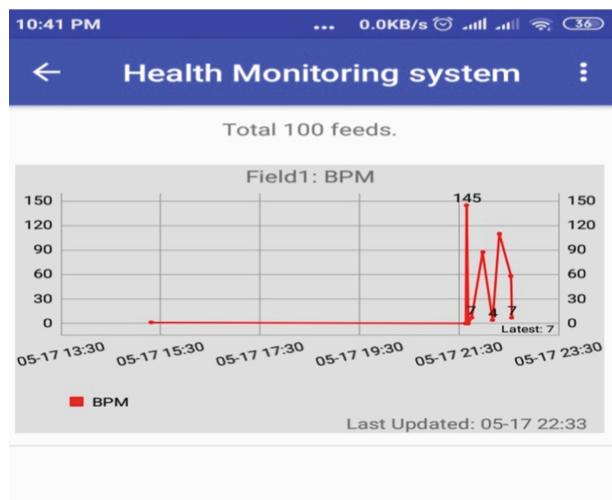


Fig. 6. Android application

5 Conclusion

In this research work, we have developed a remote Healthcare Monitoring system in order to measure the regular health parameter and send the obtained data to doctor for medical examination.

- To safeguard and increase the quality of the human life, which suffers from a lack of hospital apparatus.
- The proposed model will assist the elderly population to track their health condition in a more effective and efficient way.
- This remote monitoring system helps to detect symptoms at earlier stage.
- It can subsequently reduce the time spent at the hospital
- Also, the cost of medical apparatus required for measurement is reduced.

6 Abbreviations

- RPi – Raspberry Pi 3 B+
- IoT- Internet of Things
- ECG- Electrocardiogram
- Wi-Fi- Wireless Fidelity
- BPM- Beat per Minute.

Acknowledgement. This project is funded by the alumni of Instrumentation & Control department at Vishwakarma Institute of Technology, Pune.

References

1. Khan, S.F.: Health care monitoring system in internet of things (IoT) by using RFID. In: 2017 the 6th International Conference on Industrial Technology and Management. IEEE (2017). 978-1-5090-5330-8/17/\$31.00 ©2017
2. Chandrasekhar, T., Chakravarthi, J.S.: Wireless health monitoring system using ZigBee. Int. J. Web Technol. **02**(01) (2013). ISSN 2278-2389
3. Wan, J., Al-awlaqi, M.A.A.H., Li, M.S., O'Grady, M., Gu, X., Wang, J., Cao, N.: Wearable IoT enabled real-time health monitoring system. EURASIP J. Wirel. Commun. Netw. **2018**, 298 (2018)
4. Singh, D., Tiwary, U.S., Lee, H.J., Chung, W.Y.: Global healthcare monitoring system using 6lowpan networks. In: ICACT 2009, 15–18 February 2009. ISBN 978-89-5519-139-4
5. Krishnan, D.S.R., Gupta, S.C., Choudhury, T.: An IoT based patient health monitoring system. In: 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE-2018), Paris, France, 22–23 June 2018
6. Gómezá, J., Oviedo, B., Zhumab, E.: Patient monitoring system based on Internet of Things. In: The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016) (2016)

7. Dubey, R.K., Mishra, S., Agarwal, S., Sharma, R., Pradhan, N., Saran, V.: Patient's health monitoring system using the Internet of Things (Iot). *Int. J. Eng. Trends Technol. (IJETT)* **59** (3) (2018)
8. Raj, C., Jain, C., Arif, W., HEMAN: health monitoring and nous: an IoT based e-health care system for remote telemedicine. In: IEEE WiSPNET 2017 Conference (2017)
9. Banka, S., Madan, I., Saranya, S.S.: Smart healthcare monitoring using IoT. *Int. J. Appl. Eng. Res.* **13**(15), 11984–11989 (2018). ISSN 0973-4562
10. Saranya, M., Preethi, R., Rupasri, M., Veena, S.: A survey on health monitoring system by using IOT. *Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET)*. ISSN: 2321-9653. IC Value: 45.98; SJ Impact Factor: 6.887
11. Senthamilarasi, C., Jansi Rani, J., Vidhya, B., Aritha, H.: A smart patient health monitoring system using IoT. *International Journal of Pure and Applied Mathematics* **119**(6), 59–70 (2018). ISSN 1314-3395 (on-line version)
12. www.ti.com/lit/ds/symlink/lm35.pdf
13. <https://www.analog.com/media/en/technical-documentation/data-sheets/ad8232.pdf>
14. <https://static.raspberrypi.org/files/.../Raspberry-Pi-Model-Bplus-Product-Brief.pdf>



Performance Analysis of Optimization Algorithms Using Chirp Signal

K. Anuraj^(✉) and S. S. Poorna

Department of Electronics and Communication Engineering,
Amrita Vishwa Vidyapeetham, Amritapuri, India
anuraj19@gmail.com

Abstract. In order to evaluate the material characteristics and defects, different input signals are allowed to pass through the material. These signals are able to capture the hidden information regarding the material while traversing through it. These material signatures can be obtained by analyzing the reflected signals. This enables us to study the material properties and defects non-invasively. The different input signals can be modelled as Chirp signal, Gaussian echo, combination of echoes, etc. In this paper, analysis is done using chirp as the input signal. The parameter estimation is done using Maximum Likelihood and different optimization techniques are adopted for minimizing the error. Eventhough the results obtained for all optimization algorithms are comparable with the actual parameters, Levenberg-Marquardt algorithm gave the best fit, with minimum average absolute relative error.

Keywords: MLE · Chirp · Parameter estimation · ARE · AS · LM · SQP · TRR

1 Introduction

Parameter estimation involves calculating the approximate values of the parameters extracted from the reflected input signals. It is used in the areas pertaining to the stability analysis of rotorcraft and estimation of control derivative for designing reliable helicopter models. Mathematical and numerical method of parameter estimation and optimization are used in diverse streams like medicine, biology, environmental physics, chemistry, computer vision and image processing. The above mentioned applications are carried out using various input signals, comprising of different parameters used for diverse applications. Choice of input varies based on the applications, and the parameters are specified accordingly.

An echo signal is used for aberration detection, pattern recognition and classification [4]. The parameter estimation from ultrasonic vibrations are deployed in areas such as characterising and evaluating the structural integrity of the materials used as reflectors and in flaw detection [5, 10]. Laddada et al. [8] conducted a study on modelling of the signal and parameter estimation with Gaussian echo, using

Levenberg-Marquardt algorithm. Demirli et al. [9] have proved that the estimated parameters are unbiased and the analytical Carmer-Rao Lower Bound (CRLB) is achieved with the help of Monte-Carlo simulations.

The chirp signal is used in radar or sonar signal for estimating the location of an object during surveillance. It can also be employed for matched-filtering in the aforementioned systems [1]. Parameter estimation of chirp signals find applications in image processing as well [2]. Chirp signals helps to provide an error free digital modulation in situations where interference elimination is required [3]. In some of the applications, the phase based frequency estimation of chirp signal is done by phase unwrapping [6]. Kundu et al. [7] proposed the least square estimation technique to compute the unknown parameters of the chirp signal. In this work, the chirp signal is estimated using Maximum likelihood Estimation (MLE) and a set of optimized parameters are obtained through various optimization algorithms.

2 Chirp Signal Modelling

The specifications of reflected echoes will carry some valuable data with regard to the characteristics of the material. In order to record aforementioned features from reverberations, parameters ought to be estimated from the noisy echo using MLE [11]. MLE can handle huge amount of data, since it is less complicated. The backscattered echo can be viewed as a noise altered chirp signal given in Eq. 1.

$$Y(t) = s(u, t) + n(t) \quad (1)$$

where $Y(t)$ represents the received backscattered echo, $n(t)$ is considered as Additive White Gaussian Noise (AWGN). Different parameters of this echo are taken as a set of vectors, represented in Eq. 2.

$$u = [fs f_0 \alpha] \quad (2)$$

where f_s implies sample frequency, f_0 represents the added frequency and α , the phase of the echo. Hence $s(u, t)$ is the chirp echo model, as defined in Eq. 3.

$$s(u, t) = \cos\left(2\pi\left(\left(\frac{f_s}{20} - f_0\right)/2\right)t + f_0\right)t + \alpha \quad (3)$$

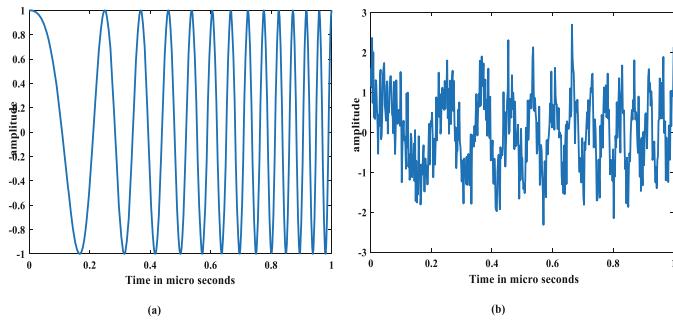


Fig. 1. (a) Original chirp signal (b) Noise altered chirp signal

3 Parameter Estimation

3.1 Maximum Likelihood Estimation

Parameter estimation is done in order to obtain the information related to the features of the material. To obtain those features, the above mentioned parameters are estimated using Maximum Likelihood Estimation (MLE). A predefined model is necessary to perform MLE and hence the ultrasonic input signal associated with an AWGN component is assumed. The parameters extracted from chirp signal are sampling frequency, centre frequency and phase. AWGN is independent and identically distributed with mean zero. Hence the covariance of the distribution will be the expected value of the squared difference between the transmitted and received signals [5]. Normally, MLE estimates the required parameters by maximizing the log likelihood function or equivalently least square minimization in the presence of AWGN.

3.2 Optimization

Least square curve fitting problem cannot yield a perfect solution on single iteration. Optimization algorithms serve as a solution to this. The initial values as well as the number of iteration are chosen adequately for the algorithm to converge to global minima. Many optimization algorithms such as, Levenberg-Marquardt (LM), Trust-Region Reflective (TRR), Active Set (AS), Quasi Newton (QN) and Sequential Quadratic Programming (SQP) can be used for this purpose [5]. These algorithms minimize a non-linear function, yielding optimal solution. The Levenberg-Marquardt algorithm assumes the initial parameters and iterates them successively, along minimum gradient direction. The Trust-Region Reflective algorithm assumes the objective function to be bounded and minimizes it. To obtain the optimized value initially, the objective function is approximated to the quadratic function which represents the trust region. Now the quadratic function area is minimized in iterative steps and the trust region dimension is changed accordingly. The Active Set algorithm uses inequality constraints to obtain an optimum solution for the objective function. A feasible region near the solution of the objective function is identified such that the constraints are greater than zero. The Quasi Newton method is a subclass of variable metric method

and is based on Newton's method. This is used to obtain the extremes of the objective function for which gradient is null and in the case where Hermission matrix computation is tedious. The Sequential quadratic programming method is used if the objective function is differentiable twice with respect to the constraints and gets reduced to Newton's method when the gradients are eliminated. A detailed description of these algorithms is explained in the previous paper [5].

4 Results and Discussion

For analysis, Chirp signal is added with WGN of SNR values 0 dB, 5 dB, 10 dB, 15 dB and 20 dB. The sample plots of input chirp signal and the 5 dB noise altered chirp echo are shown in Fig. 1. The original parameters associated with the chirp signal are selected as sampling frequency $f_s = 500$ MHz, center frequency $f_0 = 1$ MHz and phase $\alpha = 0$.

The optimization algorithms: Levenberg-Marquardt, Trust-Region Reflective, Active Set, Quasi Newton and Sequential Quadratic Programming are evaluated on noisy chirp signal for parameter estimation. For the perfect functioning of the optimization algorithms the selection of optimum intial guess is crucial. The initial guess for the chirp signal is obtained as [492 0.9 0], by iteration. This initial value helps the optimization algorithms to converge with minimum error. For each parameter estimation with optimization, Monte Carlo stimulations are carried out for 10,000 iterations and the results are obtained.

The parameter estimation using different optimization algorithms for various SNR values are given in Table 1(a) to (e). The average absolute relative error is used as an indicator for analysing the goodness of fit using optimization algorithms. Another method to improve estimation by de-noising the chirp waveform before optimization as followed in paper [5] is also adopted here. Analysis was done using Symlet-29 wavelet with level 4 de-noising. The results obtained show little improvement in estimating the parameters and hence the de-noising technique was not adopted.

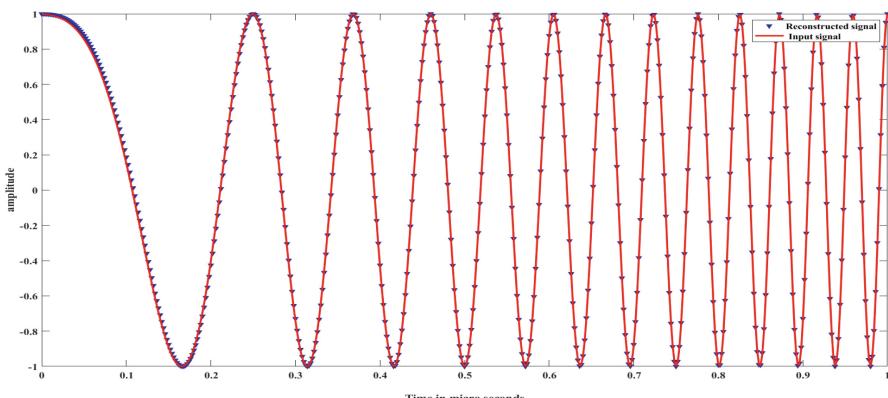


Fig. 2. Reconstructed signal along with the input after Levenberg-Marquardt algorithm

Table 1. Estimated parameters from noisy chirp using (a) LM (b) TRR (c) AS (d) QN (e) SQP algorithms for different levels of SNR

LM algorithm			TRR algorithm		
	f_s (MHz)	f_0 (MHz)		f_s (MHz)	f_0 (MHz)
0 dB	499.5784	1.008217	0.027897	504.1072	0.831582
5 dB	498.3203	1.0792	-0.0907	501.2244	0.957658
10 dB	500.273	1.001673	-0.0048	500.1517	1.010239
15 dB	499.9346	0.998493	0.013705	500.357	0.993643
20 dB	499.9692	1.00791	0.005126	499.7005	1.028816

(a)

(b)

AS algorithm			QN algorithm		
	f_s (MHz)	f_0 (MHz)		f_s (MHz)	f_0 (MHz)
0 dB	500.3186	0.993681	0.108428	497.928	1.0664
5 dB	499.556	0.960309	0.0831	500.4476	0.979614
10 dB	498.3828	1.075588	-0.05526	500.4369	0.996342
15 dB	499.3686	1.02873	-0.01423	499.8856	0.988128
20 dB	499.7163	0.998931	0.012238	500.2477	1.001842

(c)

(d)

SQP algorithm			
	f_s (MHz)	f_0 (MHz)	α
0 dB	499.5255	0.959172	0.11345
5 dB	502.7354	0.908993	0.029085
10 dB	500.3796	1.049983	-0.12516
15 dB	499.9396	1.002611	-0.01733
20 dB	499.6012	1.019701	-0.01976

(e)

The average absolute relative error (ARE) of the estimated parameters from the actual ones shows that, LM algorithm gives optimized set of parameters. The input as well as the reconstructed chirp signals using LM algorithm is shown in Fig. 2. The two signals are overlapped, showing excellent goodness of fit.

5 Conclusion

Parameter estimation with chirp input using different optimization techniques is discussed in this paper. The obtained initial guess gives good convergence for all the optimization algorithms. Among the noise with different SNR values used, better goodness of it is obtained for 10 dB. This maybe due to the fact that small amount of noise is required for better estimation. All the optimization algorithms give comparable results for estimation of parameters, the average absolute relative error (ARE) shows the variation as:

$$ARE(LM) < ARE(QN) < ARE(AS) < ARE(SQP) < ARE(TRR)$$

Eventhough wavelet de-noising was found to be effective in estimating the parameters of gaussian echo, there is no notable difference obtained in the case of chirp. Hence, wavelet de-noising was not applied here. The estimation from noisy chirp itself serves best fit for all the algorithms analysed. Hence, de-noising may not provide a notable improvement. The future work aims at the error analysis of the chirp signal using the above mentioned optimization techniques for different SNR values.

References

1. Candy, J.V.: CHIRP-Like Signals: Estimation: Detection and Processing A Sequential Model-Based Approach. No. LLNL-TR-690337-REV-1. Lawrence Livermore National Lab (LLNL), Livermore, CA (United States) (2016)
2. Lahiri, A., Kundu, D., Mitra, A.: On parameter estimation of two dimensional chirp signals. Submitted for publication (2011)
3. Djuric, P.M., Kay, S.M.: Parameter estimation of chirp signals. IEEE Trans. Acoust. Speech Signal Process. **38**(12), 2118–2126 (1990)
4. Lu, Y., Demirli, R., Cardoso, G., Saniie, J.: A successive parameter estimation algorithm for chirplet signal decomposition. IEEE Trans. Ultrason. Ferroelectr. Freq. Control **53**(11), 2121–2131 (2006)
5. Anuraj, K., Poorna, S.S., Saikumar, C.: Ultrasonic signal modelling and parameter estimation: a comparative study using optimization algorithms. In: International Conference on Soft Computing Systems, pp. 99–107. Springer, Singapore (2018)
6. Liu, X., Yu, H.: Time-domain joint parameter estimation of chirp signal based on SVR. Math. Probl. Eng. (2013)
7. Kundu, D., Nandi, S.: Parameter estimation of chirp signals in presence of stationary noise. Stat. Sin. **18**, 187–201 (2008)
8. Laddada, S., Lemlikchi, S., Djelouah, H., Si-Chaib, M.O.: Ultrasonic parameter estimation using the maximum likelihood estimation. In: 2015 4th International Conference on Electrical Engineering (ICEE), pp. 1–4. IEEE (2015)
9. Demirli, R., Saniie, J.: Model-based estimation of ultrasonic echoes. Part I: analysis and algorithms. IEEE Trans. Ultrason. Ferroelectr. Freq. Control **48**(3), 787–802 (2001)
10. Aditya, N.R., Abhijeeth, K.S., Anuraj, K., Poorna, S.S.: Error analysis of optimization algorithms in ultrasonic parameter estimation. In: IEEE ICCIC, 13 December to 15 December, at Thiagarajar College of Engineering, Madurai, Tamil Nadu (2018)
11. Sreekumar, V., Anuraj, K., Poorna, S.S., Aditya, N.R., Jeyasree, S., Abhijeeth, K.S., Ranganath, L., Reddy, K.K.S.: MSE analysis of optimization algorithms using chirp signal. In: 4th IEEE International Conference on Recent Trends on Electronics, Information & Communication Technology, RTEICT (2019)



Dual RSA Based Secure Biometric System for Finger Vein Recognition

Satyendra Singh Thakur¹ and Rajiv Srivastava²

¹ Mewar University, Chhitorghar, Rajasthan, India
Satyendrathakur04@gmail.com

² Visiting faculty Mewar University, Chhitorghar, Rajasthan, India
drrajiv_sri@yahoo.com

Abstract. Nowadays, biometric plays a vital role in various security applications like banking, medical, and defense systems. The principle behind the biometric system is measuring and checking the biometric characters of individuals. The wireless communication systems are utilized to access Biometric Recognition System (BRS) at any place. In this work, finger vein pattern based biometric system is developed and the Multiple Input Multiple Output (MIMO) - Orthogonal Frequency Division Multiplexing (OFDM) system is used for transmitting the biometric trait information (i.e., data base) from one place to another place. The recognition accuracy of the biometric system is improved by using the Hybrid Feature Extraction (HFE) and feature selection techniques. The communications over the MIMO-OFDM system is secured by using the Dual-RSA technique. The classification among the individuals are identified by using the Error Correcting Output Code based Support Vector Machine (ECOC-SVM). The combination of BRS and wireless communication system is named as BRS-MIMO-OFDM. Finally, the performance of biometric trait recognitions is calculated in terms of accuracy, precision, recall, sensitivity, specificity, false acceptance and false rejection rate. Meanwhile, the MIMO-OFDM is analyzed in terms of Mean Square Error, Peak Signal to Noise Ratio (PSNR) and Bit Error Rate (BER).

Keywords: Accuracy · Biometric recognition system · Error correcting code based support vector machine · Hybrid feature extraction · KNN based genetic algorithm

1 Introduction

Generally, the biometric system is used for classifying the individual person by using the physical characteristics [1]. In general, the biometrics are classified into behavioral biometrics and physiological biometrics. The behavioral biometrics comprise of gait measurement, signatures and voice recognition. Similarly, the physiological biometrics comprises of retinal scanning, face, DNA, hand, fingerprint and iris [2]. From the biometric traits, the suitable biometric trait is selected based on the application like environment [3]. There are various system uses the biometric-based identity management. E.g. National agencies and governments [4]. The biometric systems have more advantages than the traditional methods such as passwords/Personal Identification

Numbers (PINs). Because the passwords and PINs are forgettable [5]. The biometric personal verification system is operated in two distinct modes such as enrollment and verification. [6].

Typically, the biometric systems are classified into two types such as unimodal and multimodal. The unimodal biometric system only uses the single biometric trait for authentication. But, the multimodal biometric system uses two or more biometric traits in the recognition process [7, 8]. The selection of biometric from the various biometric traits is mainly depends on the user acceptance, required level of security, accuracy, cost and implementation time [9]. The utilization of fake biometric information in the biometric systems causes many spoofing attacks. So, the authentication of the biometric system is enhanced by introducing the security [10, 11]. The major disadvantage of the biometric systems is vulnerable to possible attacks and also it is less robust for acquisition errors [12]. The identification performance of the biometric system is affected by the distortions present in the source data [13]. The traditional biometrics are usually frayed, forged and it is susceptible to spoofing attacks [14]. In this paper, the finger vein pattern is used as an authentication merit. Finger-vein pattern has some advantages in uniqueness, universality, permanence and security [15]. The major contributions of the BRS-MIMO-OFDM methodology are stated as follows:

The recognition rate of the BRS-MIMO-OFDM methodology is improved by two ways. First one is the utilization of using the HFE. Second is using the feature selection method named as KNN based genetic algorithm.

The selected features (i.e., data base) is transferred from one place to another place using MIMO-OFDM system. The MIMO-OFDM system exploits the spatial dimension capability for enhancing the wireless link performance.

The security of the MIMO-OFDM communications are improved by the dual RSA cryptography technique. It is used for preventing the data transmission from spoofing attacks.

2 Literature Survey

Ong et al. [16] introduced two different feature descriptor for recognizing the finger vein, such as the Local Hybrid Binary Gradient Contour (LHBGC) and Hierarchical Local Binary Pattern (HLBP). The noise problem due to the inadequate finger vein image acquisition is eliminated by using the multi instance approach. If the features have redundant information, then there is a possibility for performance degradation.

Gumaei et al. [17] introduced the privacy and security in cloud computing by using the anti-spoof multispectral biometric cloud-based identification approach. The biometric used in this approach is multi-spectral palmprint as well as this approach is separated into two different phases. (1) offline enrollment phase and (2) online identification phase. Here, the RSA cryptography is used for enhancing the security of the biometric system.

Xie et al. [18] introduced the feature component-based Extreme Learning Machine (FC-ELMs) for finger vein recognition. This FC-ELMs utilizes the feature characteristics from the finger vein. The computational complexity, matching performance and stability of the recognition systems is determined with hidden neuron tuning of ELM. Here, one more filter that is the guided filter is required to reuce the background impact.

Semwal et al. [19] presented gait recognition system using different machine learning techniques. The different machine learning techniques are KNN, ANN, SVM, DNN and classifier fusion. Here, the analysis of variance (ANOVA) is used for feature selection and incremental feature selection (IFS) is used for selecting the features for the group of features. The classifier fusion is utilized to compensate the errors made by the individual classifier. The recognition accuracy of KNN, ANN, SVM are less when compared to the DNN.

Meng et al. [20] introduced the finger vein recognition system. In that, the Region of Interest (ROI) segmentation is used for preprocessing which adjusts the global deformations such as rotations and in-plane translations in the finger vein image. The genuine and imposter matching is identified by using the uniformity of the displacement fields. The texture feature of uniformity is specified as the final matching score, which is extracted from the displacement matrix.

3 BRS-MIMO-OFDM Methodology

The finger vein based biometric information is transmitted by using the MIMO-OFDM system to access the information from throughout the world. The communications through the MIMO-OFDM is secured by using the dual RSA technique. The block diagram of the BRS-MIMO-OFDM methodology is shown in Fig. 1.

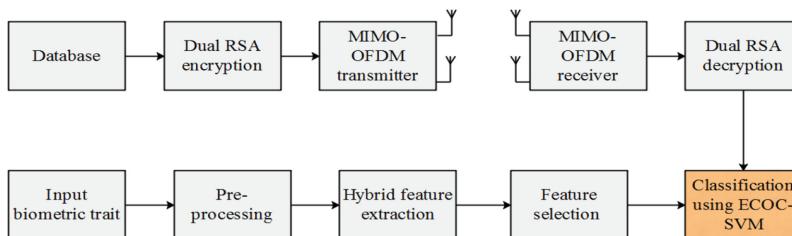


Fig. 1. Block diagram of BRS-MIMO-OFDM methodology

Figure 1 shows the architecture of the BRS-MIMO-OFDM methodology. It has three main processes such as (1) Database generation, (2) Data transmission using MIMO-OFDM and (3) testing process. The template (i.e., database) generation is performed by using the ECOC-SVM with the training sets of finger vein pattern. Additionally, these database is secured by using dual RSA and it is transmitted by using MIMO-OFDM. Finally, the query image is used in the testing stage for classifying the individuals.

3.1 Image Acquisition and Preprocessing

In this BRS-MIMO-OFDM methodology, the finger vein images are used as the key component to access the information from the biometric systems. The sample image of the finger vein pattern is shown in Fig. 2.a. Then the images are preprocessed using the Gaussian filtering which is used to remove the noise from the images. The following Fig. 2.b shows the pre-processed image of finger vein. The expression for Gaussian filtering is given in Eq. (1).

$$G(x, y) = \frac{1}{2\pi\sigma^2} e^{\frac{-x^2+y^2}{2\sigma^2}} \quad (1)$$

Where, x and y are the coordinates of the images and σ is the standard deviation.

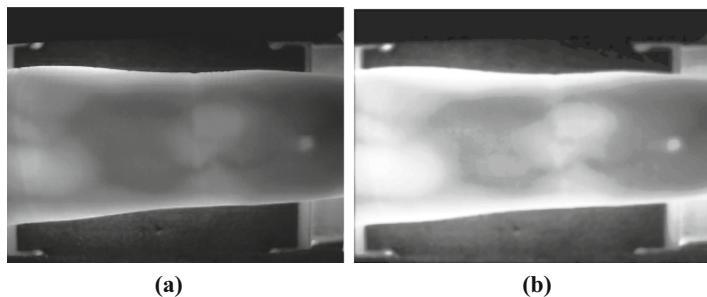


Fig. 2. a. Input image b. Preprocessed image

3.2 Hybrid Feature Extraction

There are different kind of feature extraction technologies used to extract the features such as HOG, SWT, GLCM and LBP. The features are extracted from the pre-processed image. Initially the features from the HOG, SWT and LBP features are extracted. In addition, the features from the SWT is given as the input to the GLCM to improve the recognition performance of the biometric systems. The description about the feature extraction is explained below,

3.2.1 Hog

HOG technique is a scale invariant features transformation. HOG technique is mainly depends on the accumulation of gradient directions of the pixel of small spatial area that is declared as cell. The image is divided into cells of size $N \times N$ pixels and the following Eq. (2) used for identifying the orientation ($\theta_{(x, y)}$) of the gradient in each pixel.

$$\theta_{x,y} = \tan^{-1} \frac{L(x,y+1) - L(x,y-1)}{L(x+1,y)L(x-1,y)} \quad (2)$$

Where, the intensity (i.e., grayscale) function describes the image is L.

3.2.2 Stationary Wavelet Transform and Gray Level Co-occurrence Matrix

Generally, the SWT is similar to the Discrete Wavelet Transform (DWT). In DWT, the process of up sampling and down sampling is reduced by using SWT. This reduction in up and down sampling leads to overcome the absence of the translation-invariance in DWT. In each level of the SWT output, the redundant scheme is considered and the SWT output has the same amount of sample which is given in the input. The features from the SWT is given to the GLCM. There are 11 types of features are extracted from the GLCM of pre-processed finger vein image. The extracted features are Auto correlation, Contrast, Correlation, energy, Entropy, Homogeneity, sum average, sum entropy, sum variance, difference variance and difference entropy

3.2.3 Local Binary Pattern

LBP is used for texture description which depends on the signs of differences among neighbor pixels and central pixels. In the 3×3 neighbor pixels, the LBP considers the center pixel value as the threshold. The LBP is represented in Eq. (3).

$$LBP(x_c, y_c) = \sum_{n=0}^7 2^n g(I_n - I(x_c - y_c)) \quad (3)$$

Where, $LBP(x_c, y_c)$ is the LBP value of the center pixel. I_n and $I(x_c - y_c)$ are the values of neighbour pixel and centre pixel respectively.

3.3 Feature Selection Using KNN Based Genetic Algorithm

The KNN based GA feature selection receives various features from the hybrid feature extraction to select the optimum features from the set of features. This KNN based GA feature selection is considered only important feature in the selection process. Hence, it is useful for choosing the significant and relevant features from the finger vein pattern. Furthermore, the feature selection is used during the classification to find the important feature that decreases the workload of the classifier and enhances the classification accuracy. In this BRS-MIMO-OFDM methodology, KNN based GA decrease the redundancy with-in the input voxels and also it determines the maximum relevance between output and input voxels. In initial stage of KNN based GA, the initial populations are generated which is the subset for input voxels. Next, the fitness function is computed for input voxel subsets utilizing the KNN distance algorithm that increases the mutual-information between the voxels. Finally, crossover and mutation operators are used to find the most active voxels by decreasing the redundancy based on the fitness function. The GA selects the subset of features as the chromosomes and every chromosome is sent to the KNN for computing fitness value. The KNN classifier

employs each chromosome as a mask for capturing the features. The KNN classifier defines a fitness value of each and every chromosome and GA utilizes these fitness values for the chromosome computation process. At the final stage, the GA finds an optimal subset of the feature.

3.4 Security Enhancement Using Dual RSA

Dual RSA has been introduced in this BRS-MIMO-OFDM methodology for improving the confidentiality of the biometric system. The features selected from the KNN based GA are encrypted by using Dual RSA algorithm. These encrypted features are transmitted from one place to another place using the MIMO-OFDM system. After receiving the encrypted features in the MIMO-OFDM receiver section, it is decrypted and it is processed for the classification. The dual RSA is also utilized to decrease the storage requirements.

3.4.1 Key Generation Algorithm

Input: Generate or choose large random prime numbers such as p_1, p_2, q_1 and q_2 .

Output: Public Key (e, n_1, n_2) and private key $(d_1, d_2, p_1, q_1, p_2, q_2)$.

3.4.2 Dual RSA Encryption Algorithm

Input: Plain text for encryption and receiving user's public key (e, n_1, n_2)

Here the plain text which is given to the Dual RSA encryption is the features from the finger vein pattern.

Output: The encrypted cipher-text, i.e., $X = F_v^e \bmod n$,

Where, F_v is a selected feature vector from the finger vein pattern that is plain text and X represents the cipher text from the dual RSA. Deliver the cipher text (X) to MIMO-OFDM system.

3.5 MIMO-OFDM System Model

The encrypted features from the Dual-RSA encryption algorithm is given as the input to the MIMO-OFDM system. The MIMO-OFDM system typically consists of n_T amount of transmitting antennas and n_R amount of receiving antennas. In the MIMO-OFDM transmitter section, the signal (encrypted biometric features) is converted by using a serial to parallel conversion. After transforming the signals, the IFFT and cyclic prefix insertion are performed in the respective signal. The signals from the OFDM modulators are given to the orthogonal modulation. Then the processed signal is sent to the receiver section by using the transmitter antennas of MIMO-OFDM. The cyclic prefix which is inserted in the transmitter section is eliminated in the receiver section of MIMO-OFDM. After removing the cyclic prefix, the serial to parallel conversion is applied to the signal and then the demodulation is performed over the transformed signal. The FFT is applied in the demodulated signal for transforming the signal from spatial domain to frequency domain. The transmitter's code word matrix is represented in the Eq. (4).

$$X = \begin{bmatrix} x_1^{(0)} & x_1^{(1)} & \cdots & x_1^{(N_c-1)} \\ x_2^{(0)} & x_2^{(1)} & \cdots & x_2^{(N_c-1)} \\ \vdots & \vdots & \cdots & \vdots \\ x_{nT}^{(0)} & x_{nT}^{(1)} & \cdots & x_{nT}^{(N_c-1)} \end{bmatrix}_{nT \times N_c} \quad (4)$$

Where, X is the transmitted signal; the transmitted signal by using nth subcarrier using tth transmitting antenna is $x_t^{(n)}$; T is the OFDM symbol period and N_c is the amount of carriers in the MIMO-OFDM system.

The following Eq. (5) specifies the relationship among the transmitted and received signal.

$$R = HX + N \quad (5)$$

Where, the received signal is R; the channel matrix is H and then the inter channel noise is N.

3.6 Dual RSA Decryption Algorithm

Input: The receiver's private key (d1 or d2) and the received encrypted cipher text

Output: The original plain text, i.e., $Y = R^{d1} \bmod n$ or $Y = R^{d2} \bmod n$.

Where, Y denotes the decrypted features from dual RSA.

3.7 Classification Using ECOC-SVM

The ECOC-SVM classifier is used for classifying the authenticated persons from the group of persons. It identifies the individuals by comparing two different inputs. One is the query biometric input image and another one is the data base information which is received through the MIMO-OFDM system. The bits of error occurred during the processing of image is corrected by ECOC and also this ECOC resolves multi class learning problems. The main process behind the classification of ECOC is stated as follows:

The n bit code which has the minimum hamming distance d is created. Where $n \geq [\log_2 K] + d$. The unique code word is allocated for training samples of each class to specify the class. The training sample Y is denoted as C(k) for class k. The following Eq. (6) expresses the training set of the ECOC-SVM.

$$S_Y = \{(Y, C(k)), k = 1, \dots, K\} \quad (6)$$

Where, training set is represented as S_Y , Y represents the decrypted features from the Dual RSA and C(k) respresents the training sample.

The training set has n binary functions, $f_i(Y) (i = 1, \dots, n)$ with the f_i corresponding to the i-th bit of C(k). The learning algorithm is used for training the n binary functions from S_Y . After completing the training stage, a new input sample Y_{new} is classified by n learned functions such as $f_i(Y) (i = 1, \dots, n)$. This ECOC-SVM classification is happened by achieving the n binary values that is expressed in the following Eq. (7).

$$\hat{y}_i = u\left[\hat{f}_i(Y_{new})\right] (i = 1 \dots n) \quad (7)$$

Where $u(Y) = \begin{cases} 1 & \text{if } Y \geq 0 \\ 0 & \text{otherwise} \end{cases}$

This Eq. (7) uses the learned functions of the fingerveins. Finally, the classification result among the query image and database is achieved by using the above Eq. (7).

4 Results and Discussion

The BRS-MIMO-OFDM methodology is analyzed with the help of MATLAB 2017b and the work was done on I3 system with 2 GB RAM. This biometric system is developed based on finger vein pattern. The security over the MIMO-OFDM communications is enhanced by using Dual RSA. The performance of the BRS-MIMO-OFDM methodology is analyzed in terms of accuracy, precision, recall, false acceptance rate and false rejection rate. In order to prove the effectiveness of the BRS-MIMO-OFDM methodology, the Homologous Multi-modal traits Database (SDUMLA-HMT Database) is used, which is provided by shandong university. In this BRS-MIMO-OFDM methodology only the finger vein database is used for this experiments.

4.1 Performance Analysis

In this BRS-MIMO-OFDM methodology, 10 users are considered to develop the secure unimodal biometric systems with finger vein pattern image. Here totally 180 images (18 images from each person) are taken from the SDUMLA-HMT Database for creating the database. From the 180 images, the features are extracted by using the hybrid feature extraction technique which is clearly explained in the above section. From the group of features, the optimized features are selected by KNN based genetic algorithm. The extracted features are encrypted using dual RSA cryptography technique and it is trained in the ECOC-SVM. Finally, the trained features from the SVM is stored at the database. In testing section, 30 images that are 3 images from each person are taken for testing the recognition rate of BRS-MIMO-OFDM methodology. The feature extraction and feature selection of the testing side is similar to the training section. The trained features are decrypted and then this is evaluated with the testing image.

There are four different parameters True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) are calculated to analyze the performance of the BRS-MIMO-OFDM methodology.

Table 1. Recognition performance of the BRS-MIMO-OFDM methodology

Performances	Values
Accuracy	0.966667
Sensitivity	1.000000
Specificity	0.962963
Precision	0.750000
Recall	1.000000
f_measure	0.857143
Gmean	0.981307
FAR	27.000000
FRR	0.333333

Table 2. Performance analysis of biometric system with MIMO-OFDM communications

Performances	SNR = -5	SNR = -2	SNR = 1	SNR = 4	SNR = 7	SNR = 10	SNR = 13	SNR = 16	SNR = 19
Accuracy	0.266667	0.600000	0.533333	0.800000	0.666667	0.966667	0.866667	0.900000	0.900000
Sensitivity	0.000000	0.333333	0.000000	0.666667	0.333333	1.000000	0.666667	0.666667	0.666667
Specificity	0.296296	0.629630	0.592593	0.814815	0.703704	0.962963	0.888889	0.925926	0.925926
Precision	0	0.090909	0	0.285714	0.111111	0.750000	0.400000	0.500000	0.500000
Recall	0	0.333333	0	0.666667	0.333333	1.000000	0.666667	0.666667	0.666667
f_measure	0	0.142857	0	0.400000	0.166667	0.857143	0.500000	0.571429	0.571429
Gmean	0	0.458123	0	0.737028	0.484322	0.981307	0.769800	0.785674	0.785674
FAR	9	18	17	23	20	27	25	26	26
FRR	Inf	12	Inf	3.5000	10	0.333333	2.50	2	2
MSE	3.065971	1.514819	0.850798	0.387397	0.198156	0.102095	0.049849	0.023918	0.012921
PSNR	4.865681	1.803607	0.701734	4.118433	7.029927	9.909939	13.023396	16.212723	18.887096
BER	0.079506	0.045562	0.020518	0.004425	0.000329	0	0	0	0

Tables 1 and 2 shows the performance analysis of the recognition and biometric system with MIMO-OFDM communications respectively. Figure 3 shows the BER performance of the data transmission through the MIMO-OFDM system. The BRS-MIMO-OFDM methodology provides 96.67% of accuracy during the recognition process. Meanwhile, the PSNR value of the BRS-MIMO-OFDM methodology increases while increasing the SNR value. Similarly, the MSE and BER also decreased by increasing the SNR. For example, The BER values are 0.0044 and 0 when the SNR is equal to 4 and 10 respectively. From the reduction in MSE and BER, conclude that the BRS-MIMO-OFDM methodology gives effective performance. So, the feature transmission through the MIMO-OFDM is better by considering the BER value. Moreover, the integrity and confidentiality among the communication through the MIMO-OFDM is enhanced by using the Dual RSA. This dual RSA secured the biometric trait from the spoofing attacks. Because there is a chance to hack the data from the database.

4.2 Comparative Analysis

The effectiveness of the BRS-MIMO-OFDM methodology is evaluated by comparing with two existing methods such as ANOVA [19] and PB-SIFT [20]. The ANOVA was analyzed by four classifiers such as ANN, SVM, KNN and DNN. The comparison of the BRS-MIMO-OFDM methodology with ANOVA [19] and PB-SIFT [20] is given in the following Table 3.

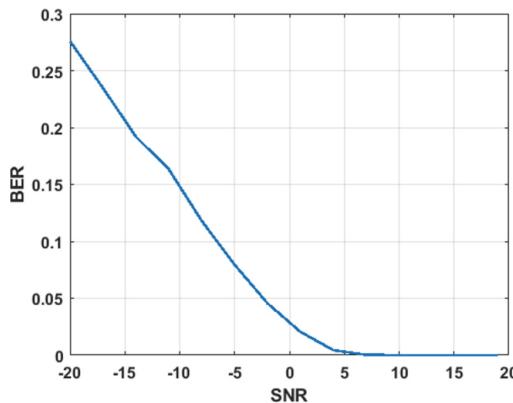


Fig. 3. BER performances of the BRS-MIMO-OFDM methodology

Table 3. Performance comparison of the BRS-MIMO-OFDM methodology

Methods	Accuracy
ANOVA- ANN [19]	90.58%
ANOVA- SVM [19]	88.31%,
ANOVA- KNN [19]	87.82%
ANOVA- DNN [19]	92.23%
MO Function [20]	84.83%
PB-SIFT [20]	94%
BRS-MIMO-OFDM methodology	96.67%

Table 3 shows the comparative analysis for the BRS-MIMO-OFDM methodology. The performance of the BRS-MIMO-OFDM methodology is high when compared to other methods named as ANOVA [19] and PB-SIFT [20]. Because, here hybrid feature extraction is used in this BRS-MIMO-OFDM methodology as well as selective features are selected by using KNN based genetic algorithm. From the finger vein pattern, an optimum features are extracted by using the hybrid feature extraction. Additionally, the number of features used for the classification is reduced by using the KNN based genetic algorithm. Moreover, this feature selection only selects the efficient features for classifying the query image. So, the number of features selected for the classification is reduced, it leads to improve the recognition accuracy.

5 Conclusion

In this work, the finger vein pattern is used as a biometric trait because finger-vein pattern remains unchanged or constant throughout human life. To make the biometric system more accessible, the biometric information is transmitted to one end to other end using the MIMO-OFDM system. There are four different feature extraction methods are used in this BRS-MIMO-OFDM methodology such as HOG, SWT, GLCM and LBP. The recognition rate of the BRS-MIMO-OFDM methodology is increased by two ways. One is the hybrid feature extraction and another one is feature selection from the set of features. The feature selection is performed by using the KNN based genetic algorithm. The confidentiality of the biometric system is improved by Dual RSA which is used to perform against the spoofing attacks. The accuracy of the BRS-MIMO-OFDM methodology is 96.67%, it is high when compared to the existing methods such as ANOVA and PB-SIFT.

References

1. Kim, D.J., Shin, J.H., Hong, K.S.: Teeth recognition based on multiple attempts in mobile device. *J. Netw. Comput. Appl.* **33**, 283–292 (2010)
2. Aly, I.D., Hesham, A.A., Nahla, B.A.: Enhancing iris recognition system performance using templates fusion. *Ain Shams Eng. J.* **3**, 133–140 (2012)
3. Jain, Y., Juneja, M.: A comparative analysis of iris and palm print based unimodal and multimodal biometric systems. In: ICSE Springer, pp. 297–306 (2017)
4. Shaikh, S.A., Rabaiotti, J.R.: Characteristic trade-offs in designing large-scale biometric-based identity management systems. *J. Netw. Comput. Appl.* **33**, 342–351 (2010)
5. Hsia, C.H., Guo, J.M., Wu, C.S.: Finger-vein recognition based on parametric-oriented corrections. *Multimed. Tools Appl.* **76**, 25179–25196 (2017)
6. Rattani, A., Marcialis, G.L., Roli, F.: Biometric system adaptation by self-update and graph-based techniques. *J. Vis. Lang. Comput.* **24**, 1–9 (2013)
7. Nair, S.A.H., Aruna, P.: Comparison of DCT, SVD and BFOA based multimodal biometric watermarking systems. *AEJ* **54**, 1161–1174 (2015)
8. Meraoumia, A., Chitroub, S., Bouridane, A.: Biometric recognition systems using multispectral imaging. In: Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations, pp. 321–347. Springer (2014)
9. Bharadi, V.A., Kekre, H.B.: Off-line signature recognition systems. *Int. J. Comput. Appl.* **1**, 0975–8887 (2014)
10. Wojtowicz, W., Ogiela, M.R.: Digital images authentication scheme based on bimodal biometric watermarking in an independent domain. *J. Vis. Commun. Image Represent.* **38**, 1–10 (2016)
11. Kim, Y., Yoo, J.H., Choi, K.: A motion and similarity-based fake detection method for biometric face recognition systems. *IEEE Trans. Consum. Electron.* **57**, 756–762 (2011)
12. De Marsico, M., Nappi, M., Riccio, D., Tortora, G.: A multiexpert collaborative biometric system for people identification. *J. Vis. Lang. Comput.* **20**, 91–100 (2009)
13. Matveev, I., Novik, V., Litvinchev, I.: Influence of degrading factors on the optimal spatial and spectral features of biometric templates. *J. Comput. Sci.* **25**, 419–424 (2018)
14. Liu, Z., Yin, Y., Wang, H., Song, S., Li, Q.: Finger vein recognition with manifold learning. *J. Netw. Comput. Appl.* **33**, 275–282 (2010)

15. Li, S., Zhang, H., Jia, G., Yang, J.: Finger vein recognition based on weighted graph structural feature encoding. In: Chinese Conference on Biometric Recognition, pp. 29–37. Springer (2018)
16. Ong, T.S., William, A., Connie, T., Goh, M.K.O.: Robust hybrid descriptors for multi-instance finger vein recognition. *Multimed. Tools Appl.* **77**, 1–29 (2018)
17. Gumaei, A., Sammouda, R., Al-Salman, A.M.S., Alsanad, A.: Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation. *J. Parallel Distrib. Comput.* **124**, 27–40 (2019)
18. Xie, S.J., Yoon, S., Yang, J., Lu, Y., Park, D.S., Zhou, B.: Feature component-based extreme learning machines for finger vein recognition. *Cogn. Comput.* **6**, 446–461 (2014)
19. Semwal, V.B., Singha, J., Sharma, P.K., Chauhan, A., Behera, B.: An optimized feature selection technique based on incremental feature analysis for bio-metric gait data classification. *Multimed. Tools Appl.* **76**, 24457–24475 (2017)
20. Meng, X., Xi, X., Yang, G., Yin, Y.: Finger vein recognition based on deformation information. *Sci. China Inf. Sci.* **61**, 052103 (2018)



TUDocChain-Securing Academic Certificate Digitally on Blockchain

Sugandha Budhiraja^(✉) and Rinkle Rani

Thapar Institute of Engineering and Technology, Patiala, India
{Sbudhiraja_mel7, raggarwal}@thapar.edu

Abstract. In the digital technology, Digital Documents become a part of organization, institution and educational field whether public or private. Digital Documents not only authorize the transition of information but also maintain the data in digital form. Academic Certificates approve the procurement of learning outcome. Certificates become necessary for people's professional careers. It is essential to save these certificates in long-term available and tamper proof ledgers. A Blockchain stores transaction in a confirmable and persistent way, therefore it is appropriate to save certificate or learning certification. Blockchain divulge fraud of certificates and its substructure learning records. This is accomplished by keeping digital crypto-hashes of learning certificates and controlling authorization integrity through the development of smart contract on Blockchain. The TUDocChain is the platform that entitles authorize the academic certificates on public ledger in a reliable and sustainable format. In this paper, we present the Blockchain for education platform as a practical solution for issuing, validating and sharing of certificate.

Keywords: Blockchain · Ethereum · Smart contract · IPFS · Digital academic certificates · Gas

1 Introduction

Blockchain is a peer to peer distributed ledger created by consensus, integrate with the system for smart contract. Blockchain is the backbone of digital cryptocurrency. Blockchain is a prominent technology, with almost daily declaration on its applicability to everyday life [1]. Blockchain technology has been implemented in different areas such as cryptocurrency in financial area, education field for securing the data in the digital form, in healthcare sector securing the patient data. Because of its decentralized and immutable properties, it is used in various sectors. Blockchain developing the current internet from “The internet of information sharing” to “The internet of Value Exchange” [2].

Academic Certificate plays an important role in education and development in companies. Students complete their degree or courses in different universities and educational institutions. After completion of their courses, universities and educational institutions award their students with degrees or issue certificates. Students receive the certificates as paper documents. Certificates include many statements, most important are:

Registration number, name of student, Certifier Signature, Address of organization, date of examination and other supplementary information.

Students receive a paper document that represent the certificate. Students can easily store paper documents or show them to any organization and person for any specific purpose. For entrance in organization or educational institute the authorities demand the previous qualified certificates as a proof even for recruitment company authority verify the credential of employee. They store the student document and maintain the certificate for a long period of time.

The substitute method to paper document are digital certificates that are cryptographically signed. Comparatively management of digital certificate is easier than the paper document but it required a lot of registry efforts. Third party easily verify the students or employee documents with the help of crypto hash of certificate.

In frame of reference of education and certification, Blockchain technology provide forged preservation of certificate. Third party easily verify the documents with the help of Blockchain features without the involvement of organization authority. In digital certificate process mainly three main steps are identified. Firstly, identity of certification authority has been created and maintained. Secondly certification authority awarded certificate to students and third step is the authenticate certificate by the recruiter or other organization authority. These three steps followed by a Blockchain based framework and adding additional feature of sharing certificate by students [3]. Blockchain education framework provide security as well as assured access and stable management of certificates according to the requirement of students, organization or educational institutions authority.

In this paper, we presented a platform TUDocChain that authorize the academic certificate on distributed public Blockchain and furnish the transparency between the students, institute and third party stakeholder. Identities of individual participated in the system is accessed by the smart contract build on ethereum platform using solidity. One contract manages the identities and second contract manages the certificates.

Interplanetary File System used as a distributed public network. IPFS generate the content address of the content. According to the size of transaction content address is generated. IPFS is the web distributed file system. To run ethereum Blockchain on the personal system ethereum virtual machine created. JSON and JavaScript is used for programming.

Nodejs use the library of JavaScript. On server side application Nodejs plays a vital role. For execution of transaction truffle deployed and migrate the smart contract on Ganache. Ganache implemented the personal Blockchain on system. Truffle configuration file is uploaded on ganache workspace. Ganache linked with Metamask with the private network to send the transaction using the ether value. Ether is required to secure the transaction on Ethereum Blockchain. This paper describes the workflow, architecture and results of the proposed system in below section.

2 Related Work

United States confronted a forgery of certificates by the Diploma Mills. The main reason behind the forgery of diplomas is manual process of managing and verification of documents. Learning Machine collaborated with MIT Media Lab start BlockCert for managing, issuing, sharing and verifying Blockchain based certificates using bitcoin platform [4, 5]. University of Nicosia issuing Blockchain based certification in bitcoin platform. In UNIC grouped hash of certification is used for verification [5].

TrueRec App introduced by SAP Innovation Center Network. TrueRec is the digital wallet it not only stores the academic certificate but all the personal documents like passport, ID Card etc. TrueRec app is controlled on Ethereum, an open Source, public, Blockchain based distributed computing platform that features smart contract (scripting) functionality which provide the facility of online contractual agreement [10].

Blockchain of Learning Logs (BOLL) managing the learning logs in Learning Record Store (LRS). BOLL provide a platform to move learning credentials from one institute to another institute. BOLL empowers existing learning information explanatory stages to get to the taking in logs from different foundations with the authorization of the students and additionally organization who initially have responsibility for logs [3].

In the field of education Sony Global Education develop a framework on IBM Blockchain. which is delivered via the IBM Cloud and powered by Hyper Ledger Fabric 1.0, a Blockchain framework and one of the Hyper ledger projects hosted by The Linux Foundation. SGE platform is used by any institution for the securing and verification of credentials [5, 11].

Harthy and his team of research publish a paper which is utilizing Blockchain to meet the all the transactions in college [12] i.e. a complete college chain. Chain include money transactions of registration and semester fees, transaction of securing certificate in ethereum platform, securing the profile of students, staff and third party stakeholders, online library access and managing published research paper.

Massive Open Online Courses (MOOC) are growing rapidly in the field of higher Education. Many platforms are there who provide online certification course. Blockchain Technology provide MOOC services by storing their universally accessible certification and transaction process [13]. Comparison of existing education applications on Blockchain shown in Table 1.

3 Proposed Methodology

In the schema of our proposed system, we first going through the literature review on existing application of Blockchain on education. Especially, we understand the concept of MIT Media Lab system named Blockcerts [14]. Blockcert implemented on bitcoin platform and uses the Open Badges for managing the records and encrypted the data using digital signature. Credence Ledger [7] architecture and Blockcert gives direction how the system worked on Blockchain. We discussed with the teachers, students and third party stakeholder that our proposed system feasible and useful for them. NodeJS, IPFS, Ganache, Metamask and truffle used for implementation of proposed system.

Table 1. Blockchain existing application on education

Application	Blockchain table	Record type	Actual data stored	Verification	Access to records
BlockCerts [4, 5]	Bitcoin	Certificates	Hash of Certificate	Open	Off-Blockchain authorization
UNIC [5]	Bitcoin	Certificates on MOOC	Grouped hash of certificates	Open	Off-Blockchain authorization
Sony Global Education [5–7]	Hyper ledger	Academic Records	N/A	N/A	N/A
Grade base [8]	Bitcoin	Imperial College Certificates	Hash of certificate, online profile and CV	Open	Off-Blockchain authorization
Stampery [5, 7, 9]	Bitcoin	Certificates	Aggregate Hash Value	Open	N/A
Credence Ledger [7]	Permissioned Blockchain (cryptocurrency is not required)	School records	Hash of Records	Open	N/A
TrueRec [10]	Ethereum	Documents like passport, certificates	Hash of documents (multichain with multi-signature)	Open	Off-Blockchain authorization
Open Certificate [7]	Ethereum	Certificate Insurance	IPFS generate the crypto hash value	Open	N/A
Blockchain of Learning Logs (BOLL) [3]	Ethereum	Different institute's transcripts link together	Smart contracts	Open	N/A

Ethereum Virtual Environment has been generated on the system. Smart Contracts has been deployed on ethereum platform using truffle. Smart Contract access the identity of issuer and student. Documents and records managed and stored using IPFS. Privacy of documents and identity managed using content address. Ether is generated from myether-wallet for paying the transaction fees.

Our purposed system is validated by uploading the college students academic certificate on our system. Certificates and individual's identity successfully secured on Blockchain. Features of our proposed system can be executed successfully.

3.1 System Overview

We proposed a Blockchain based TUDocChain of academic certificates that provide issuing, securing and verification of transcripts in immutable and secure ledger. TUDocChain supports Ethereum, open source and public ledger. The IPFS generate the content address of academic certificate. Consortium Blockchain is used in securing and verification because the certificate management system is centralized system component and verification is done by the third party or other institutes. It consists of smart contracts, holding the information of issuer and receptor with document in the public ledger.

System Architecture

An Overview of the architecture is shown in Fig. 1. Architecture consist the Blockchain involving smart contracts, a secured storage contains the information of certification Authority, parties involved into the system, issuer, certifier, Employee. The student register for degree and authorizer verify the student records and provide a unique identification or registration number. Firstly, the accreditation authority deployed the smart contracts to the Blockchain. (1) The first smart contract managing the profile of authority in the TuDocChain Blockchain for Education. (User Contract). (2) The second Smart Contract (CertificatemgmtContract) manages the degree certificate and transcript issued over the Blockchain [15]. Contracts are deployed by using truffle a testing framework using the Ethereum Virtual machine (EVM) and compiled the smart contracts. After the contract deployment authority of accreditation register the public keys of issuer in a UserContract and secure the issuer identity into the public ledger. The information of issuer is public readable. The public ledger holds the identities of issuer such as their name and country, but does not include any private information. After adding the information of certifier authority issuer add the public key of the certificate with the UserContract and give right to the issuer to issue the certificate.

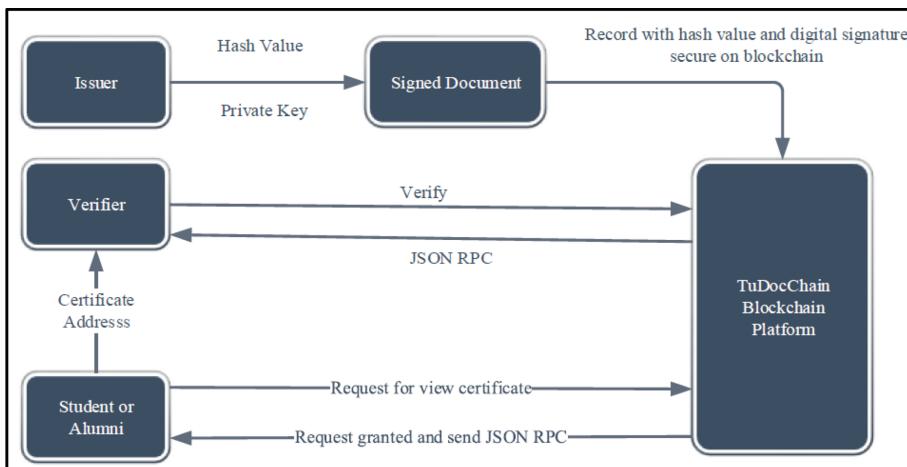


Fig. 1. Overview of TUDocChain

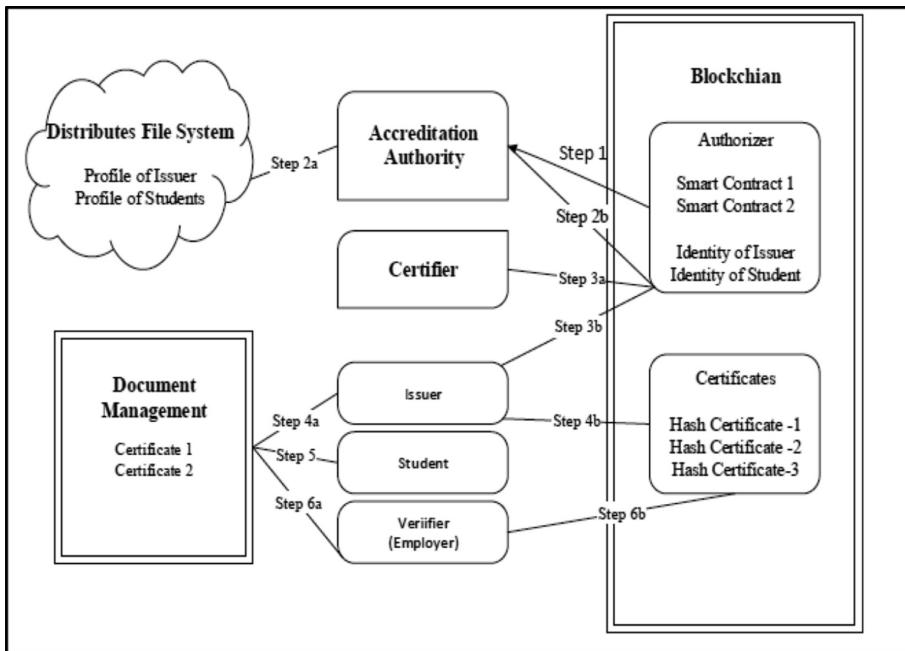


Fig. 2. System architecture

Issuing Certificate

The issuer collects the information consisted in the certificate in the JSON format. The data consist of title, name of the issuer, name of the student, and the date. Issuer signed the certificate and stored the document in the document management (Step 4a), and crypto hash value written into the Blockchain (Step 4b).

Storing Certificate

Students records are stored in the document management portfolio. Student want to apply in other institute or organization, and want to verify the documents by the employee (third party) gives their portfolio's direct link to verifier (step 5).

Verifying Certificates

Verifier verify from the crypto hash value of the certificate. (Step 6b). Verifier decrypt the document by using public key send by the issuer. If the hash value is equal to the previous value, the document is verified.

4 Implementation

Based on Ethereum Blockchain we implemented the platform of Blockchain on academic certificate. Smart Contracts written in solidity first named as **UserContract** access the profile of issuer, Certifier and student, second contract **CertificategmtContract** access the information of certificates. The Interplanetary File system(IPFS) used as a public distributed storage profile information of certificate authority.

UserContract access all the authority profile involved into the system. The UserContract give the access to accreditation authority for add, update and delete the users profile. CertificatemgmtContract access the certificate records to securing the academic certificate on Blockchain. The record consists of SHA 256-bit hash of the academic certificate, the issue date, issuer digital signature.

Ganache is a private Blockchain of ethereum development used to deploy contracts, execute the application deploy by the truffle. Truffle deployed and migrate the smart contract and connected with the Ganache workspace. For transaction Ganache has been build a connection with the metamask. MetaMask provide the interaction between the Blockchain application and the browser. Metamask introduced its own web3 instance. Certifier creates an account on metamask choose a private network, connect a localhost network 127.0.0.1:7545. As the transitions deployed on ganache and securely saved on the Blockchain then gas value decreases. Ether value deposit on Metamask. Ether generates the gas value on Ganache. Steps involved for the execution of system are, first generate the user account on ethereum all transactions gas value used from that account. Then secure all the records on IPFS and generate the Content Address. Content address provide the privacy on the system because it is a crypto hash unique value. Smart Contract access the user's identity. Both crypto hash value of the document and smart contract secured on distributed public Blockchain. Figure 3: described the picture of TUDocChain issuer Page. Issuer Page issuer register the academic certificate in the form of address deployed by UserContract.

The screenshot shows the 'Issuer Page' of the TUDocChain system. At the top, there are navigation links: 'Home Page', 'Issuer Page' (which is the active tab), 'Recipient Page', and 'Events'. The page content is divided into three main sections:

- Register certificates:** Contains fields for 'Type' (with placeholder 'Enter type of the certificate'), 'Name' (placeholder 'Enter name of the certificate'), 'Description' (placeholder 'Enter description of the certif'), and a button 'Register a new certificate'.
- Issue certificates:** Contains fields for 'Address of Recipient' (placeholder 'Enter the address of the reci') and 'Select certificate' (dropdown menu with 'Issue new certificate' option). There is also a small 'Activate Windows' watermark in the bottom right corner of this section.
- View your certificates:** Contains a field 'Enter recipient's address' and a button 'Get recipient details'.

Fig. 3. Securing the identity of user and certificate

Students view their certificate from the recipient page. Figure 4: describe that filling the address of certificate it views the certificate.

IPFS as a Public Distributes Storage

IPFS stores the hash value permanently. IPFS known as a future of web. Certificate Authority system added the address of issuer, certifier and documents of students with their identities by the hash value store in the merkle tree. Firstly, the Certificate system validate the address of verifier, issuer and certifier then add these address on IPFS.



Fig. 4. View issued certificate

Through IPFS addresses all the information stored in the Blockchain. Blockchain is unable to store massive data directly so we store transaction and individual profile information in the form of address [7, 16].

Transaction and generating block

The certification authority has to generate the account of issuer and receptor on Blockchain platform (Ethereum) [7, 17]. With the transaction of ether and gas value the records stored in Blockchain. Certifier with his identity address, gas value [17] and hash value of the record able to store the records in the Blockchain. For transaction we use [myetherwallet](#) [15, 18] and generate the private key address for the authority who want to securing the document on Blockchain. Ganache act as a Personal Blockchain for ethereum development, we deploy contracts and run testing on Ganache [15, 19]. Figure 3 shows how blocks are formed in the Blockchain. Truffle provide the environment testing framework for using Blockchain on Ethereum virtual Machine (EVM) [20].

Smart Contract and Gas Value

Ethereum is a distributed computer. Each node executes Bytecode in the form of Smart Contract on the ethereum network and then securing the resulting documents in the Blockchain. Smart Contract is a code that executed on the distributed environment like on Ethereum framework. In ethereum, smart contracts are executed it generate the bytecode as a unique address. When smart contracts deployed contracts take miner's computing power. Gas value act as a miner's computing power. Gas value is earned by investing some Ethers (ETH).

CURRENT BLOCK 10	GAS PRICE 20000000000	GAS LIMIT 521975	HARDORK PETERSBURG	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING	WORKSPACE cc	SWITCH	⚙️
BLOCK 10	MINED ON 2019-06-07 18:17:01					GAS USED 27834		1 TRANSACTION	
BLOCK 9	MINED ON 2019-06-07 18:17:00					GAS USED 2177511		1 TRANSACTION	
BLOCK 8	MINED ON 2019-06-07 18:17:00					GAS USED 368657		1 TRANSACTION	
BLOCK 7	MINED ON 2019-06-07 18:16:59					GAS USED 42834		1 TRANSACTION	
BLOCK 6	MINED ON 2019-06-07 18:16:55					GAS USED 284908		1 TRANSACTION	
BLOCK 5	MINED ON 2019-06-06 16:31:08					GAS USED 27834		1 TRANSACTION	
BLOCK 4	MINED ON 2019-06-06 16:31:08					GAS USED 2177511		1 TRANSACTION	
BLOCK 3	MINED ON 2019-06-06 16:31:07					GAS USED 368657		1 TRANSACTION	
BLOCK 2	MINED ON 2019-06-06 16:31:07					GAS USED 42834		1 TRANSACTION	

Activate Window
Go to Settings to activate this message

Fig. 5. Blocks transaction on ganache

NAME CertChain	ADDRESS 0x4892A1015D0B5048B4328d33c46E8FA60Fe7aae8	TX COUNT 0	DEPLOYED
NAME Migrations	ADDRESS 0xd53CABBA7A71953A0f53b143F0688782BCED5840	TX COUNT 1	DEPLOYED
NAME Users	ADDRESS 0x784afD2ad7E800D1Ce741370c7E10D7ba2679808	TX COUNT 0	DEPLOYED

Fig. 6. Deployed smart contracts

5 Data Security

Design of database is categorized into two parts: the public authentication data and private certificate record Fig. 2 shows the data storage schema. All the records of students secured on MongoDB NoSQL Database. In the JSON format data stored on MongoDB. Issuer access the certificate from MongoDB firstly then after converting JSON file into the PDF the records with digital signature and hash value secured on the Blockchain. Records are secured on distributed public ledger. Data accessed from central database and secured on public Blockchain so that verifier easily authorize the records from distributed public Blockchain. This proposed work increases the security of individual's information and decreased the forgery cases (Fig. 7).

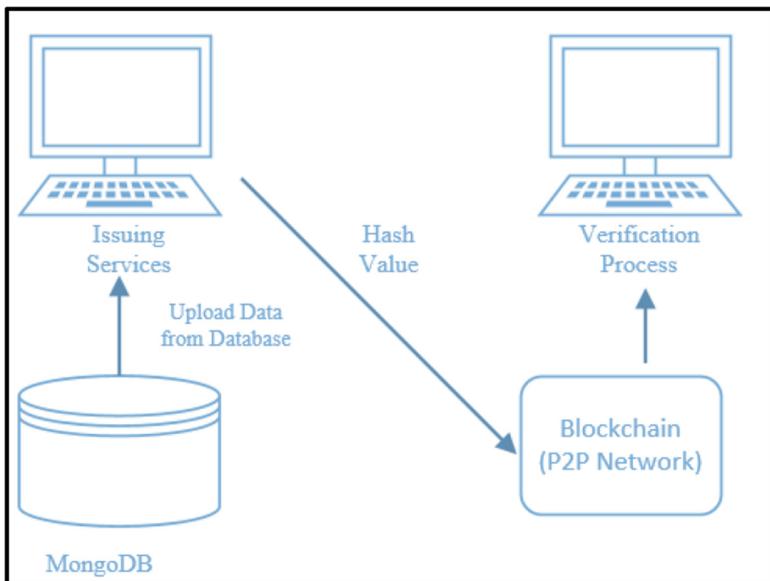


Fig. 7. Data security on blockchain and intranet [14]

6 Conclusion

In this work, we proposed a solution of authorizing the documents and securing school level documents and college academic certificates on one platform. The primary benefaction of presenting execution of Blockchain framework on ethereum entitle security and immutability of records. This paper presents an overview of the required tools and techniques for running system. The system provides digital records of students credentials that are easily verifiable by transact a gas value on Ethereum platform. It provides a verification feature for other organization employee (Third Party Stakeholders). Employee easily verify the student's records using P2P Blockchain. The documents shared securely on distributed File management as a public distributed ledger. Through this public ledger multiple entities verify the data without the need for a centralized system. But transactions required a lot of computing energy and transaction fees which is paid by the certifier. In future work, system main focus on connecting multi-institution records and online course certificate without using any transaction fees. Primary concern on maintaining privacy of individual identities implementing standard permission less Blockchain.

References

1. Grech, A., Camilleri, A.F.: Blockchain in Education Luxembourg : Publications Office of the European Union (2017)
2. Chen, G., Xu, B., Lu, M., Chen, N.-S.: Exploring blockchain technology and its potential applications for education. Smart Learn. Environ. 5(1), 1–10 (2018)

3. Ocheja, P., Flanagan, B., Ueda, H., Ogata, H.: Managing lifelong learning records through blockchain. *Res. Pract. Technol. Enhanc. Learn.* **14**(1), 4 (2019)
4. Arushanyan, V.: Nooor.io. Nooor Armenian Blockchain Association (2017). <https://nooor.io/blockchain-in-education/>
5. el Maouchi, M., Ersoy, O., Erkin, Z.: TRADE : a transparent, decentralized traceability system for the supply chain. In: 2018 Proceedings of 1st ERCIM Blockchain Work, European Society for Socially Embedded Technologies (EUSSET) (2018)
6. MIT Media Labs: MIT Media Lab (2016). <https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196>
7. Arenas, R., Fernandez, P.: CredenceLedger: a permissioned blockchain for verifiable academic credentials. In: 2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018 - Proceedings, pp. 1–6 (2018)
8. Colle, C., Knottenbelt, W.: Decentralised academic record verification using the Bitcoin block chain (2015)
9. de, A.S., Crespo, P., García, L.I.C.: Stampery Blockchain Timestamping Architecture (BTA) - Version 6, pp. 1–18 (2017)
10. SAP Labs: SAP LaBS (2017). <https://news.sap.com/2017/07/meet-trurec-by-sap-trusted-digital-credentials-powered-by-blockchain/>
11. SONY: SONY (2017). <https://www.sony.net/SonyInfo/News/Press/201708/17-071E/index.html>
12. Al Harthy, K., Al Shuhaimi, F., Juma Al Ismaily, K.K.: The upcoming Blockchain adoption in Higher-education: requirements and process. In: 2019 4th MEC International Conference on Big Data Smart City, ICBDESC 2019, pp. 1–5 (2019)
13. Mire, S.: Disruptordaily (2017). <https://www.disruptordaily.com/blockchain-use-cases-education/>
14. Github: BTcert, Github (2017). <https://github.com/BlockTechCert/BTCert>
15. Power, K.: CertChain (2018)
16. Protocol Labs: IPFS, Protocol Labs. <https://docs.ipfs.io/>
17. Ethereum: Ethereum (2016)
18. Myetherwallet: Myetherwallet (2019). <https://www.myetherwallet.com/>
19. Truffle: Truffle suite Ganache, Truffle. <https://www.trufflesuite.com/docs/ganache/overview>
20. Truffle Suite: <https://www.trufflesuite.com/docs/truffle/overview>



Enhancing Energy Efficiency in IoT (Internet of Thing) Based Application

Utkarsha Singh^(✉) and Inderveer Chana

Thapar Institute of Engineering and Technology, Patiala, India
{usingh_mel7, inderveer}@thapar.edu

Abstract. With the emergence of Internet of Thing (IoT), a gigantic rise has been seen in smart applications. IoT is going to be ubiquitous in the near future. Billions of sensors will be installed for the implementation of IoT applications which will generate a massive amount of data. Such massive amount of sensors, data and devices would cost huge amount of money. In addition to the installation cost, energy consumption by the IoT devices emerges as a prominent area of concern. Although IoT applications in themselves are considered to be very energy efficient, however their own energy consumption ratio is very high. Energy efficiency of IoT would make it the long term technology in the upcoming years. In this paper, a case study of an IoT based application is done. To reduce the energy consumption during data transmission in IoT based applications a solution is proposed and implemented into studied application to enhance its energy efficiency. Scheduling of data transmission is the proposed solution which mainly focuses on the energy consumption during continuous data transmission in IoT based applications which keeps the networking device or gateway active all the time and results in drainage of energy continuously. The proposed solution aims to reduce the energy consumption in IoT application by transmitting data to the cloud in an energy efficient way.

Keywords: Internet of Thing · Energy consumption · Energy efficiency · Scheduling · Data transmission

1 Introduction

With the advent of IoT smart living is no longer a day dream. It advantages people by saving time, cost as well as energy. According to IEEE Consumer Electronics Magazine Editor Peter Corcoran “energy is one of the three determinants of the long term sustainability of Internet of Things (the other two being privacy and security)” [1].

Real time monitoring and controlling of devices has become possible because of internet. Internet is the foremost part of IoT which helps in connecting device with device as well as device with people. IoT systems use medium to transmit data generated from IoT devices to people and that medium is the gateway. Gateway is the medium which acts as an entry and exit point for a network which is responsible for passing all the data through it prior to being routed. Figure 1 illustrates the data transmission in IoT applications through gateway. In IoT applications, number of sensors are deployed for the working of IoT devices. These sensors generate data which

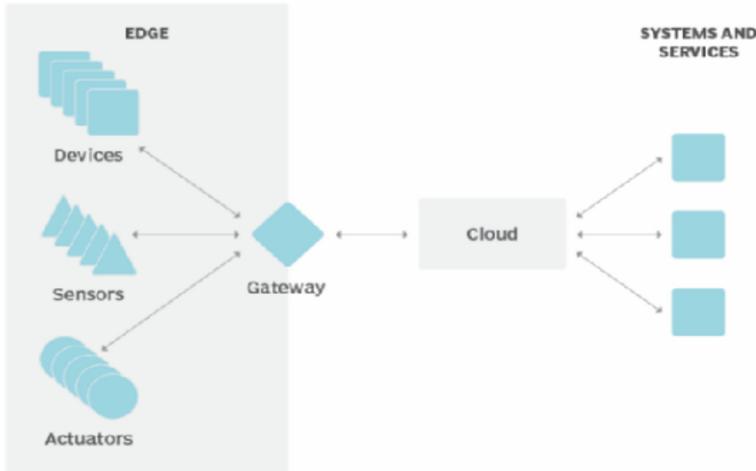


Fig. 1. Data transmission through gateway in IoT [2]

is transmitted to cloud where it gets processed. That processed data is accessed by user through an application or cloud based on the type of application. Each data should be transmitted through gateway to reach cloud. Thus, each IoT system uses gateway as a medium to transfer data to cloud.

Wi-Fi is also one of the mediums in IoT systems to transfer data from IoT devices to cloud. Each process of IoT requires energy whether they are sensing, sending, analyzing, processing and storing [3]. Thus, Wi-Fi module also requires power for their working. Batteries supply power to the whole IoT system. But the amount of current varies when data starts transmitting from the gateway or router to cloud. Gateway device draws less current i.e. consumes less power when no data is transmitted through it. But when gateway device is in active state i.e. transmitting data through it, then it draws more current i.e. consumes high power as shown in Table 1.

Table 1. Power consumption by gateway

Gateway	Mode	Data transmission	Current drawn (Less/More)	Power consumption
	Active	Yes	More	High
	Ideal	No	Less	Low

It is clear that when data is transmitted from routing device to cloud it is consuming more energy in comparison to when no data is transmitted through it. Continuous sending of data in IoT systems deployed at larger scale drains lots of energy while transmission. In this paper problem of energy consumption during continuous sending of data in IoT based applications is resolved by proposing a solution. This solution is implemented in IoT based application and a comparative analysis is done to show its efficiency in terms of energy.

2 Proposed Solution for Enhancing Energy Efficiency

Many techniques have been proposed in IoT for the efficient transmission of data through the network to reduce energy consumption. However, scheduling of data transfer i.e. at what time data should be transmitted has not been discussed in previous work. Data transfer also depends on the type of IoT application. If there is a life critical application, then data needs to be monitored continuously. But if there is an application where continuous monitoring is not required and additional features make the monitoring and controlling more easy then scheduling of data transfer can be a good strategy to save energy in IoT applications.

Scheduling of data transfer schedules the transmission of data at a particular time interval. This means that the data generated from the sensors should not be transmitted continuously on cloud hence, make the routing device ideal for some time which results in low power consumption. When the scheduled time interval arrives then only generated data at that time gets transmitted through routing device to cloud which makes the routing device active for a short period of time. Only for that period power consumption will be high and rest of the time it will remain low.

Figure 2 represents the flow of data in an IoT system at defined time interval. Defined time is the time when data needs to be transmitted to cloud depending on programmer's and application's choice. If the condition $\text{Time_interval} = \text{Defined time}$ is met, then only data is transmitted through the gateway to cloud.

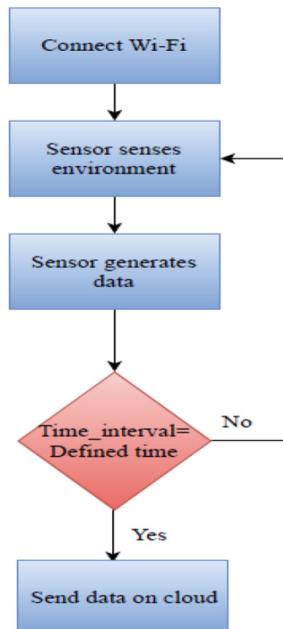


Fig. 2. Scheduling of data transmission

3 Case Study

Case study is based on smart city application i.e. smart street lighting system. The aim of this case study is to depict the existing systems of smart street light in order to represent the existing solutions being implemented to save energy in them. In contrast to existing systems, prototype of smart street lighting system is proposed with the aim to save more energy by implementing proposed scheduling data transmission solution into it.

3.1 Existing Model

In real time, automated street lights play vital role in the development of smart city. Few countries have entered in the generation of smart city by implementing real time smart applications at large scale [4–7]. Street lights are one of those applications which have been deployed at such scale. Automation of street lights results in huge energy savings. To further save energy dimming of street lights during night [6] and solar energy is used as a solution to charge batteries in small application areas [8]. Following are some real time smart street lighting system that exist in real world:

i. Twilight

It is a Dutch startup company which is using the concept of IoT to make city lighting more energy and cost efficient. It deploys motion sensors in the existing street lights which results in on-demand motion-based illumination. The streetlights automatically adjust their brightness on detecting the presence of vehicles or pedestrians. For real time monitoring and management of lights web based platform is used. This system has witnessed 50 to 70% energy saving and cut down electricity bill by 2 billion EUR per year [9].

ii. Comlight

It is a Norwegian company which has developed world's first patented control system "Motion Sensing Street Lighting System" for reducing energy wastage [6]. Street lighting control system is installed with Eagle Eye radar which senses all those activities which require optimal lighting on the road. When movement is detected by the nearest street light, it gets lit and the detection is communicated to other nearest street lights wirelessly by radio for providing full light and also get dim when no movement is detected. Eagle Eye Gateway Unit is used for remote access of street lights for monitoring purposes along with GPS [10].

iii. Telensa PLANet

It is the world's number one outdoor lighting control system which has deployed nearly 1.5 million street lights around the world. It is a connected street lighting system consisting of wireless control nodes, UNB (Ultra Narrow Band) wireless network and CMS (Central Management System). It saves energy by controlling amount of light on the basis of usage and by accurately measuring every watt. It helps in saving huge amount of energy [11].

iv. Motwane

It is an India based R&D and IoT company. Its IoT based smart street lighting solutions as JUSCO's project in Jamshedpur is the biggest smart street lighting deployment project in India where 300 smart street lights were deployed. In partnership with TATA Communications Motwane is paving way to deploy 15,000 smart street lights in India. Street lights get switched on/off or dimmed remotely from control center. Lights can also be adjusted based on the location which results in reduction of energy consumption and manpower costs [12].

The above mentioned real time applications are saving energy by adding the features of IoT i.e. automation as well as remote monitoring and controlling of lights. Also, dimming of lights based on detection of vehicles or pedestrians is one of the enhanced feature to save more energy in street lights. However, none of the applications focuses on the way the street lights sharing data on cloud. Huge amount of data is generated from these street lights and continuously sending them on cloud for monitoring purpose drains lots of energy which is not required. Hence, to witness more energy saving in IoT based street lighting system scheduling of data transmission can be a proficient solution.

3.2 Description of Proposed System

Smart street lighting system which is implemented is a prototype of an automated system where lights switched on/off according to sunlight's intensity. Status of lights are send on cloud platform for remote monitoring and controlling purposes. Automation along with remote monitoring and controlling makes the whole system an IoT system. This proposed system is based on the previous proposed work [13, 14]; however, the difference lies in the way that how data is sent on cloud. In previous work status of street lights are send on cloud continuously for remote monitoring purpose. But in real time, application area is wide due to which huge number of sensors are deployed at large scale which generates huge amount of data results in energy drainage during continuous transmission.

In the proposed system, the proposed solution i.e. scheduling of data transmission has been implemented which is discussed in previous section. Transmission of data is scheduled at an interval of 1 h so that during that duration only gateway remain active consuming more power and rest of the time it remains ideal consuming less power. Scheduling of data transmission is done just before the sending the data on cloud so that only last sensed data can be send on cloud in order to reduce data size and congestion while transmission. To save more energy along with the proposed solution LEDs are used at place of sodium vapor lights [15]. Working of whole system is based on automation. When sensor senses the surrounding environment and if sensed value is less than threshold value i.e. 90, then it indicates that there is dark i.e. night and lights get switch on and if sensed value is greater than threshold value i.e. 90, then it indicates that there is light i.e. day and lights get switch off. At an interval of 1 h the sensed value

along with threshold and light intensity (surrounding's light intensity) is transmitted to cloud which is accessible by admin for remote monitoring purpose.

Figure 3 represents the design of proposed street lighting system in which scheduling of data transmission has been implemented to save energy.

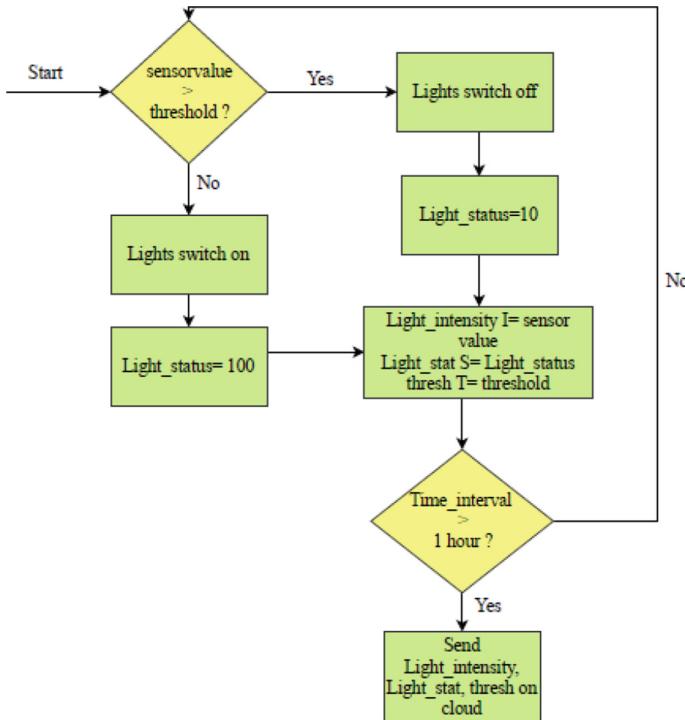


Fig. 3. Design of proposed system

4 Implementation

To implement the system hardware components like Arduino Uno, LDR, LEDs, ESP8266 are used and for coding purpose Arduino IDE software is used. ThingSpeak is also a part of software which is used as IoT cloud platform. Table 2 lists the components used during implementation of proposed system.

Firstly, LDR and ESP8266 are connected to Arduino UNO board using Male to Male and Male to Female Connectors. Four LEDs are connected with four resistors in parallel. Each LED represent different locations of college on cloud. User account is made on cloud platform ThingSpeak. Channels are created on ThingSpeak and API keys are generated accordingly. Code is written on Arduino IDE which includes: (i) switching of lights on when sunlight intensity is less than threshold value i.e. 90 and

Table 2. Tools Used

Components	Type	Purpose
Arduino Uno	Embedded system	For storing written program on its microcontroller
LDR	Photoresistor (sensor)	For sensing sunlight's intensity
LED	Lights	To get switch on/off based on sunlight's intensity
ESP8266	Wi-Fi module	For Wi-Fi connection and sending data on cloud ThingSpeak
Arduino IDE	Coding platform	For writing code to make the whole application work
ThingSpeak	Cloud platform	For remote monitoring and controlling purpose
Multimeter	Tool	For measuring power consumption of proposed system

off when sunlight intensity is more than threshold value. Light_status is set as 100 when lights are switched on, 10 when lights are switched off. (ii) Setting ESP8266 to connect with Wi-Fi. (iii) Calculation to get current time of the system to send data at an interval of 1 h. (iv) Sending of generated data on created channels of cloud. Once Wi-Fi is connected, lights status of each LED is sent on ThingSpeak at an interval of 1 h. To calculate energy consumption, first power consumption of both on and off states have been calculated, then energy is calculated.

5 Result

The proposed work provides a solution to the problem of high energy consumption in the existing smart street lighting systems. In order to save energy lights were automated on the basis of surrounding's light intensity. Figure 4 represents the on state of street lights when surrounding light intensity is less than 90 i.e. indicating night time. Similarly, Fig. 5 represents the off state of street lights when surrounding light intensity is greater than 90 i.e. indicating day time.

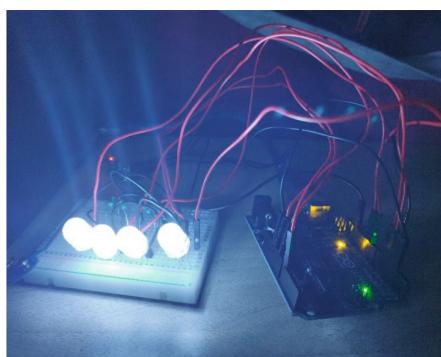


Fig. 4. On state of lights during night

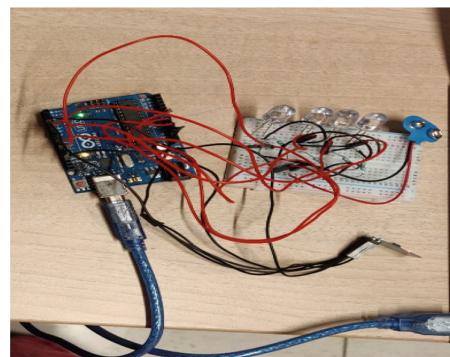


Fig. 5. Off state of lights during day

Two cases are created to show the difference between the energy consumption of whole system when data is transmitted continuously through Wi-Fi to cloud and when transmission is scheduled at an interval of 1 h. Following are the two cases:

Case I: Wi-Fi (ESP8266) Sending Data Continuously on Cloud

Figure 6 illustrates the presentation of data send continuously on cloud which is visible to admin for monitoring purpose. Hike in upward direction of Light_intensity indicates that environment's light intensity is increased i.e. day time and at the same time falling of values from 100 to 10 in Light_stat indicates that light gets switched off during day time. Threshold value 90 is constant throughout the time.

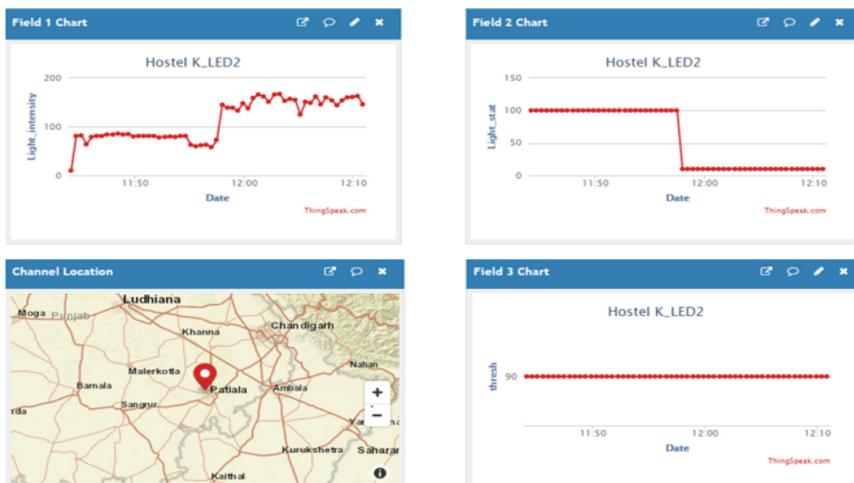


Fig. 6. Visualization of continuously sent data on cloud

For powering lights voltage of 8.31 V is supplied through DC source which remain constant throughout the working of system. Current is measured using Multimeter which varies on the basis of lights either on or off and the state of ESP8266 either active or ideal.

- (a) **Lights are off i.e. during day time**
Power $I_a = V * I = (8.31 * 400)/1000 = 3.324 \text{ W}$
- (b) **Lights are on i.e. during night time**
Power $I_b = V * I = (8.31 * 480)/1000 = 3.9888 \text{ W}$

Case II: Wi-Fi (ESP8266) Sending Data Periodically i.e. on an Interval of 1 h

Figure 7 illustrates the presentation of scheduled data transmission on cloud which is visible to admin for monitoring purpose.

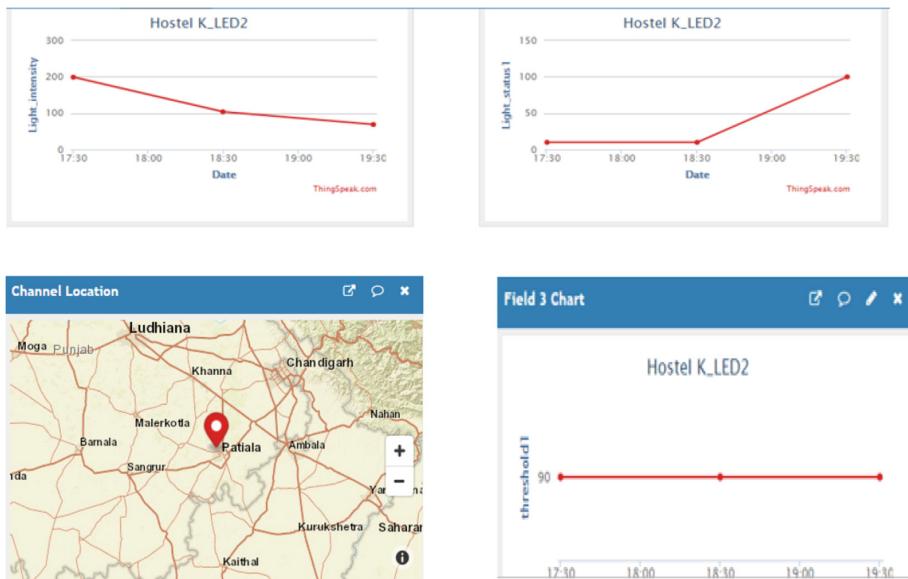


Fig. 7. Visualization of periodically sent data on cloud

Like Case I values of Light_intensity, Light_stat, thresh are showing accordingly. The only difference is that the time at which data is sent on cloud. There is a difference of 1 h between the transmission of data on cloud.

(a) **Lights are off i.e. during day time**

$$\text{Power}_{IIc} = V * I = (8.31 * 325)/1000 = 2.70075 \text{ W}$$

(b) **Lights are on i.e. during night time**

$$\text{Power}_{IId} = V * I = (8.31 * 405)/1000 = 3.36555 \text{ W}$$

Calculation of Energy Consumption

To calculate the energy consumption of lights in real time standard timing of switching on and off street lights are considered.

Duration of lights off = 6 A.M. to 7 P.M. = 13 h

Duration of lights on = 7 P.M. to 6 A.M. = 11 h

Case I: Wi-Fi (ESP8266) sending data continuously on cloud

(a) **Power Consumption per month I_a**

$$\begin{aligned} \text{Power}_{Ia} * \text{Duration of lights off} * \text{Number of days in a month} \\ = 1.29636 \text{ KWh} \end{aligned}$$

Energy Consumption I_a (E_{I_a})

$$= \text{Power Consumption per month } I_a * 3600000 \text{ J}$$

$$= 4666.896 \text{ kJ}$$

(b) **Power Consumption per month I_b**

$$\text{Power } I_b * \text{Duration of lights on} * \text{Number of days in a month}$$

$$= 1.316304 \text{ KWh}$$

Energy Consumption I_b (E_{I_b})

$$= \text{Power Consumption per month } I_b * 3600000 \text{ J}$$

$$= 4738.6944 \text{ kJ}$$

Case II: Wi-Fi (ESP8266) sending data periodically i.e. on an interval of 1 h(c) **Power Consumption per month II_c**

$$\text{Power } II_c * \text{Duration of lights off} * \text{Number of days in a month}$$

$$= 1.0532925 \text{ KWh}$$

Energy Consumption II_c (E_{II_c})

$$= \text{Power Consumption per month } II_c * 3600000 \text{ J}$$

$$= 3791.853 \text{ kJ}$$

(d) **Power Consumption per month II_d**

$$\text{Power } II_d * \text{Duration of lights on} * \text{Number of days in a month}$$

$$= 1.1106315 \text{ KWh}$$

Energy Consumption II_d (E_{II_d})

$$= \text{Power Consumption per month } II_d * 3600000 \text{ J}$$

$$= 3998.2734 \text{ kJ}$$

6 Comparative Analysis

On the basis of calculation of energy consumption, it has been observed that the proposed solution scheduling of data transmission consumes less energy in both on and off states of lights in comparison to continuous sending of data in both on and off states of lights.

Figure 8 illustrates the energy consumption of both on and off states of lights of the proposed system in both the above mentioned cases. Y- axis represents the energy consumption in kJ (kilo joules).

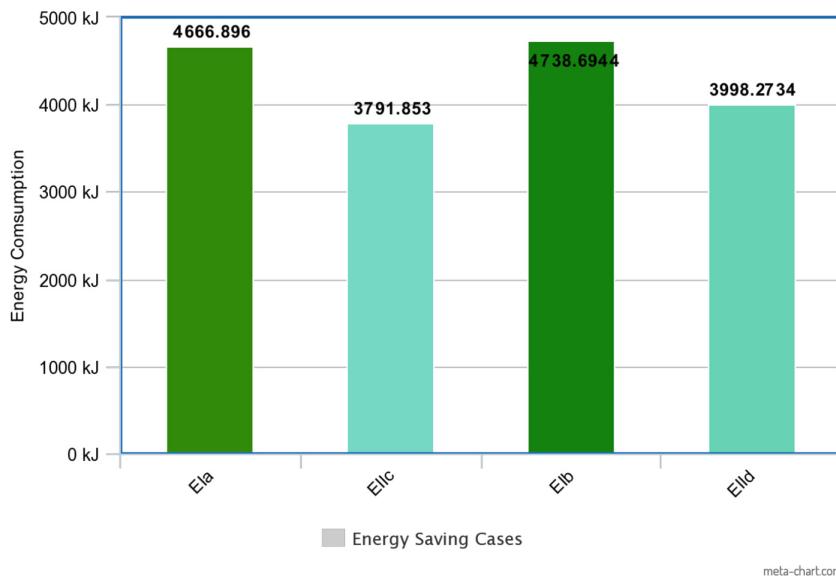


Fig. 8. Comparative analysis of energy consumption in proposed system

X - axis represents the energy consumption of implemented IoT based application in different cases as discussed above. It represents that the energy consumption of lights in off state when data is send continuously on cloud (E_{Ia}) is more than when data is send at scheduled interval of time (E_{IIc}). Similarly, energy consumption of lights in on state when data is send continuously on cloud (E_{Ib}) is more than when data is send at scheduled interval of time (E_{IId}).

Energy Efficiency off state

$$\begin{aligned}
 &= (\text{Energy Saving during off state}/ E_{Ia}) * 100 \\
 &= (875.043/4666.896) * 100 \\
 &= 18.75\%
 \end{aligned}$$

Energy efficiency of lights in off state is increased by 18.75% after implementation of proposed solution.

Energy Efficiency on state

$$\begin{aligned}
 &= (\text{Energy Saving during on state}/ E_{Ib}) * 100 \\
 &= (740.421/4738.6944) * 100 \\
 &= 15.625\%
 \end{aligned}$$

Similarly, energy efficiency of lights in on state is increased by 15.625% after implementation of proposed solution.

7 Conclusion

In this paper, it has been observed that when Wi-Fi module is in active state i.e. sending data through it, it consumes more power and when it is sending data continuously, then power consumption becomes high throughout the working of the system. And when Wi-Fi module is in ideal state i.e. not sending data through it, it consumes less power. While case study it has been noticed that there are many existing IoT based street lighting systems across the world. All these systems are saving energy by automation and remote monitoring features. However, none of the systems have focus on the energy consumption during data transmission process which results in high energy consumption. The proposed scheduling of data transmission solution in smart street lighting system saves energy by reducing energy consumption during transmission of data. The proposed solution handles the data transmission of data generated from IoT device to cloud such that transmission is scheduled at an interval of 1 h which avoids continuous data transfer and results in low energy consumption. The projected work assures the energy efficiency of proposed IoT system by verifying that periodic data transfer consumes less energy than continuous data transfer.

References

1. Energy Consumption from Internet of Things and Wireless Technology: 5G? IoT. <https://whatis5g.info/energy-consumption/>. Accessed 18 Dec 2018
2. Rouse, M.: What is a gateway? Definition from WhatIs.com. TechTarget. <https://internetofothingsagenda.techtarget.com/definition/gateway>. Accessed 19 May 2019
3. CISCO: Internet of Things At a Glance, CISCO, June 2016. <https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf>. Accessed 7 Dec 2018
4. Plus, R.: Powering up smart cities with Lithium - ion Batteries, TOSHIBA. <https://www.reuters.com/brandfeatures/road-to-a-new-day/powering-smart-cities-with-lithium-ion-batteries>. Accessed 02 May 2019
5. IPS Group: Smart Parking - The Power of Smart Technology IPS Group. IPS Group, Inc. <https://www.ipsgroupinc.com/the-power-of-smart-technology/>. Accessed 01 May 2019
6. Page, J.: A Town in Norway Installs Auto Dimming Street Lights to Cut Down on Energy Costs, Laughing Squid, 5 January 2018. <https://laughingsquid.com/auto-dimming-street-lights>. Accessed 23 Sept 2018
7. Luciano, M.: Top 10 smartest cities in the world. Advantage Business Marketing, 15 November 2017. <https://www.ecnmag.com/blog/2017/11/top-10-smallest-cities-world>. Accessed 7 June 2019
8. GI Technology: UPS for Smart City Device, Green ideas Technology. http://www.3rgit.com/Solutions/Solution/UPS_for_Smart_City_Device. Accessed 02 May 2019
9. Intelligent Lighting—Smart Street Lighting System—Street Light Sensors—Tvilight. TVILIGHT B.V. Amsterdam, 16 April 2018. <https://www.tvilight.com/>. Accessed 22 May 2019
10. Comlight: Motion Sensing Streetlighting System Solution - Comlight, Comlight AS. <https://www.comlight.no/solution/>. Accessed 1 June 2019
11. Smart City Applications—Telensa: Telensa. <https://www.telensa.com/applications#telensa-planet>. Accessed 10 May 2019

12. Tata Communications I & Jamshedpur Utilities and Services Company (JUSCO) deliver India's largest deployment of smart street lights. Tata Communications (2018). <https://www.tatacommunications.com/press-release/tata-communications-lights-the-way-for-jamshedpur-utilities-and-services-company-jusco-with-indias-largest-deployment-of-smart-streetlights/>. Accessed 10 May 2019
13. Muhamad, M., Ali, M.I.M.: IoT based solar smart LED street lighting system. In: TENCON 2018 - 2018 IEEE Region 10 Conference, pp. 1801–1806 (2018)
14. Tamilselvan, K., Deepika, K.S., Gobinath, A., Harhini, S., Gokhulraj, S.: IOT based street light monitoring system. Int. J. Intell. Advancements Res. Eng. Comput. **6**(1), 71–73 (2018)
15. Griffith, M.: Lihghting comparison: LED vs High Pressure Sodium (HPS) and Low Pressure Sodium (LPS). Stouch Lighting LED Lighting Solutions, 9 April 2019. <https://www.stouchlighting.com/blog/led-vs-hps-lps-high-and-low-pressure-sodium>. Accessed 2 June 2019



Smart Home Automation Using Fuzzy Logic and Internet of Things Technologies

Jignasha Sosa^(✉) and Jyoti Joglekar

Department of Computer Engineering, K. J. Somaiya College of Engineering,
Vidyavihar, Mumbai, India
{jignasha.s.jyoti.joglekar}@somaiya.edu

Abstract. At present, the home appliances such as light, fan, air conditioner, refrigerator, exhaust fan etc., are monitored in a manual way. With the advances of IoT technologies smart home automation is introduced for better service and optimum energy consumption. The proposed system uses Internet of Things technologies with primary goal to focus on the automatic control and monitoring of the appliances such as light and fan, without human efforts and to provide the manual operation of the appliances. This system provides an efficient energy management while using home appliances. In the proposed Home automation system the two smart devices work automatically by taking human presence and environment factors as an input and accordingly deliver a complete home automation system as an output. The energy saving and hence management can be done when smart light and smart fan switched off automatically when there is no presence of human being in the room using IR motion sensor inputs. Smart tube is automated using LDR sensor and IR motion sensor while smart fan is automated using temperature and humidity sensor with fuzzy logic as well as IR motion sensor. A mobile application is developed which is a user interface to control the devices.

Keywords: Home automation · Fuzzy logic · Smart fan · Smart light · Arduino uno · Internet of things

1 Introduction

A smart home automation system is developed using Internet of Things technologies for the devices such as light and fan. Arduino Uno microcontroller board is used for automation of light and fan. Arduino Uno microcontroller board is used with the Arduino integrated Development Environment (IDE) software to develop IoT based applications. In the proposed automation system, the smart light can be switched on and off based on the person visit count and enough light present in the room. The smart fan is switched on and off based on the person visit count to the room. The fan speed is controlled depending on the temperature and humidity parameters of an environment implemented using fuzzy logic.

2 Recent Work

The author in [1] described a smart home energy management system. The sensor data is analyzed using big data analytics. The Arduino board and Raspberry Pi board are used together for more efficient operating and controlling of the home appliances [2]. The author in [3] described, home appliances can be turned on and off and the variations are tracked with mobile application. The author has discussed in [4] about the network that consists of the hubs of sensors, actuators and other devices. By using the services of such hub, appliances can be controlled. The intelligent physical infrastructure is developed for smart home appliances, in the work of [5]. The smart home automation is implemented using Arduino Uno microcontroller board and Bluetooth Technology is described in [6–10].

The sensors are used to make the things smart. The author has presented in [11], the obstacle detection can be done using IR Sensor Module. This sensor is used to detect the count of a person who is entering inside the room and coming out of the room. The temperature and humidity can be calculated using DHT11 sensor [12]. The author has described in [13], the Bluetooth module HC-05 is used to connect the Arduino Uno microcontroller board with the mobile devices. The fuzzy logic methodology is presented and described in [14, 15].

3 Methodology

The home appliances can be operated automatically using Internet of Things technologies. In this proposed system uses microcontroller to instruct the sensors and actuators. The Arduino Uno ATmega 328P microcontroller accepts information from the sensors and analyzes the information to provide an output. The mobile application is designed that operate the smart light and fan in default and smart mode using Bluetooth connectivity. For the light system, the on and off operation can be performed in smart and default mode. The user can also operate the fan speed to off, low, medium and high in smart and default mode.

The system meets the expectations of functional requirements as well as the non-functional requirements such as usability, scalability and reliability. The software requirements of the system includes Arduino IDE for writing embedded C programs, the code is then push to the Arduino Uno. The mobile application is designed to display the status of the light and fan as on and off and fan speed status. The person is allowed to set threshold for the sensor. The hardware requirement of the system includes Arduino Uno, Sensors, and Actuators.

4 Design of the Proposed System and Implementation Details for Smart Home Appliances

The smart light and smart fan is switched on and off manually in default mode and automatically in smart mode. The block diagram of Smart Light and Smart Fan System is shown in Fig. 1.

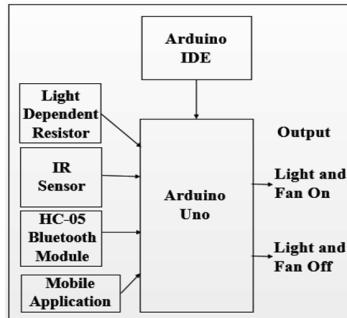


Fig. 1. Block diagram of smart light and fan system

4.1 Smart Light System

The system provides automated working of the home appliances such as light and fan. The smart light can be switched on and off automatically based on the person visit count when entering inside the room. If there is nobody present in the room, then the appliances will be switched off automatically. The user has flexibility of making a choice of operation in default mode and smart mode. The default mode allows user to switch the light manually by pressing the button on the screen of a mobile application. If a person chooses the smart mode then the appliances such as light can be operated automatically depending on light intensity evaluated from the LDR. The whole system is manipulated by the Arduino Uno microcontroller board which takes the input from the sensor and provides the output as on and off operation. The person is allowed to set the threshold of the LDR sensor manually using mobile application.

When a person enters the room, the ‘Person visit count’ is tracked by the IR sensor. The IR sensor takes the human body as an input while passing across the IR sensors located just outside and inside the door of the room. With this the human body is exposed to this human movement sensors while just entering the room and not for the long time, when the person present in the room, to reduce human body exposure to such IR motion sensors, as the effect of such sensing the body movement on human body is not yet clear. The light is switched on and off, based on the light intensity present in the room which is detected by LDR sensor. If there is darkness in the room then the light will be turned on and vice versa.

IR Sensor Module: Infrared Sensor Module is used to detect the presence of a person. In the proposed home automation system IR module is used for the bidirectional visit count of the person, entering inside and moving outside the room. The sensor also has the sensitivity adjustment which is useful for a range up to 20 cm [11].

DHT11 Temperature and Humidity Sensor Module: The DHT11 Temperature and Humidity Sensor Module is used for measuring the temperature and humidity with inbuilt NTC. The output which contains the temperature and humidity values is given as serial data using inbuilt 8 bit microcontroller [12].

HC-05 Bluetooth Module: The Bluetooth Module HC-05 is IEEE 802.15.1 standardized protocol which provides wireless communication between the board and mobile device [13].

4.2 Fan Speed Control Based Temperature and Humidity Using Fuzzy Logic

The fan speed can be controlled depending on the temperature and humidity factors of the environment. The fuzzy logic is implemented for the fan system that allows the fan speed to work in low, medium and high speed (Fig. 2).

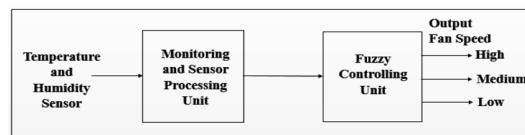


Fig. 2. Fan speed control using fuzzy logic based on temperature and humidity

The temperature and humidity is measured using DHT11 sensor. Fuzzy logic controller system is designed to control the fan speed. The smart fan can be operated at different speed. The fan speed is controlled to low, medium and high based on the input information of room temperature and humidity collected from the sensor DHT11. Three linguistic descriptors are assigned for each input and output variable. The rule-base is designed for the fuzzy logic by considering all combinations of the input variables as temperature and humidity of the room to decide the output variable speed of the fan [14]. For example if the temperature is low and humidity is low then the fan speed should be low. Similarly nine rules of the rule-base are designed. ‘Speed’ of the fan is controlled to low, medium and high. The three linguistic descriptors are defined for each input and output variables. The descriptors for temperature are low, medium and high {LT, MT, HT}. The descriptors for humidity are low, medium and high {LH, MH, HH}. The descriptors for fan speed are low, medium and high speed {LS, MS, HS}. The triangular membership functions for each input and output variable is given below (Fig. 3).

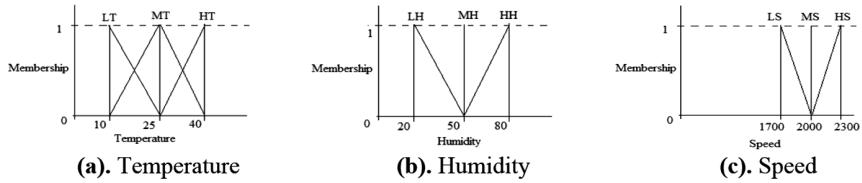


Fig. 3. Membership functions for the input and output variables for the fuzzy logic control

In this developed system temperature ranges from 0 to 40 degree Celsius. The humidity ranges from 0 to 80 RH %. The speed ranges from 1700 to 2300 rpm. The rule base is form for all nine rules, is shown in Table 1. The rule-base is implemented using fuzzy logic. The final step of defuzzification is applied on the evaluated rules to get the crisp value of the fan speed from the fuzzified output in rpm.

Table 1. Rule-base for the designed fuzzy logic

	Low humidity	Medium humidity	High humidity
Low temperature	Low speed	Low speed	Medium speed
Medium temperature	Medium speed	Medium speed	High speed
High temperature	Medium speed	Medium speed	High speed

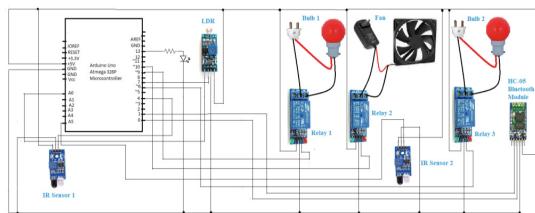


Fig. 4. Circuit diagram for smart home appliances: light and Fan

The connection setup is designed between the Arduino Uno microcontroller board, sensors, and appliances which is presented in the circuit diagram in Fig. 4. The code for the above system is written in the sketch of Arduino IDE. The pseudo code related to the system is given below.

Smart light system: Pseudo code

- 1 define infrared sensor pin, relay pin, LDR sensor pin to the pins of Arduino Uno
- 2 set the initial status of infrared sensor to high, set the threshold for LDR and initial count to zero
- 3 set the pin mode of sensors as an input and relay as an output
- 4 read the sensors value
- 5 if the count is greater than 1
 - check for enough brightness present in the room using LDR sensor
 - if threshold is smaller than set value read from LDR
 - set relay pin to low that describes darkness present in the room output as Light ON
 - else if threshold is greater than set value
 - set relay pin to high that describes brightness present in the room output as Light OFF
- 6 if count decrements
 - if count is smaller than 0
 - set relay pin to high that describes nobody present in the room and output control Light OFF
 - else
 - check for enough brightness present in the room
 - if threshold is smaller than set value read from LDR
 - set relay pin to low that describes darkness present in the room and output control Light ON
 - else if threshold is greater than set value
 - set relay pin to high that describes brightness present in the room and output control to ON

Smart fan system: Pseudo code

- 1 define infrared sensor pin and DHT sensor pin to the pins of Arduino Uno
- 2 set the initial status of infrared sensor to high, and initial count to zero
- 3 Initialize the ranges for temperature and humidity and define the ranges for each descriptors of temperature and humidity
- 4 Set the temperature and humidity variable as an input and speed variable as an output and add descriptors low, medium and high to the input and output variable.
- 5 Develop the nine fuzzy rules and create rule base with speed of fan as the output
- 6 read the temperature and humidity values from the sensor
- 7 Apply fuzzy logic control to fuzzify the input
- 8 Apply defuzzify the fuzzified input to get crisp control output
- 9 If the count is larger or equal to 1
 - The fan speed is controlled
- 10 If count decrements
 - If count is less than 0
 - set the fan OFF
- 10 else
 - The fan speed is controlled as per the control output

5 Results and Analysis

The results are gathered from the implementation system and presented some images screenshots of the mobile application in default mode and smart mode (Fig. 5).

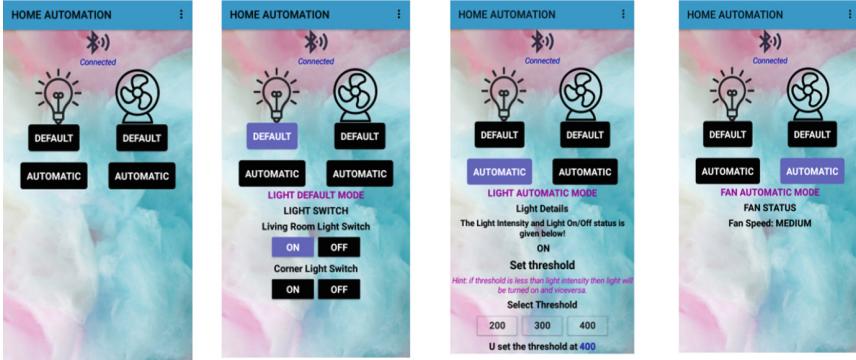


Fig. 5. Screenshots of mobile application to control remotely the mode of the devices

Following Table 2 shows some results of fan speed output based on temperature and humidity as input parameters as per the fuzzy logic.

Table 2. Fan speed in rpm depending on temperature and humidity

Temperature (C)	Humidity (RH %)	Fan speed (rpm)	Fan speed status
7	49	1736	Low
46	32	1993	Medium
35	73	2119	High

The following Figs. 6(a) and (b) are the readings of the results evaluated by applying fuzzy logic to the fan speed based on temperature and humidity. When the temperature is 12 and humidity is 25, the fan speed is 1955 rpm and when the temperature is 38 degree Celsius and humidity is 69% RH, the fan speed in rpm is 2032.

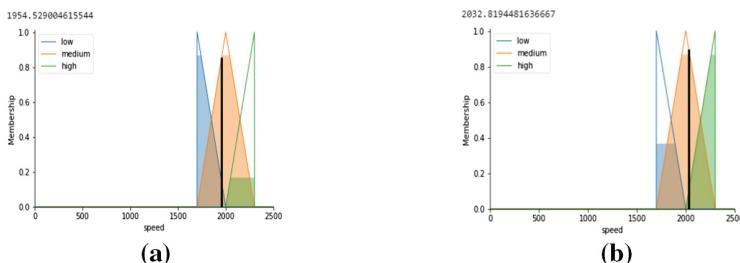


Fig. 6. (a). Test case 1 output membership function. The speed is 1955, when temperature is 12 °C and humidity is 25% (b). Test case 1 output membership function. The speed is 2032, when temperature is 38 °C and humidity is 69%

6 Conclusion

In the proposed home automation system Smart Light is switched on an off based on the persons' visit count to the room and room brightness. The Smart Fan is switched on and off based on the persons' visit count and fan speed is controlled to low, medium and high based on the novel design of the fuzzy logic controller using temperature and humidity parameters of the room. The user has flexibility of operating the appliances in default mode or smart mode. The proposed system provides and efficient energy management by saving in total expenditure of the electrical energy.

References

1. Al-Ali, A.R., Zualkernan, I.A., Rashid, M., Gupta, R., Alikarar, M.: A smart home energy management system using IoT and big data analytics approach. *IEEE Trans. Consum. Electron.* **63**(4), 426–434 (2017)
2. Harsha, S.L.S.S., Reddy, S.C., Mary, S.P.: Enhanced home automation system using Internet of Things. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, pp. 89–92 (2017)
3. Nagendra Reddy, P.S., Kumar Reddy, K.T., Kumar Reddy, P.A., Kodanda Ramaiah, G.N., Kishor, S.N.: An IoT based home automation using android application. In: 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, pp. 285–290 (2016)
4. Dey, S., Roy, A., Das, S.: Home automation using Internet of Things. In: 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, pp. 1–6 (2016)
5. Mandula, K., Parupalli, R., Murty, C.A.S., Magesh, E., Lunagariya, R.: Mobile based home automation using Internet of Things (IoT). In: 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, pp. 340–343 (2015)
6. Stauffer, H.B.: Smart enabling system for home automation. *IEEE Trans. Consum. Electron.* **37**(2), xxix–xxxv (1991)
7. Asadullah, M., Ullah, K.: Smart home automation system using Bluetooth technology. In: 2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT), Karachi, pp. 1–6 (2017)
8. Jabbar, W.A., Alsibai, M.H., Amran, N.S.S., Mahayadin, S.K.: Design and implementation of IoT-based automation system for smart home. In: 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, pp. 1–6 (2018)
9. Zhang, H., Li, G., Li, Y.: A home environment monitoring design on Arduino. In: 2018 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), Xiamen, pp. 53–56 (2018)
10. Lokhande, D.G., Mohsin, S.A.: Internet of things for ubiquitous smart home system. In: 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM), Aurangabad, pp. 314–320 (2017)
11. IR Obstacle Sensor. https://wiki.eprolabs.com/index.php?title=IR_Obstacle_Sensor. Accessed 30 Jan 2019
12. DHT11 – Temperature and Humidity Sensor. <https://components101.com/dht11-temperature-sensor>. Accessed 10 Oct 2018

13. Bluetooth Module HC-05. <https://www.electronicwings.com/sensors-modules/bluetooth-module-hc-05>
14. Lee, C.C.: Fuzzy logic in control systems: fuzzy logic controller. I. IEEE Trans. Syst. Man Cybern. **20**(2), 404–418 (1990)
15. Liu, B.-D., Chen, C.-Y., Tsao, J.-Y.: Design of adaptive fuzzy logic controller based on linguistic-hedge concepts and genetic algorithms. IEEE Trans. Syst. Man Cybern. Part B Cybern. **31**(1), 32–53 (2001)



A Survey of Block Cluster-Based Routing Schemes in Wireless Sensor Network

Vasudeva Pai^(✉) and Neetha Janis Tellis

Department of Information Science and Engineering,
N.M.A.M Institute of Engineering and Technology, Nitte, Udupi, India
paivasudeva@gmail.com, neethatellis4@gmail.com

Abstract. The WSNs involved enormous number of smart gadgets known as sensor hubs. The sensor hubs are collaborated together by numerous WSNs and these correspondence procedures are administrated by routing protocols. Execution of sensor arranges to a great extent that relies upon directing conventions, which are application based. Routing is a crucial innovation in WSNs and could be generally isolated into two classifications: flat routing and various hierarchical routing. In the paper, a review on block cluster based routing schemes for WSNs has been made. Strength, constraints of each plan are introduced.

Keywords: Wireless sensor networks (WSNS) · Block-cluster based routing · Routing schemes · Cluster head

1 Introduction

A sensor networks is a foundation contained detecting (estimating), registering, furthermore, correspondence components that enables an administrator to instrument, watch, and respond to occasions and wonders in a predefined situation. The administrator normally is a common, administrative, business, or mechanical substance. Nature can be the physical world, an organic framework, or a data innovation (IT) system [1]. Routing schemes [2] in WSN are used to discover and maintain the efficient routes, so that they can maintain a reliable and efficient communication.

WSN routing schemes could be partitioned into 3 categories based on writing survey on system structure-based routing plans: flat routing, hierarchical routing, and location-based routing [3]. In flat routing [4], all the hubs assume an equivalent job and hubs cooperate to play out a detecting task. In hierarchical routing, hubs executes different undertakings also are commonly gathered into groups dependent on particular requirements. This defines that the cluster is created and a specific task is given to a cluster head which will significantly results in lifetime, scalability, and energy efficiency of networks.

2 Routing Protocols in WSN

Routing is a way to discover a way linking source hub and the destination hub. Routing in WSNs is truly testing as the intrinsic characteristics that separates these systems from every other system. The structure of routing protocol in remote sensor networks is

influenced by a few exigent terms. The efficient correspondence can be accomplished in WSNs organizes by overcoming these variables. The classification of cluster based routing protocol is depicted in Fig. 1.

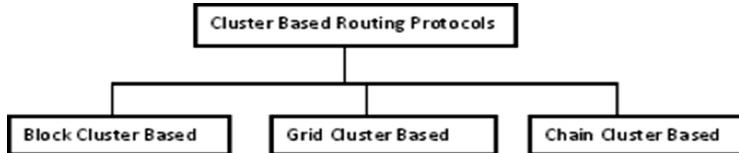


Fig. 1. Classification of cluster based routing protocol

3 Block Cluster-Based Routing Schemes

The block based routing protocols are Low-Energy Adaptive Clustering Hierarchy (LEACH), Hybrid Energy- Efficient Distributed (HEED), Unequal Clustering Size (UCS), Energy Efficient Clustering Scheme (EECS), Threshold-sensitive Energy Efficient sensor Network (TEEN), Chain-Cluster-based Mixed (CCM), LEACH with Virtual Force (LEACH-VF).

3.1 LEACH

Heinzelman [5] proposed Low-Energy Adaptive Clustering Hierarchy (LEACH) and is the first cluster-based WSN routing approaches. It has inspired many follow-up routing schemes based on clusters.

The principle objective of LEACH is to choose sensor hubs by rotation as group heads so that great energy in speaking to the base station is scattered to all sensor hubs in the network. Sensors elect themselves as neighborhood cluster heads with a specific probability at some random time. These cluster head hubs at that point communicate their status to the various sensors in the network. The hubs at that point figure out which cluster they need to join by selecting the group head that needs the base equivalence energy. After every hubs are settled into clusters, each cluster head makes a schedule for the hubs in its group. When the group head has the information from its hubs, the cluster head aggregates the information and afterward transmits the information to the base station. This is a high-energy transmission because it is far away from the base station. Since being group head depletes the battery of that hub, the cluster heads are not fixed, with the goal that energy utilization can be spread over various hubs. The activity of LEACH separates into rounds. Each round has two stages: the setup stage and steady-state stage. Groups are composed in setup stage; information is transmitted in the midst of the steady-state stage (Fig. 2).

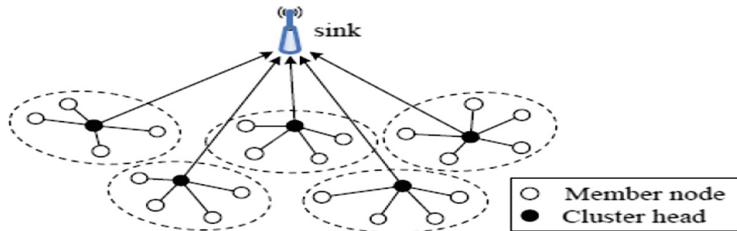


Fig. 2. Basic topology of LEACH

Advantages of LEACH [6, 7]

- (1) Each hub has an equivalent opportunity to turn into a group head, so that the heap is shared between hubs, it cannot be chosen as a cluster head in subsequent round.
- (2) Since LEACH uses Multiple Access Time Division (TDMA), it keeps cluster heads from pointless impacts.
- (3) LEACH can maintain a strategic distance from a ton of dissemination of energy by opening and shutting the correspondence interfaces of individuals in accordance with their schedule vacancies.

Disadvantages of LEACH [7]

- (1) Because it uses single-hop communication, it cannot be sent in systems spread over vast separations.
- (2) Because cluster heads are chosen based solely on probability and not on energy, LEACH cannot provide genuine adjustment of the burden.
- (3) Because group heads are selected based on probability, uniform dispersion cannot be guaranteed. In this way, the cluster heads are quite possibly packed in one piece of the system and a few hubs probably won't have any group heads in their region.
- (4) Possibility of dynamic clustering leads to additional overhead.

3.2 HEED

Hybrid Energy-Efficient Distributed (HEED) clustering was presented by Younis and Fahmy [8]. HEED's fundamental objective is to drag out system life. The main contrast among HEED and LEACH is the cluster head race; the group head race in HEED is not arbitrary. Group development depends on the intra-cluster residual energy of the hub and correspondence communication cost. Cluster heads have a greater normal residual energy than member hubs. The correspondence strategy of HEED is equivalent to LEACH.

Advantages of HEED

- (1) It is completely appropriated group based routing system.
- (2) It performs load adjustment and uniform group head conveyance due to lower control dimensions of clusters.

- (3) It accomplishes high energy effectiveness and adaptability by imparting in a multi-hop design.

Disadvantages of HEED

- (1) Energy utilization isn't adjusted on the grounds that more cluster heads are produced than the normal number.
- (2) As with LEACH, huge overhead is made because of numerous rounds.
- (3) HEED also has additional overhead attributable to some emphasis being placed on shaping groups.

3.3 UCS

The Unequal Clustering Size (UCS) model [9] was proposed by Soro et al. clusters of equivalent size may cause an uneven burden on the group heads, however an unequal size of clusters can give progressively adjusted energy utilization to cluster heads. It is primary unequal clustering scheme for WSNs. It is two-layered system model, and the sizes of the clusters contrast. The absolute number of hubs in each system relies upon the leftover energy of the cluster head. The group head is organized around the base station in two circles known as layers. Information transmission is done through numerous hops, where each group head advances its information to the nearest cluster head toward base station. Cluster heads are more unpredictable than the member hubs, and subsequently, progressively costly (Fig. 3).

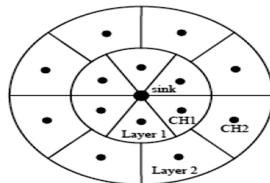


Fig. 3. Multiple-layer network topology in UCS

Advantages of UCS

- (1) To stay aware of correspondence load, the quantity of hubs in each cluster can be changed to keep up uniform energy utilization.
- (2) Compared to LEACH, UCS has lower energy utilization since it utilizes the two-layered system model and two-jump among cluster correspondences.

Disadvantages of UCS

- (1) UCS needs comprehensiveness as it is constrained by the presumption that the system is heterogeneous and that group heads are pre-decided [10].
- (2) Residual energy of common hubs is not considered, while cluster heads are constantly in the focus of the group.

- (3) Even though UCS has two-hops, it is not yet adequate for expansive range systems between cluster routing as it uses only two jumps for information transmission, and correspondence over long separations requires considerably more energy.

3.4 EECS

The Energy Efficient Clustering Scheme (EECS) was proposed by Ye et al. [11]. EECS is best suited for intermittent applications for gathering information. EECS is a LEACH expansion and varies from LEACH during group setup organize. EECS idea is to select group heads with increasingly remaining energy. It separates system into groups and they make use of direct single-hop correspondence among the cluster head and the base station. It makes uniform group heads over the system.

Advantages of EECS

- (1) EECS is building an increasingly adjusted system for the utilization of energy and correspondence load.
- (2) Since certain groups are supposed to impart a great deal of energy over long separations with the base station. EECS uses dynamic clusters estimation to take care of this issue.

Disadvantages of EECS

- (1) A large amount of energy is utilized to impart among cluster head as well as base station because of single-hop correspondences.
- (2) EECS utilizes worldwide data for communication, which includes a great deal of overhead.
- (3) Overhead unpredictability is made by rivalry between hubs in midst of cluster head election.

3.5 TEEN

Anjeshwar et al. [12] also proposed the Threshold-sensitive Energy Efficient Sensor Network (TEEN), which is a different leveled scheme for reactive systems. It is a mixture of different leveled and information-driven methodology. TEEN has a two-level grouping topology. TEEN task utilizes two edges: hard limit (H_T) and delicate edge (S_T). H_T is utilized for the detected property. S_T is utilized to indicate little variation in the estimation of detected characteristic. Here a group head sends its individuals it's H_T and S_T values. Hard edge and delicate limit attempt to diminish information interchanges (Fig. 4).

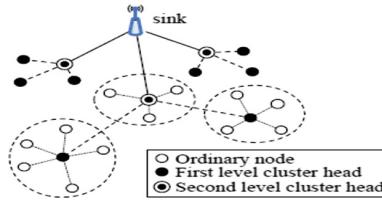


Fig. 4. The 2-tier clustering topology in TEEN

Advantages of TEEN

- (1) By differing two limits, information transmission is controlled.
- (2) It is appropriate for time-basic applications.

Disadvantages of TEEN

- (1) The primary downside is no matter where the limits are not met, hub will not convey the dust, and if hub bites the dust, it will probably not detected by the system [13].
- (2) Data might lost if cluster heads are not ready to speak with one another in the event that they are out of range from each other.

3.6 CCM

Chain-Cluster-based Mixed (CCM) routing was presented by Tang et al. [14]. It is a routing method that sorts out the sensor hubs as a level chains and a vertical cluster with just chain heads.

Stage 1: Chain-based routing Sensor hubs in every chain will send the information to their chain head utilizing chain-based routing. Every hub is situated in two-dimensional area with directions (x, y). This stage is separated into steps: Step 1 is to choose the chain head hub; the chain head is chosen in such a way as to uniformly appropriate energy utilization in the chain. Stage 2 is information transmission in the chain; CCM plans information transmission through an improved token component. After successful chain directing, it goes to second stage.

Stage 2: Cluster-based routing each chain head gets and intertwines information from its very own chain, chain heads at that point structure another group while every single other hub in every chain go into rest state. Group based routing is then separated into steps. In first Step, a cluster head is browsed among the chain-head cluster as a group after a completion of chain-based steering. The group head is picked dependent on leftover energy toward a start of cluster based routing. In Step 2, information transmission in the cluster is played out, the group head relegates an individual TDMA schedule opening for every part hub with the goal that the individuals can transmit their detected information to the group head time permitting space. The group head hub at that point combines all information and sends the intertwined information to the sink legitimately.

Advantages of CCM

- (1) In examination with LEACH, it has less vitality utilization.
- (2) In examination with PEGASIS, it has considerably less deferral.

3.7 LEACH-VF

LEACH with Virtual Force (LEACH-VF) was presented by Awad et al. [15] and applies the standards of virtual field force on every bunch inside a system so as to move the hubs to areas that expand the detecting inclusion and limit the transmitted energy. Two sorts of virtual force are utilized: an attractive force and a repulsive force. The LEACH-VF calculation can be separated into three stages. Stage 1 incorporates cluster development and setup. This stage is fundamentally the same as the one in LEACH, where the system is separated into groups by means of cluster head race, aside from in LEACH-VF the sensor hubs report their present area to the group head they are related with through the group join message. In Phase 2, the virtual power calculation and sensor hub migration are performed. Each group head applies the virtual field power standards to the sensor hubs related with it, after which the bunch head advises the sensor hubs regarding the new areas to which they should move. Stage 3 is the steady-state, or information transmission, which is equivalent to in LEACH.

Advantages of LEACH-VF over LEACH

- (1) It takes care of the issue of zones with covered detecting inclusion (i.e., regions secured by more than one sensor hub).
- (2) It takes care of the issue of detecting openings (i.e., regions with no detecting inclusion).
- (3) Some sensor hubs have inclusion outside the bunch zone in LEACH. Here these hubs can be moved to inclusion within the group zone.
- (4) In LEACH some sensor hubs are found moderately a long way from their bunch heads, however LEACH-VF moves them closer where they can in any case be valuable to the group at a lower vitality cost.

4 Conclusion

WSNs have excited an enthusiasm and critical consideration which is given to cluster based routing algorithm. In the paper, a complete overview of block-based cluster routing algorithms is presented. We examined the points of interest and characterization of block-based clustering algorithms in WSNs. The advantages and weakness of block based clustering algorithms are also listed in the paper.

References

1. Hu, F., Siddiqui, W., Cao, X.: SPECTRA: secure power-efficient clustered-topology routing algorithm in large-scale wireless micro-sensor networks. *Int. J. Inf. Technol.* **11**(2), 95–118 (2005)
2. Singh, S.P., Sharma, S.C.: A survey on cluster based routing protocols in wireless sensor networks. *Procedia Comput. Sci.* **45**, 687–695 (2015)
3. Sohraby, K., Minoli, D., Znati, T.: *Wireless Sensor Networks in Technology: Protocols and Applications*. Wiley, Hoboken (2007)
4. Sikander, G., Zafar, M.H., Raza, A., Babar, M.I., Mahmud, S.A., Khan, G.M.: A survey of cluster based routing schemes for wireless sensor network. *Smart Comput. Rev.* **3**(4), 261–275 (2013)
5. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: *Proceedings of 33rd Hawaii International Conference on System Sciences*, pp. 1–10 (2000)
6. Lai, W.K., Fan, C.S., Lin, L.Y.: Arranging cluster sizes and transmission ranges for wireless sensor networks. *Inf. Sci.* **183**(1), 117–131 (2012)
7. Liu, X.: A survey on clustering routing protocols in wireless sensor networks. *Sensors* **12**, 11113–11153 (2012)
8. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad-hoc sensor networks. *IEEE Trans. Mob. Comput.* **3**(4), 366–379 (2004)
9. Soro, S., Heinzelman, W.B.: Prolonging the lifetime of wireless sensor networks via unequal clustering. In: *Proceedings 19th IEEE International Parallel and Distributed Processing Symposium* (2005)
10. Peng, R., Qian, J., Sun, Y., Jiang, H., Lu, Z.: Energy-balanced scheme based unequal density of backbone for wireless sensor networks under coal mine. In: *Proceedings of the 2nd International Conference on Information Technology and Computer Science*, pp. 56–59, July 2010
11. Ye, M., Li, C., Chen, G., Wu, J.: EECS: an energy efficient clustering scheme in wireless sensor networks. In: *Proceedings of 24th IEEE International Performance, Computing, and Communications Conference*, pp. 535–540 (2005)
12. Manjeshwar, A., Agrawal, D.P.: TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: *Proceedings of 15th International Parallel and Distributed Processing Symposium*, pp. 2009–2015 (2001)
13. Kandris, D., Tsagkaropoulos, M., Politis, I., Tzes, A., Kotsopoulos, S.: A hybrid scheme for video transmission over wireless multimedia sensor networks. In: *Proceedings of the 17th Mediterranean Conference on Control & Automation, Makedonia Palace, Thessaloniki, Greece*, pp. 964–969, June 2009
14. Tang, F., You, I., Guo, S., Guo, M., Ma, Y.: A chain-cluster based routing algorithm for wireless sensor networks. *J. Intell. Manuf.* **23**(4), 1305–1313 (2010)
15. Awad, F.: Energy-efficient and coverage-aware clustering in wireless sensor networks. *Wirel. Eng. Technol.* **03**(03), 142–151 (2012)



Designing Features of Parallel Computational Algorithms for Solving of Applied Problems on Parallel Computing Systems of Cluster Type

Gennady Shvachych¹, Volodymyr Busygin^{1(✉)}, Khohlova Tetyana¹,
Boris Moroz², Fedorov Evhen³, and Kholod Olena⁴

¹ National Metallurgical Academy of Ukraine, Dnipro, Ukraine
busygint2009@gmail.com

² University of Technology, Dnipro, Ukraine

³ Cherkasy State Technological University, Cherkasy, Ukraine

⁴ University of Alfred Nobel University, Dnipro, Ukraine

Abstract. Paper considers problems of constructing maximum parallel forms of the algorithms of difference schemes, which are used to solve applied problems. The parallelization features are revealed by piecewise-analytical method of lines and the permutations' method. This is possible owing to the fact that the proposed approach excludes the recurrent structure for computation of the desired decision vectors, which, as a rule, leads to the rounding errors' accumulation. The parallel form of the algorithm made in this way is maximal, and, hence, has the minimum possible algorithm's implementation time using parallel computing systems.

Keywords: Multiprocessor system · Parallel algorithms · Applied problems · Finite differences · Permutation method · Parallelization

1 Problem Statement and Analysis of Recent Achievements

The urgency of the problem of developing numerical methods for solving multidimension systems of parabolic quasilinear equations describing the processes of heat and mass transfer can be considered undoubted. One of the most interesting examples of such systems can serve as the equations of hydrodynamics and metallurgical thermal physics [1–4]. This paper considers the problems of mathematical simulation of a similar class of problems on parallel computing systems of cluster type. Obviously, the mathematical simulation of large problems is impossible without computational equipment. But it turns out that for so many cases we need not just some kind of computer technology, but specifically the one with high-performance.

Currently, everything related to large computers and large problems is accompanied by the characteristic word “parallel”: parallel computers, computing systems, parallel programming languages, parallel numerical methods, etc. This term entered wide use almost immediately after the advent of the first computers. More precisely, almost immediately after realizing that the created computers are not able to solve many practical problems in an acceptable time. The way out of this situation was asking for

itself. If one computer does not cope with the problem solution at the right time, then we will try to take two, three, ten computers and force them to simultaneously work on different parts of the common problem, hoping to get the appropriate acceleration.

Therefore, parallel computing systems developed very quickly, and with the advent of computing clusters, parallel computing became accessible to many. This is due to the fact that for building clusters, as a rule, mass processors, standard network technologies and free software are used.

To date, there is a situation when the solution of one-dimensional non-stationary problems can be carried out with accuracy sufficient for most technical inquiries. About the mass solution of three-dimensional unsteady problems at the current level of technical feasibility and on the basis of traditional methods developed so far, it seems, we can only speak taking into account the following circumstances.

First, the advent of new and inexpensive means of communication for computing technology has stimulated the development of new information technologies (IT): structured programming; network operating systems; object-oriented programming, systems of parallel processing of information, etc. The organization of parallel processing of information flows, the connection of parallelization problems with the PC architecture, parallel programming systems, methods and algorithms of parallel computing - these are the key topics of the development of computing technology at this stage [5–10]. Note that in the field of global telecommunications, the leading positions are occupied by information technologies based on attracting Internet resources [4].

Secondly, by now there are certain trends in the development of computational methods with a complex logical structure, which have a higher accuracy order compared to traditional finite difference methods [11–15]. Serious progress in solving multidimensional spatial problems can be considered a series of proposals that are not quite equivalent to each other, but pursue one stereotypical goal - to reduce the task of three-dimensional distribution of the variable domain to a sequence of schemes that include unknown values only in one direction - alternately in the longitudinal, transverse and upright. A sufficiently detailed bibliography of these works is presented in [11–13]. Note that the use of implicit schemes in this case leads to systems of linear algebraic equations (SLAE) with a tridiagonal structure [15]. Thus, the adoption as a methodological basis of difference splitting schemes, firstly, provides an economical and stable implementation of numerical models using the scalar sweep method. And, secondly, it is known that the greatest effect from a parallel processor is achieved when it is used to perform matrix computations of linear algebra.

Taking into account the noted, we present the problems that need to be solved in this study:

Based on the construction of graphs of the computation process, develop algorithms characteristic of natural parallelism, which are able to ensure the effective application of a multiprocessor system. This, in particular, is an algorithm for complete parallelism by the numerical-analytical method of lines, an algorithm for parallelization by the “even-odd” reduction method.

At the same time, to propose a new approach to solving multidimensional nonstationary problems by means of full parallelization by the lines’ method. Such an approach, in comparison with the traditional one, should improve the economy, productivity and speed of computations. In addition, it should provide the highest degree of vectorization

of computations, predetermine the maximum parallel algorithmic form and, as a result, the minimum possible implementation time of algorithms on parallel computing systems.

Within the framework of decomposition algorithms based on the method of “odd-even” reduction, we propose a new approach to the distributed solution of three-diagonal systems of linear equations, which, in comparison with the known methods, is marked by a closed parallel form relative to the central grid point and a high vectorization measure.

2 Mathematical Problem Statement

Consider the solution of the Dirichlet boundary value problem for the one-dimensional heat equation

$$\frac{\partial Y}{\partial t} = \alpha \frac{\partial^2 Y}{\partial x^2}, \quad x \in [x_0, x_L], \quad t \in [t_0, T] \quad (1)$$

with initial

$$Y|_{t=t_0} = \varphi(x) \quad (2)$$

and boundary conditions

$$Y|_{x=x_0} = YW(t), \quad Y|_{x=x_L} = YL(t) \quad (3)$$

The domain of the sought function $Y(t, x)$ in the problem (1)–(3) is comparable to the grid area

$$\left. \begin{array}{l} t_j = J \times Dt1, \quad j = \overline{1, M}, \quad Dt1 = T/M, \quad M \in Z \\ x_p = p \times Dx1, \quad p = \overline{0, 2m} \quad Dx1 = (x_L - x_0)/2m, \quad m \in Z \end{array} \right\}, \quad (4)$$

wherein the introduction of the integer parameter m into the topology of building grid nodes in the spatial variable x will be highlighted below. Consider two ways of the problem discretization (1)–(3) [11–13].

The Finite Difference Method. The simplest implicit scheme in time and central differences in the x coordinate lead to SLAE

$$C_p Y_{p+1,1} - Y_{p,1} + D_p Y_{p-1,1} = f_{p,1}, \quad p = \overline{1, 2m-1}, \quad (5)$$

Wherein

$$\left. \begin{array}{l} C_p = D_p = \frac{A}{(1+2A)}, \quad A = \frac{\alpha}{Dx1^2} Dt1 \\ f_{p,1} = -\frac{YOp,1}{(1+2A)} \end{array} \right\}. \quad (6)$$

Here the grid functions $Y_{0,1} = fW(t_j)$, $Y_{2m,1} = fL(t_j)$, – carry information about the boundary conditions (3), and the right-hand sides $f_{p,1}$ – about the initial ones, since the grid functions $YO_{p,1}$ are taken from the previous j -1-st time layer. Consequently, the numerical algorithm (5), (6) is evolutionary and consists of acts of transition from one moment of time t_{j-1} to another $t_j = t_{j-1} + Dt$.

The lines method diagram [9]. After discretization of Eq. (1) with respect to the time variable, we obtain the system of second-order ordinary differential equations:

$$Y''_{p+\varepsilon_{x,1}}(\varepsilon_x) - \frac{1}{A} Y_{p+\varepsilon_{x,1}}(\varepsilon_x) = -\frac{1}{A} YO_{p+\varepsilon_{x,1}}(x), \quad (7)$$

wherein $YO_{p+\varepsilon_{x,1}}(x)$ – is the known initial function, $\varepsilon_x = \frac{(x-x_p)}{(x_{p+1}-x_p)} \in [-1, +1]$ – normalized spatial variable.

The general solution of Eq. (7) is represented in the final form:

$$Y_{p+\varepsilon_{x,1}}(\varepsilon_x) = Y^*_{p+\varepsilon_{x,1}}(\varepsilon_x) + C_p \eta \beta(\varepsilon) + D_p S \eta \beta(\varepsilon_x), \quad (8)$$

wherein C_p, D_p – the integration constants;

$Y^*_{p+\varepsilon_{x,1}}(x)$ – some particular solution of the inhomogeneous Eq. (7);

$\beta = \sqrt{\frac{1}{A}}$ – eigenvalues of the characteristic equation.

Determining integration constants C_p, D_p of the conditions for $\varepsilon_x = \pm 1$

$$Y_{p+\varepsilon_{x,1}}(\varepsilon_x)|_{\varepsilon_x \pm 1} = Y_{p \pm 1,1} \quad (9)$$

we obtain the solution of Eq. (7) in the following form:

$$\begin{aligned} Y_{p+\varepsilon_{x,1}}(\varepsilon_x) &= \left\{ Y^*_{p+\varepsilon_{x,1}}(\varepsilon_x) + \frac{S \eta \beta(1 + \varepsilon_x)}{S \eta \beta(2)} \left[Y_{p+1,1} - Y^*_{p+1,1} \right] \right. \\ &\quad \left. + \frac{S \eta \beta(1 - \varepsilon_x)}{S \eta \beta(2)} \left[Y_{p-1,1} - Y^*_{p-1,1} \right] \right\}. \end{aligned} \quad (10)$$

Putting in (10) $\varepsilon_x = 0$, we proceed from the distributed form of the solution to its discrete analogue in the form of SLAE (5), but with a different functional content:

$$\left. \begin{aligned} C_p = D_p &= \frac{S \eta \beta(1)}{S \eta \beta(2)} = \frac{1}{2C \eta \beta} \\ f_{p,1} &= C_p Y^*_{p+1,1} - Y^*_{p,1} + D_p Y^*_{p-1,1} \end{aligned} \right\}, p = \overline{1, 2m-1}, \quad (11)$$

that differs from the considered finite difference method, that has the form (6).

3 Paralleling the SLAE (5) by Permutations

The basis of the method of parallelization of the same mathematical problem - a system of linear algebraic equations in the form of (5) with functional content (6) or (11), put the algorithm of “odd-even” reduction [4]. The idea of this method is to exclude some coefficients of the system of Eq. (5) by elementary string transformations. We show that this procedure is possible if and only if the integer value of the parameter m in the topology of grid nodes along the x coordinate in (4) is, firstly, an even number, and, secondly, it satisfies the algebraic relation:

$$m = 2^{k_*}, \quad (12)$$

wherein k_* – is a natural number. The topology of countability of the internal nodes of the grid area along the x (4) coordinate for different values of the parameter m is as follows:

$$\begin{aligned} k_* &= 1, m = 2, p = \overline{1, 3}, \\ k_* &= 2, m = 4, p = \overline{1, 7}, \\ k_* &= 3, m = 8, p = \overline{1, 15}, \\ k_* &= 4, m = 16, p = \overline{1, 31} \end{aligned} \quad (13)$$

etc.

To the “odd-even” reduction algorithm operations set of a SLAE (5) to a parallel form, we assign a one-to-one correspondence to a set of points depending on the countability of the grid nodes on the set of $p = \overline{1, 2m-1}$. At the first stage of reduction, lowering and increasing the index p in SLAE (5) by one, we find:

$$\left. \begin{aligned} Y_{p-1,1} &= -f_{p-1,1} + C_{p-1}Y_{p,1} + D_{p-1}Y_{p-2,1} \\ Y_{p+1,1} &= -f_{p+1,1} + C_{p+1}Y_{p+2,1} + D_{p+1}Y_{p,1} \end{aligned} \right\}. \quad (14)$$

After substitution $Y_{p\pm 1,1}$ from relations (14) into Eq. (5), we obtain the SLAE of the same structure, but with respect to grid functions with even numbers $Y_{2,1}, Y_{4,1}, Y_{6,1}, \dots, Y_{2m-2,1}$:

$$C_p^{(1)}Y_{p+2,1} - Y_{p,1} + D_p^{(1)}Y_{p-2,1} = f_{p,1}^{(1)} \quad (15)$$

wherein

$$\left. \begin{aligned} C_p^{(1)} &= \frac{C_p^{(0)}C_{p+1}^{(0)}}{Det_1}, \quad D_p^{(1)} = \frac{D_p^{(0)}D_{p-1}^{(0)}}{Det_1} \\ f_{p,1}^{(1)} &= \left(f_{pu}^{(0)} + C_p^{(0)}f_{p+1,1}^{(0)} + D_p^{(0)}f_{p-1,1}^{(0)} \right) / Det_1 \\ Det_1 &= \left(1 - C_p^{(0)}D_{p+1}^{(0)} - D_p^{(0)}C_{p-1}^{(0)} \right) \end{aligned} \right\}, \quad p = 2, 4, \dots, 2m-2. \quad (16)$$

In relations (16), the sequences $C_p^{(0)}, D_p^{(0)}, f_{p,1}^{(0)}$ correspond to the coefficients and the right-hand sides of the original SLAE (5) in the form (6) or (11). Therefore, by eliminating variables with odd numbers, we received a SLAE two orders of magnitude lower. Having solved it, for example, by the sweep method, we can further find the values of variables with odd numbers by recalculation using Eq. (14).

To reapply this reduction process to the SLAE (15), first of all, it is necessary to construct a system of pair relations of the type (14). Lowering and increasing the index p in SLAE (15) by two units, we find:

$$\left. \begin{aligned} Y_{p-2,1} &= -f_{p-2,1}^{(1)} + C_{p-2}^{(1)} Y_{p,1} + D_{p-2}^{(1)} Y_{p-4} \\ Y_{p+2,1} &= -f_{p+1,1}^{(1)} + C_{p+2}^{(1)} Y_{p+4,1} + D_{p+2}^{(1)} Y_{p,1} \end{aligned} \right\}. \quad (17)$$

Substituting $Y_{p\pm 2,1}$ from relation (17) into Eq. (15), we obtain the SLAE of the same structure, but with respect to grid functions with even numbers of different multiplicity $Y_{4,1}, Y_{8,1}, \dots, Y_{2m-4,1}$:

$$C_p^{(2)} Y_{p+4,1} - Y_{p,1} + D_p^{(2)} Y_{p-4,1} = f_{p,1}^{(2)} \quad (18)$$

wherein

$$\left. \begin{aligned} C_p^{(2)} &= \frac{C_p^{(1)} C_{p+2}^{(1)}}{\text{Det}_2}, \quad D_p^{(1)} = \frac{D_p^{(1)} D_{p-2}^{(1)}}{\text{Det}_2}, \\ f_{p,1}^{(2)} &= \left(f_{p,1}^{(1)} + C_{p+2}^{(1)} f_{p+2,1}^{(1)} + D_p^{(1)} f_{p-2,1}^{(1)} \right) / \text{Det}_2, \\ \text{Det}_2 &= (1 - C_p^{(1)} D_{p+2}^{(1)} - D_p^{(1)} C_{p-2}^{(1)}). \end{aligned} \right\}, \quad p = 4, 8, \dots, 2m-4. \quad (19)$$

If we solve the SLAE (18) with respect to grid functions $Y_{4,1}, Y_{8,1}, \dots, Y_{2m-4,1}$, then the value of grid functions with even numbers of lower multiplicity $Y_{2,1}, Y_{6,1}$, etc. can be found by Eq. (17). Naturally, having determined the value of the grid functions with even numbers, then, using the Eq. (14), we can also determine the values of variables with odd numbers.

Obviously, repeated application of this process ultimately leads to a single equation with respect to the grid function of the central node $Y_{m,1}$. Indeed, having done this procedure successively k -times, firstly, we obtain pairwise relations for determining unknown multiplicities 2^{k-1} :

$$\left. \begin{aligned} Y_{p-2^{k-1},1} &= -f_{p-2^{k-1}}^{(k-1)} + C_{p-2^{k-1}}^{(k-1)} Y_{p,1} + D_{p-2^{k-1}}^{(k-1)} Y_{p-2^k,1} \\ Y_{p+2^{k-1},1} &= -f_{p+2^{k-1}}^{(k-1)} + C_{p+2^{k-1}}^{(k-1)} Y_{p+2^k,1} + D_{p+2^{k-1}}^{(k-1)} Y_{p,1} \end{aligned} \right\}, \quad (20)$$

and, secondly, the SLAE of the same structure, but with respect to grid functions is one order higher, i.e. multiplicities $2k$:

$$C_p^{(k)} Y_{p+2^k,1} - Y_{p,1} + D_p^{(k)} Y_{p-2^k,1} = f_{p,1}^{(k)} \quad (21)$$

wherein

$$\left. \begin{aligned} C_p^{(k)} &= \frac{C_p^{(k-1)} C_{p+2^{k-1}}^{(k-1)}}{\text{Det}_k}, \quad D_p^{(k)} = \frac{D_p^{(k-1)} D_{p-2^{k-1}}^{(k-1)}}{\text{Det}_k}, \\ f_p^{(k)} &= \frac{1}{\text{Det}_k} \left(f_{p,1}^{(k-1)} + C_p^{(k-1)} f_{p+2^{k-1},1}^{(k-1)} + D_p^{(k-1)} f_{p-2^{k-1},1}^{(k-1)} \right) \\ \text{Det}_k &= (1 - C_p^{(k-1)} D_{p+2^{k-1}}^{(k-1)} - D_p^{(k-1)} C_{p-2^{k-1}}^{(k-1)}) \end{aligned} \right\} \quad (22)$$

It is obvious that the algorithm for cyclic reduction of the original SLAE (5) to a single equation according to Eqs. (21), (22) has a dimension $k = \overline{1, k_*}$. Then, putting in relations (21), (22) $k = k_*$, and $p = 2^{k_*} = m$, we find:

$$Y_{m,1} = -f_{m,1}^{(k_*)} + C_m^{(k_*)} Y_{2m,1} + D_m^{(k_*)} Y_{0,1}, \quad (23)$$

wherein $Y_{0,1} = fw(t_j)$, $Y_{2m,1} = fL(t_j)$ are the known boundary functions (3), and the coefficients $C_m^{(k_*)}, D_m^{(k_*)}, f_{m,1}^{(k_*)}$ are the final result of the transformation of the initial parameters of SLAE (5) by the method of “odd-even” reduction of rows according to relations (21) into the final form of specific numbers.

We show that the sequence of these operations can be represented as a graph of a parallel algorithm [4].

Let $m = 2$, $p = \overline{1, 3}$. The coefficients of SLAE (5) $\{D_1, C_1, f_{1,1}\}$, $\{D_2, C_2, f_{2,1}\}$ and $\{D_3, C_3, f_{3,1}\}$ are known input data. Since for $m = 2$ for SLAE (5), the countability of the reduction process is $k = k_* = 1$, then by Eq. (22) with $k = 1$ and $p = 2$, we find

$$\left. \begin{aligned} C_2^{(1)} &= \frac{C_2^{(0)} C_3^{(0)}}{\text{Det}_1}, \quad D_2^{(1)} = \frac{D_2^{(0)} D_1^{(0)}}{\text{Det}_1} \\ f_2^{(1)} &= \frac{1}{\text{Det}_1} \left(f_{2,1}^{(0)} + C_2 f_{3,1}^{(0)} + D_2 f_{1,1}^{(0)} \right) \\ \text{Det}_1 &= (1 - C_2^{(0)} D_3^{(0)} - D_2^{(0)} C_1^{(0)}) \end{aligned} \right\} \quad (24)$$

Consequently, these quantities are quite sufficient for determining the grid function of the central site using Eq. (21). When $k = 1$ and $p = 2$ we find

$$Y_{2,1} = -f_{2,4}^{(1)} + C_2^{(1)} Y_{4,1} + D_2^{(1)} Y_{0,1}. \quad (25)$$

Further, using Eq. (20) with $k = 1$ and $p = 2$, we find the values of the grid functions $Y_{1,1}, Y_{3,1}$:

$$\left. \begin{aligned} Y_{1,1} &= -f_{1,1}^{(0)} + C_1^{(0)} Y_{2,1} + D_1^{(0)} Y_{0,1} \\ Y_{3,1} &= -f_{3,1}^{(0)} + C_3^{(0)} Y_{4,1} + D_3^{(0)} Y_{2,1} \end{aligned} \right\}, \quad (26)$$

as required.

Thus, the result of performing an operation using Eq. (25) can be interpreted as a necessary argument for performing two other operations using Eq. (26). It can be visually **depicted as a graph of the algorithm** shown in Fig. 1.

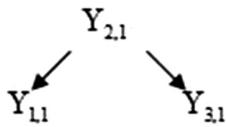


Fig. 1. The scheme of operations research SLAU (5) with $m = 2$

With $m = 2^3, p = \overline{1, 15}$ the process of reducing the original SLAE (5) to a single equation for the grid function of the central node $Y_{8,1}$ implemented in three steps of elementary string conversions. The graph of the SLAE study algorithm (5) for this case is depicted in Fig. 2.

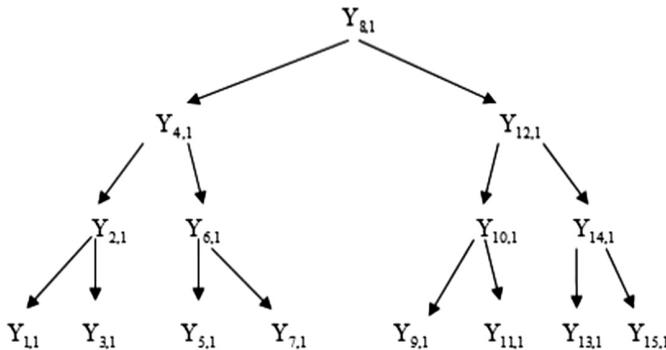


Fig. 2. Diagram of the operations of the SLAE study (5) with $m = 8$

Thus, the conducted research allowed discussing the most important properties of parallel forms of the SLAE study algorithm (5) using the “odd-even” reduction method. First, it is obvious that the use of graphs to describe and study the general problem of mapping the problems of computational mathematics of the algorithm described above to the architecture of parallel computing systems makes this procedure intuitive. Secondly, for example, from analysis of the operations sequence or SLAE (5) study

with $m = 8$, it follows that as soon as the value of the grid function of the central node is calculated $Y_{8,1}$ for zero level, variables $Y_{4,1}, Y_{12,1}$ can be calculated in parallel for the first level. After calculating the values of variables $Y_{4,1}, Y_{12,1}$ values of grid functions can be calculated in parallel $Y_{2,4}, Y_{6,1}, Y_{10,1}, Y_{14,1}$ for the second level. After calculating the values $Y_{2,1}, Y_{6,1}, Y_{10,1}, Y_{14,1}$ values of grid functions can be calculated in parallel $Y_{4,1}, Y_{3,1}, Y_{5,1}, Y_{7,1}, Y_{9,1}, Y_{11,1}, Y_{13,1}, Y_{15,1}$ for the third level. Thus, it is the third level that completes the procedure for studying the SLAE of this topology. Pay attention to the following circumstance. The algorithm graph introduced into consideration is parameterized by the parameter m and has an isomorphic structure of the branching of the vertices. There is a one-to-one correspondence between vertex numbers. The number of vertex generated by the two vertices of the lower tier is equal to the arithmetic average of the numbers of the vertices of the lower tier. Since at any level of the reduction process of the original SLAE (5) the decomposition of all intermediate systems can be performed in parallel, the algorithm discussed above has a sufficiently high degree of parallelism. Its use for solving tridiagonal systems on parallel PCs can be very promising [8].

4 Conclusions and Prospects of Further Research

When solving a number of applied problems, the researcher faces with a multitude of the most diverse and interrelated processes. This includes heat transfer and heat and mass transfer, including hydrodynamic processes in melts, taking into account changes in the state of a matter and deformation phenomena under the force and thermal loads, etc. Most of these processes can be described on the basis of differential equations of continuum mechanics, reflecting the objective laws of conservation of mass, momentum and energy. Such heat and mass transfer processes in many cases should be considered as large systems, the specificity of which is not only a large number of input and output values, but also their interconnection [1, 2, 4, 6, 7, 14, 15]. This paper considers the problems of mathematical simulation of a similar class of problems that are solved using cluster-type parallel computing systems [2, 6, 7, 9, 13–15]. This is because when solving problems of this type, the speed of computing technology should be measured in billions of operations per second. Therefore, parallel computing systems developed very quickly, and with the advent of computing clusters, parallel computing became accessible to many. This is due to the fact that for constructing clusters, as a rule, mass processors, standard network technologies and free software are used. Taking into account the above, this paper covers the issues of constructing the maximum parallel forms of the algorithms of difference schemes, which are used to solve applied problems. At the same time, the features of parallelization were revealed using the piecewise-analytical method of lines and the permutations' method.

In addition, the paper proposed a parallelization algorithm of three-diagonal systems of equations. It is known [1, 5] that most of the usual algorithms for solving three-diagonal systems of equations (methods of sweeping, decomposition of a matrix into a product of two-diagonal matrices, doubling, etc.) with several processors work, as a rule, not faster than with one processor. The reason for this is the essential sequence of

computations of these algorithms. In the proposed approach, on the contrary, many opportunities for parallelization are hidden.

References

1. Rouse, P.J.: Computational Fluid Dynamics. The World, Moscow (1980). 616
2. Shvachych, G.G., Ivaschenko, O.V., Busygin, V.V., Fedorov, Y.Y.: Parallel computational algorithms in thermal processes in metallurgy and mining. Naukovyi Visnyk Natsionalnogo Hirnychogo Universytetu. Sci. Tech. J. **4**(166), 129–137 (2018)
3. Na, T.Y.: Computational Methods in Engineering Boundary Value Problems. The World, Moscow (1982). 296
4. Ivaschenko, V.P., Shvachych, G.G., Sobolenko, A.V., Protopopov, D.V.: Information system of intellectual decision-making support of the rolling process. East Eur. J. Adv. Technol. **3**, 4–10 (2003). Иващенко В.П., Швачич Г.Г., Соболенко А. В., Протопопов Д. В.: Информационная Система Интеллектуальной Поддержки Принятия Решений Процесса Прокатки // Восточно- Европейский Журнал Передовых Технологий. 3. 4 – 10 (2003)
5. Voevodin, V.V., Voevodin, V.V.: Parallel Computations. BHV-Petersburg, Sankt Peterburg (2002). 600
6. Shvachych, G., Shlomchak, G., Moroz, B., Fedorov, E., Kozenkov, D.: Automated control of temperature regimes of alloyed steel products based on multiprocessors computing systems. Metalurgija **58**, 299–302 (2019)
7. Shvachych, G., Moroz, B., Pobocii, I., Kozenkov, D., Busygin, V.: Automated control parameters systems of technological process based on multiprocessor computing systems. In: Advances in Intelligent Systems and Computing, Las Vegas, Nevada, USA, vol. 2, p. 763. Springer (2019)
8. Evans, D.J. (ed.): Parallel Processing Systems. Moscow, p. 416 (1985)
9. Shvachych, G.G., Pobochii, I.A., Ivaschenko, E.V., Busygin, V.V.: Research of the problem of compatibility in the multi-processing compound systems. Sci. Rev. **1**(2(9)), 19–23 (2018)
10. Khokhlyuk, V.I.: Parallel algorithms for integer optimization. Radio and Communications, Moscow, 224 p. (1987)
11. Yanenko, N.N.: The Method of Fractional Steps for Solving Multidimensional Problems in Mathematical Physics. Science, Novosibirsk (1967). 196 p
12. Kovenya, V.M., Janenko, N.N.: The Method of Fractional Steps for Solving Multidimensional Problems of Mathematical Physics. Novosibirsk, 304 (1981)
13. Ivaschenko, V.P., Shvachych, G.G., Shmukin, A.A.: Parallel computations and applied problems of metallurgical thermophysics. Syst. Technol.: Reg. Interuniv. Collect. Sci. Works **123–138**, 56 (2008)
14. Ivaschenko, V.P., Shvachych, G.G., Tkach, M.A.: Specifics of constructing of maximally parallel algorithmic forms of the solving of the applied tasks. Syst. Technol.: Reg. Interuniv. Collect. Sci. Works **3–9**, 91 (2014)
15. Shvachych, G.G., Moroz, B.I., Pobochii, I.A., Ivaschenko, E.V., Busygin, V.V.: Maximally parallel forms of distributed simulation of the dynamic system. World Sci. **1**(4(32)), 12–20 (2018)



A Multi-parameter Based Resource Management Approach for Cloud Environment

Akkrabani Bharani Pradeep Kumar^(✉)
and Venkata Nageswara Rao Padmanabhuni

Department of Computer Science and Engineering, GITAM
(Deemed to Be University), Visakhapatnam, India
pradeep.peter97@gmail.com,
venkatnageswararao.padmanabhuni@gitam.edu

Abstract. In this paper, a multi-parameter based resource management (MPRM) model is proposed for dynamic provisioning instances based on the customer request submission. In MPRM three step model consist of (1) A prediction unit employed to calculate the submitted job estimated execution time (EET) and based on which it provisions the users' requests instantly or with a delay. (2) In order to balance the load of physical servers, a load balancer is employed to balance the incoming load with the help of VM while assigning. (3) In addition, a migration unit employed to balance and optimize the resource usage with the help of job queue and clustering techniques. The proposed model able to manage both large number of users' request and server load while keeping energy utilization in mind. The efficacy of the proposed model is tested with help of different randomized customized traces and is compared with different approaches.

Keywords: Cloud computing · Resource provisioning · Load balance · Live migration · Clustering

1 Introduction

The problem of green cloud computing starts from small computing units to large scale computing, storage units along with auxiliary equipments like cooling units, networking units [3]. A recent study on energy consumption of server farms [4] shows that electricity use for servers worldwide including their associated cooling and auxiliary equipment in 2005 cost US\$ 7.2 bn. The study also indicates that power consumption in that year had doubled as compared with consumption in 2020. The previous studies presents the energy consumption by these cloud data centers in 2010 is around 201.8 TWh in the whole world and this consumed energy is approx 1.1% to 1.3% of entire world's energy consumption [5]. As there is rapid growth in establishing cloud data centres [3] it is excepted to increase the cloud data center energy consumption up to 8% of the entire world by 2020 [6].

As per the current studies, at present only 11% to 50% of total resources are utilized in most of times [7], whereas these used data centers consume around 75% to 90% and

unused data centers also consume energy up to 50% [8]. Therefore virtual machine placement plays an important role in energy consumption. In this regard there have been some efforts to reduce energy consumption in cloud data center by placing VMs of underutilized servers onto moderately utilized servers and either shutdown the these servers or put these servers into sleep mode [9, 10].

Virtual machine consolidation is an implication on energy consumption in cloud data centers. The virtual machine placement VMP problem is optimization problem which places the virtual machine in physical machines in effective way [11, 12]. Number of VMP approaches proposed in the literature with different objectives [8]. All these proposed VMP approaches aims to maximize the profit and to minimize the operational cost [13]. In addition to delay based VMP load balancing and QoS awarded approaches improves the efficacy of the overall system [14, 15].

Virtual Machine Migration is one possible solution for server sprawl. Heuristic approach mentioned in [2] like load balancing, hot-spot mitigation and server consolidation is a way of managing the large VMs. When, where and which VM to migrate are necessary parameters that needed to be considered to achieve the same. In [16], a live migration process have proposed that moves memory, CPU and computational unit state of virtual machines from one machine to other. Live migration schemes differ according to the order of state transfer: *Pre-Copy Live Migration*: Implemented in most hypervisors such as VMWare, Xen and KVM, presented by Brandford et al. [18] that uses simple design and very low level communication between physical machines. In order to improve the performance, it uses a concept of pre-copy, Post-Copy Live Migration and Hybrid Post-Copy Live Migration approaches. In [17] as mentioned above is a technique that can be used to migrate VMs across the Data centers. In [19], Suresh, S, et al. proposed a virtualized system that uses the hardware level approach like Moore's lay and Chip Multi-Threading (CMT) which improve the performance because of multi-core CPUs of multiple processor cores inside a single physical CPU. In [19], according to Shu et al. the energy consumption and *makespan* associated with the resources allocated should be taken into account. In [20] author(s) proposed an improved cloud market algorithm which coordinates among market players for trading, which eventually reduces the cost cloud users. In this paper, we proposed a comprehensive prediction based VM management approach that aims to reduce energy consumption by reducing active physical servers in cloud data centres. The proposed model focuses on three key aspects of resource management. The rest of the paper is organised as follows. Section 2 presents the system model and its detailed architecture, followed by Sect. 3 presents experimental details and result discussion. Section 4 presents the conclusion.

2 Clustered Based Provisioning Model

Figure 1 presents the heuristic VM provisioning approach. The entire model is composed of three major units like, application prediction unit, cloud scheduler with load balancer and VM live migration. When the client or user sends request for new VM or reallocation of existing VM the request is received by the application mode controller. The application mode controller consists of a receiver and a predictor. The receiver

present in the application mode controller first receives the request made by the user and sends it to the predictor.

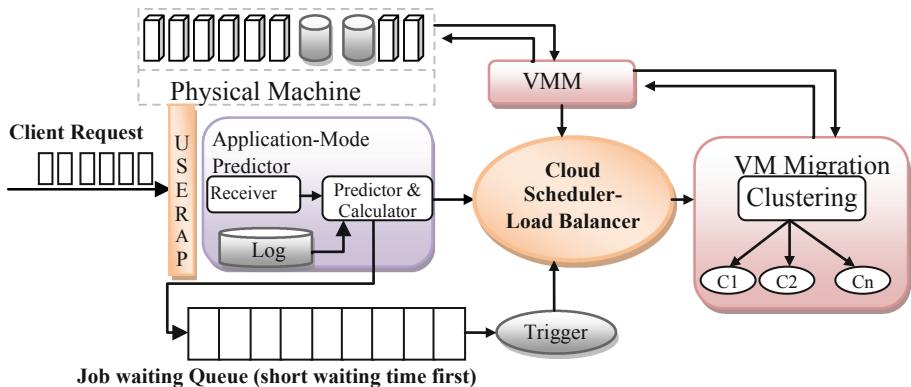


Fig. 1. Overview of MPRM model

2.1 Predictor

The main work of application mode controller is to divide the user request either into a relaxed or an immediate request accordingly which the request will be pushed into the job queue. This job is executed by the predictor present in the AMC. The job of the predictor is to predict whether the request is relaxed or immediate. Relaxed request is the request that has relaxation of time as compared to computing process. In real life scenarios, sometimes we can say most of the times the user make request to the system by estimating the most amount of time the task will take to execute or some kind of deadline in mind. The vendor can take advantage of this by calculating the exact time which the process will take. As the provider has the required amount of computing resource to calculate the same, by running necessary algorithm it can be easily found out how much time the task will take vs how much time the user has given and as the provider's job is to get the job done in or before time to satisfy the customer, where there is a large difference between the dead line and the execution time, the request is considered as relaxed mean while utilizing the remaining time to execute a task with less relaxation time. A relaxed request can be put in the waiting queue. Immediate request is the type of request that has no relaxation of time as the computing process is to be executed as soon as possible. Some cases the task can be of any industrial or government job that needs to be executed and result is mandatory as soon as possible. A short delay can't be tolerated in such cases for which this kind of request is labeled as immediate request. An immediate request is given higher priority and cannot be sent to the waiting queue. Instead request is directly sent to the cloud scheduler for instant execution.

2.2 Job Queue

The job queue is newly introduced in this model. Both relaxed and immediate request come to the queue not in any particular order, so the job queue is set to be updated on each new request. The job queue adds the request in the queue on acceptance of new request. Even after the requests are out of the AMC the requests are monitored with its remaining time for dead-line. AMC keeps track of the request as the priority may change in between the execution of tasks as the cloud environment is scalable and the task requested by the user is up to the user to decide the time required, So the request time might be changed at any time and according to that the job queue will adjust itself. The requests are sorted according to their waiting time before each job is either entered into the queue or upon addition of new request. The sorted list of task helps the queue decide which task to add to the job queue. The new request which has the shortest waiting time is added to the top of the queue. As we know, a queue in computer science has a top and a bottom where new request is added in the bottom and the removal is done at the top end of the queue. In this case, the queue is a dynamic one and is updated on each coming request. Hence, here the immediate requests are added to the top of the queue according to their waiting time and same goes for the relaxed requests and as the task list is sorted, In the end the whole list is sorted according to their waiting time. The checking is done on addition of new request in the queue. The job having shortest waiting time is executed first and then is given to the trigger. The trigger receives the request from the job queue and redirects it to the cloud scheduler.

2.3 Cloud Load Balancer

The objective of incorporating a scheduler/load balance is to schedule the incoming load in a balanced way. The primary job of the cloud scheduler is to execute the requests by sending them to the VMM to create or resize the VMs. The VMM (Virtual Machine Monitor) is a software module which enables the creation and management of virtual machines and manages the function of a virtualized environment which is employed on top of a physical machine. VMM monitors all the VM continuously in order to check imbalance situations. In such cases, load balancer balances the load by migrating the load across VMs in order to maintain the utilization level below the threshold level to minimize the energy consumption.

2.4 VM Migration

The Load Balancer or the VMM maintains the VMs by using migration techniques. In this case, the VMM maintains the VMs in form of clusters which are formed according to the CPU load across all the VMs present in the PM. Here using K-means clustering the VMs are basically divided into 3 groups, namely under-utilized clusters, balanced cluster, and over-loaded clusters.

The clustering is done by taking parameters such as CPU utilization, uptime, energy consumption. Underutilized cluster is the clusters which has more energy consumption as compared to the low CPU utilization ($\leq 30\%$ load). The VMs in these clusters are mostly ideal and hence consuming unnecessary amount of energy for a

longer period of time. This cluster causes cold-spot in the system. Balanced cluster is the type of cluster which has average consumption of energy and CPU load ($\leq 70\%$). This is called balanced as the ratio of CPU load and energy consumption is in equilibrium state which results in high efficiency of the system both in means of CPU utilization and energy consumption. We try to migrate most load from both the under-utilized and over-utilized cluster to increase the efficiency of the system as a whole. Over-loaded cluster is the type of cluster which has huge amount of energy consumption and maximum CPU load ($>70\%$). The VMs in this clusters consumes most of the CPU load which causes in high energy consumption, also known as Hot-Spot. As both the VMs in Under/over utilized clusters are not efficient, using either migration techniques or Load-Balancing techniques the clusters are managed for maximum efficiency. The under-utilized cluster migrates its load to balanced cluster to cut off the energy consumption as an under-utilized VM consumes as much energy as a balanced cluster. At times load from either balanced cluster or over loaded cluster is migrated to this cluster making it a balanced one.

2.5 K-Mean Clustering

In real life scenario, millions of servers are incorporated in a single data center and the number of VMs are operating at a single time is very large, which is very difficult and close to impossible now a days to manage using manual process. At present most of service providers' handling huge response with automated process. However, the real time usage of VMs and working PMs will still be a problem as the number of generated hot-spot, cold-spot and Load imbalance is at a real time basis, thus rather than maintaining them individually, we can maintain them by forming clusters, which consists of similar loads. Operating and maintaining them at once will be time and energy efficient and will be less complex. We can use any pre-existing clustering algorithms to group the VMs. In our paper, we are using K-Mean Clustering, As our main focus is to minimize the number of operations by taking minimum clusters and over-utilized clusters respectively.

Figure 2 presents the clustering approach, which shows the how load balancer switches from one scenario to another. In this approach, we have grouped the VMs into three clusters and are transferring load among them. The clusters are formed based on the parameters like CPU-utilization, Up-time of VM, waiting time, Dead-line as parameters. After generating the clusters, at the time of VM-migration/load-balancing, it will be easier to operate on a cluster rather than managing VMs individually. Migration will take place from over-loaded VMs to under-utilized cluster by making them balanced clusters as the load will be increased. Similarly, the load of under-utilized cluster will be transferred to the balanced cluster. The final goal is to increase the number of VMs in the balanced cluster. In case of over-utilized cluster, the load will be transferred to the clusters (under-utilized/balanced) and this will be decided according to the energy consumption i.e. in which case the energy consumption will be lower, then it will be transferred to that cluster. The migration will be both periodic and emergency situation based (server sprawl). So, that the number of VMs in a cluster that are selected for migration is limited. As it is easy to manage a constant number of VMs at a time rather than numerous. After the formation of clusters, at the time of VM-

migration/load-balancing, it will be easy to operate on a cluster rather than managing each VM individually. Migration will be done from over-loaded VMs to under-utilized clusters by making them under-utilized clusters. Similarly, the load of under-utilized cluster will be transferred to the balanced cluster. The final goal is to increase the number of VMs in the balanced cluster. In case of over-utilized cluster, the load will be transferred to the cluster (under-utilized/balanced) and that will be decided according to the energy consumption i.e. in which case the energy consumption will be lower. The migration will be both periodic and emergency situation (server sprawl). As the number of VMs in a cluster that is selected for migration is limited and it will be easier to manage a constant number of VMs at a time rather than the whole cluster.

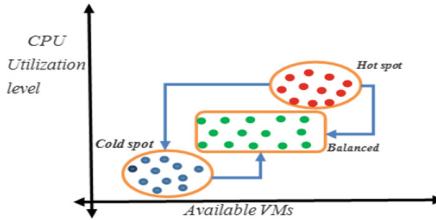
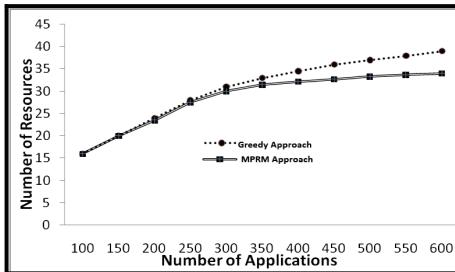
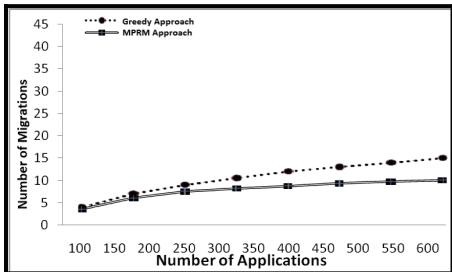
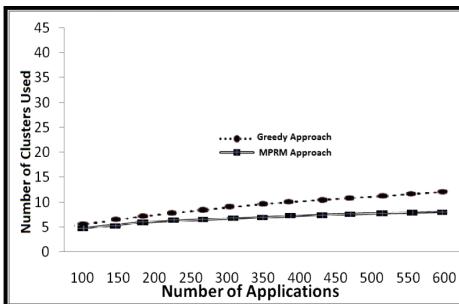
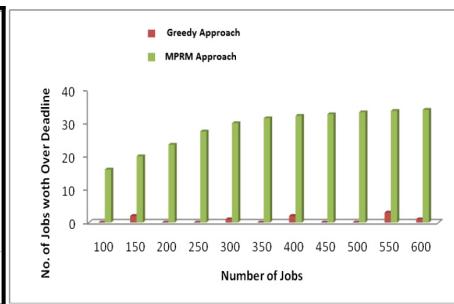


Fig. 2. Overview of clustering approach

3 Experimental Setup and Result Discussion

The proposed model is implemented using MatLab and synthesized traces are generated with the help of random approach. Figure 3 depicts the resource utilization for user submitted jobs. The proposed approach presents the efficacy of resource utilization. The proposed approach performance is close to the [3] without pre-copy and post-copy concept. Figure 4 presents the energy consumption of cloud resources (energy consumption of network devices are not considered in energy consumption model). A simple energy calculation model employed in order to calculate, and in case of complex approaches calculated range may slightly vary. Energy model is formulated using different parameters like idle time of resource and usage time as presented in [6]. Figure 4 depicts the efficacy of the proposed approach in terms of number of migration required and Fig. 5 depicts the number of clusters used to schedule the user application requests. Figure 6 depicts the efficacy of applications exceeds the provided due execution time. The proposed model efficacy is compared with few existing policies and it is found that performance of our combinatorial model is better than the existing with above mentioned simulation parameters.

**Fig. 3.** Resource utilization performance**Fig. 4.** Migration performance**Fig. 5.** Clusters performance**Fig. 6.** Application deadline performance

4 Conclusions

This paper proposes and investigates different resource provisioning approaches to reduce both application completion time and to increase the resource utilization of traces. The proposed model investigates several heuristics for instance provisioning with different types of applications and efficacy of the proposed MPRM model with clustering better than the without clustering. Experimental results depict the proposed heuristic provisioning approach with clustering improves the performance (CSU's resource utilization) around 2% to 12%, 4% to 13% in case of migrations and 8% in case of number of clusters required to provision the user requests and huge difference in case of maintaining application deadline as compared to Greedy approach.

References

1. Armbrust, M., et al.: A view of cloud computing. *Commun. ACM* **53**(4), 50–58 (2010)
2. Mishra, M., et al.: Dynamic resource management using virtual machine migrations. *IEEE Commun. Mag.* **50**(9), 34–40 (2012)
3. Greenpeace: Make it green: cloud computing and its contribution to climate change. Greenpeace International, April 2010. <http://www.thegreenitreview.com/2010/04/green-peacereports-on-climate-impact-of.html>

4. Koomey, J.G.: Estimating total power consumption by servers in the U.S. and the world. Lawrence Berkeley National Laboratory, Stanford University (2007)
5. Gao, P.X., Curtis, A.R., Wong, B., Keshav, S.: It's not easy being green. ACM SIGCOMM Comput. Commun. Rev. **42**(4), 211–222 (2012)
6. Koomey, J.: Growth in data center electricity use 2005 to 2010. Analytics Press, Oakland, August 2011. <http://www.analyticspress.com/datacenters.html>
7. Dasgupta, G., Sharma, A., Verma, A., Neogi, A., Kothari, R.: Workload management for power efficiency in virtualized data centers. Commun. ACM **54**(7), 131–141 (2011)
8. Greenberg, A., Hamilton, J., Maltz, D.A., Patel, P.: The cost of a cloud: research problems in data center networks. ACM SIGCOMM Comput. Commun. Rev. **39**(1), 68–73 (2009)
9. Meisner, D., Gold, B.T., Wenisch, T.F.: PowerNap: eliminating server idle power. In: Proceedings of 14th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2009), pp 205–216 (2009)
10. Microsoft Inc.: Explore the features: performance (2009). <http://www.microsoft.com/windows/windows-vista/features/performance.aspx>
11. Bianchini, R., Rajamony, R.: Power and energy management for server systems. Computer **37**(11), 68–76 (2004)
12. Vogels, W.: Beyond server consolidation. ACM Queue **6**(1), 20–26 (2008)
13. Xiao, Z., Chen, Q., Luo, H.P.: Automatic scaling of internet applications for cloud computing services. IEEE Trans. Comput. **63**(5), 1111–1123 (2014)
14. Harsha, L.S., Reddy, K.H.K., Roy, D.S.: A novel delay based application scheduling for energy efficient cloud operations. In: 2015 International Conference on Man and Machine Interfacing (MAMI), pp. 1–5. IEEE, December 2015
15. Mudali, G., Roy, D.S., Reddy, K.H.K.: QoS aware heuristic provisioning approach for cloud spot instances. In: 2017 International Conference on Information Technology (ICIT), pp. 73–78. IEEE, December 2017
16. Reddy, K., Mudali, G., Roy, D.S.: Energy aware heuristic scheduling of variable class constraint resources in cloud data centres. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, p. 13. ACM, March 2016
17. Shribman, A., Hudzia, B.: Pre-copy and post-copy VM live migration for memory intensive applications. In: Euro-Par Workshops (2012)
18. Bradford, R., Kotsovinos, E., Feldmann, A., Schiberg, H.: Live wide-area migration of virtual machines including local persistent state. In: VEE 2007 Proceedings of the 3rd International Conference on Virtual Execution Environments, pp. 169–179 (2007)
19. Suresh, S., Sakthivel, S.: Saivmm: self adaptive intelligent vmm scheduler for server consolidation in cloud environment. J. Theor. Appl. Inform. Technol. **68**(3) (2014)
20. Reddy, K.H.K., Mudali, G., Roy, D.S.: A novel coordinated resource provisioning approach for cooperative cloud market. J. Cloud Comput. **6**(1), 8 (2017)



A New (3, 3) Secret Sharing Cryptography Scheme for Efficient Secret Data Transmission

Ariba Tariq^(✉) and Rajitha Bakthula

Motilal Nehru National Institute of Technology Allahabad, Prayagraj, India
aribatariq.17@gmail.com, rajitha@mnnt.ac.in

Abstract. The increased rate of internet usage in data transmission has led to the tampering or loss of data over the internet. The transmitted data may contain some confidential information, wherein the privacy of the information cannot be compromised. Secret Sharing scheme is used to secure the transmitted data. It deals with hiding a secret image (text image, scenery, etc.) into various cover images and then transmitting over the web to the receiver. Thus, a secret sharing scheme is proposed in this paper where a secret image is hidden in 3 cover images using LSB (least significant bit) technique to protect it during transmission. Each share contains a part of the secret image but the secret cannot be revealed independently. After comparing the proposed method with the state-of-the-art approaches, it was found to be the best.

Keywords: Secret Sharing · Digital images · Secret image · Cover image · Stego image · LSB · PSNR · SSIM

1 Introduction

Information is becoming important in our daily lives. Its value increases when it is shared. Nowadays, it is even possible for a video, audio and images to be shared as an information. The transmission of information increases concern regarding its privacy and security. The security of information has been a concern since ancient times. Many techniques are developed to ensure the safety of the transmitted information. With the advancement of information technology, digital images have become increasingly important. It might contain some personal information therefore, its privacy cannot be compromised. Attackers may try to access unauthorized information and misuse it. The sharing of information to provide security is known as Secret Sharing [15]. For images and video, it is termed as Visual Secret Sharing scheme [1]. Secret Sharing is a scheme which actually does not involve any cryptographic techniques [9]. It was proposed at Eurocrypt'94 by Naor and Shamir [16]. It is a technique used to protect image-based secrets. Thus, Secret Sharing can be used to provide confidentiality and protection to secret images, and it makes the information undetectable [4]. In secret sharing scheme, a secret image (text-based, scenery etc.) is hidden into various cover images. Shares are obtained after embedding the secret into cover images. Each of the shares contain some part of the secret but none of the shares can reveal the secret independently. Based on the method of sharing used, either some or all of the shares are required to extract the secret.

A (t, n) secret image sharing scheme was developed by Thien and Lin [15] in 2002 that was a variant of Shamir's scheme. Later, in 2004, a (t, n) scheme with steganography and authentication algorithms was proposed by Lin and Tsai [13] that was based on polynomial interpolation. The work of Thien and Lin was extended by Wang and Su [12]. They proposed a scheme in which the size of shadow images was reduced [2]. All these techniques were secure but produced random images which can arise suspicion of attackers and therefore when such images are shared, it is subject to security threats. To increase the security, the shared images are hidden within meaningful cover images. This paper also proposes a method where the secret image is embedded within 3 meaningful cover images. The number of shares is equal to the number of cover images. It uses LSB technique as it is one of the most robust methods among various steganography methods.

1.1 Secret Sharing in Spatial Domain

The term spatial refers to space. The spatial domain [8, 10] refers to the image plane. The methods in spatial domain directly modify the pixel values in order to modify the images. The processes in spatial domain are represented as follows:

$$I_1(x, y) = T[I(x, y)]$$

Here, I is the original image, (x, y) are the pixel values for I . After applying some function T on I , we obtain the image I_1 which is the modified image. This paper uses spatial domain technique to embed the secret image into cover images. Embedding in spatial domain involves changing the LSB's [5]. For embedding process, the pixel values of an image are directly modified in the spatial domain mechanism. They involve very less modification and are therefore, simple and efficient. Thus they require less time for computation [6, 7].

The remaining sections of the paper are organised as follows. Section 2 describes the Proposed method. Results and performance analysis is discussed in Sect. 3. Section 4 finally concludes the paper with future scope.

2 Proposed Method

The proposed method is a simple method of applying embedding to hide the secret image into cover images and then extracting it from the same. It uses three meaningful cover images and one secret image (here, text-based secret image). First, the bits of the secret image are extracted and three MSB's are embedded in Cover 1, next three bits are embedded in Cover 2 and at last, the two LSB's are embedded in Cover 3. For extraction, the LSB's from each of the shares are extracted and concatenated to form the extracted secret. The embedding and extraction methods are described as follows:

2.1 Embedding Method

In this method, the inputs are three meaningful cover images and one secret image. The output is the stego image or the shares, which are obtained by applying embedding method to hide the secret image into the cover images. The shares appear similar to the cover image and cannot reveal any existence of the secret image embedded in it. The steps in this method are depicted in Fig. 1. The input cover images are of the size 512×512 . The cover images and the secret image are shown in Fig. 2, where (a), (b), (c) are the meaningful cover images and (d) is the secret image. If the size of the secret image is smaller than the cover images, it is tiled with 1's and then resized so that its size is equal to the size of the cover images. For each pixel of the secret image, the bits (b_1-b_8) are extracted. The bits b_1, b_2, b_3 are embedded in the 3 LSB's of the cover image 1. The bits b_4, b_5, b_6 are embedded in the 3 LSB's of the cover image 2 and finally, the bits b_7, b_8 are embedded in the 2 LSB's of the cover image 3. The shares obtained after embedding the bits into the cover images are termed as Share 1, Share 2 and Share 3. Algorithm 1 depicts the complete process of embedding phase.

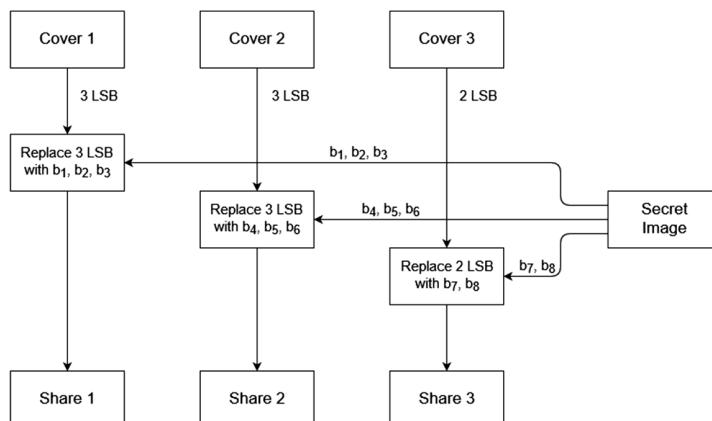


Fig. 1. Embedding method

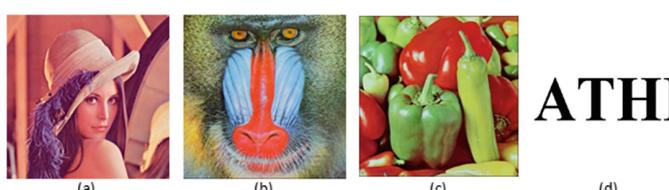


Fig. 2. (a)–(c) Cover images and (d) Secret image

Algorithm 1 Embedding Phase

```

1: procedure EMBED( $a, b, c, d$ )            $\triangleright a,b,c$  are covers,  $d$  is secret
2:    $b1 - b8 \leftarrow$  bits of secret
3:   for all pixels in secret do
4:     Replace 3 LSB's of  $a$  with  $b1, b2, b3$ 
5:     Replace 3 LSB's of  $b$  with  $b4, b5, b6$ 
6:     Replace 2 LSB's of  $c$  with  $b7, b8$ 
7:   end for
8:   return  $e, f, g$        $\triangleright e,f,g$  are shares corresponding to  $a,b,c$  respectively
9: end procedure

```

The output of the embedding method is the shares. The number of shares obtained after embedding in this method is equal to the number of cover images, i.e., 3. Figure 3 (a), (b) and (c) shows the images after the secret is embedded in Fig. 1(a), (b) and (c) cover images respectively.

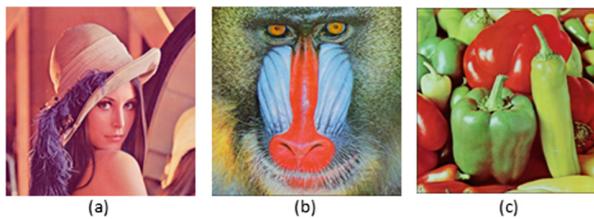


Fig. 3. Shares obtained after embedding method

2.2 Extraction Method

In this method, the input is the shares generated by applying the embedding method to hide the secret image into cover images. The secret is extracted from it. The steps in this method are depicted in Fig. 4. The LSB's are extracted from the shares correspondingly. The 3 LSB's from the share 1 are stored as b_1, b_2, b_3 . Then the 3 LSB's from share 2 are stored as b_4, b_5, b_6 . At last, the 2 LSB's from the share 3 are stored as b_7, b_8 . All the bits are finally concatenated to obtain the secret. Algorithm 2 depicts the working of the extraction phase. Figure 5 shows the original secret and the extracted secret.

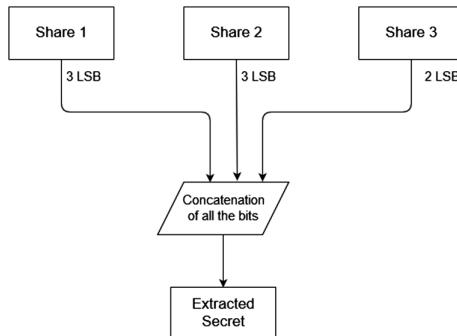


Fig. 4. Extraction method

3 Results and Performance Analysis

The obtained results are shown in Fig. 6. The Fig. 6(a)–(c) depicts the cover images and Fig. 6(d) is the original secret image that are used as input in the proposed method. Figure 6(e)–(g) depicts the three shares obtained after applying the embedding method on the cover images (a)–(c). Figure 7(a)–(c) depict the cover images and Fig. 7(d)–(f) depicts the output when the cover images (a)–(c) are tampered respectively.

Algorithm 2 Extraction Phase

```

1: procedure EXTRACT( $a, b, c$ )                                 $\triangleright a, b, c$  are shares
2:    $b1 - b8 \leftarrow 0$ 
3:   for each pixel do
4:     Extract 3 LSB's from  $a$  and store as  $b1, b2, b3$ 
5:     Extract 3 LSB's from  $b$  and store as  $b4, b5, b6$ 
6:     Extract 2 LSB's from  $c$  and store as  $b7, b8$ 
7:   end for
8:    $e \leftarrow b1-b8$ 
9:   return  $e$                                                $\triangleright e$  is the extracted secret
10: end procedure
  
```



Fig. 5. (a) Original secret, (b) Decrypted secret image

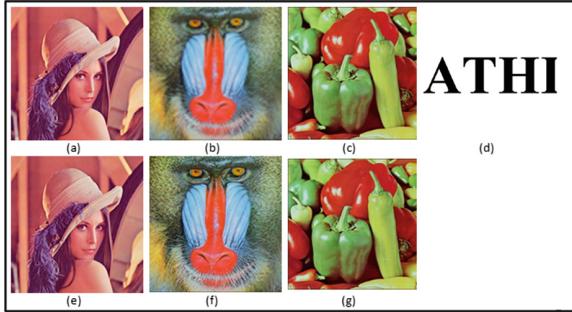


Fig. 6. (a)–(c) Cover images, (d) Secret image, (e)–(g) Shares after applying embedding method to cover images (a)–(c) respectively

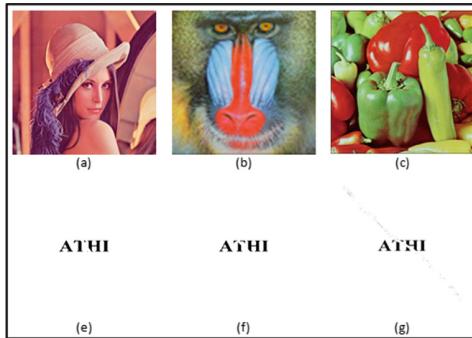


Fig. 7. (a)–(c) are cover images, (d)–(f) are the extracted secret after tampering (a)–(c) respectively.

3.1 Performance Analysis

The MSE, RMSE, PSNR and SSIM metrics [3, 14] are estimated for evaluating the performance of the proposed method.

Table 1 depicts the comparison of MSE, RMSE, SSIM and PSNR values between the cover images and the shared images. Figure 8(a) shows the above comparison using graph. Table 2 presents the SSIM values when the received images are tampered (the size of the secret image = the size of the cover images). Table 3 shows the SSIM values when the received images are tampered (the size of the secret image < size of the cover image). The comparison of proposed method with the literature methods is shown in Table 4. Figure 8(b) shows the same comparison with the help of graph. The method proposed in this paper is found to be the best with higher SSIM values and PSNR values when compared to the literature methods. (a) Lin and Tsai [13], (b) Chang et al. [11] and (c) Proposed Method based on PSNR values.

Table 1. Comparison of Cover images with the corresponding Shares

Image	MSE	RMSE	PSNR	SSIM
Cover 1 and Share 1	5.85	2.42	40.46	0.99
Cover 2 and Share 2	5.82	2.41	40.48	1.00
Cover 3 and Share 3	3.80	1.95	42.33	0.99

Table 2. Performance of the proposed method after tampering (size of secret image = size of cover image)

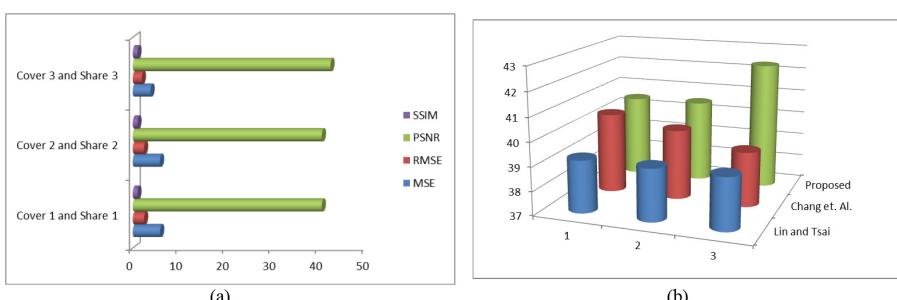
Image	MSE
Before tampering	1.00
After tampering Share 1	0.97
After tampering Share 2	0.98
After tampering Share 3	0.99

Table 3. Performance of the proposed method after tampering (size of secret image < size of cover image)

Image	MSE
Before tampering	1.00
After tampering Share 1	0.94
After tampering Share 2	0.96
After tampering Share 3	0.98

Table 4. Comparison of proposed method with state-of-the-art approaches using PSNR values

Image	Lin and Tsai	Chang et al.	Proposed method
Lena	39.20 dB	40.37 dB	40.46 dB
Baboon	39.18 dB	39.94 dB	40.48 dB
Peppers	39.17 dB	39.30 dB	42.33 dB

**Fig. 8.** (a) Comparison of cover images with the corresponding shares, (b) Comparison of proposed method with the literature method

4 Conclusion and Future Work

The proposed method embeds the secret image into three cover images using LSB (least significant bit) technique, which means that the method is fragile. Firstly, 3 MSB's are extracted from the secret and embedded into cover 1, next 3 bits are embedded into cover 2 and 2 LSB's are embedded into cover 3. Here proposed method embeds the secret in three cover images using LSB bits. The proposed method is compared via different tampering on cover images independently and found to be robust. Results revealed that the method is robust with 94% similarity even after tampering the MSB bits.

In future, the proposed work can be extended for medical images because with the advancement of biomedical systems and telemedicine, medical images are transmitted over the network for research, education and consultations wherein security is at the top priority.

References

- Yan, X., Lu, Y., Liu, L.: A general progressive secret image sharing construction method. *Sig. Process. Image Commun.* **71**, 66–75 (2019)
- Guo, Y., Ma, Z., Zhao, M.: Polynomial based progressive secret image sharing scheme with smaller shadow size. *IEEE Access* **7**, 73782–73789 (2019)
- Sara, U., Akter, M., Uddin, M.S.: Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study. *J. Comput. Commun.* **7**, 8–18 (2019)
- Liao, X., et al.: Medical JPEG image steganography based on preserving inter-block dependencies. *Comput. Electr. Eng.* **67**, 320–329 (2018)
- Sagar, P.R., Chakra, J.P.S., Purushothama, B.R.: Pixel position based efficient image secret sharing scheme. In: Recent Findings in Intelligent Computing Techniques, pp. 527–533. Springer, Singapore (2018)
- Bakthula, R., Shivani, S., Agarwal, S.: Self authenticating medical X-ray images for telemedicine applications. *Multimed. Tools Appl.* **77**(7), 8375–8392 (2018)
- Rajitha, B., Srivastava, M., Agarwal, S.: Edge preserved de-noising method for medical x-ray images using wavelet packet transformation. In: Emerging Research in Computing, Information, Communication and Applications, pp. 449–467. Springer, New Delhi (2016)
- Salehi, S., Balafar, M.A.: An investigation on image secret sharing. *Int. J. Secur. Appl.* **9**(3), 163–190 (2015)
- Shyu, S.J.: Visual secret sharing with meaningful shares. In: 2014 Science and Information Conference. IEEE (2014)
- Surekha, B., Swamy, G.N.: A spatial domain public image watermarking. *Int. J. Secur. Appl.* **5**(1), 1–12 (2011)
- Chang, C.-C., Chen, Y.-H., Wang, H.-C.: Meaningful secret sharing technique with authentication and remedy abilities. *Inf. Sci.* **181**(14), 3073–3084 (2011)
- Wang, R.-Z., Su, C.-H.: Secret image sharing with smaller shadow images. *Pattern Recogn. Lett.* **27**(6), 551–555 (2006)

13. Lin, C.-C., Tsai, W.-H.: Secret image sharing with steganography and authentication. *J. Syst. Softw.* **73**(3), 405–414 (2004)
14. Wang, Z., et al.: Image quality assessment: from error visibility to structural similarity. *IEEE Trans. Image Process.* **13**(4), 600–612 (2004)
15. Thien, C.-C., Lin, J.-C.: Secret image sharing. *Comput. Graph.* **26**(5), 765–770 (2002)
16. Naor, M., Shamir, A.: Visual cryptography. In: *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, Heidelberg (1994)



Comparison Between RSA Algorithm and Modified RSA Algorithm Used in Cloud Computing

Bushra Shaheen^(✉) and Farheen Siddiqui

Jamia Hamdard, New Delhi, India
bushrashaheen11@gmail.com,
fsiddiqui@jamiahAMDARD.ac.in

Abstract. The primary operation performed by cloud computing is to provide dynamic storage capacity and security to its users. The main benefit from using the cloud computing is the reduction in the economic expenditure and ease in the accessibility of data. This whole mechanism involves various security algorithms; still there are some security issues which needs to be solved. In this paper, various security algorithms have been discussed in order to analyze the performance of the algorithms and to find out that which encryption algorithm is better for the data protection in the cloud computing platform. The mainly concerned algorithms in this paper are RSA Algorithm and Modification in RSA Encryption Algorithm (MREA). One of the modifications in RSA encryption algorithm is named as Homomorphic Encryption Algorithm.

Keywords: Cloud computing · Data security · Encryption algorithm · RSA · Modified RSA · Encryption time · Decryption time

1 Introduction

Cloud computing is a technology that provides humongous amount of the capacity of data over the network: public or private. But the main concern attached with this evolving technology is the security issue. Data privacy and maintaining the confidentiality of data is one of the main demands of today's company or organization.

The information about remaining paper is as follows: Sect. 2 blows light on the literature review. Section 3 gives the main objective of this paper. In Sect. 4, comparisons have been done on both the algorithms on the basis of different criteria. Now Sect. 5, conclusion of this paper have been discussed on the basis of performance of both the encryption algorithm used in cloud computing.

2 Literature Review

In this section, brief description of cloud computing and its security issues is given and analyzing which encryption algorithm will be best to use in order to secure the cloud data more appropriately. The main concern of this paper is the comparison between the

two encryption algorithms, one is RSA Algorithm and another one is Modified RSA Encryption Algorithm (MREA). Comparison have been done on various basis as like the encryption speed, decryption speed, based on security, based on changing the modulus of key length.

Rivest, Shamir and Adleman proposed a method for the implementation of public-key cryptosystem whose security is partly due to the complexity of huge numbers being factored. If our method's security proves to be adequate, it allows for the establishment of secure communications without the use of couriers to carry keys, and it also allows digitized documents to "sign". Once the method has been able to withstand all attacks for a long enough time, it can be used with a reasonable amount of condensation [3].

The encryption function is the only candidate known to the authors for a "one-way trap-door permutation.

In the paper of Ayele A and Sreenivasarao, an approach is introduced as a technique to use two public key and a certain mathematical relationship to implement a public key cryptosystem (RSA) [6].

Such two public keys are sent individually, which prevents the attacking player from gaining the complete understanding of the key and deciphering the public statement. For high security but lower speed scheme, the suggested RSA algorithm is used.

3 Objective

The main objective of this paper is the comparison between the programming mechanism of RSA encryption algorithm and Modified RSA Encryption Algorithm.

4 Comparison Between Both the Algorithms

Rivest-Shamir-Adleman (RSA)

RSA was created in 1977 by Ron Rivest, Adi Shamir and Len Adleman as a public key cipher. It is the most common cryptographic key algorithm among asymmetric algorithm. This algorithm utilizes different size of the information block and keys of different sizes. For both encryption and decryption, it uses asymmetric keys. It generates the public and private keys by using two prime numbers. For encryption and decryption purposes, these two distinct keys are used. The algorithm is summarized using two prime numbers, encryption and decryption [14].

RSA is currently used in hundreds of software products and can be used for key exchange, digital signatures, or tiny information blocks encryption. For an open communication channel in order to maintain secure communication and authentication, this algorithm is used particularly.

While comparing RSA algorithm efficiency with DES and 3DES, when selecting small p & q values (prime numbers) for key design, the encryption method becomes too weak and one can decrypt the details utilizing discrete probability theory and side channel approaches. On the other side, if big p & q lengths are chosen, the efficiency will be reduced compared to DES [14] (Fig. 1).

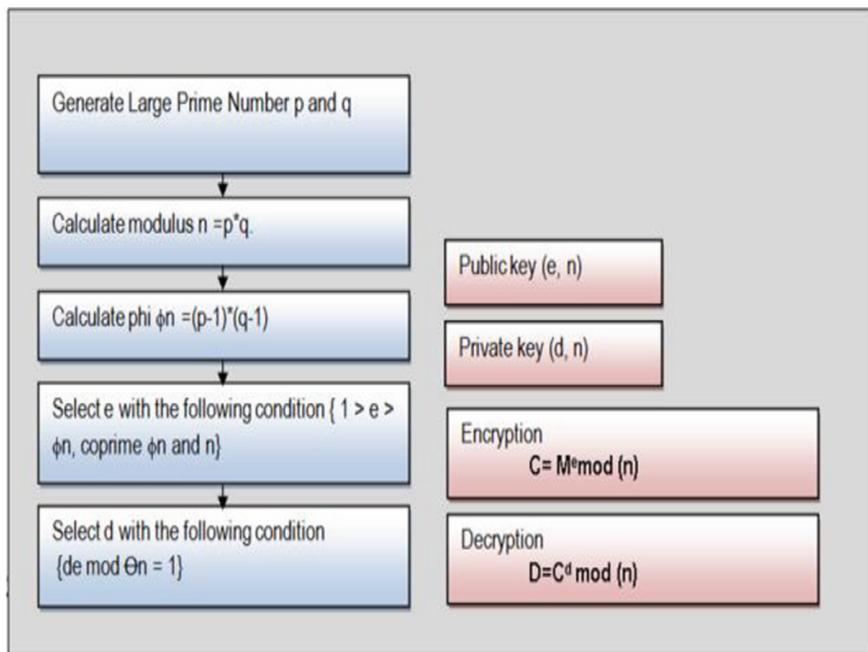


Fig. 1. The original RSA flow of key generation, encryption and decryption

Homomorphic Encryption Algorithm (MREA)

Homomorphic algorithm is one of the modifications done in RSA. This algorithm was developed in 1978. Homomorphic algorithm is an encryption algorithm which performs computation on cipher texts and generates an encrypted result as well as decrypted result when needed [11, 12] (Fig. 2).

Size of n, m, d and random no. (bits)	Public key size (bits)	Chunk size (bits)	Key generation time (ms)	Encryption time (ms)	Decryption time (ms)	Total execution time (ms)
256	256	128	484	329	156	969
512	256	128	172	1672	968	2812
512	256	256	172	890	485	1547
1024	256	128	625	11625	6938	19188
1024	256	256	625	5860	3515	10000
1024	256	512	625	2969	1797	5391
2048	512	128	8125	99891	53609	161625
2048	512	256	8125	47157	31797	87079
2048	512	512	8125	22094	13515	43734
2048	512	1024	8125	11219	7016	26360

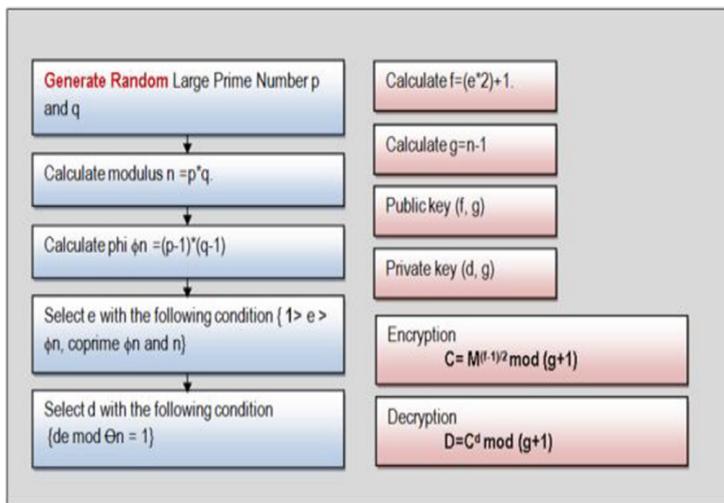


Fig. 2. The Modified RSA flow of Key generation, encryption and decryption

After effect of changing the modulus length m, n and chunk size on the size of two different private keys, key generation time, encryption time and decryption time of original RSA cryptosystem [2].

Size of n, m, d and random no. (bits)	Public key size (bits)	Chunk size (bits)	Key generation time (ms)	Encryption time (ms)	Decryption time (ms)	Total execution time (ms)
256	256	128	469	109	62	640
512	256	128	140	188	218	546
512	256	256	140	109	141	390
1024	256	128	469	484	1453	2406
1024	256	256	469	281	735	1485
1024	256	512	469	172	375	1016
2048	512	128	2453	2953	15203	20609
2048	512	256	2453	1547	5609	9609
2048	512	512	2453	812	2750	6015
2048	512	1024	2453	515	1375	4343

After effects of changing the modulus length m, n and chunk size on the size of two different private keys, key generation time, encryption time and decryption time for Modification in RSA Encryption Algorithm [2] (Figs. 3 and 4).

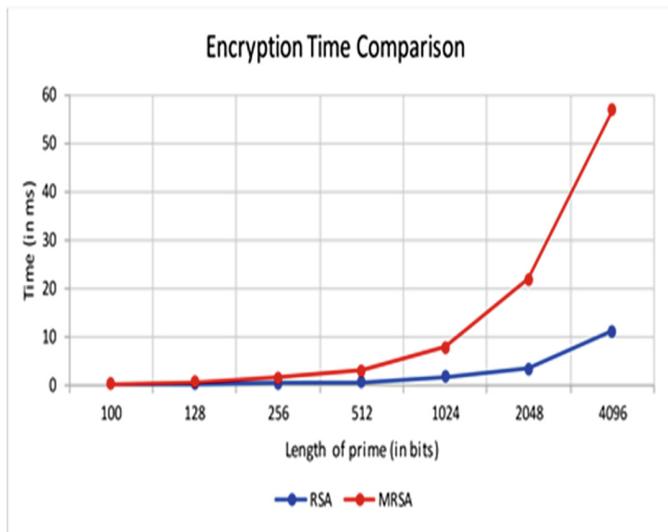


Fig. 3. Encryption time graph between RSA and MREA (Modified RSA)

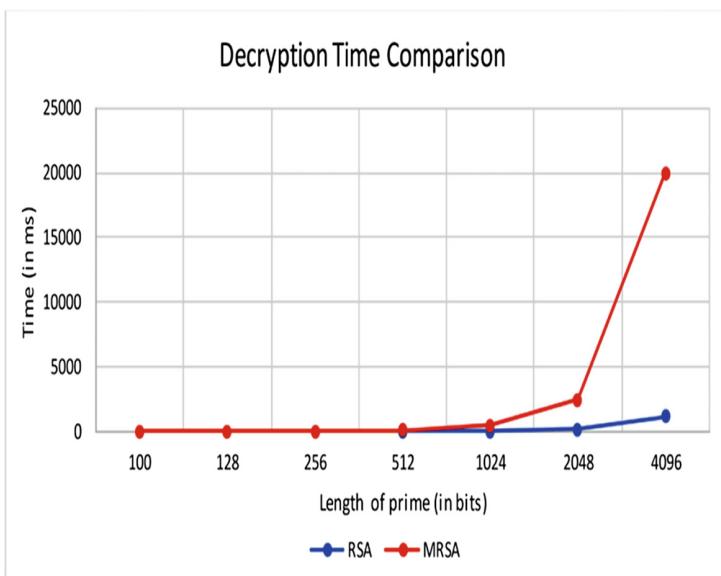


Fig. 4. Decryption time graph between RSA and MREA (Modified RSA)

5 Conclusion

Strength of the algorithm depends on large prime number's which have been used as three variables p, q and r. Compared to the existing algorithm, it is very difficult to break the large prime numbers into three distinct variables [5].

Before starting the algorithm variables p, q, d and e are stored in two different database tables. Then at the time of encryption and decryption, we take the index value corresponding to the value of e and d from the database table and exchange instead of the original key (e, d). Security is therefore increased [5].

Before starting the process, keys are stored offline in the proposed method. Thus compared to the primary RSA method, the process speed is increased [5]. So we can clearly resolve that Modification in RSA Encryption Algorithm (MREA) is more secure and more efficient than original RSA Encryption Algorithm.

References

1. Hemanth, P.N., Raj, N.A., Yadav, N.: Secure data transfer by implementing mixed algorithms. In: Recent findings in intelligent computing techniques, pp. 79–85. Springer, Singapore (2019)
2. Intila, C., Gerardo, B., Medina, R.: A study of public key ‘e’ in RSA algorithm. In: IOP Conference Series: Materials Science and Engineering, vol. 482, no. 1, p. 012016. IOP Publishing (2019)
3. Degadwala, D., Mer, U., Modi, N.: A novel security approach for data migration using ECC & MAES algorithms. Utsav and Modi, Nimit, A Novel Security Approach for Data Migration using ECC & MAES Algorithms, 9 August 2019 (2019)
4. Akhter, S., Chowdhury, M.B.: Bangla and English text cryptography based on modified blowfish and Lempel-Ziv-Welch algorithm to minimize execution time. In: 2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), pp. 96–101. IEEE (2019)
5. Deshpande, V., Das, D.: Efficient searching over encrypted database: methodology and algorithms. In: International Conference on Distributed Computing and Internet Technology, pp. 327–338. Springer, Cham (2019)
6. Kannan, M., Priya, C., Vaishnavi, S.: A comparative analysis of DES, AES and RSA crypt algorithms for network security in cloud computing (2019)
7. Sai, M.K., Reddy, P.L., Krishna, R., Siva, N., Teja, R., Prakash, K.B.: Hybrid encryption for medical applications using advanced algorithms in internet of things. Indian J. Public Health Res. Dev. **10**(6) (2019)
8. Mahmood, G.S., Huang, D.J., Jaleel, B.A.: Achieving an effective, confidentiality and integrity of data in cloud computing. IJ Netw. Secur. **21**(2), 326–332 (2019)
9. Thewar, P., Tiwari, A., Shah, P., Desai, C.: CARS: a hybrid security approach to secure cloud data through mobile devices (2019). SSRN 3370126
10. Zhang, F., Chen, Y., Meng, W., Wu, Q.: Hybrid encryption algorithms for medical data storage security in cloud database. Int. J. Database Manage. Syst. (IJDMMS) **11** (2019)

11. Mahmood, G.S., Huang, D.J., Jaleel, B.A.: A Secure cloud computing system by using encryption and access control model. *J. Inform. Process. Syst.* **15**(3) (2019)
12. Khan, S.A., Aggarwal, R.K., Kulkarni, S.: Enhanced homomorphic encryption scheme with PSO for encryption of cloud data. In: 2019 5th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 395–400. IEEE (2019)



Database as a Service for Cloud Based Video Surveillance System

Sumit Kumar^(✉), Vasudeva Rao Prasadula,
and Shivakumar Murugesh

Bharat Electronics Limited, Bangalore, India
{sumit_kumar, vasudevaraoprasadula,
shivakumarm}@bel.co.in

Abstract. In recent times, cloud computing has become the widely accepted technology for moving the database over the cloud, which has brought revolution in the IT industry, this term is recently coined as Database as a Service (DBaaS). Mostly cloud databases are used for data intensive applications such as data warehousing, data mining and monitoring purpose. On the advent of smart cities concept, massively scalable video surveillance has become the necessity in public area. In this paper, we proposed a database as a service to support video surveillance system on the cloud environment with real time video analytics. In this regard, we have explored Trove (Open stack cloud DBaaS component) to facilitate scalability and availability for the video surveillance system furthermore we have also proposed data processing architecture based on open CV, Apache Kafka and Apache spark.

Keywords: Cloud computing · Database as a Service (DBaaS) · Trove · Apache Spark · Apache Kafka

1 Introduction

Cloud Computing is the newly developed technology to virtualize IT systems and to access the needed applications on the Internet, through web-based applications. This has reduced the IT costs for hardware or servers. The cloud database will become the most adopted technology for storing huge data for data analytics by many companies in the world. Most of these cloud databases are either on the public cloud or their pay per use is very much costly. In this regards, we have explored the trove component of open stack cloud (A open source cloud) which provides RDBMS and NoSQL flavor of cloud databases like MongoDB, CouchDB, Mysql and etc. In this paper, we have proposed a scalable video surveillance system as we know video analysis needs a massive computer, data resources and network to deal with the computational, transmission and storage challenges of video streams coming from hundreds of cameras. To overcome the data storage challenge, we proposed a database as a service cloud storage mechanism to facilitate the video surveillance system. The main objective of the paper is to explore the database as a service for the scalable video surveillance system and provide the real-time video analytics on the cloud environment using open source platforms like Apache Spark, Apache Kafka, and open CV. This paper has been divided into five

sections. The Sect. 2, describes Cloud databases as a service. Section 3 discusses the video surveillance system and its salient feature. Section 4 describes the video analytics architectures followed by conclusions.

2 Database as a Service

In the era of the digital world, where data (video, audio, text) is growing very fast and storing and accessing of this kind of data has become an issue which led to the emergence of a cloud database. The cloud database is implemented over the cloud computing service that means it utilizes the hardware and software resources of the cloud service provider. It is not a conventional way of taking the relational database and deploying it over a cloud server. It means that the database as a service is giving you the functionality to add additional nodes when required online, and increasing the performance of the database. At present, available cloud databases provide high scalability, flexibility, availability, and performance at a very reasonable price. Microsoft's SQL Azure, Amazon's Simple DB, Amazon RDS, Google Cloud SQL, Database.com, Mongo Atlas and Oracle database are the commonly used databases in the Cloud [3]. These cloud databases are run on a pay as you go model (Fig. 1).

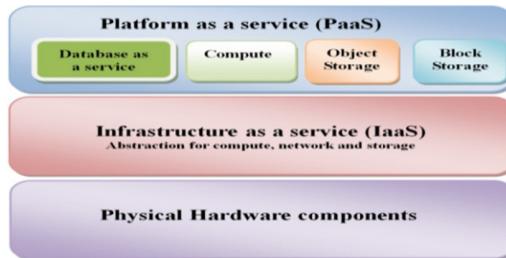


Fig. 1. Database as a service

These API can be access by the users using web or console application. Through these API user may use to configure and manage the database instances and even provision and de-provision database instances. In the following section, we are describing the Open Stack cloud database as a service.

2.1 Open Stack Trove (Database as a Service)

For open stack cloud, Trove component provides DBaaS service. The Trove provide a reliable and scalable cloud database service providing functionality for both relational and non-relational database engines (Fig. 2).

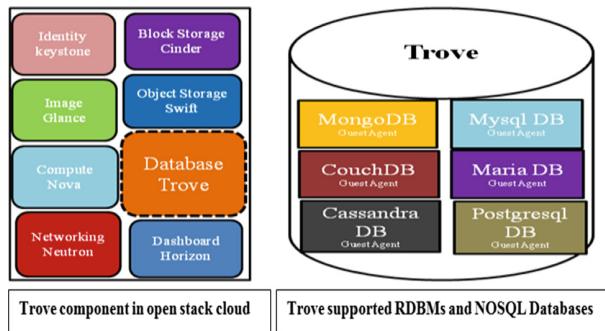


Fig. 2. Trove - DBaaS on the Open StackDatabase as a service

Trove currently support CouchBase, CouchDB, MySQL, MongoDB, Percona, Oracle, Redis with many more currently under development. Trove provides APIs to automate tasks like backup, clustering, replication and failover. Trove cluster management is better than any database service available in the IT market. We can create, shrink and grow database clusters directly through the Trove API or GUI.

3 Video Surveillance System

In the recent years, Smart cities program bring the great opportunities for cloud based video surveillance system. In [5], author proposes a Hadoop distributed file system to store the videos of the surveillance system.

3.1 System Design

In this section, we, first of all, explain the overall architecture of the video surveillance system for the cloud environment. Then we will explain the video data storage using cloud computing. In this paper, we design a flexible, scalable and reliable cloud-based video surveillance system (Fig. 3).

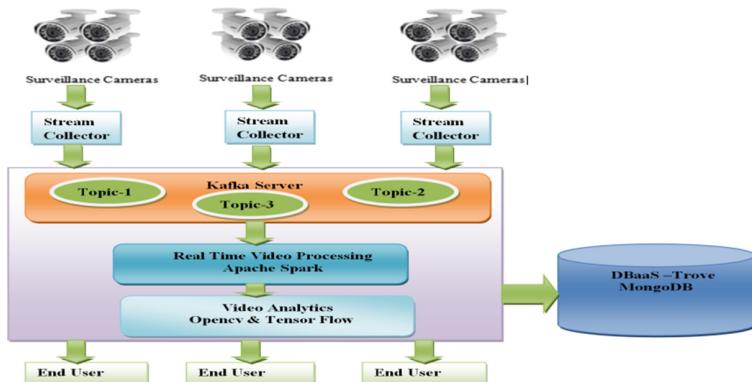


Fig. 3. Functional architecture of video surveillance system on the cloud

3.1.1 Video Stream Collector

This module is collecting large scale real-time videos from the IP cameras with a camera id number and some meta-data information like timestamp, video codec, frame's width and height. After collecting the real-time video frame, stream collector module bundle these information's in JSON format and sending these bundles to the Kafka Server.

3.1.2 Kafka Server-Streaming as a Service

Kafka plug-in of mirantis openstack cloud, provides streaming as a service. Kafka is a fast, scalable, durable and fault-tolerant publisher-subscriber messaging system. In this module, we are creating the topic in Kafka server as per the geographic location of cameras. Stream collector sending the data bundles to the specified topic of Kafka server then Kafka topics data bundle, we are using for the real-time video surveillance system and real-time video analytics.

3.1.3 Spark-Real Time Processing

For this module we are using Apache Spark, an open source parallel processing framework for running large-scale real time data processing. This module work as consumer that means it gets that data bundles from the Kafka server topic and performs the real time processing.

3.1.4 Video Analytics on the Cloud

In this research we have designed a video surveillance system with real-time video monitoring, tracking of objects and face recognition analytics. Since our system is supporting large scale real-time video analytics, we have proposed a hybrid parallel computing based on the Spark framework. The results suggest that the proposed system is hugely beneficial for real-time video analytics and video processing.

3.1.5 Distributed Storage System on the Cloud

The video data is coming from the hundreds or thousands of cameras. We are providing a database as a service for the video surveillance system. It stores video stream data on the cloud object storage and meta-data about the stream is stored in the MongoDB. For this paper, we are using Mongo DB as a cloud database. Moreover, MongoDB is horizontally scalable, highly available and it supports JSON based storage.

3.2 Deployment Design

Cloud-based video surveillance system needs a lot of bandwidth to support the huge amount of video sources that raise a lot of network traffic issues. To overcome these issues, close by private cloud could save the network traffic as compared to the public cloud. But the public cloud is more feasible than the private to create a robust surveillance system. In this research, we have proposed two types of deployment scenarios. The first one build for private cloud and second one build for the public cloud (Fig. 4).

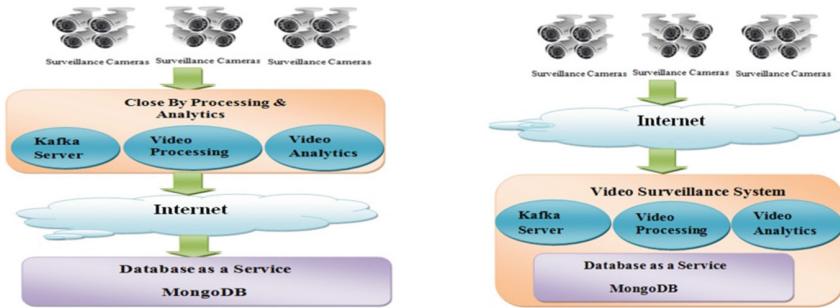


Fig. 4. Private and public deployment scenario

3.2.1 Private Cloud Deployment Scenario

There are the two major mechanisms we have used for this research, first centralized storage mechanism and second are closeby data processing mechanism. In the first mechanism, data will always store in the centralized storage location which is highly available and scalable. The second mechanism stores the streaming from the video source locally and provides remote processing and analytic features.

3.2.2 Public Cloud Deployment Scenario

In this mechanism all the video sources are connected by internet with the public cloud data centre. These video sources are located at different geographical locations. Hence more bandwidth is required for scaling the system. However this deployment scenario is suitable for the small usage.

4 Video Analytic Architecture

Video analytics is the most crucial part of the video surveillance system. Consequently, video analysis is a resource-intensive process and need massive computational, transmission and storage challenges [6]. To overcome these challenges, we proposed a cloud-based video analytics architecture, which consists of three main components named as video analytics server, video analytics client and video analytics approaches.

4.1 Video Analytics Server (VAS)

The VAS is the core component of our surveillance system and performs the video stream analysis. The analysis of the live video stream is performed by the selected video analysis approach. After performing the analysis of the video, the result and meta-data about the live stream are stored on the cloud object storage and cloud databases respectively (Fig. 5).

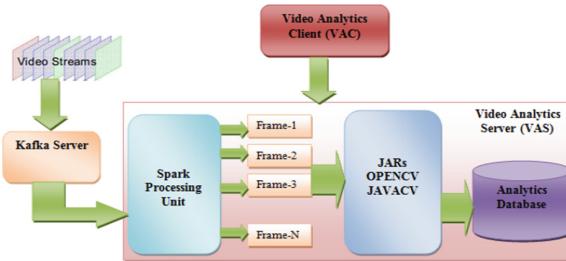


Fig. 5. Overall video analytic architecture

4.2 Video Analytics Client (VAC)

The VAC will be deployed on the cloud which can be used by the end user through the internet. The VAC will be responsible for the end-user interaction with VAS. VAC will provide the functionality to the end-user to perform the video analysis approaches.

4.3 Video Analytics Approaches

For video processing, we are using open source: computer vision and machine learning API like:- opencv and tensor flow. In this paper, we are performing three main video analysis tasks: object detection, object recognition and object tracking.

4.3.1 Object Detection

In the following paper, for object detection, we are using Haar Feature-based Cascade Classifier. Furthermore, the cascade classifier approach reduces the time and resource for object detection. Training data set of cascade classifier are stored on the compute cloud.

4.3.2 Object Recognition

object recognition is the extended version of object detection. This is widely used for face recognition, number plate recognition, and handwriting recognition. We have used the opencv harr training utility for training both the cascade classifiers. For training purpose, we have taken 30×30 fixed size input images.

4.3.3 Object Tracking

For the purpose of object tracking, we used TLD (tracking, learning, and detection) algorithm of opencv 3.1 version. This algorithm works the best under the occlusion over multiple frames and also track best over scale changes.

5 Conclusion

Database as a service for a cloud-based video surveillance system, video analytics architecture and approaches has been presented and discussed in this paper. The main focus was to leverages the open source API's and framework. Cloud databases handle

the huge data generated from hundreds or thousands of cameras moreover Cloud databases have its own advantage: highly reliable, scalable and cost-effective. In the future, we would like to extend our framework for the smart environment using the Internet of Things (IoTs). We could also explore the deep learning algorithms for the better result of video analysis.

References

1. Abdullah, T., Anjum, A., Tariq, M., Baltaci, Y., Antonopoulos, N.: Traffic monitoring using video analytics in clouds. In: 7th IEEE/ACM International Conference on Utility and Cloud Computing (UCC), pp. 39–48 (2014)
2. MacDorman, K.F., Nobuta, H., Koizumi, S., Ishiguro, H.: Memory based attention control for activity recognition at a subway station. *IEEE Multimed.* **14**(2), 38–49 (2007)
3. Stauffer, C., Grimson, W.E.L.: Learning patterns of activity using real-time tracking. *IEEE Trans. Pattern Anal. Mach. Intell.* **22**(8), 747–757 (2000)
4. Stauffer, C., Grimson, W.: Adaptive background mixture models for real-time tracking. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 246–252 (1999)
5. Viola, P., Jones, M.: Rapid object detection using a boosted cascade of simple features. In: IEEE Conference on Computer Vision and Pattern Recognition, pp. 511–518 (2001)
6. Lin, Y., Lv, F., Zhu, S., Yang, M., Cour, T., Yu, K., Cao, L., Huang, T.: Large-scale image classification: fast feature extraction and SVM training. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2011)
7. Vi-system. <http://www.agentvi.com>
8. SmartCCTV. <http://www.smartcctvltd.com>
9. Shende, S.B., Chapke, P.P.: Cloud database management system (CDBMS). *Compusoft* **4**(1), 1462 (2015)
10. Zheng, X., Fu, M., Chugh, M.: Big data storage and management in SaaS applications. *J. Commun. Inform. Netw.* **2**(3), 18–29 (2017)
11. Bosh Security System: IVA 5.60 intelligent video analysis. Bosh Security System, Technical report (2014)
12. Feng, J., Wen, P., Liu, J., Li, H.: Elastic stream cloud (ESC): a stream-oriented cloud computing platform for rich internet application. In: International Conference on High Performance Computing and Simulation (2010)
13. Network deployment chart from NUUO CMS illustration. <http://gsf.com.my/dvr/NUUO/NUUOCms.htm>. Accessed June 2012
14. VGuard. <http://www.vguardinternational.com/cms/>. Accessed 26 Feb 2012
15. Amazon S3 Storage Service. <http://aws.amazon.com/es/s3/>. Accessed 26 Feb 2012
16. Nikam, V., Meshram, B.B.: Parallel and scalable rules based classifier using map-reduce paradigm on hadoop cloud. *Int. J. Adv. Technol. Eng. Sci.* **02**(08), 558–568 (2014)



Relative Hand Movement and Voice Control Based Home Automation and PC

Shashwat Sanket¹, Jayraj Thakor¹, Piyush Kapoor¹,
Karrmany Pande², Suyash V. Shrivastav³, and R. Maheswari¹⁽⁾

¹ SCSE, Vellore Institute of Technology, Chennai, India
maheswari.r@vit.ac.in

² SELECT, Vellore Institute of Technology, Chennai, India

³ SENSE, Vellore Institute of Technology, Chennai, India

Abstract. Hand gesture recognition is one of the significant research domains in the computer science field to which people have paid attention in the past decade. It has been considered as a highly successful technology, where it saves time to unlock any device and provide high stability with an increased accuracy rate. It provides a simple interface for humans to communicate with machines. This paper describes an external hardware-independent system which can control electrical appliances using hand gesture and voice control. We will be using a subpart of this field which is measuring the distance of relative hand movement with respect to the sensors used. The system uses a distance-measuring technique to provide certain functionalities to external hardware. The relative hand movement is recognized using ultrasonic sensors and voice pattern is recognized using analog to digital converter. The hardware part of the ultrasonic sensor is interfaced with Arduino. After getting the sound speed (sonic speed) and time between emission and reception, the distance can be calculated and provide necessary functionalities. In Voice Control Google Speech Recognition is used to convert speech to text and provide the desired functionalities. The workflow of the entire system is controlled using Arduino and Python code.

Keywords: External hardware independent system · Relative hand movement · Distance measuring technique · Ultrasonic sensor · Arduino · Voice control · Google Speech Recognition · Python

1 Introduction

This prototype model of Relative Hand Movement and Voice Control Based Home Automation and PC, is an amalgamation of hardware and software. The prototype, a precursor of its kind, uses electronic components in conjunction with software codes to control software's present on our laptops and desktops. This working is achieved by integrating an ultrasonic sensor which uses the technique of Leap motion to recognize different patterns. At its elementary stage videos in our laptop at any platform, be it

offline or online, can be controlled by relative hand movement using the mentioned ultrasonic sensors. The prototype is programmed to receive and interpret dictation or to understand and carry out spoken commands along with measuring the distance of our hand from the sensor and performing the task assigned for that distance. To further embroider the outlook of our product we have inculcated voice recognition which will allow the user to communicate to the software and add to its ease to access. In addition to this, the device can control and regulate close to hand electrical appliances too. These Electrical devices will be controlled by giving gesture or voice commands. In short, we will be giving the user never before had experience by literally giving them the control of their house in their hand.

2 Proposed System

The system is embedded with Arduino UNO (Atmega328), Bluetooth Sensor HC-05, Ultrasonic sensors, and a software application. Our system uses two input sources, primary being relative hand distance, which is measured by ultrasonic sensors, and secondary as voice. The system performs distinct functionalities using these two inputs. These various electronic components when used in conjunction with the software application, built on python programming language, helps us to perform various tasks on software (offline/online videos) and hardware (electrical appliances control and regulation). We can pause and start a video, increase or decrease its volume, forward play it or backward play it as to our liking. On the hardware part, we will be able to switch on and off a device just by giving the system command as “SWITCH ON [APPLIANCE]” or by just flowing our hand past by the respective sensor. These commands that will be given to the system can be set according to user preferences.

Arduino UNO

The Arduino is a microcontroller-based open-source electronic prototyping board which can be programmed on an Arduino software. The microcontroller used is Atmega328P by Atmel company. The Arduino software user-friendly version of C++ thereby making it easier to learn. Arduino Uno operates at a voltage of 5 V and can be powered by through an AC-DC adaptor or a battery [15].

Bluetooth Sensor HC-05

Our Bluetooth module has several pins, studying from the state the Rx, Tx, the ground and the Vcc and key pins. Vcc and ground will supply the power to the Bluetooth module by completing the circuit to which the Bluetooth module is attached. The sensor communicates via serial communication and for that purpose the Rx and Tx are connected to the Rx and Tx of the microcontroller.

4 Channel-Relay

Relay is one of the simplest components of electronics available to use. In simple terms, it is nothing but a switch which directs the supply to the connected load whenever it is switched on. A 4-channel relay is nothing but 4 single relays attached to one board so that different loads can be controlled using a single Vcc and Ground. the instruction of when to switch on a load is given by the Arduino connected to the relay.

Ultrasonic Sensor (HC-SR04)

HC SR04 is an ultrasonic sensor module provided with 4 pins Vcc, ground Trigg and Echo. This module is helpful in measuring distance from 2 cm to 400 cm with an accuracy to 3 mm. It includes a receiver, a transmitter and a control circuit. An ultrasonic sound is emitted which on contact with an object is reflected. The reflected sound is sensed by the receiver and distance is calculated by travel time and speed of sound. Distance will be half as the time taken is from the transmitter back to receiver and distance measured is twice so the distance calculated is halved to get the accurate distance (Fig. 1).

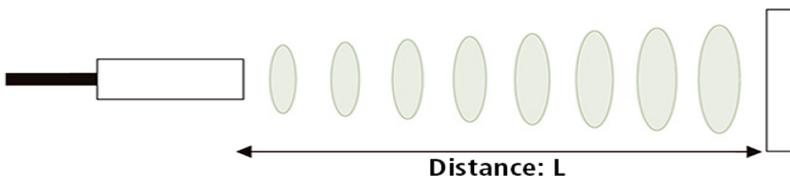


Fig. 1. Sonic speed-emission/reception

$$\text{Distance } L = \frac{1}{2} \times T \times C$$

Figure 2 shows the block diagram of the proposed voice system containing Ultrasonic sensors. Arduino, ADC (Analog Digital Converter). Relay controller and Video/Audio APP.

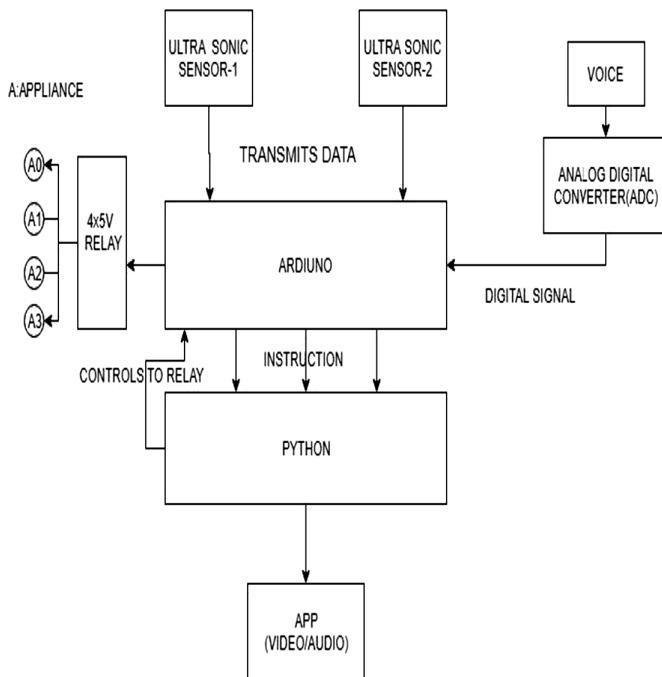


Fig. 2. Block diagram of voice system

Ultrasonic Sensors

There are two ultrasonic sensors in the circuit which detects the hand distance and sends the data to python to process it and perform desired instructions.

4 × 5 V Relay

This is a 5 V 4 channel relay which acts as a switch and is connected to the appliances.

Analog Digital Converter (ADC)

This is used to convert the voice signal to digital form so that it can be processed by the Arduino.

Arduino

In this paper, we have used Arduino UNO. This is an open-source microcontroller board. It has 14 Digital pins, 6 Analog pins. It can be powered by a USB cable or a 9 V battery.

Python

This processes the control signals sent by arduino and in-turn controls the audio or video applications running on the device i.e. Arduino receives the data from ultrasonic sensors and the voice input, then Arduino sends this control signal to python which interprets the signal and performs the function defined in code.

3 Implementation

Implementing Relative Hand Movement Recognition

When a user performs hand movements in-front of ultrasonic sensors, the time between the emission and reception is sent to the Arduino where distance of left hand from the left sensor and distance of right hand from the right sensor is calculated using the formula [4].

$$L = \frac{1}{2} \times T \times 0.034 \text{ (sonic speed)} \quad (1)$$

Using these distances, we define certain patterns on the basis of (L = Left Distance, R = Right Distance) and corresponding abbreviations for the respective pattern. One Simple Pattern is illustrated.

Pseudo Code (Arduino code)

```

upperBound = 20
lowerBound = 10
function GetControlSignal(trigger,echo,upperBound,lowerBound)
    leftHandDistance = findDistance(trigger,echo)
    if leftHandDistance < upperBound and leftHandDistance > lowerBound then
        return "Left Control Signal"
    while leftHandDistance <= 2*upperBound //increasing the width
        leftHandDistance = findDistance(trigger,echo) // get the current hand distance
    if leftHandDistance < lowerBound
        return "Volume Up"
    if leftHandDistance > upperBound
        return "Volume Down"
    
```

Adding some necessary delay will increase the performance of the system. These abbreviations are outputted on the serial terminal. Which is then read by the system software application. Which is built on python programming language? A Sample is illustrated have used abbreviations to control video or electrical appliances PyAutoGUI, Serial, Pybluez are used as an external library.

Implementing Voice Recognition

Here in this prototype the system used Google Speech Recognition to convert speech to text and from that it define specific functionalities accordingly.

Sample Code (To convert voice to text and text to voice):

```
#include pytsx, speech recognition as an external library.

import speech_recognition
import pytsx

engine = pytsx.init()

def listn():#Recognise function
    r=sr.Recognizer()
    with sr.Microphone() as source:
        print("Speak")
        audio = r.listen(source)
        data=r.recognize_google(audio)
    return(data)

def speak(data):
    print(data)
    engine.say(data)
    engine.runAndWait()
```

Figure 3 shows the circuit diagram of voice system and Fig. 4 illustrates the implementation snapshot.

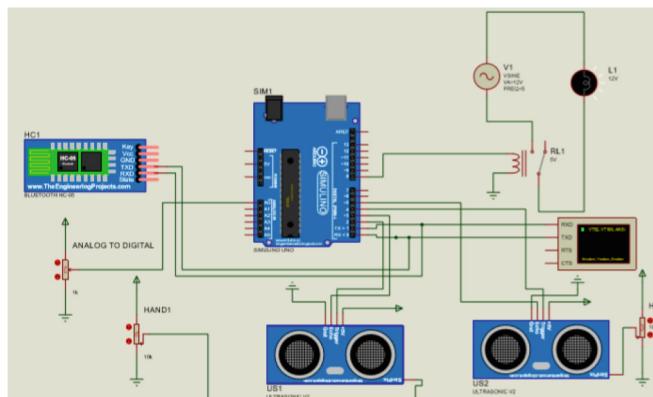


Fig. 3. Circuit design of voice system



Fig. 4. Snapshot of proposed voice system

Testing and analysis

Table 1 shows the statistical and analysis of gesture patterns. Figure 5 shows the graphical representation of the gesture pattern analysis.

Table 1. Statistical analysis

Gesture Pattern (GP)	Gesture performed	Correctly recognized	Accuracy (%)
GP 1	58	54	93.1
GP 2	61	55	90.1
GP 3	65	57	87.8
GP 4	55	49	89.2
GP 5	67	63	94.3

EFFICIENCY ANALYSIS

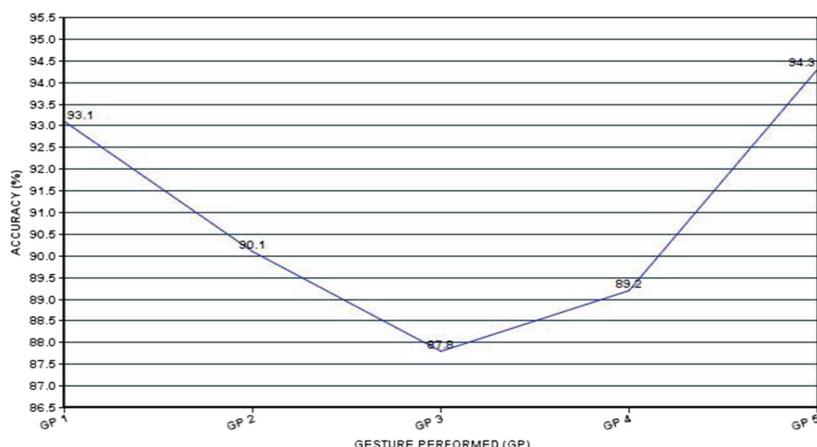


Fig. 5. Graphical representation of gesture pattern

Conclusion and Future Trends

A small prototype for our proposed system has been implemented and tested as illustrated. The system can control video operations and electrical appliance through relative hand movement using ultrasonic sensor and the same through voice. Based on the simulations performed we have achieved more than 75% accuracy.

The System can be extended by including more sensors like gyroscopic sensor, accelerometer. Using these sensors, we can create a greater number of distinct patterns, thus providing more functionalities.

References

1. Comic, N., Cerseato, P., De Natale, F.G.B.: Natural human machine interface using an interactive virtual blackboard. In: Proceedings of ICIP 2007, pp.181–184 (2007)
2. Pang, Y.Y., Ismail, N.A., Gilbert, P.L.S.: A real time vision-based hand gesture interaction. In: Fourth Asia International Conference on Mathematical Analytical Modelling and Computer Simulation, pp. 237–242 (2010)
3. Schellingerhout, R., Smitsman, A.W., Cox, R.F.A.: Evolving patterns of haptic exploration in visually impaired infants. *Infant Behav. Dev.* **28**, 360–388 (2005)
4. Marcel, S., Bernier, O., Viallet, J.E., Collobert, D.: Hand gesture recognition using input output hidden markov models. In: Proceedings of the FG'2000 Conference on Automatic Face and Gesture Recognition (2000)
5. Wu, X., Yang, C., Wang, Y., Li, H., Xu, S.: An intelligent interactive system based on hand gesture recognition algorithm and kinect. IEEE (2012)
6. Wachs, J.P., Kolsch, M., Stern, H., Edan, Y.: Vision-based hand-gesture applications. *Commun. ACM* **54**, 60–71 (2011)
7. https://en.wikipedia.org/wiki/Category:Gesture_recognition
8. <https://www.electronicshub.org/voice-activated-home-automation/>
9. Rehman, A., Arif, R., Khursheed, H.: Voice controlled home automation system for the elderly or disabled people. *J. Appl. Environ. Biol. Sci.* **4**, 55–64 (2014)
10. Khan, I., Arif, M., Khalid, M.F., Ali, R., Khan, Q., Ahmad, S.: Voice controlled home automation system. *Int. J. Res. Comput. Commun. Technol.* **6**, 148–154 (2017)
11. Jain, G.: Vision-based hand gesture pose estimation for mobile devices. University of Toronto (2009)
12. Moeslund, T.B., Norgaard, L.: A brief overview of hand gestures used in wearable human-computer interfaces. Technical report, Aalborg University, Denmark (2002)
13. Maheswari, R., Rani, S.S., Sharmila, P., Rajarao, S.: Personalized secured api for application developer. In: Smart Innovations in communications and Computational Sciences. Advances in Intelligent Systems and Computing, vol.851, pp. 401–412. Springer (2018)
14. Rautaray, S.S., Agrawal, A.: A novel human computer interface based on hand gesture recognition using computer vision techniques. In: Proceedings of ACM IITM 2010, pp. 292–296 (2010)
15. <https://www.hackerearth.com/blog/developers/a-tour-of-the-arduino-uno-board>



Design Strategies for Handling Data Skew in MapReduce Framework

Avinash Potluri^{1,2(✉)}, S. Nagesh Bhattu³, N. V. Narendra Kumar²,
and R. B. V. Subramanyam¹

¹ National Institute of Technology Warangal, Warangal, India
potluri.avinash1@gmail.com

² Institute for Development and Research in Banking Technology, Hyderabad, India
³ National Institute of Technology Andhra Pradesh, Tadepalligudem, India

Abstract. Multiway spatial join has drawn significant interest in research community because of its wide range of applications. Multiway spatial join further enjoys lots of applications in location based services. The analysis of communication cost is vital in the performance analysis of computing distributed multiway spatial join due to the skew observed in real world data. We analyze the performance of multiway spatial join using two strategies for addressing skew (a) whether to have a constraint on the number of reducers or (b) to have a constraint on the size of the input to the reducer (reducer is a computing facility). Our study gives a solution to address the issue of skew and to minimize the cost for communication in a network. We propose two algorithms, which study the trade-offs between the two strategies. We conducted experiments on real world datasets shows the performance in various scenarios. Based on the learning we provide insights into the selection of appropriate strategies for a given task.

Keywords: Distributed computing · Skew · Communication cost

1 Introduction

The need to process huge amount of data has become a mandate in today's real world scenario. Distributed computing provides a mechanism to use large scale resources for efficient computation. Consider the following scenario where there is a fixed amount of work to be done and there are some agents employed to compute the work. Our study deals with the optimal selection of one the following two strategies. The first one is to divide the work into equal number of parts and assign it to the available agents. The second one is to analyse and decide, the amount of work to be given to an individual agent and employ those many agents to complete the work. This example can be directly mapped to distributed computing frameworks like mapreduce. A distributed computing facility has some reducers to perform a particular task. The problem lies in deciding whether to optimize based on the number of reducers or on the size

of the input given to the reducers. The selected strategy directly impacts the performance, cost for computation, network load and many other factors.

We study the impact of these strategies, while computing multi-way spatial join using distributed computing paradigm like mapreduce. Communication cost remains a vital component in distributed computing. Minimizing the cost of communication among the reducers gives significant improvement in performance. Another component that impacts is skew in data. Moreover, the reason for uneven distribution of load across the reducers is because of the skew in data. This adds a notable overhead, which shows a crucial impact on the performance. There are some task scheduling algorithms [14] for minimizing the execution time. Our study in this paper is to emphasize the factors that can influence the network overhead. We propose two design strategies for handling skew by further reducing the network overhead. We further analyse, which strategy can be best suitable for evenly balancing the load across the reducers for a specified task.

1.1 Contributions

- We compare two diverse techniques, one by keeping constraints on the size of the input to the reducer and the other by fixing the number of reducers.
- We show the trade-offs between the two strategies in handling the skew.
- We present the analysis and experimental results for the proposed algorithms on two real world datasets.

The organization of the paper is as follows: In Sect. 2, the related works are summarized. In Sect. 3, the preliminaries required for understanding the problem are explained. Section 4 gives the overview of the proposed algorithms along with the pseudocode. In Sect. 5 the detailed experimental evaluation with description of datasets is given. In Sect. 6 we conclude the paper.

2 Related Work

A technique to perform multi-way joins based on the degree information is studied in [10]. This work focus on equijoins on relational tables. The relation between fractional edge packing of the query and the amount of communication in the cases where the data is skewed and skew-free is explored in [4, 15]. The worst case optimal parallel algorithms for a conjunctive query is analysed in [11]. Algorithms that best suit for complex querying systems based on parallel architecture in both distributed and sequential scenarios were evaluated and optimized by [5, 7]. Several variations of relational join algorithms considering both theoretical and practical perspectives were studied by [9, 13]. The lower and upper bounds of computing a query on a huge database using distributed servers is studied in [3, 8]. A map-reduce based system namely skewtune has been developed by [2, 12] and [1] to handle skew. A task scheduling in cloud using better load balancing algorithms is studied in [14].

3 Preliminaries

3.1 Distributed Computing

In this era of distributed computing, map-reduce framework has significant importance for processing massive amounts of data. This framework works on the principle of key and value pairs. A map-reduce task can be computed in two phases namely mapper phase and reduce phase. In detail a complete map-reduce execution has to perform map phase, split phase, shuffle phase and reduce phase. Initially the input data is partitioned into fixed parts called blocks. Based on the user defined map function each block is processed in parallel and a particular key is assigned. In the shuffle phase all the same keys are mapped to a single reducer where the reducer function performs the user desired task. In particular a huge task is further divided into much smaller tasks and computed in parallel across the available resources. We used hadoop distributed computing facility to do the analysis of the algorithms.

3.2 Task for Computation

For analysing the efficiency of the proposed algorithms, we selected a spatial data processing task. With the availability of massive amount of spatial data, for scalable and efficient processing, we used distributed computing. The desired task is as follows: we need to find the regions of cities, forests and rivers that are covered under cell towers range. All this information is available in the form of latitudes and longitudes and hence named spatial data. For computing this, we need to perform a multi-way spatial join among cities dataset, forests dataset, rivers dataset and cell towers dataset. We finally obtain the overlapping regions of cities, forests, rivers and cell towers. Let C be cities, F be forests, R be rivers and CT be cell towers. For each $c \in C$, $f \in F$, $r \in R$ and $ct \in CT$ a join operation is performed and the result is obtained if there is an overlap between c , f , r and ct . For instance, Fig. 1 shows that there are spatial objects distributed across the computing facilitates based on their spatial position. The spatial objects $r2$, $r3$, $r4$ and $r5$ are assumed to be one of $c \in C$, $f \in F$, $r \in R$ and $ct \in CT$ where we identify the overlap. The overlap region is highlighted in Fig. 1 for $r2$, $r3$, $r4$ and $r5$ spatial objects. Here we have a total of 25 reducers. The spatial objects $r6$ and $r7$ are assumed to be computed at 6th reducer.

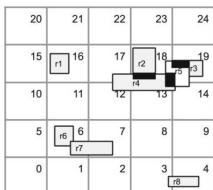


Fig. 1. Processing spatial data in a grid

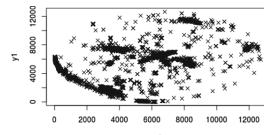


Fig. 2. Skew in real world data

3.3 Skew: The Need for Load Balancing

In the real world, huge amount of data is generated through location-based-services with the massive increase in usage. This real world data inherits skew in it. For skewed data, when the data is distributed among the distributed computing facilities for processing, even when 90% of the reducers completes the job, the final output is obtained only after the completion of remaining 10% reducers. This is because of the uneven distribution of data among the cluster machines, which is affecting the performance. In this scenario there is need to balance the load across the reducers. We need to employ a suitable strategy for better computation of the job. Figure 2 shows the skew in real world data. It is observed that in few places the data distribution is more dense and in most of the places the data distribution is sparse. The optimal selection of the proposed strategies can yield a better solution to distribute the load evenly across the reducers, even for skewed datasets.

4 Our Approach

We propose and analyze two key design strategies for distributing the load across the reducers. The algorithms for the proposed design strategies are Fixed Grid strategy (FGS) and Fixed Input Size (FIS) strategy. The number of reducers needed for computing a particular task can either be static or dynamic based on the selection of the design strategy. The key ideas of the algorithms is to evenly balance the load even for skewed data. The detailed specifications of the algorithms are discussed below. We use the term reducer instead for computing facility or resource.

4.1 Fixed Size Grid - FSG

The first design strategy assumes that, there are fixed number of resources available for computation. The proposed algorithm Fixed Size Grid is designed to have fixed number of reducers for computing any given task. Initially we fix the number of reducers for the task that need to be performed. Later the work is distribute across the spanned reducers.

Let the size of the dataset be W and let the number of reducers be n . The size of each node be s . We assume that $W >> n * s$. For a single node to process (s) amount of data it takes $O(t)$. The total time T taken for computing the complete task is given in Eq. 1.

$$T = \lceil \frac{W}{s * n} \rceil * O(t) \quad (1)$$

The design of Fixed Size Grid strategy is to compute a task by defining a fixed n . For a fixed n the total work W is assigned by dividing it into s parts. When the load is distributed among the reducers and computed, the performance of the algorithm is shown in Tables 1 and 2.

4.2 Fixed Size Input - FSI

The second design strategy assumes that, there are some resources available for computation. Assume the available resources are sufficient for computing any given task. Initially we fix the size of the input that needs to be given to a reducer for processing. Based on this dynamic number of reducers are spanned to compute the specified task. Let the size of the dataset be W and let the number of reducers be m . The size of each node be t . We assume that $W \gg m*t$. For a single node to process (t) amount of data it takes $O(t)$. The total time T taken for computing the complete task is given in Eq. 2.

$$T = \lceil \frac{W}{t * m} \rceil * O(t) \quad (2)$$

The design of Fixed Size Input strategy is to compute a task by predefining a size on the input given to a reducer m . For a fixed m the total work W is divided and assigned to the reducers. The performance of both these strategies are analysed in Tables 1 and 2.

4.3 Pseudocode for FSG and FSI

The pseudocode for Fixed Grid Strategy is as follows: Let the total work be W . The number of reducers available are n . The maximum capacity of the reducer is s . c_w is a set of works assigned to the available reducers. Each reducer i is assigned with work w_i . The work assigned to a reducer is a part of the total work W , which is W/s .

Algorithm 1. FSG

```

Input : W (TotalWork) , n (No. of Reducers)
Initialization : i = 0
s : # Max.CapacityofEachReducer
c_w : = { w_i | i = 1, 2, 3, ..., n } where w_i is the work assigned to the reducer i at
time t and c_w is a set of works assigned to the reducers
while i < n   do
    w_i ← W/s
end while

```

The pseudocode for Fixed Input Strategy is as follows: Let the total work be W . The maximum size of the input that can be given to a reducer is s . Assume that there are W/s number of reducers available. So, n the number of reducers is W/s (+1 for convenience). c_w is a set of works assigned to the available reducers. Each reducer i is assigned with work w_i . The work assigned to a reducer is a part of the total work W , which is W/n .

Algorithm 2. FSI

Input : W (TotalWork) , s (Max. size of input to a reducer)
Initialization : $i = 0$
 n (No. of Reducers) : $= W/s + 1$
 c_w : $= \{ w_i \mid i = 1, 2, 3, \dots, n \}$ where w_i is the work assigned to the reducer i at time t and c_w is a set of works assigned to the reducers
while $i < n$ **do**
 $w_i \leftarrow W/n$
end while

5 Experimental Evaluation

5.1 Datasets

To analyse the performance of the proposed methods, we considered two real time datasets Gowalla [6] and Brightkite [6]. Gowalla is an social networking site where the check-in data of the users is collected. This is location based service. The size of the dataset is varied from 1 million records to 4 million records with an overlap factor of 100. Similarly Brightkite is also a location based service where users are provided with a platform to share their checkin information. The size of the dataset is varied from 1 million to 2 million and with overlap factor of 100 and 200.

5.2 Results

The Table 1 shows the performance of brightkite dataset for Fixed Size Grid strategy. It is observed that the performance of the algorithm is shown in terms of time. The algorithm performed well for a fixed grid of 9*9 where as the performance is inferior for fixed grid sizes of 4*4 and 25*25. The Table 2 shows the performance for gowalla dataset. The FGS algorithm has superior performance for 9*9 grid and inferior performance for 4*4 and 25*25 grids.

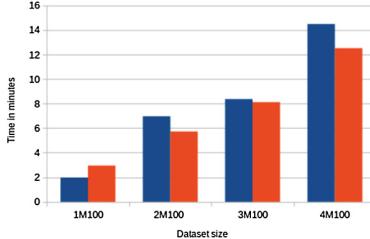
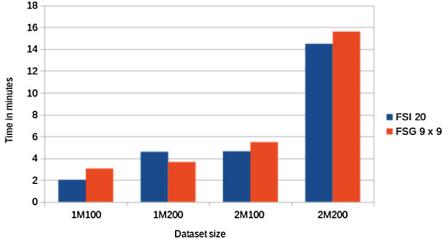
Table 1. Turn-around time for Brightkite FSG

Dataset size	FSG 4*4	FSG 9*9	FSG 25*25	FSI 20	FSI 30	FSI 40	FSI 80
1M100	3 m 46 s	2 m 57 s	6 m 1 s	2 m 37 s	1 m 59 s	2 m 9 s	2 m 30 s
2M100	7 m 23 s	5 m 44 s	8 m 7 s	5 m 22 s	6 m 58 s	7 m 2 s	8 m 54 s
3M100	15 m 2 s	8 m 7 s	10 m 31 s	8 m 17 s	8 m 22 s	17 m 15 s	17 m 11 s
4M100	26 m 34 s	12 m 31 s	14 m 53 s	28 m 36 s	14 m 29 s	21 m 48 s	43 m 44 s

The Table 1 shows the performance of the FSI algorithm for brightkite dataset. The algorithm has better performance when the size of the input is 30. For the input of sizes is 20, 40 and 80 the algorithm has inferior performance. The Table 2 shows the performance of FSI algorithm for gowalla dataset. The

Table 2. Turn-around time for Gowalla FSG

Dataset size	FSG 4*4	FSG 9*9	FSG 25*25	FSI 20	FSI 30	FSI 40	FSI 80
1M100	4 m 20 s	3 m 3 s	6 m 40 s	2 m 1 s	2 m 0 s	4 m 50 s	2 m 5 s
1M200	4 m 31 s	3 m 39 s	7 m 22 s	4 m 35 s	4 m 34 s	4 m 31 s	4 m 43 s
2M100	8 m 52 s	5 m 28 s	8 m 15 s	4 m 38 s	5 m 16 s	9 m 4 s	10 m 37 s
2M200	24 m 11 s	15 m 36 s	15 m 48 s	14 m 29 s	22 m 22 s	50 m 23 s	1 h 27 s

**Fig. 3.** Gowalla FSI vs FSG**Fig. 4.** Brightkite FSI vs FSG

algorithm has better performance at the input size of 20 where as for input sizes 30, 40 and 80 the performance is inferior.

Figure 3 shows that the FSI algorithm has better performance when compared to FSG algorithm. For the input size of FSI at 20 and for the grid size of 9*9 FSG, the performance of the FSI is increasing with the increase in the size of the dataset and the overlap factor. Figure 4 shows that the FSG algorithm has better performance when compared to FSI algorithm. For the input size of FSI at 30 and for the grid size of 9*9 FSG, the difference in time is increasing with the increase in the size of the dataset.

For the data that needs to be processed without more exchanges via network we need to select a Fixed Size Grid strategy and for data that needs more exchanges via network we need to select Fixed Size Input strategy. The experimentation shown in Sect. 5 shows the performance of the algorithms at various workloads.

6 Conclusions

We proposed two design strategies, Fixed Size Input and Fixed Size Grid, varying the constraint on input size to a reducer and on the number of reducers. Our analysis helps in deciding an effective strategy, to achieve better performance in distributed computing platforms. We show the performance of these two strategies in terms of turn around time on two real world datasets. We illustrated the cases where FSI and FSG is suitable.

References

1. Afrati, F.N., Stasinopoulos, N., Ullman, J.D., Vassilakopoulos, A.: SharesSkew: an algorithm to handle skew for joins in mapreduce. *Inform. Syst.* **77**, 129–150 (2018)
2. Afrati, F.N., Ullman, J.D.: Optimizing joins in a map-reduce environment. In: Proceedings of the 13th International Conference on Extending Database Technology, pp. 99–110. ACM (2010)
3. Beame, P., Koutris, P., Suciu, D.: Communication steps for parallel query processing. In: Proceedings of the 32nd ACM SIGMOD-SIGACT-SIGAI Symposium on Principles of Database Systems, pp. 273–284. ACM (2013)
4. Beame, P., Koutris, P., Suciu, D.: Skew in parallel query processing. In: Proceedings of the 33rd ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems, pp. 212–223. ACM (2014)
5. Cheng, L., Kotoulas, S., Liu, Q., Wang, Y.: Load-balancing distributed outer joins through operator decomposition. *J. Parallel Distrib. Comput.* (2019)
6. Cho, E., Myers, S.A., Leskovec, J.: Friendship and mobility: user movement in location-based social networks. In: Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 1082–1090. ACM (2011)
7. Chu, S., Balazinska, M., Suciu, D.: From theory to practice: efficient join query evaluation in a parallel database system. In: Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data, pp. 63–78. ACM (2015)
8. Gavagsaz, E., Rezaee, A., Javadi, H.H.S.: Load balancing in join algorithms for skewed data in mapreduce systems. *J. Supercomput.* **75**(1), 228–254 (2019)
9. Irandoost, M.A., Rahmani, A.M., Setayeshi, S.: MapReduce data skewness handling: a systematic literature review. *Int. J. Parallel Program.* 1–44 (2019)
10. Joglekar, M., Re, C.: It's all a matter of degree: using degree information to optimize multiway joins. arXiv preprint [arXiv:1508.01239](https://arxiv.org/abs/1508.01239) (2015)
11. Koutris, P., Beame, P., Suciu, D.: Worst-case optimal algorithms for parallel query processing. In: LIPICS-Leibniz International Proceedings in Informatics, vol. 48. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik (2016)
12. Kwon, Y., Balazinska, M., Howe, B., Rolia, J.: Skewtune in action: mitigating skew in mapreduce applications. *Proc. VLDB Endow.* **5**(12), 1934–1937 (2012)
13. Ngo, H.Q., Ré, C., Rudra, A.: Skew strikes back: new developments in the theory of join algorithms. arXiv preprint [arXiv:1310.3314](https://arxiv.org/abs/1310.3314) (2013)
14. Shi, Y., Qian, K.: LBMM: a load balancing based task scheduling algorithm for cloud. In: Future of Information and Communication Conference, pp. 706–712. Springer (2019)
15. Wang, Z., Chen, Q., Suo, B., Pan, W., Li, Z.: Reducing partition skew on mapreduce: an incremental allocation approach. *Front. Comput. Sci.* **13**(5), 960–975 (2019)



Implementation of Visible Foreground Abstraction Algorithm in MATLAB Using Raspberry Pi

M. L. J. Shruthi¹(✉), B. K. Harsha¹, and G. Indumathi²

¹ CMR Institute of Technology, Bengaluru, Karnataka, India
shruthimlc@gmail.com

² Cambridge Institute of Technology, Bengaluru, Karnataka, India

Abstract. The Visual Surveillance system has been an active subject matter due to its importance in security purpose. Detection of moving objects in a video sequence is obligatory in many computer vision applications. The present Visual Surveillance system is not smart enough to take its own actions based on the observations. Crime rate can be reduced greatly if the surveillance systems are able to take their own actions based on the observations. This can be achieved by implementing algorithms with compact hardware in the surveillance system. This paper depicts the real time hardware implementation of Visible Foreground Abstraction (VFA) algorithm in raspberry pi. In this work, the main concentration is the design of VFA algorithm in MATLAB® and its implementation using Raspberry Pi module. The design and implementation has yielded better accuracy than previous algorithms.

Keywords: Motion · Image · Implementation · Raspberry · Surveillance

1 Introduction

Surveillance is a process of monitoring the object or people's behaviour. The word surveillance is normally used to describe the distant observation by means of electronic equipment and other technologies [1].

For an epoch, video monitoring in public places like malls, banks, jewellery shops, super markets etc. has become one of our prime concerns and it acts as a crime deterrent. They work on the principle of motion detection.

Motion detection is the process of detecting moving object with respect to background. Some of the commonly used motion detection algorithms are simple background subtraction, subsequent frame difference, optical flow and ViBe [2].

Background subtraction method is one of the widely used algorithm for separating foreground elements from the background scene in a video frame structure. This algorithm is extremely easy to implement and use but it is not efficient in the case of dynamic background [3]. Figure 1 shows the block diagram of a simple background subtraction algorithm. In the model, current frame is subtracted from the background model set. To identify the elements as foreground, a threshold is used. This is also called as simple frame differencing method.

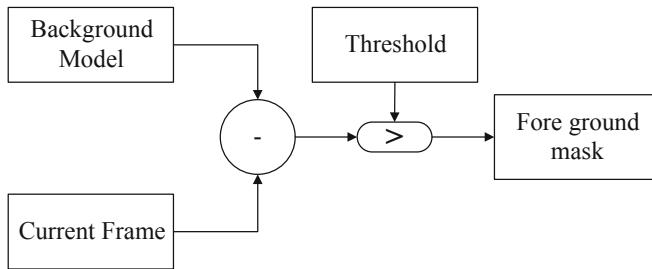


Fig. 1. Simple background subtraction model

Subsequent frame differencing method is also identified as temporal difference method. In the method, the difference between the frame at time t_1 and the frame at time $t_1 - 1$ is calculated. If the result is greater than the predefined threshold value, then the pixel is considered as background element else it is considered as foreground element [1]. The block diagram of frame differencing is as shown in the Fig. 2.

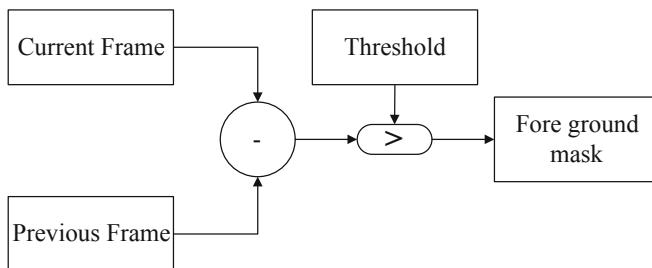


Fig. 2. Subsequent frame difference method

The background model in Visual Background Extraction (ViBE) algorithm is a set of perceived pixel values. Thus, this method differs with respect to other methods that concentrate on probability distribution functions. Thus background model selected by ViBE points at the difficulties of selecting correct probability distribution and its updation.

The extracted output of background subtraction algorithm contains noise and features and detection accuracy needs to be improved. In this paper, VFA algorithm is presented to overcome these issues. It is proven to perform well with respect to other traditional methods, in terms of its high detection rates and low computational time. Implementation of ViBE algorithm is done in [12].

Hitherto many motion detection algorithms have been designed:

Wang and Zhao [4] proposed motion detection using simple background subtraction technique. Here the video frames are comprised of series of images which contains geometrical information of the target, and extracts related information to analyse the motion of the target. Decision of whether the pixel belongs to background is done by the algorithm.

Rakibe and Patil [5] proposed motion detection algorithm based on threshold. After the subtraction between the current frame and the previous frame, the threshold is applied to decide upon the pixel belonging to foreground or background. Ensuing this, morphological process is applied to remove the noise and to solve the background interruption difficulties.

Kavitha and Tejaswini [6] presented a motion detection algorithm. In this, work has been carried out to prevail over the simple background subtraction algorithm. In this method, light is thrown on illumination changes that affect the result, such as removal of shadow.

Shafie and Alie [7] have designed an algorithm based on optical flow. Optical flow can occur from the relative motion of the object and the viewer. In the method, region is segmented into belonging to background or foreground based on the discontinuities in optical flow.

Real time detection method is proposed by Lu and Yang in [8]. In this algorithm, a combination of temporal differencing method, optical flow method, double background filtering method and morphological processing method is specified to achieve better performance.

With the aforementioned algorithms, there is a necessity to improve upon real time provision. VFA concentrates on the same. In the following segment, the methodology for VFA algorithm is discussed.

2 Methodology

VFA is a foreground object segmentation algorithm. The background model of VFA consists of pixels in the neighbourhood which depends upon a probability distribution function and foreground is extracted by comparing the current pixel with the background. This algorithm is modelled in three steps.

2.1 Background Modelling

The algorithm uses the first frame to initialize its background model or sample space. Each pixel point (x, y) , uses the space distribution features and checks if the neighbouring pixel point has similar pixel value [9]. The neighbouring pixel points that have different pixel values will turn out to be the sample space values. The sample space or background model size is M which is based on M neighbourhood pixel points. The background model at $t = 0$ (time) is given by (1) [9].

$$M(0) = \{v_1(x, y), v_2(x, y), \dots, v_N(x, y)\} \quad (1)$$

2.2 Foreground Detection

After background modelling, foreground detection is achieved in two simple processes [1]. First, check whether the current pixel belongs to the N pixel sample space or not. Based on the above method calculate the number of pixels in foreground and background.

Assume r is the Euclidean distance between pixels (r is 20 for monochromatic image). Compute the absolute difference between each pixel in current frame with all N pixel intensity of the sample space in the previous frame at the same location [1]. The pre-detected pixels can be formulated by (2)

$$g(x, y) = \begin{cases} |c(x, y) - b(x, y)| > r \\ |c(x, y) - b(x, y)| \leq r \end{cases} \quad (2)$$

$$N_i(x, y) = \begin{cases} 1 & \text{num} < \# \min \\ 0 & \text{num} \geq \# \min \end{cases} \quad (3)$$

When $N(x, y) = 1$ denotes the current pixel $c(x, y)$ is foreground pixel point
 $N(x, y) = 0$ denotes the current pixel $c(x, y)$ is background pixel point.

2.3 Updating Background Model

VFA algorithm uses the Conservative strategy to update the background model. If a pixel belongs to background, a random sample pixel point in the background model has to be substituted as that pixel value [11].

Connecting MATLAB to Raspberry pi 3B+

Download the Support Package for Raspberry Pi Hardware. This can be downloaded from the MATLAB Toolstrip Add-Ons or by typing “targetinstaller” in the Command Line. The Support Package installer will lead through the installation process. Install all the software required to run on a Raspberry Pi. After downloading the Support Package for Raspberry Pi, connect the Raspberry Pi Hardware [12].

The Steps that are to be followed are as follows: Remove the SD memory card from the host computer and insert into the Raspberry Pi Hardware. Connect an Ethernet cable to the board. Connect the other end of the ethernet cable to a network or directly to the host computer. Connect a 5 V micro USB power supply to the board. The power supply should be rated at least 700 mA.

The connection of the hardware (Raspberry Pi 3B+) to the Simulink software is established after configuring the board [12].

Flow chart for the proposed algorithm is as shown in Fig. 3.

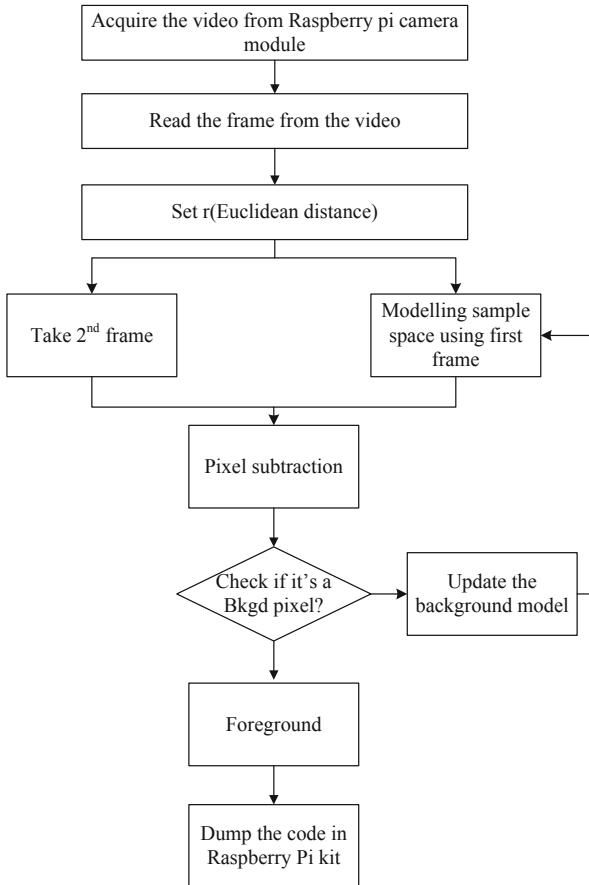


Fig. 3. Flow chart of the proposed algorithm

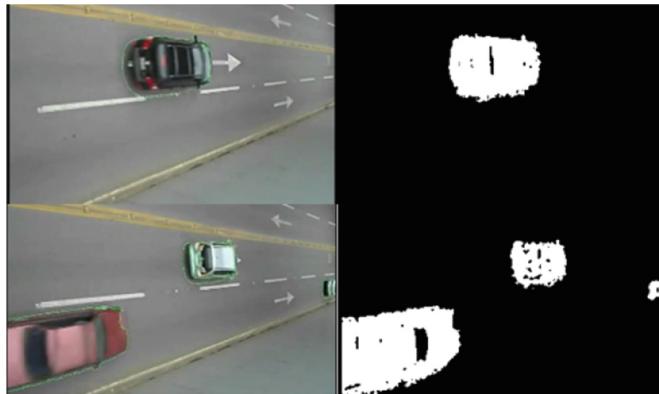
3 Results and Discussion

The proposed algorithm is implemented on Raspberry Pi 3B+ 1.4 GHz 64-bit quad ARM Cortex-A53 CPU, 1 GB LPDDR2 RAM at 900 MHz, with Raspbian Software and OpenCV. The frame sequence used is baseline/Highway and the video frames are 176×320 pixels in size.

The time taken to process the 303-frame sequence using original ViBe Algorithm is 19312 ms, so the processing speed is 63.73 ms per frame. The total processing speed of the proposed method is 17914 ms, so the processing speed is 59.12 ms per frame. The same is shown in Table 1. Accuracy is improved compared to the original ViBE algorithm that is visible through the results in Fig. 4. In the figure, the frames are shown in the left side and the comparative result is shown in the right. The white colored regions indicate that there is motion and black indicates that the region belongs to background.

Table 1. The comparison of computation time

Method	Total time	Average time
Original ViBE	19312 ms	63.73 ms
Proposed method	17914 ms	59.12 ms

**Fig. 4.** Original frame and result of VFA algorithm

4 Conclusion and Future Scope

In the proposed implementation of the algorithm, accuracy is increased but the processing speed is decreased. The experimental results show that this method can achieve motion detection at a limited additional cost when compared with other hardware implementation. Raspberry pi is compact, lightweight hardware and suitable for the real time implementation. The limitation of this algorithm is that it involves the appearance of ghost as in the original ViBE algorithm.

References

1. Gupta, P., Singh, Y., Gupt, M.: Moving object detection using frame difference, background subtraction and SOBS for video surveillance application. In: The Proceedings of the 3rd International Conference System Modeling and Advancement in Research Trends (2014)
2. Hammami, M., Jarraya, S., Ben-Abdallah, H.: A comparative study of proposed moving object detection method, in general of next generation information technology. *J. Next Gener. Inform. Technol.* (2011)
3. Shruthi, M.L.J., Indumathi, G.: Motion tracking using pixel subtraction method. In: The Proceedings of IEEE 2017 International Conference on Computing Methodologies and Communication (2017)
4. Wang, Z., Zhao, Y., Zhang, J., Guo, Y.: Research on motion detection on video surveillance system. In: the Proceedings of 3rd International Conference on Image and Signal Processing, vol. 1, pp. 193–197, October 2010

5. Rakibe, R.S., Patil, B.B.: Background subtraction algorithm based motion detection. *Int. J. Sci. Res. Publ.* **3**(5), 14 (2019)
6. Kavitha, K., Tejaswini, A.: VIBE: background detection and subtraction for image sequences in video. *Int. J. Comput. Sci. Inform. Technol.* **3**, 5223–5226 (2012)
7. Alli, M.H., Hafiz, F., Shafie, A.: Motion detection techniques using optical flow. *J. World Acad. Sci. Eng. Technol.* **32**, 559–561 (2009)
8. Lu, N., Wang, J., Wu, Q.H., Yang, L.: An improved motion detection method for real time surveillance. *J. Comput. Sci.* **1** (2008)
9. Zhang, Y., Zhao, X., Tan, M.: Motion detection based on improved sobel and ViBe algorithm. In: the Proceedings of the 35th Chinese Control Conference, 27–29 July 2016
10. Chun-Hyok, P., Hai, Z., Hongbo, Z., Yilin, P.: A novel motion detection approach based on the improved ViBe Algorithm. In: The Proceedings of the 28th Chinese Control and Detection Conference (2016)
11. Kryjak, T., Gorgon, M.: Real time implementation of the ViBe foreground object segmentation algorithm. In: The Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (2013)
12. Connection to Raspberry pi Hardware-MATLAB And Simulink-MathWorks



A New Hardware Design and Implementation of QPSK Modulator in Normal and 4-QAM Mode for 5G Communication Networks

R. Rameshkumar^{1(✉)} and J. N. Swaminathan²

¹ KLEF, Vaddeswaram, Guntur 522502, Andhra Pradesh, India
rameshmit07@gmail.com

² Department of ECE, QIS College of Engineering and Technology,
Ongole, Andhra Pradesh, India
swaminathan@qiscet.edu.in

Abstract. Digital information can be represented by Quadrature Phase Shift Keying (QPSK) modulation scheme. In order to represent digital data, a finite variety of different signals is used in modulation schemes. For the representation of digital signals, QPSK uses four unique phases. Due to the key features and performance efficiency in bit error rate and optimal bandwidth, QPSK is commonly used in several modern digital communication based applications. Satellite, wireless and mobile communication uses this technology. QPSK modulators made with mux, counters and balanced modulators are already available in the market. Due to the use of transformers for making these devices, they turn out to be bulky. This paper propose a general purpose IC based novel QPSK modulator. This efficiently reduces the size and thereby the complexity of the circuit.

Keywords: Quadrature Phase Shift Keying (QPSK) · Pseudo Random Binary Sequence (PRBS) · Bit splitter · Multiplexer · Binary Phase Shift Keying (BPSK)

1 Introduction

QPSK or Quadrature Phase-Shift Keying is a higher order modulation scheme used in digital modulation. A QPSK signal can be generated by independently modulating two carriers in quadrature ($\pm \cos \omega t$ and $\pm \sin \omega t$). Traditionally, QPSK waveform will be generated by multiplying sine and cosine waveforms with odd and even bits from input bit stream as shown in Fig. 1. It uses two balanced modulator each fed with carrier signals generated from local oscillator. In our experiment, we try to generate QPSK waveform without using balanced modulator or multiplier [2] as shown in Fig. 2. A Pseudo Random Binary Sequence (PRBS) generator is used to generate random binary data. The Serial to Parallel Converter splits the incoming data into even and odd bits. Even and odd bits are used as address lines of 8:1 Multiplexer (4051). The signals, $\pm \cos \omega t$, $\pm \sin \omega t$ are generated using function generators, phase shifter, inverters are given to the input lines of multiplexer. Depending on Even and Odd bits, multiplexer chooses any one of these signals to form the QPSK waveform. In this project we use

CMOS IC instead of TTL ICs. In CMOS ICs all unused pins must be grounded to ensure proper functioning of the IC.

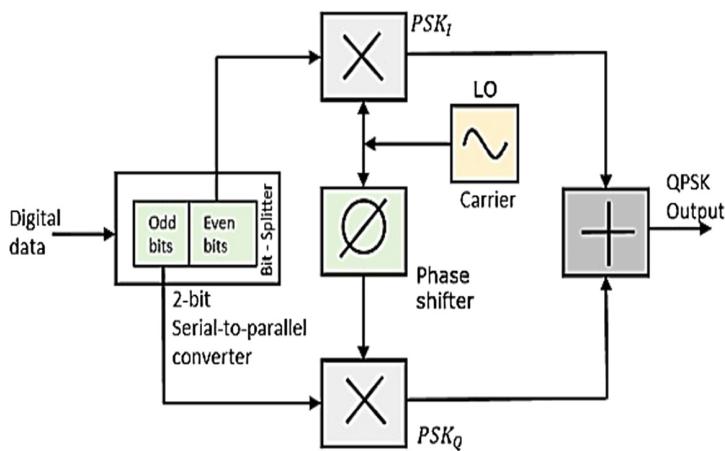


Fig. 1. Classical method of QPSK generation [3]

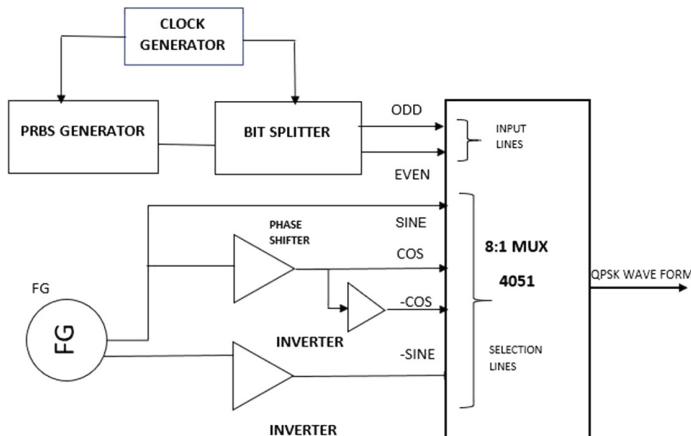


Fig. 2. Proposed method of QPSK

2 QPSK Constellation and Waveforms

In BPSK, there are two symbols since we use only one bit. Hence the phase shift required between the symbols is $360/2 = 180^\circ$. QPSK has two bits per symbol and hence there are 4 combinations: 00, 01, 10, 11. So the phase difference between any two successive symbols is $360/4 = 90^\circ$ [1]. These phase shifts are produced corresponding to 4 different combinations of I and Q data (or Odd and Even data) (Table 1 and Fig. 3).

Table 1. QPSK wave form in 4-QAM mode

Even	Odd	Phase	Waveform
1	1	45°	A
0	1	135°	B
0	0	225°	C
1	0	315°	D

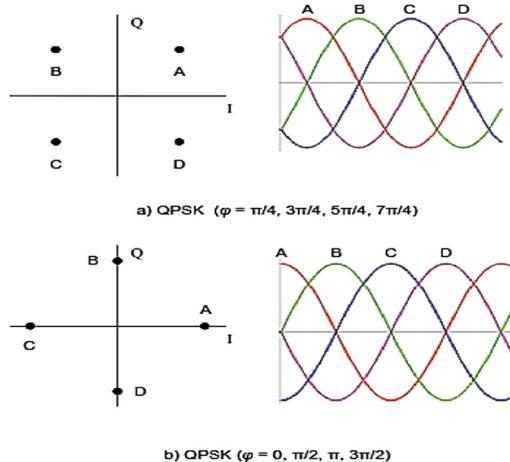


Fig. 3. QPSK constellation and waveforms

In Fig. 4, first wave form is PRBS data. 2nd and 3rd wave are I and Q output from bit splitter. The last wave form is QPSK wave form. Note that the waveform changes phases.

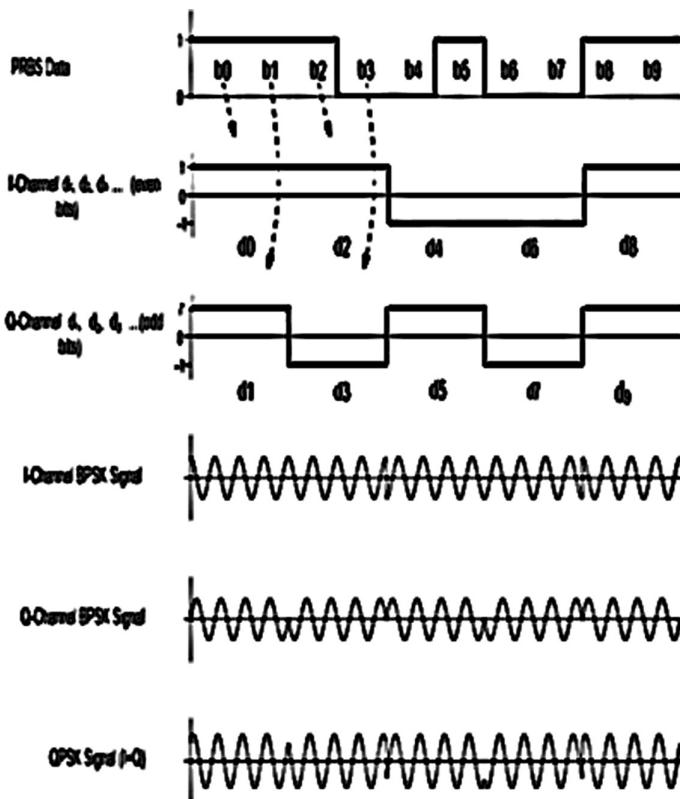


Fig. 4. QPSK wave form and timing diagram

3 QPSK Modulator

3.1 Clock Pulse Generator

An astable multivibrator using 555 timer is used as clock frequency (square wave) generator is shown in Fig. 5. This clock is used to feed clock signal to PRBS generator and bit splitter. $R_1 = 3.3 \text{ k}\Omega$ $R_2 = 5.6 \text{ k}\Omega$ $C = 0.1 \mu\text{F}$ Clock frequency $f = 1/T$ $T = T_{on} + T_{off}$ $T_{on} = 0.69R_2C = 0.3864 \text{ ms}$ $T_{off} = 0.69(R_1 + R_2)C = 0.6141 \text{ ms}$ $T = 1 \text{ ms}$ $f = \frac{1}{T} = 1 \text{ kHz}$.

3.2 PN-Sequence Generator

The random bit generator generates a bit sequence (PN-sequence) that is used as input data for our QPSK modulator [4]. A PN-sequence generator circuit is constructed (Fig. 6) using linear feedback shift register (LFSR). The output of 3rd and 4th flipflops are combined using XOR gate and fed back to the D input of first flipflop. We use four

D flip-flops (4013) and one XOR gate (4030) so we can generate $24-1 = 15$ bits (1 1 1 1 0 0 0 1 0 0 1 1 0 1 0) and then the bits sequence (15 bits) will be repeated periodically. The output of last flipflop (i-4) is fed to the bit splitter (Fig. 7). The even and odd bit sequence are given in the Table 2. The Even bit sequence: 11000100 and odd bit sequence: 11010111.

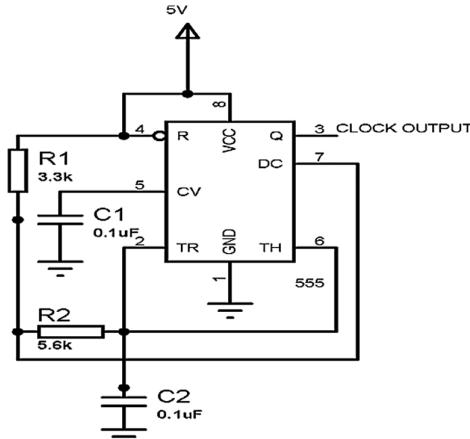


Fig. 5. 555 timer as astable multivibrator

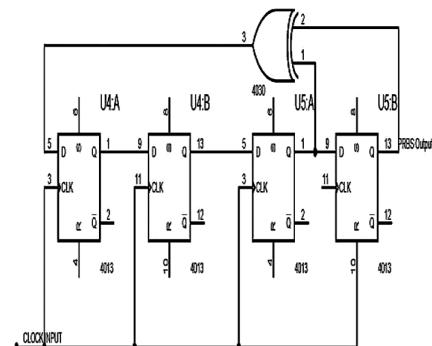


Fig. 6. PN-sequence generator

Table 2. PRBS output sequence

X_{i-1}	X_{i-2}	X_{i-3}	X_{i-4}	X_i	Even	Odd
1	1	1	1	0	1	
0	1	1	1	0		1
0	0	1	1	0	1	
0	0	0	1	1		1
1	0	0	0	0	0	
0	1	0	0	0		0
0	0	1	0	1	0	
1	0	0	1	1		1
1	1	0	0	0	0	
0	1	1	0	1		0
1	0	1	1	0	1	
0	1	0	1	1		1
1	0	1	0	1	0	
1	1	0	1	1		1
1	1	1	0	1	0	
1	1	1	1	0		1

The clock pulse is taken from the astable multivibrator. Hence the data rate is same as that of the clock frequency.

3.3 Frequency Divider & Bit Splitter

This stage divides the input bit sequence from PRBS into even and odd bits. Bit splitter is comprised by 3 D flip-flops(4013) (Fig. 7). The first D flipflop (Q and \bar{Q} shorted) divides the input clock into two. Now, Q and \bar{Q} outputs of first flipflop are given as clock to flipflops A and B. Data to A & B is from PRBSwhose common input data is from PRBS generator. Flipflop A shifts only even bits (0, 2, 4...) and flipflop B shifts only Odd bits (1, 3, 5, ...) (Fig. 8).

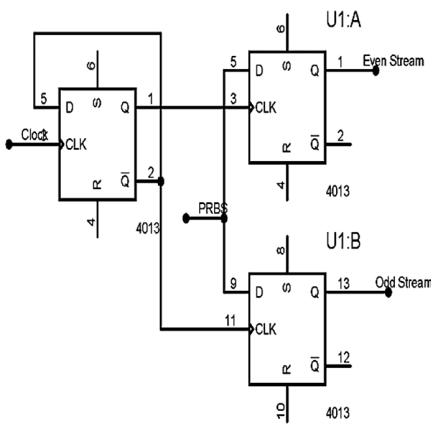


Fig. 7. Bit splitter

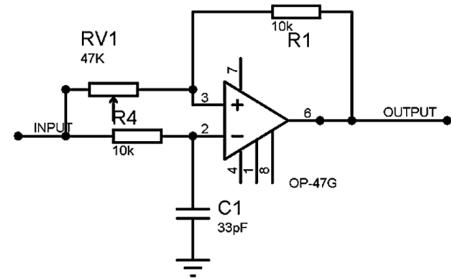


Fig. 8. Phase shifter

3.4 Integrated Circuit Diagram

Below is the complete circuit diagram of QPSK modulator. The power supply given to ICs 4013, 4030, 4051 is 5 V and for Op-amp 741 is ± 9 V. A 4 bit PRBS generator is constructed by below steps.

1. Construct the clock generator as shown in the circuit diagram (Fig. 5)
2. Construct the PRBS generator as shown in Fig. 6
3. Using three D flip-flops (4013) construct the frequency divider and bit splitter as shown in the circuit diagram (Fig. 7)
4. Using function generator, get the carrier frequency $\sin \omega t$. Feed this to 90° phase shifter to get $\cos \omega t$.
5. Feed $\sin \omega t$ and $\cos \omega t$ to inverters to get $-\sin \omega t$ and $-\cos \omega t$
6. Construct the multiplexer and feed $\pm \sin \omega t$, $\pm \cos \omega t$ to input lines and I and Q data to selection lines as shown in the circuit diagram.
7. Observe the QPSK waveform from 3rd pin of Mux (4051). Adjust the potentiometer of phase shifters to get accurate phase shifts.

4 Results and Discussion

Upper waveform is clock pulse obtained from the Astable multivibrator output and lower one is PRBS data. The waveform swings between 0 and 5 V. (Unipolar) We can observe the pattern 100110101111000 from the lower waveform. For each complete cycle of square wave, one bit is assumed. This pattern will repeat periodically for every 15 bits (Figs. 9, 10, 11 and 12).

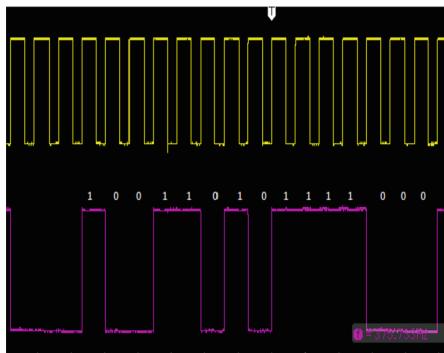


Fig. 9. Clock pulse and PRBS data

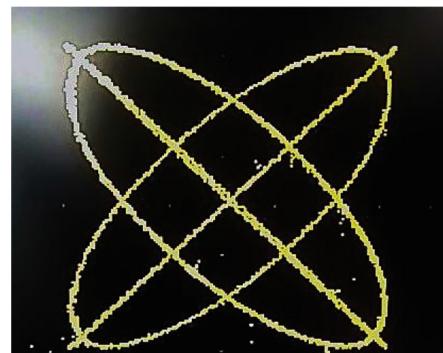


Fig. 10. QPSK waveform (4 QAM)

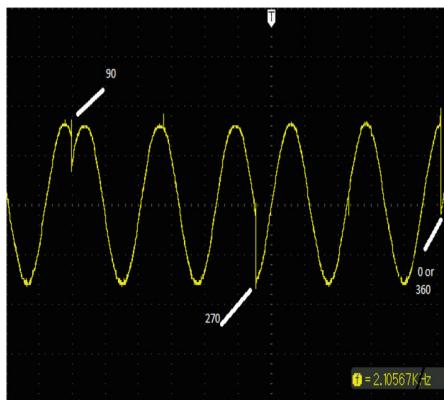


Fig. 11. QPSK waveform1

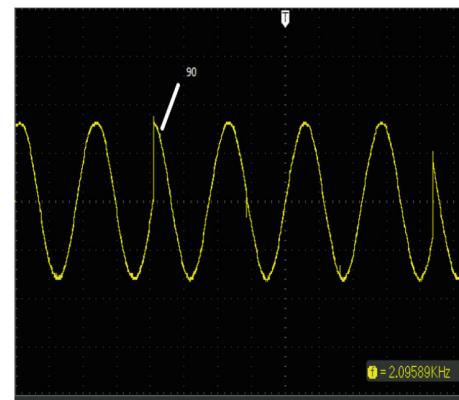


Fig. 12. QPSK waveform2

5 Conclusion

The four unique phases of a QPSK signal are clearly expressed in the waveforms shown in the result section. It is beyond the traditional textbook methodology. QPSK and similar solid applications can be demonstrated and implemented using easily available general purpose ICs. This overcomes the bulkiness, complexity and cost of

the balanced modulators that use transformers in their circuits. Other ICs such as MC1496 provide higher accuracy but are more complex and expensive. These drawbacks are overcome by the proposed circuit.

Acknowledgement. The Author like to acknowledge **Er.Koneru Satyanarayana**, President of K L Deemed to be University,Green Fields, Vaddeswaram, Andhra Pradesh, India for providing facility to do the research work.

References

1. Chowdhury, M.A.N., Mahfuz, M.U., Chowdhury, S.H., Kabir, M.M.: Design of an improved QPSK modulation technique in wireless communication systems. In: IEEE International Conference on Electrical Information and Communication Technology (EICT) (2017)
2. Pareek, V.: A novel implementation of QPSK modulator on FPGA. In: IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS) (2016)
3. Birla, N., Gautam, N., Patel, J., Balaji, P.: A novel QPSK modulator. In: IEEE International Conference on Advanced Communications, Control and Computing Technologies (2014)
4. Jain, M., Kesharwani, P., Malviya, A.K., Khare, K., Shandilya, P., Haldar, S., Rai, H., Aggarwal, S.: Performance optimized digital QPSK modulator. In: International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (2017)



A Novel Approach for the Run-Time Reconfiguration of Heterogeneous Applications in a Smart Home Monitoring System

K. S. Rekha¹(✉), A. D. Kulkarni², and H. D. Phaneendra¹

¹ Department of CS&E, The National Institute of Engineering, Mysuru, India
rekha_kowdle@yahoo.co.in, hdphane@nie.ac.in

² Department of E&E, The National Institute of Engineering, Mysuru, India
nieadk@gmail.com

Abstract. The Run-time Reconfiguration is implemented in many of the applications like Home Automation, Structural Health Monitoring Systems, Intrusion Detection Systems, Fire Detection Systems etc. It is required to dynamically reconfigure the applications based on the changing needs. Since all these applications runs on different networks, there is a demand to run the heterogeneous applications on the same network. The objective of this paper is to develop an adaptive model for run-time reconfigurations of Heterogeneous applications in a Smart Home Monitoring System using Wireless Sensor Networks and Internet Of Things. The intelligent mechanism would dynamically reconfigure itself and run only the required application. The proposed system saves the power and memory consumption.

Keywords: Internet of Things (IOT) · Run-time reconfigurations · Dynamic reconfiguration · Wireless Sensor Networks (WSN)

1 Introduction

An application deployed for specific purpose requires a dedicated platform of the Wireless Sensor Network to support its functionality. Sometimes, there may be cases, where many of these applications are combined together and run as a single application on the WSN. If such individual wireless sensor network platform is required for each application, then the system would result in power and memory overhead. A framework is proposed to support the runtime reconfiguration of Heterogeneous applications with less power and memory consumption.

The organization of the paper is as follows. The Sect. 2 describes the works carried out in the dynamic reconfiguration of heterogeneous applications of WSN. The Sect. 3 addresses the issues related to the multiple monitoring of heterogeneous applications. The Sect. 4 presents the design of the smart home monitoring system. The Sect. 5 proposes an algorithm for run-time reconfiguration of the Home Automation System. In Sect. 6, the results based on the memory and power consumptions are discussed. In Sect. 7, the Concluding remarks are discussed.

2 Related Works in Dynamic Reconfiguration of Heterogeneous Applications of Wireless Sensor Networks

The applications based on WSN and IOT works in highly dynamic environment where the demand changes with respect to the changing context. To meet the increasing demands of the applications the runtime reconfigurations can be implemented at the sensor node level, network level and on the heterogeneous applications level.

In [1], Kunal et al. have proposed a smart home monitoring system specially designed for the benefit of handicapped and aged people. The system helps to control the home appliances and alert the user during the critical situations. The automated system provides the remote control of lighting through the micro-controller.

In [2], Sharma et al. have designed a system for Home Automation. The system saves the electricity consumption and reduce human efforts. The Home Automation system data is sent to cloud.

In [3], Babu et al. have designed a home automation system using Raspberry pi. The data is sent to the cloud. The different applications are monitored as well as controlled remotely.

In [4], Kousalya et al. have proposed and implemented an IOT system for the smart home automation. The system is built on a Node MCU module for the control and security of the home. The image is captured through the camera and sent to the owner when the intruder is detected.

In [5], Tanya et al. have proposed a smart Home system for security purpose. The intruder is identified with the help of the haar algorithm. The image is taken from the live video streaming and saved into the data base. To save the memory the image captured is converted into the grey scale. This is developed for remotely controlled and uses the Wi-Fi for transmission of the data's.

In [6], Vinay sagar et al. have proposed a automation system based on distributed networks. The system consists of server and sensors for monitoring and control task. The proposed system uses the Wi-Fi to connect the sensors to the server.

In [7], Pawar et al. have developed a prototype for Home Automation system. The prototype will control the devices using Android smart phone. The control mechanism works either connecting to Bluetooth or to the Internet. The Bluetooth is used for connectivity when the user is within short range of the system otherwise the online option is selected.

In [8], Satapathy et al. have proposed a home monitoring system with Arduino UNO microcontroller with WiFi. The system can monitor remotely and control the device using the smart phone application. The system is designed for security purpose with low cost.

In [9], Soliman et al. have designed an IOTsystem for smart home automation. The system is designed with Arduiono UNO for two cases namely the Wireless and Wire-line based. The system works for both manually and automatically under different operational modes. During the wireless mode the Arduino UNO is used where as during wire-line the Field Programmable Gate Array is used.

In [10], Gurav et al. have designed and implemented an IOT based Home Monitoring system. The system will automatically switch on/off lights, fans, gas using the sensor and the process is managed by the interface based on the android application.

In [11], Sudharani et al. have proposed a home automation system using Arduino and internet of things (IOT) which employs the embedded block and script programming for Arduino and sensors. This automation includes controlling of home appliances and also smart controlling of water system.

In [12], Gagan have designed a smart home monitoring for aged and handicapped persons. An alerting mechanisms will inform the user about the change in the context. The system is built with intel galileo board and various sensors to monitor and control the electrical appliances at home.

In [13], Panwar et al. have designed a IOT based home automation system. The system monitors as well as control the devices through a central host PC and mobile based application.

In [14], Ortiz et al. have addressed the dynamic changes in feature models in sensor networks product families, where nodes of the network demand dynamic reconfiguration at post-deployment time. A specific module called Alter Product Runtime Mechanism (APRM) was implemented.

In [15], Benkan et al. have proposed an reconfigurable architecture for plug-and-play wireless sensor network testbeds. The reconfigurable architecture support the functionality and testing of standard protocol stacks.

3 Problem Statement

There is a need for a Framework to support the multiple heterogeneous applications on the same WSN. The run-time reconfiguration is implemented on the heterogeneous applications of the Smart Home Monitoring System. If the multiple applications are running for 24×7 , then the memory and power consumption will be very high. The updated versions of code has to be injected depending on the varying context. The storage and management of data is difficult. There is a need for an intelligent mechanism in a WSN system which would dynamically reconfigure itself and run only one application based on the need. This context switching based on the dynamic need saves the memory and power consumption.

4 System Design

There are two heterogeneous applications namely Fire Monitoring system and Intrusion Detection system implemented on the same WSN for Home Automation Application. The Runtime Reconfiguration network consists of Raspberry Pi and Aurdino Board with many sensors such as PIR Motion Sensor, DHT 11 Humidity & Temperature Sensor and Gas Sensor. The software programs are written using python and embedded C.

4.1 Hardware Requirements

- Arduino
The Arduino is used to interface with the sensors and to send the sensor data to the Raspberry Pi.
- Raspberry Pi
The Raspberry Pi is used to interface with the Arduino. It sends the Sensor data to the Firebase Database. It also update the actuator values using the database.
- Intrusion Detection System
A Laser modules continuously emits light which is received by an LDR, if the contact is broken, a buzzer is triggered.
- Lighting System
A PIR Module continuously tracks movements to detect presence of people and based on presence, lights and fans inside a room are turned on or off.
- Fire Monitoring System
A DHT11 Module continuously monitors presence of poisonous/toxic gases, if there's any exceed in the gas parameter levels, an alarm (buzzer) is triggered.

4.2 Software Requirements

- Firebase
The Firebase is used to store the sensor values and to send the data to the actuators.
- Heroku
The Heroku is used to host the Web-Application. This can be used to control the intrusion detection system and to view the sensor values. Python is used to run the Scripts in Raspberry Pi for the desired functionality and to run the Web Application.
- Flask
The Flask is a framework in Python used to run the Web Application.
- Embedded C
The Embedded C is used for writing the code for the functionality of the Arduino.

5 Implementations

The entire system works majorly with two modules, the Normal Mode and the Dynamic Mode. The Normal Mode works before the Reconfiguration and the dynamic mode works during the runtime reconfiguration. The steps for Runtime Reconfigurations of Home Automation System is shown in Algorithm 5.1.

5.1 Algorithm for Runtime Reconfigurations of Home Automation System

1. Begin
2. #Define System Configuration <Config_Id>
3. Set Config_Id{intrusion_detect=0, Fire_Monitor=0}

4. Configuration Monitoring{collection_sensor_values(gas, ldr, pir)}
5. If (event_id(PIR==1)) //any motion detected by PIR sensor?
6. Switch from Monitoring_state to Emergency_state1
7. Set event_id(intrusion_detect=0, Fire_Monitor=1, gas=1, pir=0, ldr=1)
8. Else If(event_id(INTR==1))
9. Switch from Monitoring_state to Emergency_state2//Intrusion detection system
10. Set event_id(intrusion_detect=1, Fire_Monitor=0, gas=0, PIR=1, LDR=0)
11. Check if the ((timer >=60 s)
12. If (PIR==0 && Intr==0))
13. Switch from Emergency_State to Monitoring_State(go to step 4)
14. Else sense the input till the time exceeds
15. End

During the normal mode, when the Home Automation system is turned on, the indoor sensors and outdoor sensors will be ON until the reconfiguration is triggered. If any motion detected by the PIR sensor, the system would switch from normal monitoring_state to emergency_state1, then turn on the Climate Control & Gas Sensor System & turn off the Intrusion Detection System. If the INTR is 1, then switch from monitoring_state to emergency_state2.

The values of intrusion_detect is set 1 and the Fire_Monitor will be 0. The gas & LDR sensors are disabled and PIR sensor is enabled. The status of PIR and Intr is checked for every 60 s. If the PIR is 0 & intrusion value is 1 then the system will shift from emergency_state to Monitoring_state(go to step 4). In the normal mode, when the system is turned on, both indoor unit sensors and outdoor sensors stay on, until reconfiguration is triggered. The Fig. 1 shows the Intrusion detection toggling off immediately detecting the motion. The PIR is triggered by then motion inside house, the sensor network is reconfigured, Soon it will turn on the climate control and gas sensor system. But turn off the intrusion detection since someone is already sensed inside the house.

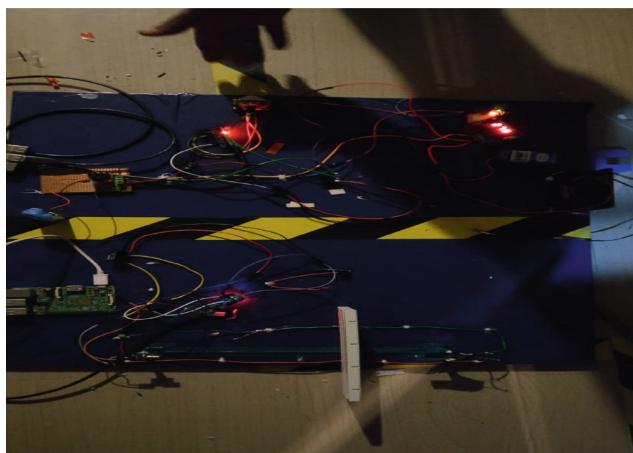


Fig. 1. Intrusion detection system toggling to OFF state

The Intrusion detection system toggles to OFF state and the Fire Monitoring system toggles to ON State. Figure 2 shows the Fire Monitoring System in action.



Fig. 2. Fire monitoring system in action.

6 Results and Discussions

The status of the sensed data can be observed in the Firebase database indicating values of Actuator and Sensors. When pir is 0 (no one in house) intr becomes 1 meaning it turns on intrusion detection. The Fig. 3 shows the values of Actuators and Sensors. When intrusion is 1 all the sensors are turned off inside the home.

Fig. 3. Values of actuators and sensors

6.1 Power Consumption

The Power Consumption is monitored for the different cases. The Fig. 4 power consumption for normal mode and dynamic mode. During the case-A, when the system is turned on, all sensors that are connected will turn on, conventional systems stay this way, but on trigger from either PIR or intrusion, the reconfigure happens and the values can be sent as an alert messages to the Mobile phone by installing the Sensor Monitor Application. The system during the normal mode, when all the sensors are ON, the power consumption is around 2212.5 mw.

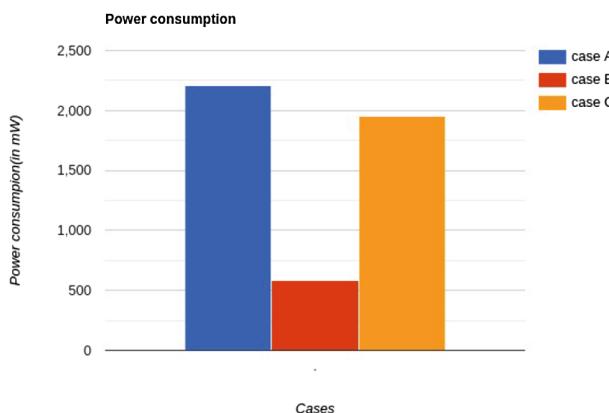


Fig. 4. Power consumption for normal mode & dynamic mode

During the Reconfiguration mode, the case-B when there is no one inside the house only Laser module and Proximity sensor will be ON, the power consumption is around 580 mw. In case-C, when people inside the house then the DHT11, MQ-2 Gas sensor, Temperature Sensor and Proximity sensor will be ON, the power consumption is 1957.5 mw. The runtime reconfiguration reduces the network congestion by sending only part of programming to the intended node to sense the data rather than resending the full code.

6.2 Memory Consumption

The Memory Consumption for Normal mode and dynamic mode are shown in Fig. 5. The Bandwidth consumption for Normal mode that is for case-1, when all sensors are ON is 5 bytes/second, where as in case-2, only 2 bytes/second will be consumed and in case-3, it is 4 bytes/sec. When an average of case-2 and case-3 is taken in case-4 it is 3bytes/second, we can save bandwidth of around 20% to 60% or on an average of 40% in Reconfiguration mode compared to the normal mode which is consuming bandwidth of 100%. The Fig. 5. shows the memory/Bandwidth consumption during the Normal Mode and dynamic mode. In dynamic mode, 3 different values are taken for case-A when all the sensors are ON, case-B when Laser module and Proximity sensor will be

ON. In case-C, when there are people inside the house, the DHT11, MQ-2 Gas sensor, Temperature Sensor and Proximity sensor will be ON.

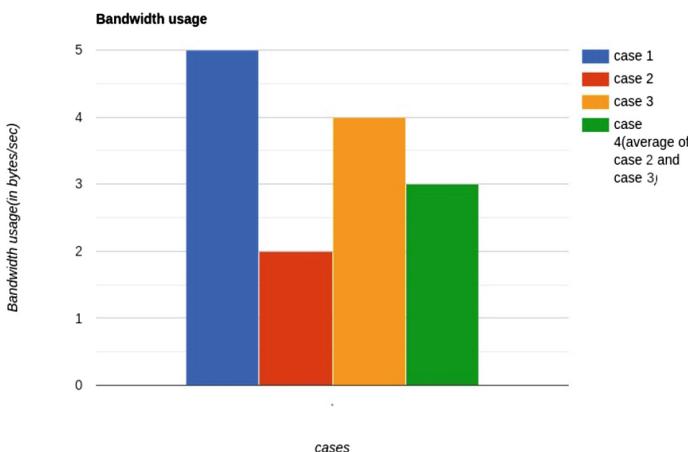


Fig. 5. Memory consumption for normal mode & dynamic mode

7 Conclusion

In this paper, we proposed a novel approach for solving the reconfiguration issue of the heterogeneous applications in a Home Monitoring System using the WSN and IOT. The Normal Mode and the dynamic Runtime Reconfiguration mode are implemented and Tested. In the proposed system, there is no need of running both the applications 24×7 . The Normal mode and dynamic mode will be selected based on the context. The reprogramming is done only to the intended nodes to avoid the network congestion. The code updates are sent only to the active application thereby saving the power, memory. The dynamic Runtime Reconfiguration implemented on the Heterogeneous applications in the Home Monitoring System is efficient, real-time and scalable.

References

1. Kunal, D., Tushar, D., Pooja, U., Vaibhav, Z.: Smart home automation using IOT. Int. J. Adv. Res. Comput. Commun. Eng. **5**(2) (2016)
2. Sharma, A., Shukla, S., Shukla, P., Singh, A., Kulkarni, V.: IOT based energy consumption and security control in home automation system. IOSR J. Comput. Eng. (IOSR-JCE) (2017). e-ISSN 2278-0661, p-ISSN 2278-8727
3. Babu, M.K.N., Lakshmi, K.V., Bhargavi, K.S., Ravi, A., Sasidhar, K.: IOT based home automation system using raspberry pi with web server. Int. J. Innov. Res. Sci. **7**(3) (2018)
4. Kousalya, S., Reddi Priya, G., Vasanthi, R., Venkatesh, B.: IOT based smart security and smart home automation. Int. J. Eng. Res. Technol. (IJERT) **7**(04) (2018). ISSN 2278-0181
5. Tanaya, Vadivukarasi, K.: Home security system using IOT. Int. J. Pure Appl. Math. **119** (15), 1863–1868 (2018)

6. Vinay Sagar, K.N., Kusuma, S.M., Gohane, S.P.: Home automation using internet of things. *Int. Res. J. Eng. Technol. (IRJET)* **02**(03) (2015)
7. Pawar, A., Sharan, R., Patil, R.: Home automation using bluetooth and IOT. *Int. J. Innov. Res. Comput. Commun. Eng.* **6**(2) (2018)
8. Satapathy, L.M., ‘O’ Anusandhan, S.: Arduino based home automation using Internet of things (IoT). *Int. J. Pure Appl. Math.* **118**(17), 769–778 (2018)
9. Soliman, M.S., Dwairi, M.O., Sulayman, I.I.M.A., Almalki, S.H.A.: Towards the design and implementation a smart home automation system based on internet of things approach. *Int. J. Appl. Eng. Res.* **12**(11), 2731–2737 (2017). ISSN 0973-4562
10. Gurav, U., Patil, C.: IOT based interactive controlling and monitoring system for home automation. *Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET)* **5**(9) (2016)
11. Sudharani, V., Siva, D., Vijaya Raju, M.: Smart home automation system using arduino and IOT. *Int. J. Sci. Res. (IJSR)*, **7**(9) (2018). ISSN 2319-7064
12. Gagan: IOT based system for person with physicaldisability. *Int. J. Innov. Res. Electr. Electron. Instr. Control Eng.* **4**(2) (2016)
13. Panwar, G., Maurya, R., Rawat, R., Kanswal, R., Ranjan, P.: Home automation using IOT application. *Int. J. Smart Home* **11**(9), 1–8 (2017)
14. Ortiz, Ó., García, A.B., Capilla,R., Bosch,J., Hinchev, M.: Runtime variability for dynamic reconfiguration in wireless sensor network product line. In: SPLC, vol. II, 02–07 September. ACM, Salvador (2012). 978-1-4503-1095-6/12/09
15. Békan, A., Mohorcic, M., Cinkelj, J., Fortuna, C.: An architecture for fully reconfigurable plug-and-play wireless sensor network testbed. In: EEE GLOBECOM, Global Communications Conference (GLOBECOM). IEEE GLOBECOM (2015). <http://globecon2015.ieee-globecon.org/>



Implementation of Internet of Things and Protocol

Rishabh^(✉) and Hemant Gianey

Department of Computer Science and Engineering,
Thapar Institute of Engineering and Technology, Patiala, Punjab, India
{rrishabh_bemba16,hemant.k}@thapar.edu

Abstract. From past decades, Communication plays an indispensable role in exchanging the ideas and develop a better understanding among the individuals. The revolutionary concept of the internet of things has connected many real world objects and their environment to the internet and other wireless networks. In the near future, IoT aims to unify everything by transforming the physical world around us into intelligent virtual environment, which enables the machine to machine (M2M) communication. The main purpose of this research paper is to provide an overview of the different types of architectures available for IoT and the protocols that governs its functioning.

Keywords: IoT · Protocols · Bluetooth · Zigbee · Architecture · M2M

1 Introduction

With the advancement in technology the internet has become an integral part of the present life style. IoT has great importance in reducing the efforts of humans and making their life easy [1]. Using hardware is much easier than dealing directly with the application. IoT can control any device without human involvement remotely. In IoT many physical devices are connected together over a network to perform a specific task in coordination with each other. There are many architectures of IoT which are discussed in detail. Apart from having different types of architectures it also consists of various components like sensors, actuators, processors. Sensors are the input devices which take data from the surrounding in the form of analog signals and process them in order to convert them into digital form which is easily processed by the processor. Actuators are devices which converts electrical energy into physical energy in the form of movement. Due to wireless connection between the devices they can be placed in different locations depending upon the wireless connection used. Wireless sensors play an important role in sending the data from one place to another. Wireless sensor networks are the combination of large small sized sensor combined witlessly. They are connected with each other in order to increase the processing power of a lot system. There is a base station to control all the devices. They are used in the field of habit monitoring, security and military, collect real-time data and many more. There are various benefits for connecting the base station to the cloud. As there are numerous options available for processing the data. The data can be sent to various areas across the globe for various purposes.

2 Related Work

Each and every organization has the continuous availability of data desk, which gives data, notice messages and many notifications to their clients and staff. Due to IoT frameworks, the data maintenance and processing has become easier. Numerous individuals hold the view that cities and the world itself will be overlaid with sensing and activation. Comparative work has already been done by numerous individuals across the globe.

IoT emerges as the intelligently connected gadgets and frameworks to assemble information from embedded sensors and actuators and other physical objects. IoT is anticipated to spread quickly in the near future. A new dimension of functionalities has the ability to improve the quality of life of consumers and efficiency of ventures, by opening up an innovative research opportunity in the traditional communication researches. Farooq et al. [1] portrays the concept of sensor networks which has been made practically by the joining of microelectro-mechanical frameworks innovation and wireless communications. Firstly, the sensor systems with their corresponding applications and detection assignment are investigated, and concurring that the review components impacting the plan of sensor arrangement is provided. At that point calculations and conventions created for each layer and the communication engineering for sensor networks is sketched out. Ketshabetswe et al. [2] has created an Electronic Information Work area Framework. Here they are utilizing SMS based approach but in distinctive way. The framework is planned to work independently without the requirement of any human administrator and when an understudy or worker needs any data, they will need to send an SMS to this framework which can react with the data required by client. Menon et al. [3] discussed the reason of investigate is to learn about the feasibility of IoT in bus transportation framework in Singapore. Singapore, which is actually exceptionally progressed but still, has scope of progression in their transportation system made a framework by utilizing IoT for the customer to understand and assess diverse transport choices in an efficient manner. Secondary investigation was utilized to foresee arrival timings of buses as well as the rush inside each bus. Sharma et al. [4] discussed various protocols which are required for communication along with their application on different layers. They also compared the efficiency of different protocols on different layers. Ammar et al. [5] discussed various security aspects which can be used in the current scenario. They also included aws security in his work. Bui et al. [6] discussed protocols like 6LoWPAN which connects to ipv6 protocol and provide infrastructure to IoT platforms.

2.1 Need of IoT and its Applications

IoT Technology Stack is consist of device hardware, device software, communication, cloud platform and cloud applications [7, 12]. Device hardware is the most basic part of the IoT project. We have to choose the IoT device according to the needs of the type of work we are doing. If we are doing any complex task we have to use more complex hardware as if we are using raspberry pi we have sufficient memory but if we replace raspberry pi with the arduino, the arduino may not work properly. More importantly we have to take a look at our needs before deciding the hardware we need. Device software

is also very important part of the IoT technology stack. Software provides a mind to the hardware. There are various types of operating system like Linux, windows, Solaris, Brillo etc. which can be used as a base for running different software on it. Communication is a method of exchanging the information. This is most important to decide it carefully. Communication decides the topology of the system. Cloud Platform is the backbone of the IoT platform. This is further divided into various parts. First one is Analytics that refer to search the data from the large chunk of data and finding the patterns from the data another one is Cloud API's API stand for application program interface. These are the interfaces between the service which we want to use and the device. They control the usage. This also provides facility to process the data in realtime. Cloud applications provide services like storage to the device. Applications can be developed using cloud based or web based. These depend upon the requirements of the user client. These are of internal facing or customer centric. IoT has many applications like it can be used in various applications like smart homes, smart farming, wearables, smart watches and much more (Fig. 1).

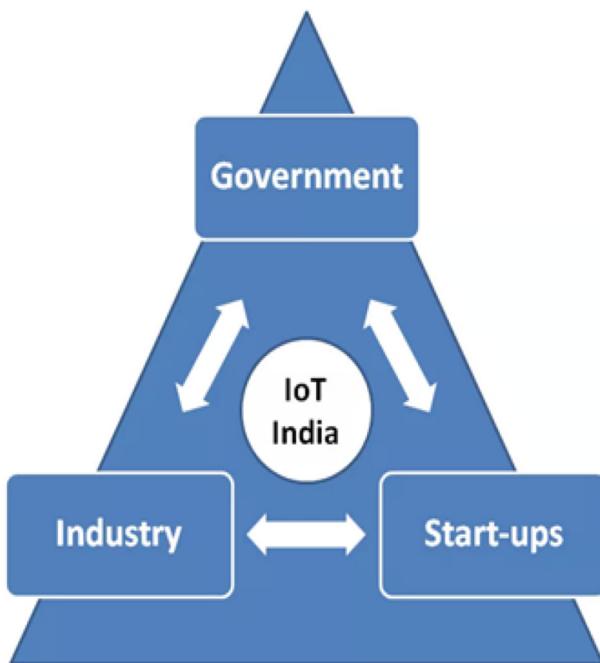


Fig. 1. IoT network protocol stack

3 Architecture and Protocols

[5] In this section we are defining architecture and protocol for internet of things.

3.1 Architecture

There are different types of architecture in IOT the most common architecture are 5 layer, fog based, cloud based and representative architecture.

3.1.1 Five Layer Architecture

It consists of perception layer, transport layer, processing layer, application layer and last one business layer. Application layer which provide various services as per user requirement that include smart cities and smart health. Perception Layer is the basic layer which constitutes sensors to sense the input data which collect and analyze the information of the environment. Transport Layer is responsible for Taking input from perception layer and proceed with this information to processing layer over a network. Processing Layer is the middle layer of this architecture which manages and analyze the data as well as provide services to lower layer. Business Layer is the most important layer of this architecture which manage all the above layers.

3.1.2 Cloud Based Architecture

The cloud based framework provide flexible services consist of storage and consistency of information [8]. On extending grid and cluster based computing we get cloud architecture that is helpful in collecting resources at a single point. Different types of services provided by cloud architecture include Infrastructure as a service, the second one is platform as a service and the last one is software as a service. Cloud based framework act as basic version for sending novel applications to fog based nodes (Fig. 2).

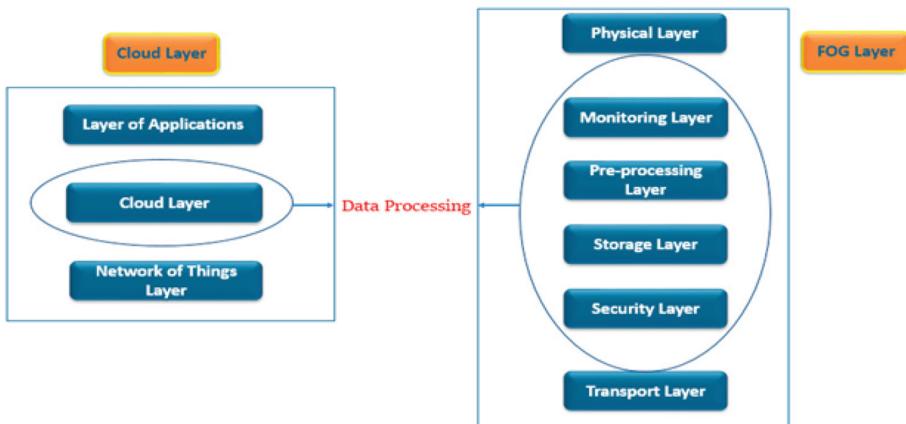


Fig. 2. Fog and cloud based architecture

3.1.3 Fog Based Architecture

Fog based architecture also known by other name i.e. edge based architecture is extended version of cloud based architecture which provide monitoring services, pre-processing, storage as well as privacy between physical and transport layer [9]. Handling of user request is better in fog computing as compared to cloud based architecture. Due to flexible infrastructure of fog based architecture it has tremendous applications as well as low response time. Basically fog based architecture consists of four layers which include monitoring layer which check availability of resources, processing layer analyses the data using different filtering operations, Storage Layer helps in storage of different format as per requirements or depends on need of suitable protocols and last one is Privacy Layer which provide privacy status to data as well as helpful in encryption and decryption of data.

3.1.4 Representative Architecture

This architecture is a part of social IoT [5]. It consists of server and object side, where the server side consists of three layers i.e. base layer consist of database for storing data, second layer is component layer which helps in interaction between devices and the top most layer is the application layer which provide various services to user. Another side is object side which consist of two layers where the initial layer is object layer which allows communication between devices with the help of protocol and the next layer is social layer which manage the implementation of user applications.

3.2 Protocols

Protocols are a set of rules [10]. The different types of protocols IoT include

Bluetooth: Bluetooth is a wireless technology that covers small distance to link different devices like mobile, laptops and other network devices. We use it transfer files or to transfer small amount of data. We use this technology over short range i.e. 50–150 m and device must have Bluetooth 4.2 core specification with basic data rate of 1 Mbps. It uses Ultra High Frequency radio waves from 2.4–2.485 GHz. We find Bluetooth technology in Smartphone, smart watches, laptops, wireless speakers and in wireless headsets. Bluetooth consist of low layer stack and upper layer stack. Low stack layer consist of radio layer, baseband controller and link manager protocol (LMP) while upper stack layer consist of Logical Link Control and Adaptation Protocol (L2CAP) and Service Discovery Protocol (SDP). Radio is base layer of Bluetooth stack protocol. This layer describes characteristics of transceiver and is responsible for modulation/demodulation for transfer data. Baseband controller defines the packet format, timing for transmission and receiving, control on channel. LMP establish and maintains the link between upper and lower stack layers. L2CAP is above the HCI(host controller Interface) and check the communication between upper and lower layer. SDP gives device information, service provided etc. information to other Bluetooth devices.

Zigbee: Zigbee is a wireless technology used for small scale projects[11]. We use this technology over small range i.e. 10–100 m. This technology is operate at 2.4 GHz and exchanges data at low data rates i.e. 250 kbps over short area. This technology has various applications in agriculture, automotive sensing, smart homes, remote control

etc. In this we see different layers. The physical layer (PHY) that is base layer use for modulation and modulation of incoming/outgoing signals. Medium Access Layer (MAC) is above the PHY layer. These layer use carriers sense multiple access collision avoidance (CSMA) to access the network to transfer data. Network layer (NEW) is above the MAC layer, it starts a network, route discovery, check the connection and disconnection. Application Support (APS) Sub layer use for data managing services. Application Framework provide key value pair and generic message services.

4 Conclusion

By integrating IoT as the underlying communication architecture, the communication between various devices becomes easier and secured in nature. In this Paper we describe various architectures and protocols for IoT. In this survey, we have observed that the cloud and fog based architecture is better than the other types of architecture due to its high performance, flexible infrastructure as well as the service provided by fog based architecture also remains useful in many applications. Instead of using single protocol it is analyzed that multiple protocols in single application will gain a significantly more research importance.

References

1. Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., Kamal, T.: A review on Internet of Things (IoT). *Int. J. Comput. Appl.* **113**(1), 1–7 (2015)
2. Ketshabetswe, L.K., Zungeru, A.M., Mangwala, M., Chuma, J.M., Sigweni, B.: Communication protocols for wireless sensor networks: a survey and comparison. *Heliyon* **5**(5), e01591 (2019)
3. Menon, A., Sinha, R., Ediga, D., Iyer, S.: Implementation of Internet of Things in bus transport system of Singapore address for correspondence. *Asian J. Eng. Res.* **1**(IV), 8–17 (2013)
4. Sharma, C., Mata, S., Devi, V.: Constrained IoT systems. In: 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages, pp. 1–6 (2018)
5. Ammar, M., Russello, G., Crispo, B.: Internet of Things: a survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **38**, 8–27 (2018)
6. Castellani, A.P., Bui, N., Casari, P., Rossi, M., Shelby, Z., Zorzi, M.: Architecture and protocols for the Internet of Things: a case study. In: IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshop, pp. 678–683, March 2010 (2010)
7. Kalmeshwar, M., Prasad, N.: Internet Of Things: architecture, issues and applications. *Int. J. Eng. Res. Appl.* **07**(06), 85–88 (2017)
8. Sharma, V., Tiwari, R.: A review paper on ‘IOT’ & It’s smart applications. *Int. J. Sci. Eng. Technol. Res.* **5**(2), 472–476 (2016)
9. Adhikari, M., Gianey, H.: Energy efficient offloading strategy in fog-cloud environment for IoT applications. *Internet Things* **6**, 100053 (2019)

10. Johnson, D., Ketel, M.: IoT: application protocols and security. *Int. J. Comput. Netw. Inf. Secur.* **11**(4), 1–8 (2019)
11. Madakam, S., Ramaswamy, R., Tripathi, S.: Internet of Things (IoT): a literature review. *J. Comput. Commun.* **3**(May), 164–173 (2015)
12. Lakhwani, K., Gianey, H., Agarwal, N., Gupta, S.: Development of IoT for smart agriculture a review. In: *Emerging Trends in Expert Applications and Security*, pp. 425–432. Springer, Singapore (2019)



Hacker Forum Exploit and Classification for Proactive Cyber Threat Intelligence

Apurv Singh Gautam^(✉), Yamini Gahlot, and Pooja Kamat

Department of Computer Science and Information Technology,
Symbiosis Institute of Technology, Pune, India
{apurv.gautam, yamini.gahlot,
pooja.kamat}@sitpune.edu.in

Abstract. The exponential growth in data and technology have brought in prospects for progressively destructive cyber-attacks. Traditional security controls are struggling to match with the intricacy of cybercriminal tools and methods, organizations are now looking for better approaches to strengthen their cyber security capabilities. Cyber Threat Intelligence (CTI) in real-time is one such proactive approach which ensures that deployed appliances, security solutions and strategies are continually evaluated or optimized. Amongst various platforms for threat intelligence, hacker forums deliver affluent metadata, and thousands of Tools, Techniques, and Procedures (TTP). This research paper employs machine learning and deep learning approach using neural networks to automatically classify hacker forum data into predefined categories and develop interactive visualizations that enables CTI practitioners to probe collected data for proactive and opportune CTI. The results from this research shows that among all the models, deep learning model RNN GRU gives the best classification results with 99.025% accuracy and 96.56% precision.

Keywords: Cyber Threat Intelligence · Neural networks · Hacker forums · Machine learning · Deep learning · Text classification

1 Introduction

With 2.5 quintillion bytes of data created each day, the need to shield information from malicious actors is a concern at the highest levels of businesses and governments worldwide. In 2018, cybercrime costs accelerated with organizations spending nearly 11.7 million dollars on security measures.

Cyber Threat Intelligence (CTI) in real-time is a proactive approach which ensures that deployed appliances, security solutions and strategies are continually evaluated or optimized. Threat intelligence and related analytics are now emerging as key capabilities for any modern cybersecurity platform, which needs to be able to collect and analyze CTI for better security automation [1].

Threat Intelligence feeds can assist the organizations by identifying threat indicators and recommend steps to prevent the attack or infection. Threat indicators or Indicators of Compromise (IOC) comprise of IP addresses, URLs, Domain names, email addresses, registry keys, hashes, DLLs, and many more.

Hacker forums are a great way to capture these threat indicators as majority of hackers communicate over these forums and share information about security threats. Analysis of data from hacker forums can help organizations to get more understanding on potential attackers, motive behind the attack, and tools and techniques utilized by them. This allows security practitioners to expand their knowledge base, discover attack trends and take necessary actions and measures to deal with such threats.

This paper focuses on hacker forums that is publicly available on the Internet. These forums have a great potential for valuable threat intelligence that is analyzed using different machine learning and deep learning algorithms in this research. Therefore, we accredit that this research will show the importance of knowledge which can be extracted from these sources that can be used to protect any organizations' assets.

2 Problem Description

Security practitioners implement security countermeasures every time to protect their organizations' assets which is an ongoing process. In today's era, access to exploits is relatively easy for anyone with/without the proper knowledge of that exploit. This is possible because of the so-called hacking-as-a-service that enabled for anyone to easily launch a cyber-attack.

Most of the hackers communicate over hacking forums to exchange services but unfortunately, little is being done to make use of their content for enhancing the existing security controls. One of the main challenges with this is there are large amounts of data on hacker forums that is not related to cyber threats and therefore manual analysis must be done to collect related data. Manual analysis of such large collection of data can be cumbersome and is time consuming, and an inefficient way.

3 Motivation and Benefits

This research takes its motivation from big giants like Fire Eye, IBM, Palo Alto, LookingGlass, etc. that are into Threat Intelligence business and are regularly looking for efficient methods to enhance their cyber security controls. An effective approach for this is the analysis of data from hacker forums to get more understanding on potential attackers, their motivation behind the attack, and their tools and techniques for the attack. This allows security practitioners to extend their knowledge base of potential threats and take required actions and measures to deal with such threats.

4 Related Work

We present the literature review on threat intelligence and utilization of machine learning and deep learning on hacker forums. The literature review is attained from research sites using searches like "threat intelligence", "hacker forums", "ML in threat intelligence", "threat intelligence using hacker forum", etc. [16].

Our literature review can be grouped into 3 streams: (i) identification of threat actors, (ii) threat intelligence from dark web, (iii) threat intelligence from logs/events/other sources.

4.1 Identification of Threat Actors

Majority of researches we observed pondered over identification of threat actors. The research papers by Grisham et al. [4] and Samtani et al. [3, 9] both uses social network analysis for identifying key threat actors and the relation between threat actors and the threat posts.

4.2 Threat Intelligence from Deep/Dark Web

The research paper by Nunes et al. [5] uses darknet/deepnet for the purpose of identifying emerging cyber threats using ML models. They presented an operational system for this purpose. Similarly, research paper by Sagar Samtani et al. used real time collection and analysis of data from hacker forums using ML and DL models. Both these research paper uses English forums for their research. The research paper by Ranade et al. [7] uses multilingual forums for data collection specifically Russian and English forums.

4.3 Threat Intelligence from Logs/Events/Other Sources

We found many research papers talking about threat intelligence using security events and logs from the computer systems. The research paper by Mavroeidis et al. [13] uses sysmon logs for threat intelligence and in a similar way, research patent by Cohen, Haifa et al. [14] utilizes correlation of events for the same.

Moreover, we also found several research using data from different web sources for threat intelligence. The research paper by Goyal et al. [11] uses data from twitter, blogs, vulnerability databases and honeypots and the research paper by Anna Sapienza et al. uses only twitter and blogs for data collection. We also found one research paper by Li et al. [10] utilizing OSINT for threat intelligence.

5 Research Methodology

5.1 Dataset Construction

The first step of breaking down sources for threat intelligence is the identification and aggregation of the data. Data on Hacker forums is available in the form of multilingual human conversations amongst hackers [1]. However, the collection of data from hacker forums is challenging due to all the counter step enforced by the administrators of such platforms including captchas, blacklists, registration, invitation only access, etc. Specialized web crawlers were customized to collect data from such source.

The dataset must be labelled if we want to build a model that doesn't have posts irrelevant to security. We have constructed a dataset in a publicly available forum by manual labelling some of the posts. Common security keywords were used to

categorize the text through skimming in the class *relevant or irrelevant*. Common Cyber Security keywords include antivirus, backdoor, botnet, firewall, hijack, infect, keylogger, malware, ddos, 0day, etc.

5.2 Preprocessing

There are two steps in preprocessing i.e., data preparation and data cleaning. In data preparation, relevant fields are extracted from unprocessed data and are stored in non-relational databases. These fields include thread date, author name, post data, thread title, etc. In data cleaning, those parts are removed that act as noise that include whitespaces, uppercase characters are converted into lowercase, etc. As for this research we took data from [AZSecure-data.org](#) [15] and it was already preprocessed (Fig. 1).

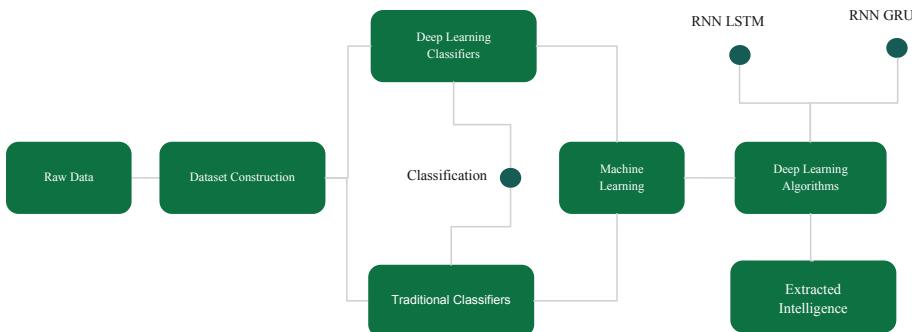


Fig. 1. Research methodology

5.3 Deep Learning

A Recurrent Neural Network (RNN) is used for classifying hacker forum posts. An RNN was chosen for classification because it surpasses performance in classifying text data. We have used two RNN variants on the dataset. These include a Gated Recurrent Unit (GRU) RNN, and a Long Short-Term Memory (LSTM) RNN. The data used to train and test these RNNs was provided by AZSecure-data.org with conversation posts from hacker forums.

1. RNN LSTM

RNNs have a memory state that gives advantage over traditional neural networks. They have multiple layers that interact in a very special way. They have an input gate, a forget gate and an output gate.

2. RNN GRU

GRUs are easier to train as they are simpler than LSTM in their structure. They have a gating network signal that controls the present input and previous memory to produce the result of current state.

6 Experiments and Results

6.1 Forum Collection Statistics

Table 1 as shown below, depicts the name of the forum we used for the research and number of threads along with relevant threads.

Table 1. Forum statistics

Forum	Language	No. of threads	No of relevant threads
CrackingArena	English	44,927	7,114

6.2 Deep Learning Model Statistics

Table 2 as shown below depicts the accuracy and precision of both the models used for this research i.e., RNN LSTM and RNN GRU.

Table 2. RNN model statistics

Model	Accuracy	Precision
RNN LSTM	0.9894497863247863	0.9490284426921993
RNN GRU	0.9902510683760684	0.9656434807096592

Figure 2 shows the accuracy graph between LSTM and GRU. We can see that RNN LSTM has 98.94% accuracy whereas RNN GRU has 99.025% accuracy.

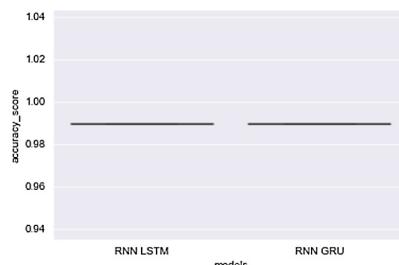


Fig. 2. Accuracy graph (LSTM & GRU)

Figure 3 shows the precision graph between LSTM and GRU. We can see that RNN LSTM has 94.9% precision whereas RNN GRU has 96.56% precision.

We can see from both the visualizations that RNN GRU gives slightly better scores than RNN LSTM.

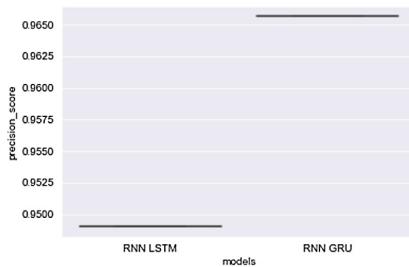


Fig. 3. Precision graph (LSTM & GRU)

7 Conclusion

This research demonstrates the use of cyber threat intelligence in classifying cyber-attacks from hacker forums. The focus of this is to show how intelligence can be elicited from hacker forums that continuously engages with security keywords and texts. Even though most of the security practitioners have knowledge about these hacker forums, little is being done to make use of their content for enhancing the existing security controls.

Our research shows how the contents of these hacker forums can be used for the discovery of threat indicators like zero-day exploits, malicious email addresses, malicious IP addresses, leaked credentials, etc. using machine learning and deep learning concepts that can be used by security practitioners to stop an incoming attack or improve their system. The value of the acquired CTI shows that this research can be harnessed in commercial environment that is not being utilized yet.

In future, this research can be expanded to collect data from different hacker forums. We just covered English forum data in our research, but it can be expanded to other languages also including Russian, German, etc. Preprocessing of these hacker forum data gives us with names of users posting the content and we can perform Social Network analysis to get more insights on type of users and their posts and activity. Lastly, a Time Series Analysis can be used for obtaining timely intelligence.

References

1. Deliu, I.: Extracting cyber threat intelligence from hacker forums, Master's thesis. NTNU (2017)
2. Williams, R., Samtani, S., Patton, M., Chen, H.: Incremental hacker forum exploit collection and classification for proactive cyber threat intelligence: an exploratory study, pp. 94–99 (2018). <https://doi.org/10.1109/isi.2018.8587336>
3. Samtani, S., Chinn, R., Chen, H., Nunemaker, J.: Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *J. Manag. Inf. Syst.* **34**, 1023–1053 (2017). <https://doi.org/10.1080/07421222.2017.1394049>
4. Grisham, J., Samtani, S., Patton, M., Chen, H.: Identifying mobile malware and key threat actors in online hacker forums for proactive cyber threat intelligence, pp. 13–18 (2017). <https://doi.org/10.1109/isi.2017.8004867>

5. Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., Robertson, J., Shakarian, J., Thart, A., Shakarian, P.: DarkNet and DeepNet mining for proactive cybersecurity threat intelligence, pp. 7–12 (2016). <https://doi.org/10.1109/isi.2016.7745435>
6. Kim, B.I., Kim, N., Lee, S., Cho, H., Park, J.: A study on a cyber threat intelligence analysis (CTI) platform for the proactive detection of cyber attacks based on automated analysis. In: 2018 International Conference on Platform Technology and Service (PlatCon), Jeju, pp. 1–6 (2018)
7. Ranade, P., Mittal, S., Joshi, A., Joshi, K.P.: Understanding multi-lingual threat intelligence for AI based cyber-defense systems. In: IEEE International Symposium on Technologies for Homeland Security, October 2018
8. Kim, D., Kim, H.K.: Automated dataset generation system for collaborative research of cyber threat intelligence analysis. CoRR, abs/1811.10050 (2018)
9. Samtani, S., Chinn, K., Larson, C., Chen, H.: AZSecure hacker assets portal: cyber threat intelligence and malware analysis. In: 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, pp. 19–24 (2016)
10. Li, K., Wen, H., Li, H., Zhu, H., Sun, L.: Security OSIF: toward automatic discovery and analysis of event based cyber threat intelligence. In: 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Guangzhou, pp. 741–747 (2018)
11. Goyal, P., Hossain, K.S., Deb, A., Tavabi, N., Bartley, N., Abeliuk, A., Ferrara, E., Lerman, K.: Discovering signals from web sources to predict cyber attacks. CoRR, abs/1806.03342 (2018)
12. Sapienza, A., Ernala, S.K., Bessi, A., Lerman, K., Ferrara, E.: DISCOVER: mining online chatter for emerging cyber threats. In: Companion Proceedings of the Web Conference 2018 (WWW 2018). International World Wide Web Conferences Steering Committee, pp. 983–990. Republic and Canton of Geneva, Switzerland (2018)
13. Mavroeidis, V., Jøsang, A.: Data-driven threat hunting using sysmon. In: Proceedings of the 2nd International Conference on Cryptography, Security and Privacy, pp. 82–88. ACM, March 2018
14. Cohen, R., Chesla, A., Medalion, S., Katz, R.: U.S. Patent Application No. 15/433,647 (2018)
15. Other Forums: AZSecure-data.org. <https://www.azsecure-data.org/other-forums.html>. Accessed 20 Apr 2019
16. Related Words - Find Words Related to Another Word. <https://relatedwords.org/relatedto/cyber%20security>. Accessed 20 Apr 2019
17. Pennington, J.: August 2014. <https://nlp.stanford.edu/projects/glove/>. Accessed 20 Apr 2019



A Systematic Approach on Design of Automation System for Tea Farming Based on Embedded Wireless Sensor Network

Hemarjit Ningombam¹(✉) and O. P. Roy²

¹ Electronics and Communication Engineering, Dibrugarh University,
Dibrugarh, India

nhsingh@dibr. ac. in

² Electrical Engineering, North Eastern Regional Institute of Science
and Technology, Nirjuli, India

Abstract. To conserve the tea farming sector and to maintain the quality of the tea product an efficient system is in need to control and maintain the agricultural processes as well. In this paper, a systematic approach of an automation system for tea farming using ZIGBEE wireless networks has been implemented to monitor and control tea plantation in north east India. Embedded multi-sensing and actuator nodes are distributed around the farms and used to measure the parameters necessary in controlling agricultural process. Farm level information's, combined with their positions information, are relayed to the centralized decision support system by the ZIGBEE wireless sensor networks. Accordingly, necessary control signal will generate and transmit, only at the targeted positions or area to control feedback action at time. The propose technology can broadly be applied into various area of tea plantation, viz. Irrigation management, pest management, fertilizer control, frost control, sunshine hour/intensity management etc. The user friendly Graphical User Interface (GUI) has designed remembering that the framework will be utilized generally by the farmers. The approach, won't just improve the efficiency, however will also reduce farm input cost and minimize environmental impacts.

Keywords: GUI · Tea farming · Wireless sensor networks · ZIGBEE

1 Introduction

The quality of tea is the result of both agricultural and industrial process. The industrial process consists withering, cutting, drying etc. and the agricultural process: irrigation, manuring, plucking, pest control, light intensity control etc. [4, 7]. To accomplish significant returns and quality tea, exact parameters of soils and plants conditions necessary to realize the different contributions to soil which are being needed to increase the fertility and manures in soil with the goal that compelling management strategies can be put into area. Environmental information monitoring and analysis have great achievements in the recent years. Some system using satellite imaging technologies lead to high cost and less effective. Normal laboratory analysis and manual decision making of the large input parameters take long time even using

sophisticated instruments [2]. Quick and quality decisions with timely and effective control/response perform at the farm level can enhance the agricultural productivity and quality of the products.

1.1 Need of Wireless Sensor Network (WSN) in Tea Plantation

As indicated by researchers, utilization of remote of remote sensing could demonstrate to be a significant instrument in checking the health of tea bush and also delineation of affected areas by pests and diseases. At present, floods and water logging have caused serious damages to tea farms of low-lying regions and subsequently, yield and quality have impressively declined. The unearthly reflectance of a tea field consistently fluctuates with respect to phonology, stage type and crop health and these could be carefully monitored and measured using the multiple sensors from remote locations. Information from remotely sensed data can be fed into decision support system which when combined with auxiliary information can provide best cultural practice being implied in the cropping system. Stresses related with moistures deficiency, temperature, and light force and so on must be identified early enough to give a chance to the grower for undertaking moderation measures [6]. It would enable the grower to distinguish regions inside a field which are encountering troubles, so that they can apply necessary remedies.

Physically laying the signal cable in plantation field is very difficult especially in hilly areas. Also various insects and animals may damage the cable. So, wireless topology can be the best solution here. As stated above, a WSN topology may be deployed in the field and it transmits data through wireless route to the main server. WSN integrates sensing, wireless and processing technologies capable to monitor various physical parameters maintaining accuracy of sensors. These parameters are processed and transmitted to a centralized data storage system from where they may be accessed and analyzed. The flexibility or reusability features of WSN make it suitable in tea farming [5]. The WSN can withstand harsh environmental conditions too.

2 General Architecture of WSN

As depict in Fig. 1 a wireless sensor network based system provides interface for different sensors with data processing facilities. The system is also equipped with wireless communication units that allow sensed data be processed and transmitted according to desired algorithm. The principle goal of the WSN is to develop a system to which passes data to a central support system by collecting data from sensors of various node of a network through wireless communication. In general architecture the architecture of WSN is the aggregates of various nodes. Each nodes are accompanied with wireless module, requires sensors and actuator s. With proper routing algorithm all the sensor nodes information can be communicated within nodes as well as with decision support system.

The system is to be designed with expandability and flexibility in mind i.e. the system should allow for further sensors and nodes to be added. Some primary and secondary objective of WSN should be:

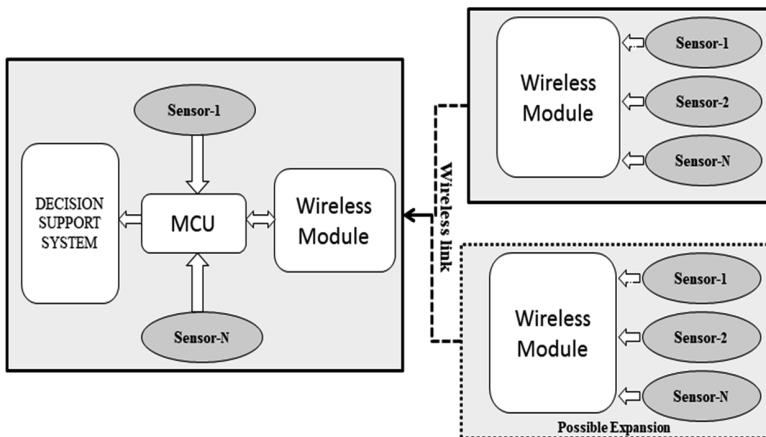


Fig. 1. General architecture of WSN system

Primary:

- Create a wireless data transmission system
- Collect sensor data
- Communicate data to the centralized decision support system.

Secondary:

- Implement a frequency scan
- Implement frequency hopping
- Provide an estimation of distance between nodes
- Implement a battery level monitor.

To improve the robustness, to make system efficient and increase the life, selection of wireless system should be based on some criteria like: *Communication range*: higher the wireless range, better the system.

Power consumption: Battery power is essential as direct AC power will decrease the mobility of node. Power consumption should be very low. The selection of sensors is as important as the selection of wireless system considering the features like a *large span of measuring range, accuracy of the measurement, power consumption, and size* as well.

3 The Tea Farm Management

The propose technology can broadly be applied into various area of tea plantation, viz. Irrigation management, Pest management, Fertilizer control, Frost control and Sunshine hour/intensity management.

The sensors that can be connected to the node are Soil pH, leaf wetness, solar radiation, soil Moisture, wind speed and direction; soil Temperature, Relative Humidity and temperature [2]. These sensor readings can be integrated with a decision and

control system that will aid the management and control of resources to the farm as desired.

The work has to be carried out with following contributions:

- i. To design and develop an embedded multi sensing and actuator module. (Sensor node)
- ii. To acquire, store, and analyze responses of sensors parameters to different field conditions
- iii. Development of embedded actuator module to applied the efficient control to
 - Irrigation management process
 - Pest management process
 - Fertilizer control process
 - Frost control process.
- iv. Development of a decision support software which facilitates, signal preprocessing, feature extraction, debugging and realizing the automation control system
- v. Development of efficient routing algorithm of the sensors network ZIG-BEE networks for tea farming
- vi. Development and realization GUI for monitoring and control.

4 Proposed System Architecture

Simple field level deployment architecture of sensor nodes and decision support system or unit is shown in the Fig. 2. As per the range of coverage of the wireless sensor module (here ZIGBEE RF module) the nodes are distributed along the farm area. For

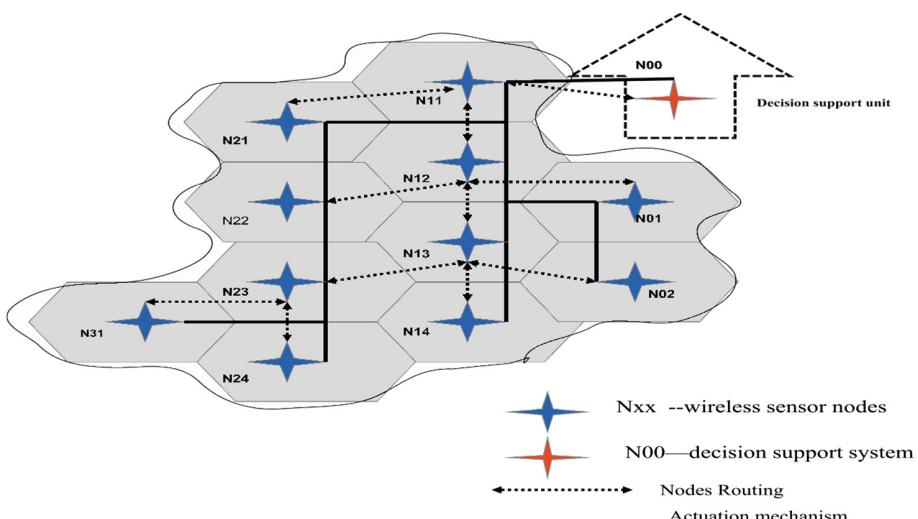


Fig. 2. A sample - field level WSN deployment architecture

systematic and ease to access better to distribute nodes in column-row matrix preferably [3]. The electronics module on every sensor hub is a reconfigurable unit that performs directional communication, computation, and external or internal data storage. Each sensor nodes associated with feedback control mechanism have been provided actuation unit along with the sensing unit to allow control action transmitted from the decision support unit. Since the wireless communication range capacity of any RF wireless module is fixed. As instance, the sensor node N23 act as coordinator node between node N21 and N24 in the implemented wireless sensor network. The coordinator node accumulates information from the at least two nearby sensor hubs in a period – multiplexed way, which aides in staying away from impacts collisions of information transmissions [1, 9]. Along with its own sensor data and data accompanied with address of others neighbouring nodes which were aggregated, are then transmitted to the next higher layer gateways nodes through wireless link. The upper level sensor node then transmits the sensor information received from the coordinators and from sensors to the remote computer terminal i.e. decision support system node through wireless link. The decision support system terminal has the facility of information logging and decision support algorithms along with fast and powerful processing capabilities. A user-friendly Graphical User Interface (GUI) has been attached to the developed system remembering that the system will be used mainly by the farmers.

4.1 ZIGBEE RF Module WSN

In this developed module, the XBEE-RF unit fabricated by DIGI is utilized to give the required remote communication link amongst sensor nodes and decision support unit. The modules are configured to meet IEEE 802.15.4 standards and provide self – organized, multi-hop, and reliable mesh networking with best power back up. This device can participate in two different modes in a Network: a reduced-function device (RFD) and a full-function device (FFD). X-CTU is a Windows-based application given by DIGI's. This program was intended to collaborate with the firmware records found on DIGI's RF units and to give an easy to-utilize graphical user interface to them [11]. X-CTU is designed to function with most of the operating system. It will give distinctive functions like: setting COM port and arrange that port to fit the RF settings, enables users to perform a range test between two radio devices, get to the radios' firmware utilizing AT commands, radio' firmware settings by means of a graphical user interface and furthermore permits users the capacity to change firmware variants. On context of power management, the nodes which function limited to sensing can be configured to End device protocol to safe power consumption by putting in sleep mode.

ZIGBEE supported protocol architecture are shown in Fig. 3. Configuration wise, the coordinator and the router are almost same only that router should have the routing information. Both should be in active state throughout the process.

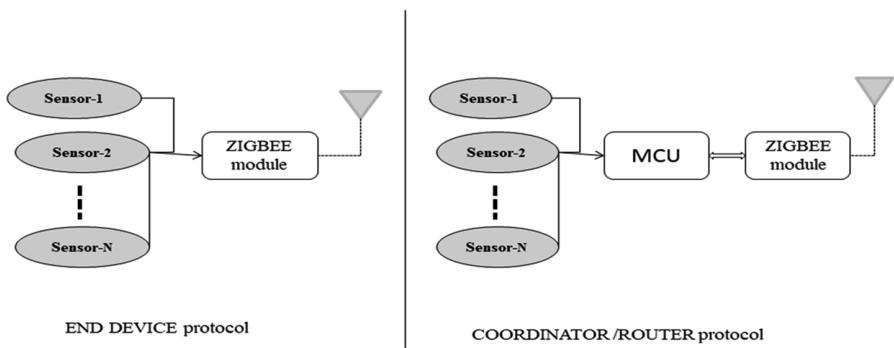


Fig. 3. Basic models of sensor nodes

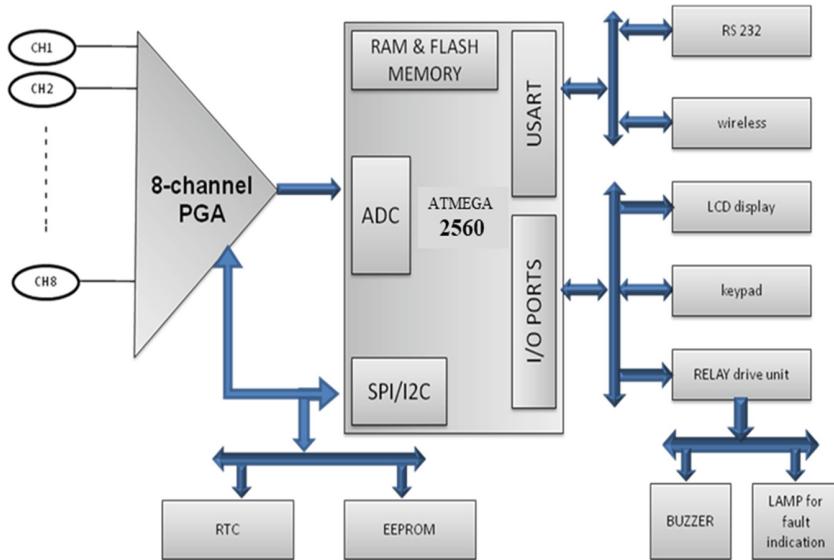


Fig. 4. Wireless sensor node

5 Multi-sensing and Actuator Module

A wireless multi sensing and actuator system (wireless sensor node) has been developed (Fig. 4) for monitoring of different field parameters related to tea farming, consisting of solar radiation sensors, ambient temperature, soil temperature, soil moisture, relative humidity, soil pH, etc.

The embedded system mainly consists with a sensing unit, a user interface unit, a wireless or a wired communication unit and a data storage block. It has provision for driving actuation unit for controlling actions. The sensing module is of sufficiently small in size and it has the feature to interface multi sensors along the single channel of

ADC so that other ports can utilize in controlling others process. This embedded sensing module allows connection of eight different sensors to the signal conditioning unit. External signal conditioning circuit is not required. Every single required excitation and linearization are given on the module. The user must set before use to select the type of sensor/channel and the range of measurement using key pad provided. For eight sensors there is only one module. The control unit consists of a microcontroller, programmable gain amplifier (MCP6S28), ADC and a power supply. To make the system more compact 8 bit Atmega2560 has been used which has most of the peripherals on chip. Programmable gain amplifier (MCP6S28) gives the designer digital control over an amplifier using a serial interface (SPI bus). The stored set point from the internal memory of the microcontroller (flash) can be select using switch for each input parameters. The set value can be changed by using switches according to need. The program compares set values and sensing values than make alarm sound if sensing value exceed set point. Set points values can be adjusted later if needed through switches provided on the module by the user.

Similarly, for all the inputs, using corresponding switch set point value can be set for respective sensors inputs. Alarm circuit is excited through an open collector source transistor array (ULN2003). Sensing data are stored in flash memory of the atmega2560 microcontroller and as well as on the serial EEPROM via I2C bus interface. The wired module RS232 or unpaid wireless module Xbee transceiver, which has data transmitting capacity up to 1.6 km at 2.4 GHz are used to transmit the measure parameter values and their set - point values and as well as to LCD unit simultaneously. The nodes operate under stored program control [10]. The ADC embedded on the controller performs periodic scans of the sensors connected. The acquisition time and conversion time should be enough fast to avoid any data loses during the real time interfacing of the system. The sensor interface electronic is required to transfer the electrical signal from sensor modules to the computational platform.

6 Distance Measurement of ZIGBEE Based Sensor Node

For testing of wireless transmission link at different points two wireless Xbee transceiver module are used. The module transmits data up to 1 mile for outdoors range (LOS) and 100 m in indoor range at frequency 2.4 GHz [10]. It has sensitivity of -100 dBm. Using Eqs. (1) and (2) the power received and transmission losses have been calculated at different coverage [8]. The RF power meter is used for measurement of power.

$$L(\text{dB}) = -20 \log_{10}(\lambda/4\pi d); \quad (1)$$

L = signal loss in free space (dB) and d = distance (meters).

$$Pr = (Pt Gr Gt \lambda^2)/((4\pi)^2 d^2 L); \quad (2)$$

Pr = power received at receiver, Pt = transmitted power 100 mW; Gr & Gt = antenna gain at receiver and transmitter = 2.1 dB.

The line of sight distances between two points has been calculated using the help of Google map. Google Earth maps can be downloaded at frees of cost and has the facility to calculate distance between two selected modules under the Tool option by selecting the ruler [5]. Using simple Pythagoras theorem, indoor ranges has been calculated. From Fig. 5, Free space loss increases as the distance between the transceiver increase and as distance increases, received power decreases. As depicts in Tables 1 and 2 respectively, to improve transmission performance of signals through wireless medium, the low baud rate along with low frequency range and line of sight range is required to minimize the signal loss.

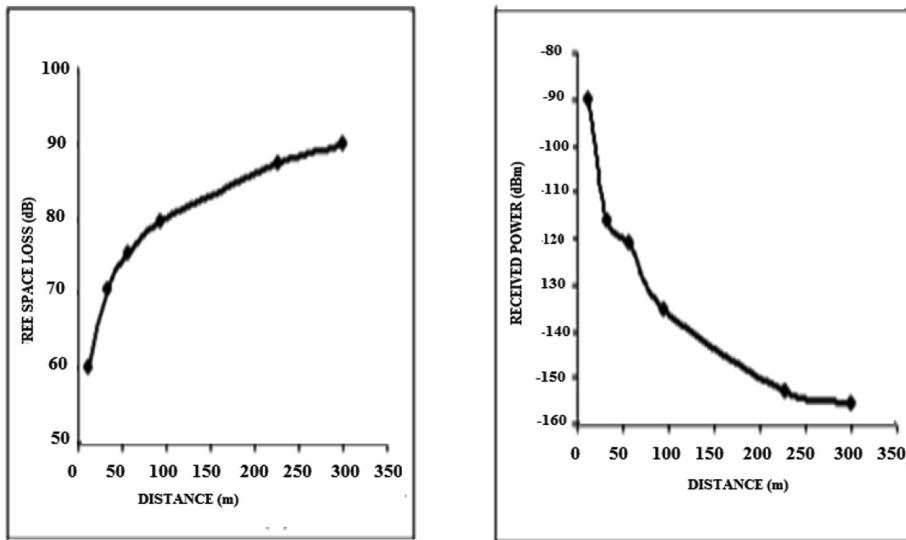


Fig. 5. Received power and free space plots

7 Graphical User Interface (GUI) Realization

Microsoft VISUAL BASIC is used to implement the GUI. This GUI helps the user to manage the measured sensors values into text format and can used for further analysis. The GUI receives the real time farm parameters from the sensors through wireless module and displays it on the computer screen. It also provides graphical icons and visual indicators of the farm status [9]. Also retrieve the real time operating system time and display the corresponding field data along with time, which can be used by the users while saving data in the external memory platform. The GUI communicates with a ZIGBEE module using the computer serial port.

Table 1. Outdoor characteristics

SL	BAUD RATE (bps)	Distance (m) with obstacles	Distance (m) with line of sight	Information loss	
				YES	NO
1	1200	-	<45		✓
		57	-	✓	
		64	-		
		-	227		✓
2	9600	-	<45		✓
		57	-	✓	
		64	-		
		-	227		✓
3	19200	57	<45	✓	
		64	-		
		-	227		✓

Table 2. Indoor characteristics

SL	BAUD RATE (bps)	Distance (m)	Information loss	
			NO	YES
1	1200	<19	✓	
		32		
		57		✓
		62		
2	9600	<19	✓	
		33		
		58		✓
		63		
3	19200	<20	✓	
		33		
		57		✓
		62		

The serial port communication is performed using the MS Com control component of Visual Basic. The MS Com communicates with the XIGBEE module on the com port where ZIGBEE is connected with the settings of 9600 baud, 8 data bits, no parity and 1 stop bit Fig. 6 shows the architecture of the developed GUI. The purpose of the GUI is to collect data from the sensor nodes and save data to a file and displayed in the form of graph and map. The GUI has a feature to report out the saved data in the form of text, HTML files and also can be printed out with a printer. For the sensor's set points can be set at real time using the GUI and also controls the relays in the remote sensing nodes. Keeping in mind that the system will be mainly used by the farmers, it has been made very user friendly.

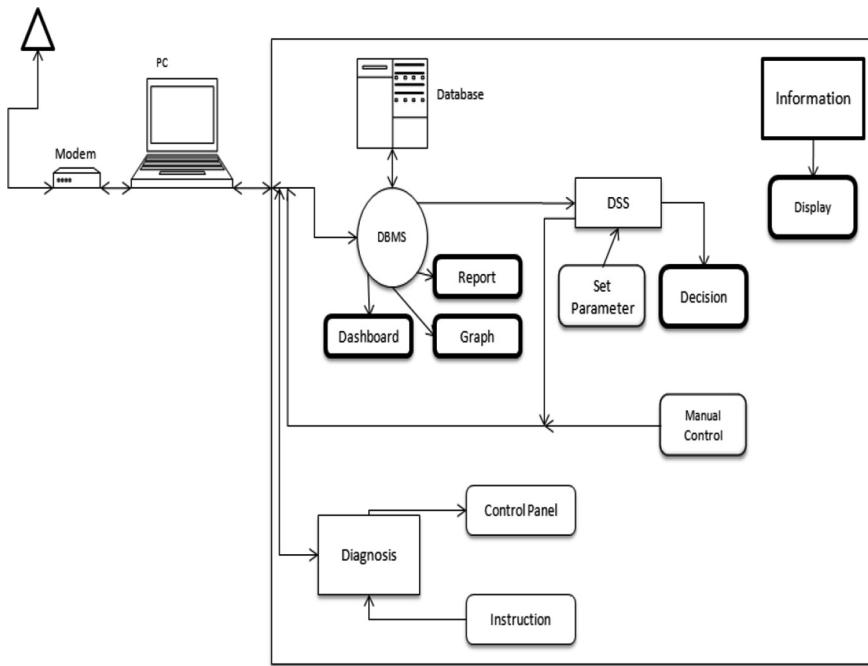


Fig. 6. Graphical user interface (GUI) architecture

8 Conclusion

Application of WSN in tea farms monitoring and control lead to a new dimension for real time data acquisition. The ranges and coverage can be configured as per desired, preferably lower frequencies for better ranges. With well structured and organized routing algorithm will make system performance better and reliable.

Automated decision support system decreases the human dependency and maintains the optimum farms parameters for plant growth. The developed system eliminates the requirement of natural laboratory analysis of farms parameters, making the decision making process faster and reliable.

GUI interfacing will make the system more users friendly and provide handling comfort to farmers. Pictorial representation of the measured information will lead to ease and accurate in decision taken. In future we plan to expand our work by testing on more sensors nodes and their data analysis. Expanding more control solutions are the other main directions of our future works.

References

1. Kodali, R.K., Soratkal, S.R., Boppana, L.: WSN in coffee cultivation. In: International Conference on Computing, Communication and Automation (ICCCA2016), pp. 661–666 (2016)
2. Deepika, G., Rajapirian, P.: Wireless sensor network in precision agriculture: a survey. In: 2016 IEEE Conference (2016)
3. Kannamma, M.B., Chanthini, B., Manivannan, D.: Controlling and monitoring process in industrial automation using Zigbee. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 806–810 (2013)
4. Hong, C., Shuhui, Z.: A temperature auto-monitoring and frost prevention real time control system based on a Z-BEE Networks for the tea Farm. In: 2012 IEEE Symposium on Electrical and Electronics Engineering (EEESYM), pp. 644–647 (2012)
5. Kumar, K.N., Prapakaran, R.: ZigBee wireless sensor network technology study for paddy crop field monitoring. In: International Conference on VLSI, Communication & Instrumentation (2011)
6. A compilation of lectures notes. Tea Field Management. Tea Research Association, Tocklai, Jorhat, India (2011)
7. Sun, D., Jiang, S., Wang, W., Tang, J.: WSN design and implementation in a tea plantation for drought monitoring. In: 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, pp. 156–159 (2010)
8. Propagation Characteristics of Wireless Channels. Lecture 2. http://www.cs.mdx.ac.uk/staffpages/apietukastriku/lecturenotes_2002_2003/lecture2.ppt. 11 November 2008
9. Verma, S., Chug, N., Gadre, D.V.: Wireless sensor network for crop field monitoring. In: 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (2010)
10. Anand, C., Sadistap, S., Bindal, S., Rao, K.S.N.: Multi-sensor embedded system for agro-industrial applications. In: 2009 Third International Conference on Sensor Technologies and Applications (2009)
11. Vijaya Laxmi, H., Narendra, M.: Communication b/w mobile-robots' and PC controller based on ZigBee network. Int. J. Eng. Res. Appl. **1**(4), 1432–1435 (2011)



Effect of Fault Tolerance in the Field of Cloud Computing

A. H. M. Shahariar Parvez¹, Md. Robiul Alam Robel²,
Mohammad Abdur Rouf³, Prajjoy Podder^{4(✉)}, and Subrato Bharati¹

¹ Ranada Prasad Shaha University, Narayanganj, Bangladesh

sha0131@gmail.com, subratobharatil@gmail.com

² Department of CSE, Cumilla University, Cumilla, Bangladesh

alam. robel@gmail.com

³ Department of CSE, Dhaka University of Engineering and Technology,
Dhaka, Bangladesh

marouf.cse@duet.ac.bd

⁴ Department of ECE, Khulna University of Engineering and Technology,
Khulna, Bangladesh

prajjoypodder@gmail.com

Abstract. Cloud Computing has enabled the availability of various software, platforms and infrastructural resources as scalable services on demand over the internet. However, the performance of cloud computing services is hampered due to their inherent vulnerability to failures owing to the scale at which they operate. Fault tolerance is a major concern to guarantee availability and reliability of critical services as well as application execution. In order to minimize failure impact on the system and application execution, failures should be anticipated and proactively handled. This paper presents a comprehensive overview of fault tolerance-related issues in cloud computing; emphasizing upon the significant concepts, architectural details, and the state-of-art techniques and methods. The objective is to provide insights into the existing fault tolerance approaches as well as challenges yet required to be overcome.

Keywords: Cloud computing · Distributed networks · Faults and failures · Low latency fault tolerance · Data center

1 Introduction

According to U.S. National Institute of Standards and Technology (NIST), Cloud computing is basically a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources such as storage, network servers etc. These resources can be quickly provisioned and released with least management effort or service provider interaction [1].

Cloud computing refers to involve the virtual computing with three main services to be executed which are: Infrastructures as a service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [2, 3]. It comprises the area of distributed and utility computing with never forgetting networking. No value can be put on in this

“cloud computing” without internet, overall networking infrastructures. Buyya et al. [4] defined the Cloud computing in terms of distributed computing. Ever since the introduction of the cloud computing another thing had arisen as a challenge in the path of the technique which is the term ‘fault tolerance’ [7]. There are several physical and virtual issues that blocks the success of establishment of this computing methodology. These are referred as ‘faults’ and the measurement of ‘fault tolerance’ defines how successful one particular cloud computing is. Figure 1 shows a basic diagram to understand cloud computing.

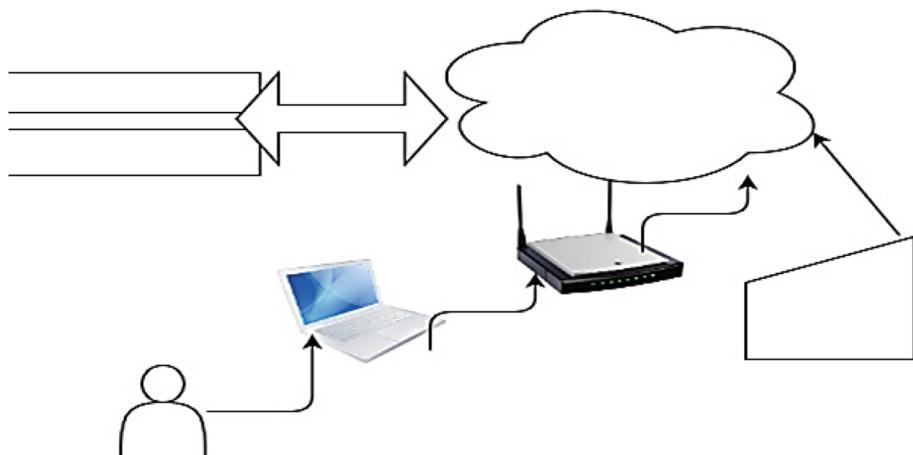


Fig. 1. Cloud computing basics

Fault Tolerance is related to reliability, successful operation, and absence of breakdowns. A fault tolerance based system should be capable to examine faults in particular software or hardware components, failures of power or other varieties of unexpected adversities and still fulfil its specification [5, 6]. At the end of the paper the following things will be known:

1. Clear concept about fault tolerances in the field of cloud computing
2. Properties and infrastructures to avoid fault tolerance in cloud computing (existing methods)
3. Way of overcoming newly introduced problems in fault tolerances.

2 Importance of Cloud Computing

Several points can be introduced for the importance of cloud computing. They are:

1. It has the characteristics of cross platform integration
2. It is cost effective

3. User can recombine and reuse the resources according to their need and requirements
4. Service quality ensures the increase of number of users
5. It has the suitable interface as per user demand which ensures scalability.

The following figure illustrates the basic functionality of cloud computing (Fig. 2).

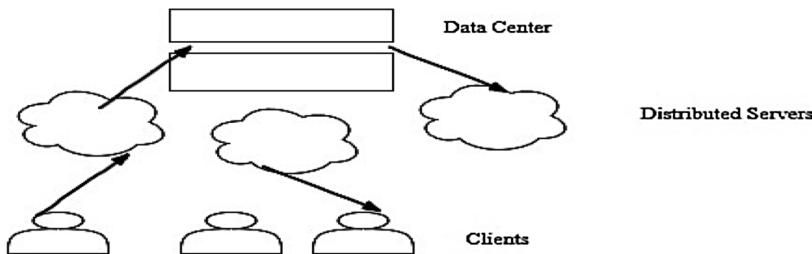


Fig. 2. Basic functionality of cloud computing

3 Flowcharts of Different Level of Cloud Computing

In the flowcharts given below (Fig. 3), the ‘YES/NO’ straight-line indicates the faults or obstacles depending on the situation or decision.

From the flowchart it will be known that how the real scenario works between the data center and distributed networks. Sometimes there is a check in the flowchart which gives the output as either blunders or accuracy which is the main objectives of the flowchart.

Figure 3 illustrates the process the cloud computing system between distributed networks and clients.

As the above flowchart (Fig. 3) picturised above bears a valid meaning which is described below step by step:

- (a) It appears as the relationship to the user between physical data center and virtual network
- (b) In the first order it checks whether a real physical data center is available or not.
- (c) Then as the rules of the flowchart it further goes and check whether there is a valid network connection or not.
- (d) If there is a problem either in the physical data center or the virtual center the process goes repeatedly until the problem is resolved.
- (e) If the problem is resolved then there appears an interface with which the intended users can interact.
- (f) After the creation of the interface by some means there starts the exchange of data which in one word CLOUD COMPUTING phase.
- (g) There is also a token running parallelly whether the whole system is running smoothly or not which is referred as FAULTS FINDING.
- (h) If there is any problem then before resolving the issue appeared, there is no further process.
- (i) Otherwise shows the available status to both the distributed networks and clients.

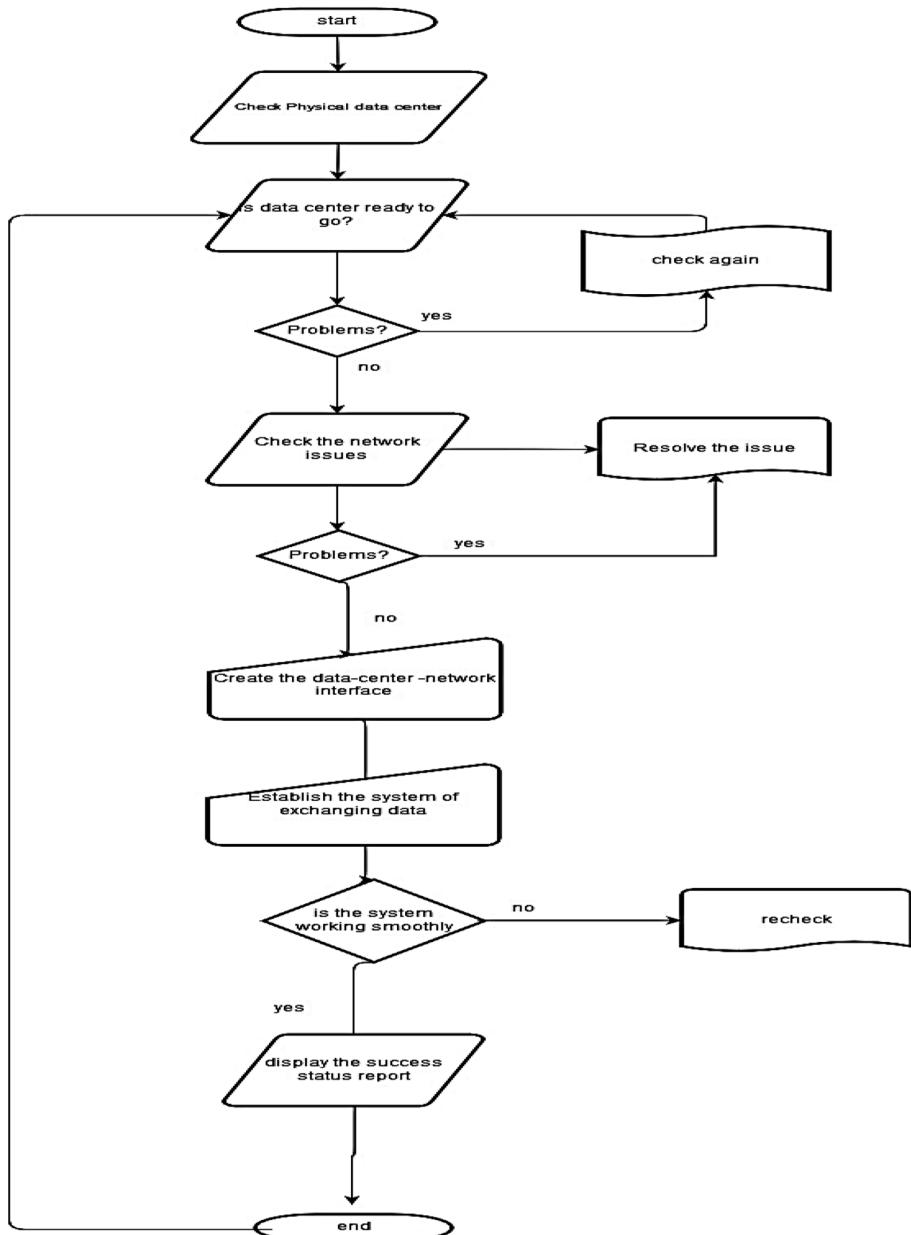


Fig. 3. Flowchart between Data center and network

Figure 4 is a flowchart based relationship between the distributed networks and clients which is described as step by step:

- (a) Here all the action begins from the client end as cloud matters to the users extensively.

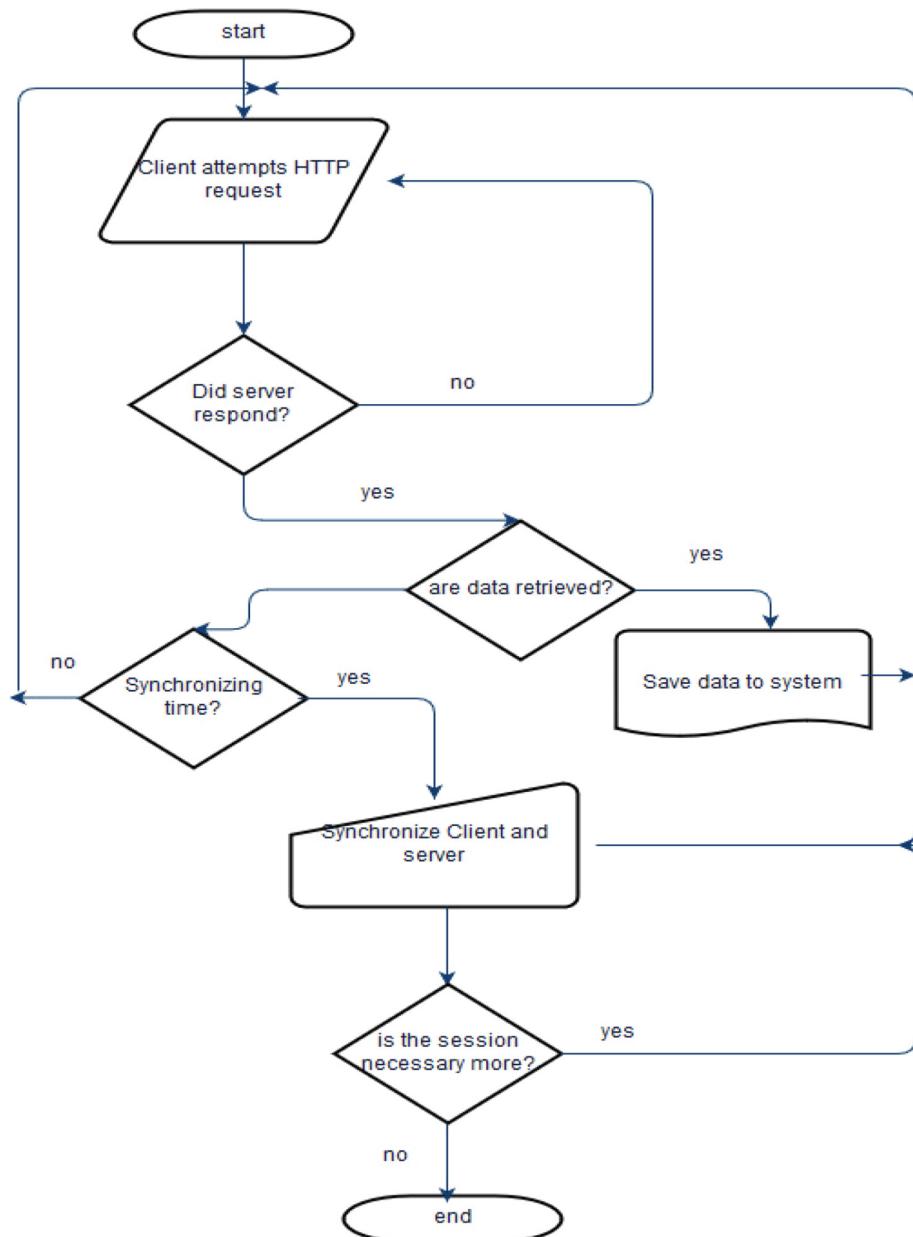


Fig. 4. Flowchart between distributed networks and clients

- (b) Clients make HTTP/HTTPS server or data request.
- (c) Then clients get success or error report depending on several parameter like internet connection or the availability of the server as described in Fig. 3.
- (d) If the previous step is successful then the clients retrieve or interact (upload or download) with the necessary data otherwise clients check the reasons behind the errors.
- (e) If the problem is resolved (if found in previous step) then clients modify data (save, edit, delete etc.) otherwise several parameters force the clients to go to the initial step which can be called RESTART.
- (f) Clients terminate the session with the server either from boredom to resolve the issue or the need is ended with no hazards done.

4 Fault Tolerance

Generally, fault tolerance is all about the abstraction of how flawless a particular cloud based or server based computing is. The fault in a cloud computing replicates whether there is any failure in any parts of the computing. This process comprises the following things:

- Discrepancies in network connection
- Are the physical devices working smoothly?
- Is there any obstacles maintaining the overall infrastructure?

Thus a system is measured how many faults it can handle that is the tolerance of fault. That is why Fault tolerance represents how bad or good a system of cloud computing is. Techniques that need to be followed in fault tolerances are:

- (a) Make priorities for the services
- (b) Give special priorities for the database as it generates other important parts
- (c) Later, take a test of the infrastructures and take note of the overall system
- (d) Take the number of obstacles while performing the computing which measures how good or bad the established system is
- (e) Try to reduce the faults as much as possible with proper ALGORITHMIC way.

5 Detection of Fault in Cloud Computing - A Point Out Description

5.1 Infrastructure Failure

Infrastructure combines both the hardware and software. Hardware is the physical devices that gives the format for real existence of the system and software gives the overall interface for cloud computing. So both software and failure cause the infrastructure failure [8].

Deadlock or hanging situation and system crash are the results of Software failure. It arises due to the overflow of data or the lack of management of data.

Hardware failure occurs due to the proper management of physical devices. It will be shortened.

5.2 Security Issue Related Failure

Besides the normal systematic failure which causes the faults in the cloud computing, there are other issues like cyber related issues which also causes the faults [9]. This issue comprises the cyber threat, phishing, hacking, malware attack etc. (Fig. 5).

6 Cloud Computing-Fault Handling Techniques

It is not fully possible to tackle the faults that arise in the cloud computing. But the frequency of the faults can be tackled or reduced to get better performance. At the whole system combines major three components those are data center, distributed system and Clients, the faults also be tolerated at these levels [10, 11]. There is some systematic procedure which can be followed during the execution. Those are:

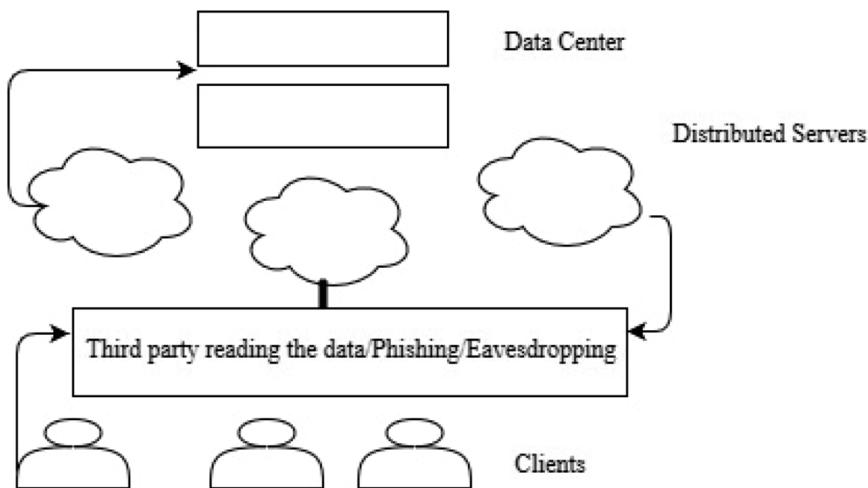
- Failure detector approaches can be followed in Physical data center level.
- Several properties like accuracy, speed, completeness etc. should be followed to keep the tracks of faults and thus the solution can be found depending on the properties.
- Breaches in security is the big issue when it comes about server-based faults and client based faults. So is it strongly recommended that security management should be at its best level.
- Different middleware must be followed to tolerate the frequently arisen faults in cloud computing.
- Software related faults in client level can be avoided by using the fully authorized licensed based software.
- Sometimes overflow of data causes fault. So data should be handled carefully.

7 Fault-Tolerant Models - An Abstract Way of Fault Tolerance

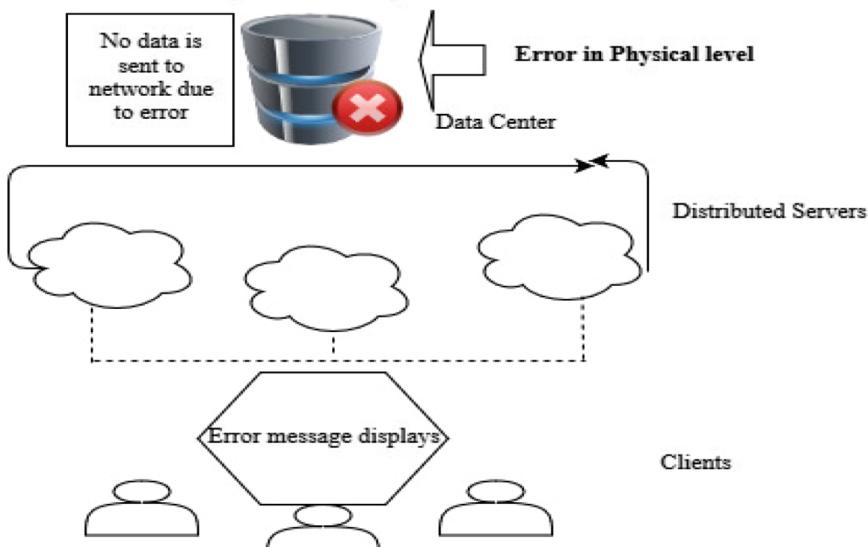
Several models are now widely followed which are:

- Fault tolerance model for real time cloud computing which is known as AFTRC. It helps executing real time applications. It follows proactive fault strategy.
- Middleware based model is known as low latency fault tolerance which is abbreviated as LLFT. It is best for distributed server based application.
- Schedule workflow tolerant system is also used which is known as FTWS. It uses the resubmission technique. A tracker is used for keeping the priorities for the tasks. It then schedules the best workflow for the computing.

Besides these models there are other models available like FTM, CANDY, FT-CLOUD, VEGA-WARDEN etc.



Block diagram for Security level failure



Block diagram for Physical level failure

Fig. 5. Block diagram for the failures-Rise of faults in cloud computing

8 Conclusion

In modern computation technology, cloud computing has become a hot cake and it provides the large amount of resource access and lesser cost service provisioning. The most important cloud services are reliability and availability. Fault tolerance system can

be considered one of the chief parts of any system because it guarantees the system in order to continue the working process during any failure or fault. Fault tolerance systems help in impeding as well as tolerating faults in the system, which may occur either due to hardware or software failure. The main motive to employ fault tolerance techniques in cloud computing is to achieve failure recovery, high reliability and enhance availability. A simplified general overview of cloud computing and the effect of fault tolerance in the domain of cloud computing has been demonstrated in this research work.

References

1. Mell, P., Grance, T.: The NIST definition of cloud computing Natl. Inst. Stand. Technol. NIST Spec. Publ. **145**, 7 (2011)
2. Savu, L.: Cloud computing: deployment models, delivery models, risks and research challenges. In: 2011 International Conference on Computer and Management, CAMAN 2011 (2011)
3. Bokhari, M.U., Shallal, Q.M., Tamandani, Y.K.: Cloud computing service models: a comparative study. In: IEEE International Conference on Computing for Sustainable Global Development, INDIACom, pp. 16–18 (2016)
4. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Brandic, I.: Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Gener. Comput. Syst. **25**(6), 17 (2009)
5. Kumari, P., Kaur, P.: A survey of fault tolerance in cloud computing. J. King Saud Univ. – Comput. Inf. Sci. (2018). <https://doi.org/10.1016/j.jksuci.2018.09.021>
6. Charity, T.J., Hua, G.C.: Resource reliability using fault tolerance in cloud computing. In: 2016 2nd International Conference on Next Generation Computing Technologies (NGCT), pp. 65–71 (2016)
7. Prathiba, S., Sowvarnica, S.: Survey of failures and fault tolerance in cloud. In: Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies, ICCCT 2017, pp. 169–172 (2017)
8. Ataallah, S.M.A., Nassar, S.M., Hemayed, E.E.: Fault tolerance in cloud computing – survey. In: 11th International Computer Engineering Conference, no. 1, pp. 241–245 (2015)
9. Hosseini, S.M., Arani, M.G.: Fault-tolerance techniques in cloud storage: a survey. Int. J. Database Theor. Appl. **8**(4), 183–190 (2015)
10. Bala, A., Chana, I.: Fault tolerance-challenges, techniques and implementation in cloud computing. Int. J. Comput. Sci. **9**(1), 288–293 (2012)
11. Mukwevho, M.A., Celik, T.: Toward a smart cloud: a review of fault-tolerance methods in cloud systems. IEEE Trans. Serv. Comput. **13**74(c), 1–18 (2018)



Disaster Site Map Generation Using Wireless Sensor Networks

P. S. Mohan Vaishnav^(✉), K. Sai Haneesh, Ch. Sai Srikanth,
Ch. Koundinya, and Subhasri Duttagupta

Department of Computer Science and Engineering,
Amrita Vishwa Vidyapeetham, Amritapuri, India
mohanvaishnav98@gmail.com

Abstract. Emergency evacuation is the most important task at a site, struck by a disaster and the task is best accomplished when an up-to-date map of the disaster site is readily available. This paper addresses the problem of generating a disaster site map of a building on fire using wireless sensor networks (WSN) which is dynamically updated to reflect the current state of disaster. Our technique assumes that the building structure is known apriori and makes use of localization and interpolation to generate hazard values at fine granularity. Interpolation allows us to obtain hazard values at places where there is no sensors and localization (using a selected UWB sensors) provides the approximate locations information of sensor measuring hazard values. Using realistic fire values, through simulation, we compare the generated map with the actual hazard values generated map and show that our technique achieves almost 90% accuracy.

Keywords: Wireless Sensor Networks (WSN) · Fire generation · Localization · Ultra Wide Band (UWB)

1 Introduction

Wireless Sensors Networks (WSN) for disaster management is a novel application since it can provide useful information about the disaster and help in the rescue process. Due to complex building structure in modern cities, in case of building fire, often the lives of victims as well as the first responders are at stake and the information affected by the fire is unavailable. Dynamically generated map on the intensity of the disaster can help providing a route to the rescue teams as well as can be reported to the rescue commander outside the building to plan out better strategy. The problem is challenging since the fire can spread very fast and it requires an efficient technique to compute the hazard map and update it frequently. Compared to earlier techniques of disaster map generation that use image sensors, we propose an efficient disaster site map generation technique using wireless sensor networks measuring temperature and smoke around the building.

A naive and the simple approach for dynamic map generation would be to deploy the sensor nodes and collect the sensor data along with the room information from all the sensors in that region and then construct the map at the sink node. But this would cause sensors to perform a lot of communications which is not energy efficient. Rather,

we track the dynamics of fire using fire growth models [3] and predict the spread of the fire at different parts of building. Further, our technique employs well known methods of localization and interpolation technique and compute the latest disaster site map using a few sensors around the building. We do assume that the building information in terms of the number of rooms in each floor and the number of wings is known a-priori.

To achieve the required results, there are a few challenges we need to deal with. First of all, we need an efficient cost-effective indoor localization technique such that all the sensor location information is obtained. The location information is required for the next phase of interpolation that involves computing hazard values for a room of the building where there is no sensor deployed. Additional challenge is that we need an efficient in network technique that can be used to compute the hazard map in a distributed manner. In this paper, we essentially focus on the integrated technique that uses localization of sensors and interpolation. Further, we built a fire spread model for the building and obtain the temperature values at a specific interval of time for each room in the building. After we get the simulation values, we compare these values with the detailed map we generate through our technique. Thus, the validation of the technique is done for accuracy. Thus, we make the following contributions for hazard map generation.

- We provide a cost-effective method for generating disaster map using wireless sensor networks.
- Our technique uses interpolation to obtain fire values at locations where there are no sensors. Thus, it requires less dense deployment of sensors across the building.
- Using realistic fire values through simulation, we show that our map generation technique obtains accuracy close to 90% for a large building.

2 Related Work

Authors in [2] propose Internet of things (IoT) based disaster relief system for the map generation that deals with congestion control of data transmission but we assume sparse deployment of sensors. In this paper, we have not considered sending sensor values to a data aggregator for in network computation of the hazard map but this can be easily performed using any cluster-based routing in WSN [10] or similar to delay tolerant routing [8]. [11] deals with distributed event detection in Wireless Sensor Network for Disaster Management which primarily uses machine learning techniques for event detection. The technique in [13] provides us with the application of interpolation in sparse locations and forms a basis for map generation. Authors in [12] focus on geometric predictive based approach and [15] focus on efficient path for evacuation from the building during the time of calamity and the papers do not deal with estimating the fire values which is the main focus in this paper. The authors in [5] propose sequence-based localization schema along with building information modeling (BIM) for the map generation. Their technique improves the room level localization accuracy but they do not deal with dynamic update of the map. The work in [6] offers a mapping service using multi-modal sensors which dynamically responds to environment change but their technique may result in loss of accuracy when the map gets

updated. In [9], the authors deal with establishing communications with incident management system and identify the possibility of fire or gas leaks when a building is collapsing. Paper [14] deals with the analysis of performance of self-organization structures in Delay Torrent Networks (DTN). This process enables the nodes to conserve their power and can establish efficient connectivity with other nodes during localization.

3 System Design

The design of hazard map generation technique is governed by the principle that the technique should be robust and work with noisy data since in a disaster scenario we may not expect high quality of data. At the same time, the technique should be cost effective and should work with minimum human intervention. Moreover, the generated map should provide accurate information at the room-level so that rescue operation is done efficiently. The system in the simulation comprises of three main modules as given below.

3.1 Fire Spread Generation Model

The purpose of this module is to generate building fire information in most real-like scenario. Fire Spread is a complex process which depends on many factors such as adjacent rooms of the building, presence of windows and doors in a room and amount of combustible material present in the room, wind speed etc. We assume that initially sensors are deployed randomly in different parts of the building. These sensors measure temperature and smoke. To simulate fire spread, we follow the fire growth equations as mentioned in [3] where heat generated due to fire is being tracked. The following equation captures the heat generated due to fire.

$$Q = \alpha(t - t_{ig})^2 \quad (1)$$

Where t_{ig} gives the time instant when fire is triggered and t is the present time instant and Q in (kW) gives the heat generated due to fire. α parameter is the fire growth coefficient and it varies for different rooms. Initially only a single room is on fire and is referred to as the fire source. Then, based on this equation, the fire spreads to remaining building. To simulate real-life situation, we have given different furniture values in each room which reflects the amount of combustible materials present in the room. Rooms with higher furniture values are given a higher parameter. Thus, using the above fire spread model, we obtain the ignition time i.e. the time at which the room catches the fire. After ignition, we generate fire values for each room in the building at each specified intervals of time.

3.2 Interpolation for Obtaining Dense Information

For the accurate map generation, we require sensor values for each room in the building. But random deployment of sensors in the building can provide only hazard

values at a few rooms. Then, additional information is obtained through interpolation of existing sensor values. Hence, the problem of map generation can be viewed as the problem of interpolation from sparse and irregular points. We use Shepards algorithm for this purpose [4] which obtains an interpolated value based on observations from near-by sensors. The algorithm is explained below.

Shepards algorithm is basically an inverse distance weighted interpolation algorithm. It is a continuous function where weighted average of data is inversely proportional to the distance from the interpolated locations. That means, farther a point from interpolated location, the less effect it has on interpolated values.

The above Shepards algorithm in this case is modified as given below:

$$\text{temp}(x, y) = \frac{\sum_{i=1}^N d_i \times \text{value}_i}{\sum d_i} \quad (2)$$

Where $\text{temp}(x, y)$ is the interpolated temperature value at point (x, y) , d_i is the distance of sensor i from the interpolated location and value_i is the corresponding temperature value at sensor i .

The characteristics of their algorithm is that it is amenable to distributed computation where nodes can compute their own contributions and the information can be aggregated at a data aggregator node. The contributions of each sensor reduce with respect to its distance of sensor from the point of interpolation. Based on the sensor observations and interpolated values at intermediate rooms, we obtain the hazard values for every part of the building. But for interpolating the sensor values, we require the location information of the sensors which is obtained through the localization modules as described in the following section.

3.3 Localization of Sensor Nodes

The first step in finding the fire values in a building is to determine the sensors location. Sensor location technique can be attributed to the concept of localization. Localization refers to the finding the location of an object in either closed or open field. Rather than deploying the sensors randomly, we let the sensors localize themselves based on certain reference points. The deployed nodes can interpolate the values which are at a specific distance from them.

To have reference sensors, we deploy Ultra Wide Band (UWB) [1] sensors which serve as a reference sensor node for the other deployed sensors. UWB sensors send periodically beacons and other usual heat sensors receive these signals and based on RSS values they calculate their distance from the UWB sensors. Once the distance from the UWB sensor is obtained, we use trilateration algorithm to find the location of other heat sensors.

Trilateration Algorithm: Trilateration algorithm is basically used to find the coordinates of the sensor nodes with reference to the anchor nodes (reference nodes). The basic concept of trilateration algorithm [7] is that the node whose coordinates has to be found lies along the circumference of a circle centered at anchor and radius equal to the node-anchor distance. In general, for a two-dimensional space, at least three non-

collinear anchors are needed. Since, we are dealing with a three-dimensional building structure, we need at least four non-coplanar anchors.

4 Experimental Results

We use MATLAB to build a simple simulator for generating the building on fire. Based on real-like scenarios we have a fire source and it gets spread to the entire building within a given time interval. The objective of our experiments is to validate the proposed strategy for accurately generating the hazard map which is shown as a surface plot.

4.1 Fire Spread Model

This model as mentioned forms the analysis and replication of data which can serve as a means for comparison. After the implementation of the algorithm, we obtain a matrix where the first column refers to the room number, second column refers to the ignition time and rest of the columns (depending on interval of time) refers to the temperature variation for a particular floor. We simulate a building with 120 rooms spread over three floors, each floor has two wings. The module is capable of generating more complex building. X-axis represents building number, Y-axis represents floor number, Z-axis represents the fire value.

In the surface plots Figs. 1 and 2, fire values of one of the wings of the building are included, X-axis values from 1 to 20 indicates the room number in the 1st wing of the building.

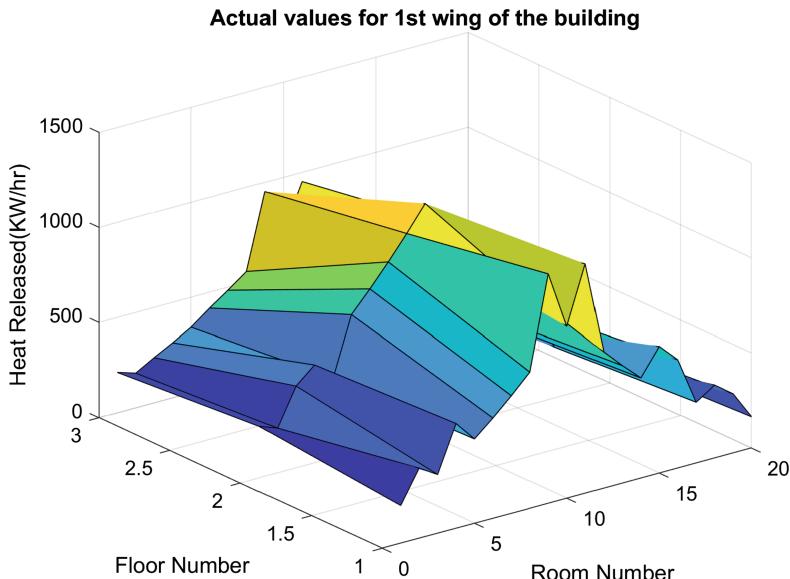


Fig. 1. Actual values fire plot

Interpolation as mentioned earlier enables us to compute fire values at sparse locations where there are no sensors. After applying the interpolation algorithm, we obtain the plot as shown in the Fig. 2.

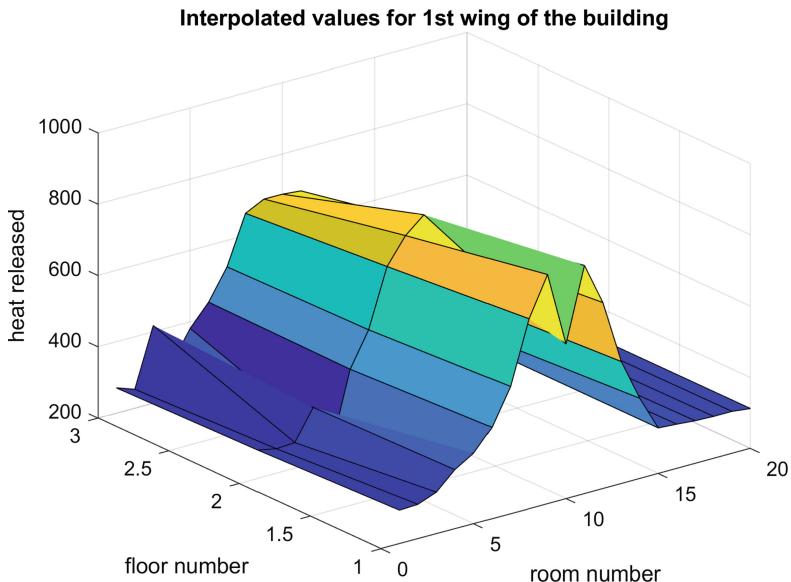


Fig. 2. Plot obtained through interpolation

Interpolation plot is relatively a smooth plot when compared to the plot of actual fire generation. This is because, the actual fire spread plot takes into consideration of furniture values, that is representing realistic scenario of the disaster, thus causing sharp curves in the plot.

However when we try to find the accuracy of our interpolation algorithm, (in this case the error factor), from the Fig. 3, we find that there are 77 values which contribute to 20% error factor, 30 values which contribute to 40% error factor and 5 values which contribute to 60% error factor. From the above observation, we infer the applicability of Shepards algorithm for interpolation in the case of building on fire.

4.2 Localization

Localization refers to the finding the location of an object in either closed or open field. Even though the sensors are deployed randomly, we let the sensors localize themselves based on certain reference points. We use UWB sensors as the reference node based on which we can determine location of other sensors. We ensure that UWB sensors are uniformly deployed in building. The 3D coordinates of the UWB sensors in the building are expressed in terms of floor, room number and wing number as follows: [3, 1, 1], [3, 18, 1], [1, 10, 1], [2, 10, 2].

UWB sensors send periodically beacons and other usual temperature sensors receive these signals and based on RSS values, they calculate their distance from the UWB sensors. Once the distance from the UWB sensors is obtained, a trilateration algorithm is used to localize other temperature sensors. Using the location of UWB sensors as reference nodes, we obtain the location of heat sensors. The basic concept of trilateration algorithm is that the node whose coordinates has to be found lies along the circumference of a circle centered at anchor node and the radius as equal to the distance of the node from the anchors. In general, for a two-dimensional space, at least three non-collinear anchors are needed. Since, we are dealing with a three-dimensional building structure, we need at least four non-coplanar anchors.

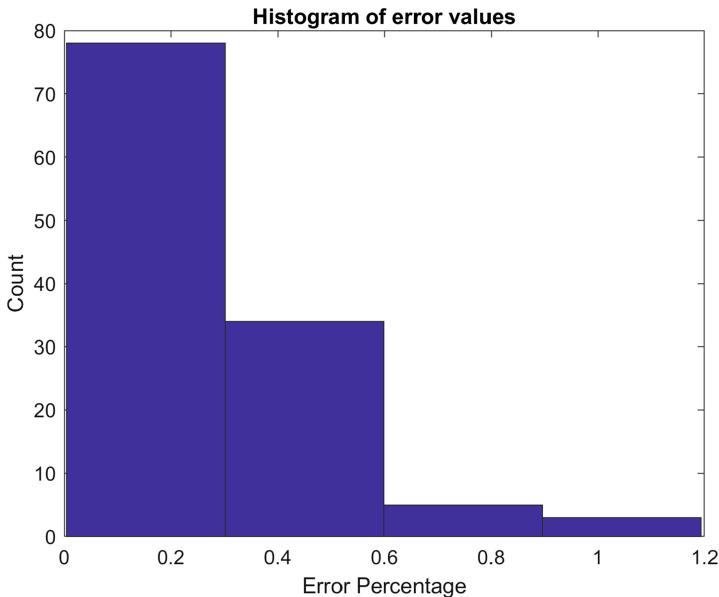


Fig. 3. Interpolation histogram

5 Conclusion and Future Enhancements

In this paper, we present an innovative way of obtaining the hazard values for a building on fire without doing image capturing. Further, we explore and develop a fire generation model for a building that can be extended to any type of building architecture. This fire generation model forms the basis for comparison between the actual fire spread values and interpolated fire spread values. Furthermore, we use a unique combination of two techniques trilateration and interpolation to represent the current state of a disaster with high accuracy. Localization provides us with information regarding the location of sensors in the building which in turn is used by the interpolation model for fire value prediction. The Ultra Wide Band (UWB) sensors act as references for the other temperature sensors to localize themselves. Interpolation, on the other hand, uses the sensor locations as provided by the localization module and obtains the fire values at dense locations. Using the interpolated values, we generate a plot and compare this plot with the actual plot as generated by the fire spread model.

The main advantage of these modules comes from the fact that the computational time required for these modules is comparatively less. Computational time forms the basic requirement for the map generation because, in the case of disaster, the algorithm requires to perform fast and accurately. Because of this advantage, the same technique can be considered for tracking outdoor fire spread with certain modifications but the concept of utilizing multiple complementary techniques can be used in other disaster scenarios as well.

References

1. Alarifi, A., Al-Salman, A., Alsaleh, M., Alnafessah, A.: Ultra wideband indoor positioning technologies: analysis and recent advances. In: International Conference on Cyberworlds (2016)
2. Arbia, D.B., MahtabAlam, M., Kadri, A., Hamida, E.B., Attia, R.: Enhanced IoT - based end-to-end emergency and disaster relief system. *J. Sens. Actuator Netw.* **6**, 19 (2017)
3. Cheng, H., Hadjisophocleou, G.V.: Dynamic model of fire spread in building. *Fire Saf. J.* **46**, 211–224 (2014)
4. Hammoudeh, M., Newman, R., Dennett, C., Mount, S.: Interpolation techniques for building a continuous map from discrete wireless sensor network data. *Wirel. Commun. Mob. Comput.* (2011). <https://doi.org/10.1002/wcm.1139>. <https://onlinelibrary.wiley.com/>
5. Li, N., Becerik-Gerber, B., Krishnamachari, B., Soibelman, L.: A BIM centered indoor localization algorithm to support building fire emergency response operations. *Autom. Constr.* **42**, 78–89 (2014)
6. Hammoudeh, M., Newman, R., Sarah, C., Aldabbas, O.: Map as a service: a framework for visualising and maximising information return from multi-modal wireless sensor networks. *Sensors (Basel, Switzerland)* **15**(9), 22970–23003 (2015)
7. Paul, A.K., Sato, T.: Localization in wireless sensor networks: a survey on algorithms, measurement techniques, applications and challenges. *Sens. Actuator Netw.* **6**, 24 (2017)
8. Raj, D., Ramesh, M.V., Duttagupta, S.: Delay tolerant routing protocol for heterogeneous marine vehicular mobile ad-hoc network. In: International Conference on Pervasive Computing and Communications Workshop (2017)

9. Rao, S., Nithya, G.K., Rakesh, K.: Development of a wireless sensor network for detecting fire and gas leaks in a collapsing building. In: International Conference on Computing, Communications and Networking Technologies (ICCCNT) (2014)
10. Sreevidya, B., Rajesh, M.: Enhanced energy optimized cluster based on demand routing protocol for wireless sensor networks. In: International Conference on Advances in Computing, Communications and Informatics (2017)
11. Bahrepour, M., Meratnia, N., Poel, M., Taghikhaki, Z., Havinga, P.J.: Distributed event detection in wireless sensor networks for disaster management. In: International Conference on Intelligent Networking and Collaborative Systems (2010)
12. Gelenbe, E., Wu, F.J.: Large scale simulation for human evacuation and rescue. *Comput. Math. Appl.* **64**, 3869–3880 (2012)
13. Tynan, R., O'Hare, G., Marsh, D., O'Kane, D.: Interpolation for wireless sensor network coverage. In: Second IEEE Workshop on Embedded Networked Sensors (2005)
14. Smys, S., Raj, J.: A self-organized structure for mobility management in wireless networks. *Comput. Electr. Eng.* **48**, 153–163 (2015)
15. Duttagupta, S., Gopan, A.M.: Efficient evacuation path in a building on fire. In: International Conference on Innovation in Electronics and Communication Engineering (2019)



LRD: Loop Free Routing Using Distributed Intermediate Variable in Mobile Adhoc Network

O. S. Gnana prakasi^(✉) and P. Kanmani

Department of Computer Science Engineering,
Christ (Deemed to be University), Bengaluru, India
{gnana.prakasi, kanmani.p}@christuniversity.in

Abstract. One of the critical challenges in the design of the mobile adhoc networks is to design an efficient routing protocol. Mobility is an unique characteristics of wireless network, which leads to unreliable communication links and loss of data packets. We present a new algorithm, Loop Free Routing with DIV (LRD) is introduced which prevents loops and count to infinity problem using intermediate variables. In addition it finds the shortest path between source and destination. The analysis shows that DIV is compatible with all the routing protocol as it is independent of the underlying environment. The proposed algorithm LRD is compared with the existing algorithm of DIV to prove its applicability in the any routing environment. The simulation results show that LRD excels AODV routing protocol while considering throughput and packet delivery ratio. The new algorithm assures that the routing protocol is shortest loop-free path and outperforms all other loop-free routing algorithms previously proposed from the stand point of complexities and computations.

Keywords: Distance-vector routing · Loop Free Routing · Neighbor node · Shortest path

1 Introduction

A Mobile Ad-hoc Network (MANET) is a self-organizing and self-configuring nodes connected to each other dynamically when the nodes come together in each other communication range. The important characteristic feature of MANET is that the structure of the networks changes dynamically, due to the mobility nature of the nodes connected in the network. Routing the packets between the source and the destination in a dynamic environment is an major issue as the packets are transferred through one or more intermediate nodes. To invoke this, a routine procedure is needed to find a path from the source to reach the destination. While routing the packets from source to destination there is a possibility of same nodes get back the packet leading to the loop in the path. This, Loop is a common problem in routing in MANET and lead to count to infinity problem as the packets will comes back to the same nodes repeatedly leads a loop and will not reach the destination. In addition, the presence of this loop, artificially

increasing the traffic loads in the network that induces network congestion. This lead to performance degradation in the networks by increasing in packet loss and delay.

To avoid routing loops from occurring we have designed LRD algorithm which uses the concept of node value. Each node is assigned a random unique vale based on which the successor node is selected such that the selected node's value is less than its own value. By, using this property a loop free path is got from source to destination. We have integrated the proposed algorithm in AODV and proved that it is more efficient compared to the existing loop free techniques.

The paper is organized as follows: Sect. 2 summarizes related researches in the routing algorithms. Section 3 gives a brief introduction and the working model of the LRD protocol. Section 4 shows the simulation results and graphical analysis of the proposed LRD protocol with AODV protocol. Finally Sect. 5 concludes the works and the future scope of the work

2 Related Work

Enhanced Interior Gate Routing Protocol (EIGRP) computes the best path using Dif-fusing Update Algorithm (DUAL) [17] to minimize the problems routing loops and count-to-infinity. Metric-based Topology Investigation (RMTI) protocol [18], helps to detects the presence of loops by examining incoming routing updatations. Rather than periodic updating, the Triggered RIP (TRIP) [19] replaces by complete triggered update when a topology change is detected. [1] proposed a distributed routing algorithm that guarantees loop-freedom at all times. [2, 6, 15] shows the performance analysis of the routing protocols with adov, [3] shows the optimal forwarding state of the data packet without any loops by combing local protection scheme. [4] present the Dynamic Incremental Routing (DIR) protocol by maintaining the feasible distance with respect to the destination. [5] shows the collision free path by examining the minimal control energy. [7] analyse the issues for link failure in wireless mesh networks and proposed an analytical model for apparent link-failures. [8] evaluate the life time of wireless links through statistical models in a mobile ad hoc network. [9] discussed and analyzed the performance issues of different proactive and reactive routing protocols in an ad hoc networks. [10] reduces the control packets in a highly dynamic environment, in which each node neither maintains routing nor floods the network. [11] selects the routes based on signal strength of the node. [13] analyze the various performance issues of AODV protocol with and with out LTE network. [14] proposes a secure routing protocol using fuzzy rules for link predication. [16] shows a detailed survey of Adov routing protocol. [12] proposed a hybrid algorithm to ensure the Quality of service in AODV routing.

3 Proposed Work

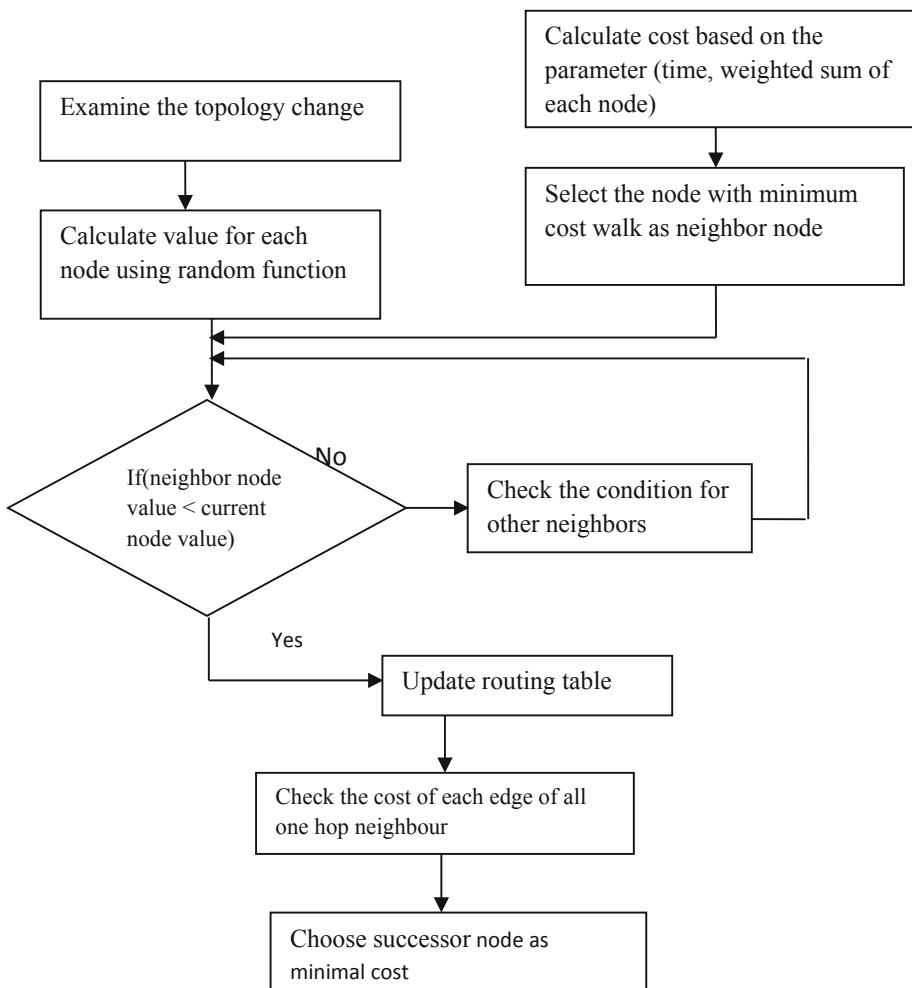
3.1 System Model

Formation of infinite loops is one of main issue in mobile ad hoc networks as the packet came back to the same node while routing the packets from source to destination. This increases the network traffic which affects the performance of MANETs in terms of delay and network overhead. To overcome this problem we proposed a new algorithm Loop Free Routing with DIV (LRD) is introduced which prevents the formation of loops and count to infinity using help of distributed intermediate variables (DIV). The usage of DIV [1] is compatible with all the routing protocol as it is independent of the underlying environment. But, DIV is using the shortest path to reach destination. So, in this paper we integrate the computation of shortest path with DIV to find a loop free shortest path. Hence, the proposed algorithm, Loop Free Routing with DIV (LRD) helps to find loop free path by distributed intermediate variable and shortest path by bellman ford algorithm.

Examine the routing topology for changes such as node position, node's transmission range, node's stability and link between the nodes in the routing environment. Then it calls a random function which calculates random value and assigns that value to the node present in the topology. In this way all the nodes are assigned unique random value as their node value.

Figure 1 shows the work flow of the algorithm. If node wants to transmit a packet, first it need to compute the neighbor node value and the cost to reach the current node. This helps to avoid the loop formation and the shortest path to reach destination. According to the decreasing value property, it states that a node is allowed to select set of neighbor nodes as its one hop neighbour only if the neighbor node's value is less than its own value. These set of one hop neighbour node, now computes the cost of reaching the one hop neighbour based on the time and weighted sum of each nodes. The node with the minimum cost walk will be selected as the successor neighbor node. This is an iterative process and the conditions are checked till the routing path from source to destination is established.

Once the successor node is selected the routing table is updated with the following changes. Thus, the routing table contains the updated information like value of the node, successor node and routing path. This updated path is the loop free and also the shortest path from source to destination. In case of further changes in the topology, the routing table will be updated by performing the above procedure.

**Fig.1.** Work flow of LRD

3.2 Algorithm

In the above algorithm, N_i denotes the set of nodes, $N_i \rightarrow \text{nexthop}$ represents the nexthop nodes in the node set, $N_o \rightarrow$ denotes set of one-hop neighbours in the node set. For each node in the network, node value is calculated in an arbitrary manner by using random function. Whenever there is a change in the topology, the value assigned to the node modified accordingly. When the source node requests to send the packet to the destination node, route discovery process is initialized. During this process, the node checks to see whether the node value of the neighboring node is less than its own node value. If this condition is satisfied, then the neighboring node is assigned as the nexthop of that node. This is an iterative process. It is done till the route to the destination is established.

Algorithm: LRD Implementation

N_i – Node set

$N_i \rightarrow \text{nexthop}$ – next hop of node N_i

N_o -- set of one-hop neighbor

S_i – Successor of node N_i

1. For each node N_i in the network, calculate node value.

$N_i \rightarrow \text{nodeval} = \text{calcost}();$

/* calcost calculates node value */

2. $\text{calcost}()$ assigns a random value (arbitrary value) to each node present in the network.

3. Choose $N_i \rightarrow \text{nexthop}$ as a one-hop neighbour node successor node

If ($N_i \rightarrow \text{nexthop} \rightarrow \text{nodeval} < N_j \rightarrow \text{nodeval}$)

then

$N_o[] = N_i \rightarrow \text{nexthop}[];$

4. Assign cost and walk time to reach the neighbor node

$d_{ij}(t)$ - time to reach node ‘j’ from ‘i’ through edge(i,j) initiating at

time ‘t’

d_{ij}^* - minimum travel time for the crossing the edge (i,j)

$e_{ij}(t)$ – additional time required for traversing the edge(i,j) initiating at

time ‘t’

e^* - maximum additional time time on any edge

$c_{ij}(t)$ – cost on traversing the edge(i,j)

$$e_{ij}(t) = d_{ij}(t) - d_{ij}^*$$

$$c_{ij}(t) = \beta d_{ij}(t) + (\alpha - \beta) d_{ij}^* \quad // \alpha, \beta - \text{specified non-negative integers.}$$

5. Choose the node with low cost as Successor node.

For each N_o in the one-hop neighbour list

Compare cost of each node and select the node with low cost.

6. Use $\langle S_i \rangle$ as successor of shortest and loop free path to reach the destination
-

Once the loop free one neighbours are identified and listed. Next we have to select successor node with node as the smallest cost to reach the one hop. The two main parameters consider for finding shortest path are travel time and cost. $d_{ij}(t)$ denotes the travel time on the edge (i, j) starting at time ‘t’ and $c_{ij}(t)$ denotes the cost on traversing the edge (i, j) based on the travel time. After computing $d_{ij}(t)$ and $c_{ij}(t)$ for all the edges, path with minimum travel time and cost is selected as the successor node. The process continue until reach the destination. Thus the loop free shortest path computed from the source to destination.

4 Simulation Results

Figure 2 shows throughput for two routing protocols (AODV, AODV with DIV). The throughput values increase accordingly to time after integrating DIV with AODV. It has higher throughput value compared to AODV.

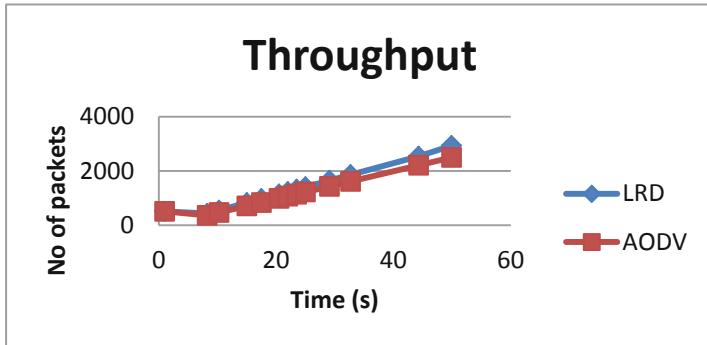


Fig. 2. Throughput

- *Packet Loss*

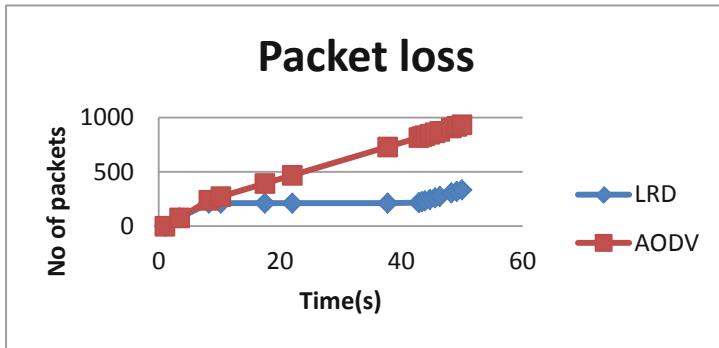


Fig. 3. Packet loss

Figure 3 shows packet loss for two routing protocols (AODV, AODV with DIV). It shows that the packet loss decreases as the time increases. So It has better throughput when compared to AODV.

Table 1 shows the simulation results of two routing protocols (AODV, AODV with DIV). After integrating DIV with AODV throughput gets increased and packet loss gets reduced.

Table 1. Simulation results

Parameters	AODV	LRD
Average throughput (kbps)	409.19	478.66
End to end delay (ms)	8.62242	8.62242
Packet delivery ratio	0.9914	0.9937

5 Conclusion

The proposed algorithm **Loop Free Routing with DIV (LRD)** avoids the loop problem and the count to infinity problem in the ad hoc networks. This is achieved by computing the node value using the intermediate variable with random cost. The algorithm also calculates the shortest path from source to destination considering the time and weighted sum of each node. It finds the minimum cost walk and node value to find the shortest loop free path. By doing so, it improves the performance and reduces the end to end delay occurring in it which is shown by the comparative analysis. Also, LRD is compatible with any routing environment.

References

1. Ray, S., Guérin, R., Kwong, K.W., Sofia, R.: Always acyclic distributed path computation. *IEEE/ACM Trans. Netw.* **18**(1), 307–319 (2010)
2. Al-Mekhlafi, Z.G., Hassan, R.: Evaluation study on routing information protocol and dynamic source routing in Ad-Hoc network. In: 7th International Conference on IT in Asia (CITA) (2011)
3. Francois, P., Bonaventure, O.: Avoiding Transient loops during the convergence of link-state routing protocols. *IEEE Trans. Netw.* **15**(6), 148–160 (2007)
4. Rangarajan, H., Garcia-Luna-Aceves, J.J.: Achieving loop-free incremental routing in Ad Hoc networks. *IEEE Trans. Netw.* **12**(5S), 764–789 (2007)
5. Yang, J., Qu, Z., Wang, J., Conrad, K.: Comparison of optimal solutions to real-time path planning for a mobile vehicle. *IEEE Trans. Syst. Man Cybern. - Part A: Syst. Hum.* **40**(4), 721–731 (2010)
6. Shohidul Islam, Md., Naim Hider, Md.: An extensive comparison among DSDV, DSR, AODV protocol in MANET. *Int. J. Comput. Appl.* **15**(2), 5–10 (2011)
7. Egeland, G., Engelstad, P.E., Li, F.Y.: The performance of WirelessyMesh networks with apparent link failures. *Wireless Mesh Network*, India (2011)
8. Wu, X., Hamid, R., Sadjadpour: Link dynamics in MANETs with restricted node mobility: modeling and applications. *IEEE Trans. Wirel. Commun.* **23**(5), 1–11 (2009)
9. Garcia-Luna-Aceves, J.J.: Performance analysis of proactive and reactive routing protocols for Ad hoc networks. *Int. J. Comput. Appl.* **1**(14), 587–597 (2010)
10. Iyengar, N.C., Narayana, S.: An efficient and secure routing protocol in Mobile Ad-hoc networks. *Int. J. Comput. Netw. Commun.* **2**(3), 28–36 (2010)
11. Mamoun, M.H.: A novel technique for the route selection in DSR routing protocol. *Int. J. Video Image Process. Netw. Secur.* **11**(3), 1–4 (2011)
12. Shrivastava, M., Sahu, M., Rizvi, M.A., Ahmad, K.: IAODV: an improved Aodv routing protocol for MANET. *Int. J. Adv. Res. Comput. Sci.* **9**, 2 (2018)

13. Mashal, A., Kulkarni, V.R., Kulkarni, S.A.: Implementation and analysis of AODV routing protocol with and without LTE network. *Int. J. Comput. Appl.* **171**(4), 32–35 (2017)
14. Garg, M.K., Singh, N., Verma, P.: Fuzzy rule-based approach for design and analysis of a trust-based secure routing protocol for MANETs. *Procedia Comput. Sci.* **132**, 653–658 (2018)
15. Soi, V., Sabo, T., Dhaliwal, B.S.: Performance comparison of DSR and AODV routing protocol in mobile Ad hoc. *Int. J. Comput. Intell. Res.* **13**(7), 1605–1616 (2017)
16. Singh, M., Kumar, S.: A survey: Ad-hoc on demand distance vector (AODV) protocol. *Int. J. Comput. Appl.* **161**(1), 38–44 (2017)
17. Zhao, C., Liu, Y., Liu, K.: A more efficient diffusing update algorithm for loop-free routing. In: 5th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1–4, China (2009)
18. Bohdanowicz, F., Dickel, H., Steigner, Ch.: Metric-based topology investigation. In: Eighth International Conference on Networks, pp. 176–184, Gosier (2009)
19. Gani, A., Hassan, M.K., Zaidan, A.A., Zaidan, B.B.: Intelligent routing information protocol using full triggered update mechanism. *Int. J. Phys. Sci.* **6**, 2750–2761 (2011)



Activity Classifier: A Novel Approach Using Naïve Bayes Classification

G. Muneeswari^(✉), D. Daniel, and K. Natarajan

Department of CSE, Faculty of Engineering, Christ (Deemed to be) University,
Bangalore, India

{muneeswari.g, daniel.d,
natarajan.k}@christuniversity.in

Abstract. Activity movements have been recognized in various applications for elderly needs, athletes activities measurements and various fields of real time environments. In this paper, a novel idea has been proposed for the classification of some of the day to day activities like walking, running, fall forward, fall backward etc. All the movements are captured using a Light Blue Bean device incorporated with a Bluetooth module and a tri-axial acceleration sensor. The acceleration sensor continuously reads the activities of a person and the Arduino is designed to continuously read the values of the sensor that works in collaboration with a mobile phone or computer. For the effective classification of a person's activity correctly, Naïve Bayes Classifier is used. The entire Arduino along with acceleration sensor can be easily attached to the foot of a person right at the beginning of the user starts performing any activity. For the evaluation purpose, mainly four protocols are considered like walking, running, falling in the forward direction and falling in the backward direction. Initially five healthy adults were taken for the sample test. The results obtained are consistent in the various test cases and the device showed an overall accuracy of 90.67%.

Keywords: Acceleration sensor · Bluetooth Low Energy · Internet of Things · Activity classifier · Naïve Bayes Classification

1 Introduction

In recent years, there has been vast developments in Information Technology that have enabled simpler and smarter methods for movement classification. The classification of movements can be of great aid in a large number of cases, most importantly in the analysis of gait. It is used in various areas that include analyzing the running pattern of athletes or sprinters, in diagnosing physical conditions that require physio-therapeutic correction and so on. Currently, it is widely used in the monitoring of senior citizens in their home environment. Various solutions for the detection of falls among the elderly have been developed based on the tracking of their movement. The advancement over Internet of Things (IoT) can tremendously increase the life style of elderly and needy people [1]. Moreover, supporting methods such as Bluetooth Low Energy have made the development of such devices much cheaper and more power efficient [2]. This paper aims to design and develop a low cost and smart system that can help in detecting

and classifying activities performed by the user. In order to achieve this, a Bluetooth Arduino Microcontroller that uses very less power consuming connection has been used. In order to detect the movements, an accelerometer embedded in the device is used.

In this paper, Sect. 2 focuses on literature survey, Sect. 3 discusses about the system architecture and the working methodology is depicted in Sect. 4. The evaluation results are discussed in Sect. 5 and conclusion is illustrated in Sect. 6.

2 Literature Survey

There are various existing methods to track the movements made by the user namely using computer vision, wearable sensors and Pyroelectric Infrared sensors. The first method uses computer vision. This method takes aid of multiple cameras placed at different angles to capture the movement of the user. This solution focused particularly on classifying a fall. The data obtained from the camera served as an input to an algorithm that classified whether a fall has occurred or not. One drawback of this solution is the high cost associated with the setup of multiple cameras. Also, other activities such as bending down or sitting were found to be misclassified [3]. Another method uses a wireless sensor based wearable system. This system makes use of acceleration and gyroscopic sensors which are placed on the hand and the foot of the user. This method used supervised classification methods to classify the six activities that they had considered for the study but this method was found to be complex and computationally expensive [4]. Another solution that used wearable sensors focused on the detection of a fall. This method involved placing a GPS and GSM module on the user's hip. This device can run for two days on a coin cell battery and is hence not very power efficient and it may also misclassify a bending action as falling. Also, the attachment to the hip would be uncomfortable for the user [5].

Another method that has been proposed is a person movement detection system based on PIR sensors. These sensors sensors were placed on the ceiling and the walls of a hallway for this study. Various Machine Learning technologies were employed to classify the direction of the movement, speed at which the movement occurred, the original distance between the body and the sensor and the direction in which the subject was walking. But this method does not recognize other movements such as falling and it is not feasible to include such a system in our daily life [6].

3 Overview of Classification

The proposed system of activity classifier is shown in Fig. 1. The first step is the attachment of the Light Blue Bean to the user's footwear. In the home environment the device can be attached to an ankle band that has to be worn by the user. After the attachment, Bluetooth Low Energy connection has to be established between the acceleration sensor device and the person's smartphone.

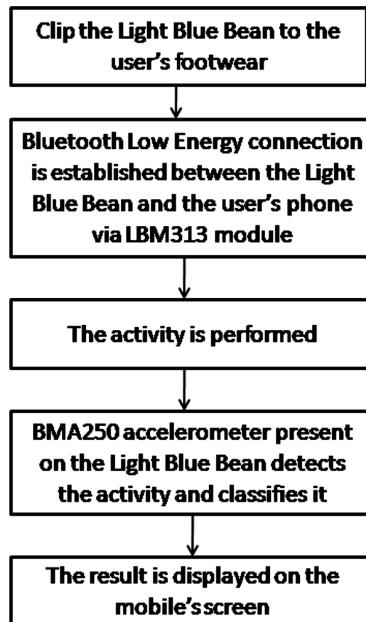


Fig. 1. Activity classifier

The third step is to perform the activity. In this case, the activities considered are running, walking, falling forward and falling backward. The BMA250 acceleration sensor senses the acceleration in the three axes. When each of the above activities are performed, the readings captured via acceleration sensor on the x axis will go for major change. With the help of the observed acceleration values and the Naïve Bayes Classifier, the activities are classified. The result is then displayed on the user's PC/Laptop/Smartphone.

4 Activity Classification Protocol

4.1 Data Acquisition

For implementing the proposed solution, the device with three major modules are used. The Arduino Microcontroller that uses the AtMega328p Arduino Microcontroller and the LBM313 Bluetooth Module. This is because the host is allowed to sleep until it has to perform an operation [7]. The AtMega328p module is used to program the device to record the accelerometer values. Additionally, the Light Blue Bean is embedded with a BMA250 accelerometer which is a triaxial acceleration sensor that records the acceleration in the x, y and z axes (Fig. 2).

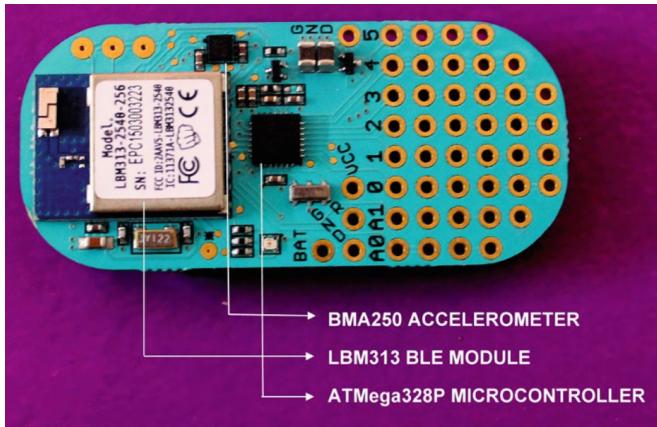


Fig. 2. Light Blue Bean

For effective classification of evaluation of performance and classify the activities, Naïve Bayes classifier is used. Naïve Bayes classifier was chosen as it gives good results even for a small number of observations. Forty data points are considered for each scenario and testing as well as training is performed. Among many classification techniques, it is found that the Naïve Bayes Classifier is very easy to implement and shows better F Measure, AUC and Accuracy when compared with the Decision Tree [8]. The performance metrics used for evaluation depends on efficiency, specificity, sensitivity and F-measure [9, 10]. Several parameters had been taken to measure the accuracy of certain bluetooth devices [11] and the location can be identified with tapping sense connected to mobile devices [12–14].

4.2 Experimental Protocol

The Light Blue Bean was attached to the footwear of the persons and the following protocols are followed for evaluation design.

Protocol 1: The devise readings are recorded for about ten seconds and the evaluation is carried out in a lab space were the subjects are requested to walk.

Protocol 2: The subjects were asked to run in a free lab environment and the accelerometer readings were recorded for ten seconds.

Protocol 3: The subjects were requested to fall in the forward direction. The accelerometer readings were recorded for ten seconds which included the falling motion as well as the duration the subject remained on the floor.

Protocol 4: The subjects were requested to fall in the backward direction. The accelerometer readings were recorded for ten seconds which once again, included the duration the victim remained on the floor.

5 Evaluation Results

In Fig. 3, the sensor values for the fall forward direction is illustrated. In the same way Fig. 4 indicates fall backward readings. The x-axis is the time for the protocol and the sensor reading is drawn on the y-axis with the raw format.

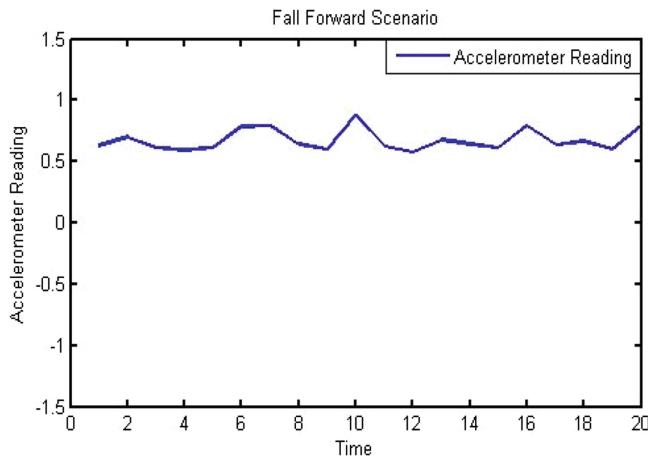


Fig. 3. Accelerometer data in the fall forward scenario

The average value of acceleration in the x direction in the falling backward phase for the representative subject is -0.779 and that in falling forward is about 0.824 .

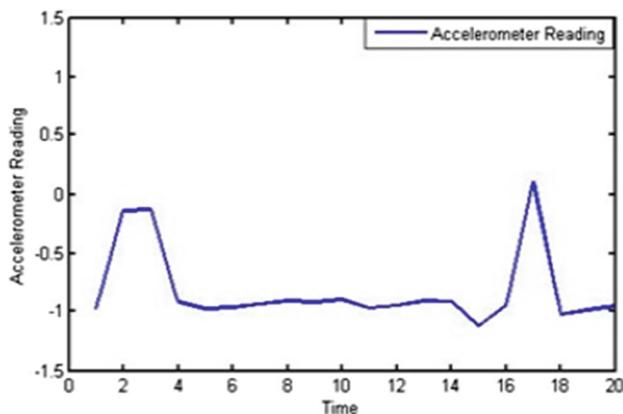


Fig. 4. Accelerometer data in the fall backward scenario

The scenarios related to walking is depicted through Fig. 5 and the average values of the accelerometer readings are in the running scenario is 1.104 and in the Walking scenario is 0.287.

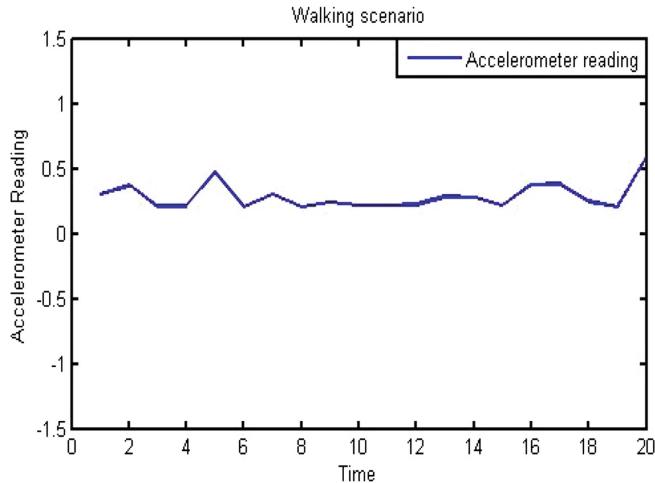


Fig. 5. Accelerometer data in the walking scenario

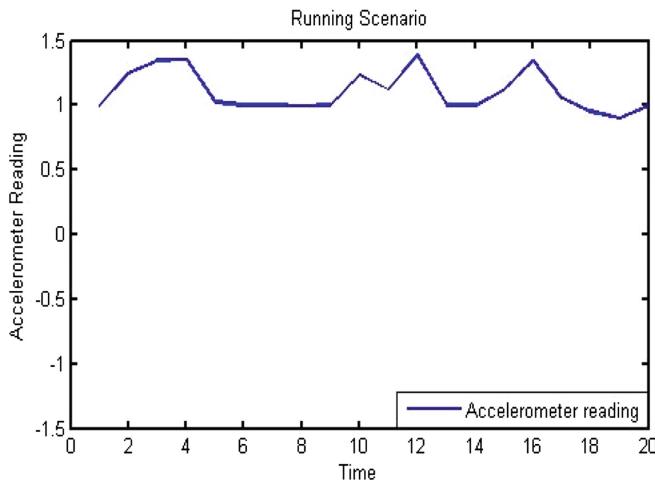


Fig. 6. Accelerometer data in the running scenario

The scenarios related to running is depicted through Fig. 6 respectively. The average values of the accelerometer readings are in the Running scenario is 1.104 and in the Walking scenario is 0.287.

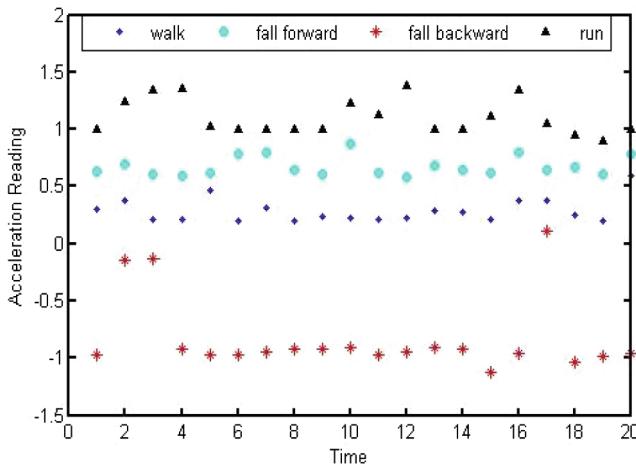


Fig. 7. Scatterplot representation of the four scenarios

A graphical representation of scatter plot is illustrated in Fig. 7 for walking, running, falling backward and falling forward across all the samples. The statistical values with mean and standard deviation for four scenarios considered, namely, walking, running, fall backward and fall forward are represented in Table 1 along with minimum and maximum values.

Table 1. Statistical analysis

Action	Minimum value	maximum value	Mean	Standard deviation
Walking	0.202	0.591	0.287	0.104
Fall backward	-0.977	-1.07	-0.779	0.336
Fall forward	0.592	0.951	0.824	0.094
Running	0.9004	1.3865	1.104	0.155

In Table 2 the relevant metrics for evaluation results are represented and it shows maximum efficiency using Naïve Bayes Classification technique.

Table 2. Naïve Bayes Classifier performance

Performance Metrics	Results
Efficiency	90.67%
Specificity	91.7%
Sensitivity	91.7%
F-Measure	0.917
AUC	0.977

6 Conclusion

This paper aimed to develop a smart, low cost device that could classify basic activities. The working was based on the use of a tri-axial accelerometer clipped to the footwear of healthy adults. This device can be used anywhere in any environment. The automated system gave an overall accuracy of 90.67%. The assumption was that the person's feet were at the walking level throughout the experiment. By trying out a wide range of new scenarios and with more number of subjects can improve the reliability and robustness of the system. In the future, this system can be used for detecting a fall or the analyzing the speed or gait of athletes and so on.

References

- Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Internet of Things: vision, applications and research challenges. *Ad Hoc Netw. Int. J.* **10**(7), 1497–1516 (2012)
- Siekkinen, M., Hienkari, M., Nurminen, J.K., Nieminen, J.: How low energy is Bluetooth low energy? Comparative measurements with ZigBee/802.15.4 2012. In: IEEE Wireless Communications and Networking Conference Workshops, pp. 232–237 (2012)
- Zhang, Z., Becker, E., Arora, R., Athitsos, V.: Experiments with computer vision methods for fall detection. In: PETRA '10 (2010)
- Varkey, J.P., Pompili, D., Walls, T.A.: Human motion recognition using wireless sensor based wearable system. *J. Pers. Ubiquit. Comput.* **23**(4), 234–239 (2011)
- Wu, F., Zhao, H., Zhao, Y., Zhong, H.: Development of a wearable-sensor-based fall detection system. *Int. J. Telemed. Appl.* **2015**(576364), 11 (2015)
- Yun, J., Lee, S.-S.: Human movement detection and identification using pyroelectric infrared sensors. *Sensors* **14**, 8057–8081 (2014)
- Liu, J., Chen, C., Ma, Y., Xu, Y.: Energy analysis of device discovery for Bluetooth low energy. In: IEEE Vehicular Technology Conference, pp. 1–5 (2013)
- Ashari, A., Paryudi, I., Tjoa, A.M.: Performance comparision between Naïve Bayes, descision tree and k-nearest neighbour in searching in an energy simulation tool. *Int. J. Adv. Comput. Sci. Appl.* **4**(11) (2013)
- Zhang, X., Barkhaus, P., Rymer, W., Zhou, P.: Machine learning for supporting diagnosis of amyotrophic lateral sclerosis using surface electromyogram. *IEEE Trans. Neural Syst. Rehabil. Eng.* **22**(1), 96–103 (2013)
- Hajian-Tilaki, K.: Receiver operating characteristic (ROC) curve analysis for medical diagnostic test evaluation. *Casp. J. Intern. Med.* **4**(2), 627–635 (2013)
- Viswanath, N., Pakyala, N.V., Muneeswari, G.: Smart-foot device for women safety. In: IEEE TENSYMP 2016, Sanur, Bali Island, Indonesia (2016)
- Viswanath, N., Pakyala, N.V., Muneeswari, G.: The design and development of an automated fall detection system for geriatrics. In: Proceedings of BSSI. Indian Institute of Technology Madras (2016)
- Frank, V.J., Muneeswari, G.: A novel approach for gait analysis using activity classifier for medical analysis. *Biomed. Res. (Spec. Issue)* **20**(1) (2017)
- Constantinescu, Z., Vladoiu, M.: Challenges in safety, security, and privacy in the development of vehicle tracking system. In: 17th International Conference System Theory, Control and Computing (ICSTCC), Sinaia (2013)



Virtual Machine Allocation in Heterogeneous Cloud for Load Balancing Based on Virtual Machine Classification

Badshaha Mulla¹(✉), C. Rama Krishna¹, and Raj Kumar Tickoo²

¹ Computer Science and Engineering Department,
National Institute of Technical Teachers Training and Research (NITTTR),
Chandigarh, India

badshamulla@gmail.com, ramakrishna.challa@gmail.com
² National Informatics Centre, Punjab State Unit, Chandigarh, India
rk.tickoo@nic.in

Abstract. Many organizations are turning to cloud users because of the potential benefits of the cloud. The increasing popularity of cloud services has brought several difficulties as well. Balancing the workload among the available resources at cloud datacenter is one of them and becomes a crucial task. The cloud service provider needs an effective mechanism for achieving workload balance to meet the demands of large numbers of users. To overcome this, many different approaches are suggested in the literature. But still, there is scope to improve the performance of the heterogeneous cloud. The method of distribution of workload among resources needs to consider the processing capability of each resource. Here, in this work, we propose a method “VAHC (VM Allocation in Heterogeneous Cloud for Load Balancing Based on VM Classification)” for allocation of VM based on its classification. The median is used for effective classification of VMs into two groups based on their capacities. This work focuses on minimizing the response time and time required for processing the request in the heterogeneous cloud. The performance of this work is analyzed and compared with “Equally Spread Current Execution (ESCE)”, “Throttled”, and “Round Robin (RR)” Algorithms. The results of the proposed method showed a considerable reduction of 16% in response time whereas 29% in time required processing the request at the datacenter.

Keywords: VM Allocation · VM Classification · Load balancing · Heterogeneous cloud · CloudAnalyst

1 Introduction

The potential benefits of cloud have attracted huge numbers of users across the globe. As per the Forbes report [1] published in 2008, 83% of the total workload of enterprises will be shifted in the cloud by the year 2020. Despite growing popularity and providing a number of advantages over the traditional computing paradigms, cloud computing is facing the number of challenges. Some challenges are addressed by many researchers and practitioners. Some common challenges are performance, privacy and security,

reliability, scheduling and load balancing, resource management, scalability, Quality of Service, etc. [2–5].

The increase in the users of cloud service has forced cloud service providers to adopt an efficient mechanism for handling the workload. The balancing of workload among the available resources becomes a key challenge for cloud service providers [6–8]. This affects the performance of cloud in terms of the response time of user request, the processing time of the request, overall cost incurred to cloud service provider, etc. [9]. In literature, different approaches and algorithms like “Equally Spread Current Execution (ESCE)”, “Throttled”, “Round Robin (RR)” etc. have been proposed and widely used to enhance the performance of cloud [10, 11]. Still, the issues like heterogeneous resources at the datacenter, poor quality of services, improper resource utilization, etc. needs attention while the distribution of workload among available resources.

The load balancing process uniformly distributes the incoming workload among the available resources [12, 13]. The situations like some computing resources are having a high workload while some are ideal or having little workload are avoided using efficient load balancing mechanism. In literature, this load balancing algorithms are categorized according to various criteria and represented in Fig. 1 [14, 15].

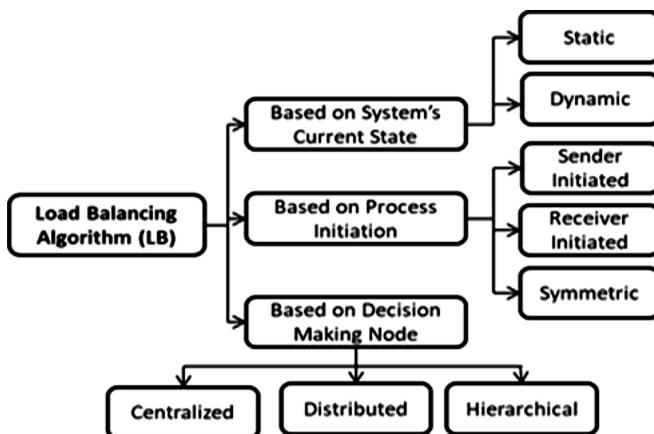


Fig. 1. Types of load balancing algorithms

A general model for load balancing have been proposed and used in the literature [13, 16]. Load balancing model is shown in Fig. 2.

When Data Center Controller (DCC) receives cloud users request, the DCC forward these requests to the load balancer component of the cloud for identification and the selection of Virtual Machine (VM) for the execution of user request. The load balancer uses the “Load Balancing Algorithm” for allocating the VM for processing the current request. This algorithm identifies and decides the appropriate VM for allocation of the next request based on the performance goals. VM process the requests of the cloud users using its processing elements. The users across the globe request the services from the cloud provider randomly. These requests need to be assigned to

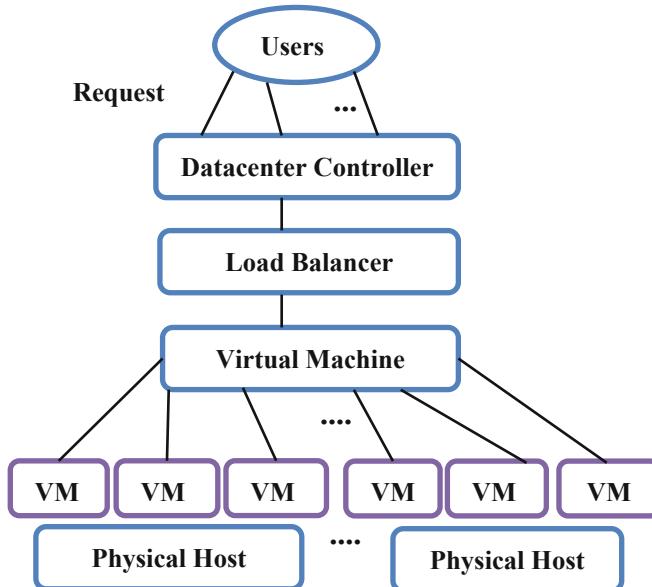


Fig. 2. Load balancing model [13]

appropriate VMs for efficient processing. Lack of effective load balancing mechanism can degrade the performance of cloud system such as quality of services (QoS), resource utilization, and the total cost incurred to the service provider.

This work proposes an efficient method called VAHC for allocation of VM in heterogeneous cloud based on their classification. The median is used for effective classification of VMs into two groups based on their capacities. This work focuses on minimizing the response time and time required for processing the request in the heterogeneous cloud. The performance of this work is analyzed and compared with Equally Spread Current Execution (ESCE), Throttled, and Round Robin (RR), and Throttled Algorithms. Obtained results demonstrate that, our proposed VAHC method has significantly reduced the response time and datacenter processing time.

The remaining paper is divided into five sections. Section 2 discusses some related studies for this work. The detail of propose work is described in Sect. 3. Section 4 discusses the simulation configuration and setup required for this work. Section 5 provides a discussion on results. The last Sect. 6 provides remarks about the conclusions.

2 Related Work

Many researchers have contributed different approaches and algorithms in order to improve the performance of the cloud system using load balancing. Here, we are briefly discussing some of them which focus on providing better response time and processing time of datacenter.

The “Round Robin (RR)” algorithm is based on the concept of quantum time. The time is divided into equal slots and every VM is allotted unique time slot. The tasks are executed on VM for the limited time as per the length of the slot. The capacity of VM is not been considered and VMs are randomly selected in circular fashion [17, 18]. The Shortest Job First (SJF) algorithm, execute the tasks depending upon their task length. The tasks are executed in ascending order of their task length. Due to this, the task with maximum length might get starved and results in longer response time.

Yeboah et al. [19] have introduced the “Round Robin Shortest Job First (RRSJF) method by combining RR with SJF algorithm. In this, first tasks are arranged in ascending order as per their task length. Then, these sorted tasks are executed in a round-robin manner. The result showed a minimum average waiting time and turnaround time as compared to RR. Elmougy et al. [20] have proposed hybrid algorithm using SJF and RR algorithms. Instead of fixed time quantum, the authors have used dynamic time quantum for balancing short size and long size tasks. The starvation of long size task has been partly reduced. The results of this algorithm showed minimum response and waiting time as compared to SJF, RR. But, still in both the cases of enhancement the preemption is required and it may affect the overall response time.

Equally Spread Current Execution Load (ESCS) algorithm described in [21, 22], distributes the current user requests on available VMs equally. The load balancer constantly monitors a list of VMs with the number of tasks allocated. Based on this list it distributes the incoming requests to the least loaded available VMs. Throttled algorithm is based on the concept of thresholding [10, 11, 23, 24]. In this, only predefined number of user requests are allocated to a VM based on threshold value. When it receives further requests, they will be queued until the VM becomes available. This may affect the overall response and datacenter processing time. In both algorithms, actual and current capacity of VM have not been considered.

Rani et al. [25] have proposed “A Hybrid Approach of Round Robin, Throttle & Equally Spaced Technique for Load Balancing in Cloud Environment”. The proposed algorithm aims at uniform distribution of the load among the VMs in DCC and decreasing the response and overall processing time of DCC. This hybrid algorithm makes use of Throttled, ESCE, and RR algorithm. In the proposed algorithm initially, user tasks are allocated to available VMs in a round-robin manner. For the next request, using throttle load balance technique, the requested resources are checked & allocation is made to the appropriate server. The server utilization is also checked with a specified threshold ($>75\%$) while the distribution of load among the VMs. Authors have concluded that due to the combined features proposed scheduling algorithm works efficiently in load distribution.

Elrotub and Gherbi [26] have discussed the classification technique for grouping of VMs on the basis of the CPU as well as RAM utilization, and also grouping the user tasks based on their sizes and the information present in the log files. VMs have classified into five different groups. As per the size of the task and its required resource, the tasks are classified into three types such as heavy tasks, medium tasks, and light tasks. The primary focus of this research work is to present an approach for the allocation of a task to VM and to achieve a high QoS to users by optimizing the use of available resources. The authors have used Weka tool to visualize the classification process using tree J48 method. No practical implementation or simulation is used to analyze the performance of this technique.

In this work, we are focusing on the heterogeneity of resources and consideration of the actual capacity of each VM during the distribution of workload. For the performance analysis of this method, we have compared the results of the proposed method with ESCE, Throttled, and RR algorithms.

3 Proposed VAHC Method (VM Allocation in Heterogeneous Cloud for Load Balancing Based on VM Classification)

This method primarily focuses on assigning incoming request of cloud users to the virtual machines according to its processor power. Our method works intelligently in a heterogeneous cloud to properly balance the workload among the available resources of cloud datacenter. The basic working of the proposed method is given in the following Fig. 3.

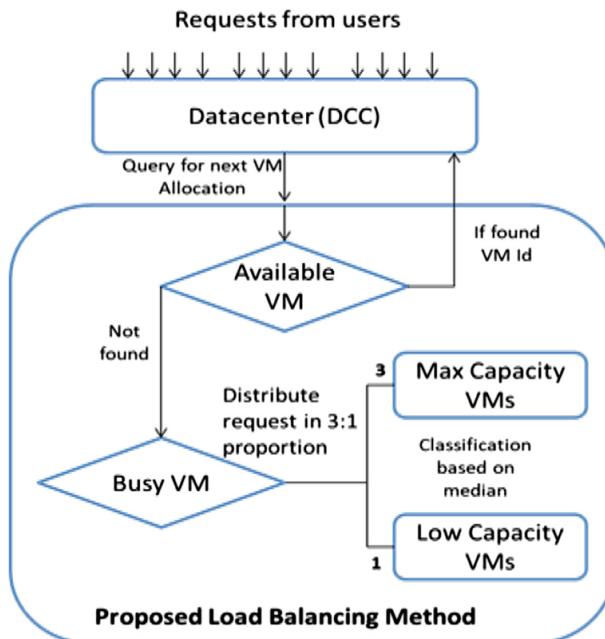


Fig. 3. Working of the proposed VAHC method

In this method, it maintains two index tables for holding the indices of Available and Busy virtual machines. The existing throttled algorithm maintains a single index table, but separating Available and Busy VMs into two tables helps in improving the response time of cloud user [27]. The second attempt is made to again enhance the response and datacenter processing time by allocating the incoming requests to VMs in a Busy index table when no VM is found in Available index table. In contrast, throttled algorithm puts incoming requests in the waiting queue if it does not find the VM in Available index table.

For each new request, this method first looks into the Available table, and if it finds one the request is allocated to respective VM. If it doesn't find any VM, the algorithm

employs a method to first classify the Busy VMs into two categories namely MaxCapacityVMs and LowCapacityVMs. The MaxCapacityVMs group contains the VMs which are having higher capacity than the median, whereas the VMs with lesser capacity than the median are placed in LowCapacityVMs. For this classification task, the first capacity of each Busy VM is calculated. Next, the median capacity is selected for dividing VMs into either of these categories. A median is a good option as some VM may have very high capacity and some with very low.

After this classification, the method distributes the incoming requests into these categories of VMs with 3:1 proportion. In simple words, first 3 requests are allocated on MaxCapacityVMs and next request on LowCapacityVMs in a round-robin fashion. This is done because after classification the higher capacity VMs becomes a part of MaxCapacityVMs group whereas low capacity VMs becomes a part of LowCapacityVMs group. In the heterogeneous cloud, we can offer extra workload on the VMs with high capacity than the other VMs. This helps in reducing the response and datacenter processing time.

The steps involved in VAHC method are represented in Algorithm 1.

Algorithm 1: Proposed Method for VM Allocation based on their Classification

Input: Incoming requests from cloud users, Available VMs in datacentre

Output: Allocation of requests to VMs

Step 1: Maintains *Available* and *Busy* index tables.

Step 2: New request is arrived at DCC

Step 3: DCC queries to the algorithm for a VM allocation

Step 4: Algorithm parse the *Available* index table of VMs :

if *VM found* **then**

The found VM's index is provided to DCC, the DCC forwards this request to the VM having the particular index.

Also, a notification about this allocation is provided to the algorithm for further updates in index tables.

else

The algorithm checks all VMs *Busy* index table and do the following tasks.

Classification

Calculate the capacity of each VM and sort accordingly.

Calculate the **median** capacity

Based on the median divide the VMs in *MaxCapacityVMs* and *LowCapacityVMs*.

Distribution

Distribute requests in 3:1 proportion among the above categories VMs.

Select VM in each of these categories in round robin fashion.

Step 5: VM responds to DCC after the completion of processing the request. In turns, DCC informs algorithm for necessary updates in index tables.

Step 6: Repeat from Step 2 as and when a new request arrives.

4 Simulation Setup

The simulator is used for the execution and analyzing the performance of the proposed method. Many simulators are available for the modeling the cloud environment e.g. CloudSim, GreenCloud, CloudAnalyst, etc. [9]. In this work, we have used CloudAnalyst simulator. This simulator provides ease to create and configure userbase across the globe. Its graphical user interface provides flexibility in defining the characteristics of datacenters, virtual machines, network latency, etc. [10, 11]. Figure 4 shows the architecture of this simulator.

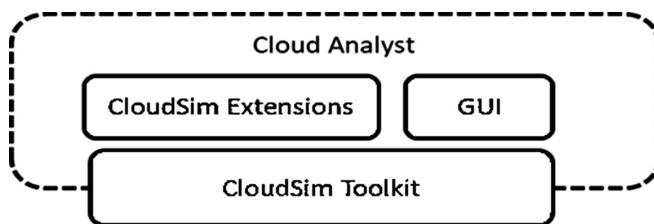


Fig. 4. CloudAnalyst simulator

For performance analysis of our work, we have considered the Facebook application. We have configured the number of users in a simulator as per the Facebook statistics published in [28]. We used the data at a normalized scale (1/200)th for the simplicity purpose. Figure 5 represents the characteristics of userbase configured in a simulator. The CloudAnalyst simulator provides a way to save the details about the

Main Configuration									Data Center Configuration		Advanced																																																	
Simulation Duration: <input type="text" value="60"/> min																																																												
User bases:																																																												
<table border="1"> <thead> <tr> <th>Name</th> <th>Region</th> <th>Requests per User per Hr</th> <th>Data Size per Request (bytes)</th> <th>Peak Hours Start (GMT)</th> <th>Peak Hours End (GMT)</th> <th>Avg Peak Users</th> <th>Avg Off-Peak Users</th> </tr> </thead> <tbody> <tr><td>UB1</td><td>0</td><td>12</td><td>100</td><td>13</td><td>15</td><td>130000</td><td>13000</td></tr> <tr><td>UB2</td><td>1</td><td>12</td><td>100</td><td>15</td><td>17</td><td>135000</td><td>13500</td></tr> <tr><td>UB3</td><td>2</td><td>12</td><td>100</td><td>20</td><td>22</td><td>170000</td><td>17000</td></tr> <tr><td>UB4</td><td>3</td><td>12</td><td>100</td><td>1</td><td>3</td><td>400000</td><td>40000</td></tr> <tr><td>UB5</td><td>4</td><td>12</td><td>100</td><td>21</td><td>23</td><td>85000</td><td>8500</td></tr> </tbody> </table>									Name	Region	Requests per User per Hr	Data Size per Request (bytes)	Peak Hours Start (GMT)	Peak Hours End (GMT)	Avg Peak Users	Avg Off-Peak Users	UB1	0	12	100	13	15	130000	13000	UB2	1	12	100	15	17	135000	13500	UB3	2	12	100	20	22	170000	17000	UB4	3	12	100	1	3	400000	40000	UB5	4	12	100	21	23	85000	8500	<input type="button" value="Add New"/>		<input type="button" value="Remove"/>	
Name	Region	Requests per User per Hr	Data Size per Request (bytes)	Peak Hours Start (GMT)	Peak Hours End (GMT)	Avg Peak Users	Avg Off-Peak Users																																																					
UB1	0	12	100	13	15	130000	13000																																																					
UB2	1	12	100	15	17	135000	13500																																																					
UB3	2	12	100	20	22	170000	17000																																																					
UB4	3	12	100	1	3	400000	40000																																																					
UB5	4	12	100	21	23	85000	8500																																																					
Application Deployment Configuration:									Service Broker Policy: <input type="button" value="Optimise Response Time"/>																																																			
<table border="1"> <thead> <tr> <th>Data Center</th> <th># VMs</th> <th>Image Size</th> <th>Memory</th> <th>BW</th> </tr> </thead> <tbody> <tr><td>DC1</td><td>50</td><td>10000</td><td>512</td><td>1000</td></tr> <tr><td colspan="5"> </td></tr> </tbody> </table>									Data Center	# VMs	Image Size	Memory	BW	DC1	50	10000	512	1000						<input type="button" value="Add New"/>		<input type="button" value="Remove"/>																																		
Data Center	# VMs	Image Size	Memory	BW																																																								
DC1	50	10000	512	1000																																																								

Fig. 5. Userbase characteristics configuration

configurations in the file (with .sim extension). The similar setup configuration is used for analyzing the performances of our algorithm with other algorithms (“Round Robin (RR)”, “Equally Spread Current Execution (ESCE)”, and “Throttled”).

This work is focusing on the performance of the cloud in a heterogeneous cloud datacenter. To simulate the heterogeneity in cloud datacenter resources we have configured physical machines with different RAM (1 GB/2 GB/4 GB), processors, and its speed. Figure 6 shows the datacenter characteristics.

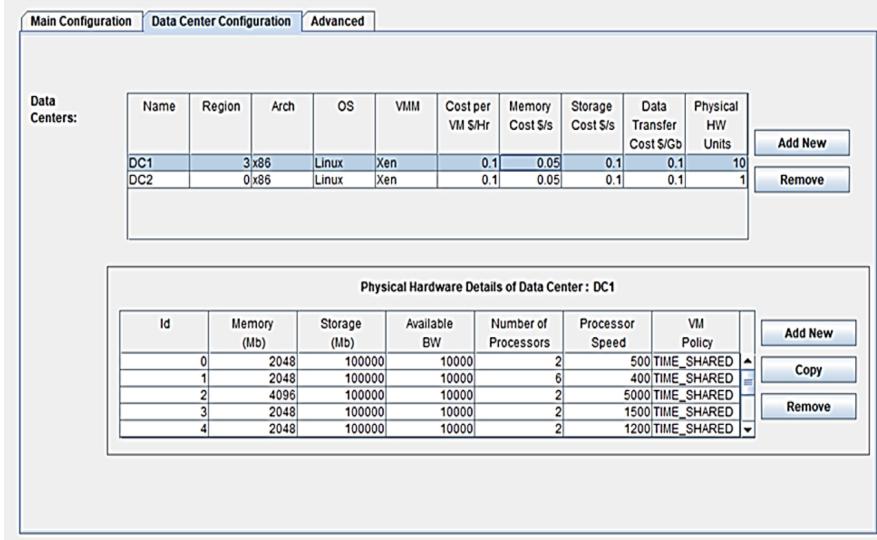


Fig. 6. Datacenter characteristics configuration

We have created different simulation scenarios for analyzing the behavior of our method in different situations. In cloud, services are offered on-demand and most of the time providers need to scale up or scale down the resources as per the demands. To consider this flexibility we have created three different scenarios by changing the datacenters, VMs, and its broker policies. The details are given in the following Table 1.

Table 1. Different scenarios considered for simulation

Scenario	Number of datacenters (DCs)	Number of VMs	Service broker policy
1	One	50	Closest datacenter
2	Two	25 in Each DC	Closest datacenter
3	Two	25 in Each DC	Performance optimized
4	Two	50 in Each DC	Performance optimized
5	Three	25 in Each DC	Performance optimized

5 Results and Discussion

The analysis of obtained results are carried out on the basis of average response time. Also, the datacenter processing time is used for result comparison. The configuration for the simulations and different scenarios discussed in the previous section are used to perform the simulations experiments. Simulations are repeated for each scene for different algorithms.

The simulation experiment with the configuration mentioned in each scenario is carried out using Round Robin (RR), ESCE, Throttled and Proposed VAHC method. The obtained results of average response time are represented in Table 2 and the results of average datacenter processing time are represented in Table 3.

Table 2. Average response time comparison

Algorithm/Scenario	1	2	3	4	5
ESCE	805.06	928.38	881.21	933.05	636.27
RR	801.21	907.70	889.03	920.34	561.35
Throttled	719.80	1110.4	1078.33	833.52	523.68
Proposed Method	602.34	768.54	746.73	662.06	442.66

Table 3. Average datacenter processing time comparison

Algorithm/Scenario	1	2	3	4	5
ESCE	396.95	584.67	511.72	569.44	420.21
RR	393.08	564.07	517.59	557.39	328.85
Throttled	313.96	767.87	714.48	473.03	298.81
Proposed Method	196.66	427.15	383.95	303.33	226.18

We have used different scenarios to analyze the behavior of the proposed method on the performance of cloud in terms of response and processing time. The broker policy is also changed in scenarios to see its effect. From the results, we can say that the Performance Optimized Policy provides better performance. As compared to other algorithms, the proposed method has shown a significant reduction of 16% in average response time of cloud user request and 29% on average datacenter processing time.

This is due to the fact that the proposed method allocates the incoming request to the VMs according to its actual capacity. The 3:1 ratio for distributing the request among high capacity and low capacity VMs, keeps the VMs utilized instead of waiting for the VMs to become available. The use of the median for classification also effectively distributes VMs into two groups. The median effectively handles outliers and also the skewed data.

6 Conclusion

The performance of the cloud system depends upon the number of challenges. In this paper, the load balancing issue related to the heterogeneous cloud has been addressed. This work proposes an effective mechanism for distributing the workload among the available resources based on their capability to enhance the performance of heterogeneous cloud system. The response time reduction and also the datacenter processing time reduction in the heterogeneous cloud is the main focus of this work. An attempt is made to classify the VMs according to its capacity and used the advantages of a median in classification. The obtained results have shown the proposed method have outperformed ESCE, Round Robin (RR) and Throttled algorithms considerably in terms of both parameters.

References

1. Louis Columbus, LogicMonitor's Cloud Vision 2020: The Future of the Cloud Study. <https://www.forbes.com/sites/louis columbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#4ad96e796261>
2. Furht, B., Escalante, A.: Handbook of Cloud Computing, vol. 63, no. 3, pp. 67–76. Springer, New York (2006)
3. Garg, A.: A literature review of various load balancing techniques in cloud computing environment. *Big Data Anal.* **654**, 667–675 (2018)
4. Sridhar, S., Smys, S.: A hybrid multilevel authentication scheme for private cloud environment. In: 10th IEEE International Conference on Intelligent Systems and Control (ISCO), pp. 1–5 (2016)
5. Karthiban, K., Smys, S.: Privacy preserving approaches in cloud computing, In: 2nd IEEE International Conference on Inventive Systems and Control (ICISC), pp. 462–467 (2018)
6. Roy, S., Md Alam, H., Sen, S.K., Nazmul, H., Md Rashid, A.A.: Measuring the performance on load balancing algorithms. *Glob. J. Comput. Sci. Technol.* **19**(1), 41–49 (2019)
7. Siddiqui, S., Darbari, M., Diwakar, Y.: A comprehensive study of challenges and issues in cloud computing. *Soft Comput. Signal Process.* **900**, 325–344 (2019)
8. Mesbahi, M., Rahmani, A.M.: Load balancing in cloud computing: a state of the art survey. *Int. J. Mod. Educ. Comput. Sci.* **8**(3), 64–78 (2016)
9. Kumar, M., Sharma, S.C., Goel, A., Singh, S.P.: A comprehensive survey for scheduling techniques in cloud computing. *J. Netw. Comput. Appl.* **143**(1), 1–33 (2019)
10. Bhathiya, W., Buyya, R.: Cloudanalyst: a cloudsim-based tool for modelling and analysis of large scale cloud computing environments. *MEDC Proj. Rep.* **22**(6), 433–659 (2009)
11. Bhathiya, W., Rodrigo, N.C., Buyya, R.: CloudAnalyst: a CloudSim-based visual modeller for analysing cloud computing environments and applications. In: IEEE International Conference on Advanced Information Networking and Applications, pp. 446–452 (2010)
12. Sui, X., Dan, L., Li, L., Huan, W., Hongwei, Y.: Virtual machine scheduling strategy based on machine learning algorithms for load balancing. *EURASIP J. Wirel. Commun. Netw.* **2019**(1), 1–16 (2019)
13. Xu, M., Tian, W., Buyya, R.: A survey on load balancing algorithms for virtual machines placement in cloud computing. *Concurr. Comput.: Pract. Exp.* **29**(12), 1–16 (2017)
14. Kumar, P., Kumar, K.: Issues and challenges of load balancing techniques in cloud computing: a survey. *ACM Comput. Surv.* **51**(6), 1–35 (2019)

15. Mishra, N.K.: Load balancing techniques: need, objectives and major challenges in cloud computing-a systematic review. *Int. J. Comput. Appl.* **131**(18), 975–8887 (2015)
16. Ghomi, E.J., Rahmani, A.M., Qader, N.N.: Load-balancing algorithms in cloud computing: a survey. *J. Netw. Comput. Appl.* **88**, 50–71 (2017)
17. Shoja, H., Nahid, H., Azizi, R.: A comparative survey on load balancing algorithms in cloud computing. In: IEEE 5th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–5 (2014)
18. Shah, M.D.: allocation of virtual machines in cloud computing using load balancing algorithm. *Int. J. Comput. Sci. Inf. Technol. (IJCSITS)* **3**(1), 93–95 (2013)
19. Yeboah, T., Odabi, I., Hiran, K.K.: An integration of round robin with shortest job first algorithm for cloud computing environment. *Int. Conf. Manag. Commun. Technol.* **3**, 1–5 (2015)
20. Elmougy, S., Sarhan, S., Joundy, M.: A novel hybrid of shortest job first and round robin with dynamic variable quantum time task scheduling technique. *J. Cloud Comput.* **6**(1), 1–12 (2017)
21. Singh, K., Mahaan, R.: Equally spread current execution load algorithm - a novel approach for improving data centre's performance in cloud computing. *Int. J. Future Revolut. Comput. Sci. Commun. Eng.* **4**(8), 8–10 (2018)
22. Lamba, S., Kumar, D.: A comparative study on load balancing algorithms with different service broker policies in cloud computing. *Int. J. Comput. Sci. Inf. Technol.* **5**(4), 5671–5677 (2014)
23. Tyagi, V., Kumar, T.: ORT broker policy: reduce cost and response time using throttled load balancing algorithm. *Procedia Comput. Sci.* **48**, 217–221 (2015)
24. Mesbahi, M.R., Hashemi, M., Rahmani, A.M.: Performance evaluation and analysis of load balancing algorithms in cloud computing environments. In: IEEE 2nd International Conference on Web Research (ICWR), pp. 145–151 (2016)
25. Rani, S., Kalan, K., Rana, S.: A hybrid approach of round Robin, Throttle & equally spaced technique for load balancing in cloud environment. *Int. J. Innov. Adv. Comput. Sci.* **6**(8), 116–121 (2017)
26. Elrotub, M., Gherbi, A.: Virtual machine classification-based approach to enhanced workload balancing for cloud computing applications. *Procedia Comput. Sci.* **130**, 683–688 (2018)
27. Phi, N.X., Tin, C.T., Nguyen, L., Thu, K., Hung, T.C.: Proposed load balancing algorithm to reduce response time and processing time on cloud computing. *Int. J. Comput. Netw. Commun.* **10**(3), 87–98 (2018)
28. Internet World Facebook Stats. <http://www.internetworldstats.com>



Task Scheduling Algorithms in Cloud Computing: A Survey

Linz Tom^{1(✉)} and V. R. Bindu²

¹ Department of Computer Science, Assumption College,
Changanacherry, Kerala, India

linzassum@gmail.com

² School of Computer Sciences, Mahatma Gandhi University,
Kottayam, Kerala, India
binduvr@mgu.ac.in

Abstract. Cloudcomputing has transformed the world of communication systems into a new modern way. A cloud system consists of a vast variety of resources like processors, memory and software that are distributed all around the world. Task scheduling has a critical part in the performance and service of the cloud system. Plenty of task scheduling algorithms exist whose aim is to intensify the overall quality of the system. This article investigates and categorizes these algorithms based on task scheduling metrics of the cloud environment.

Keywords: Cloud system · Cloud deployment models and services · Task scheduling · Scheduling metrics

1 Introduction

Cloudcomputing is a leading technique for bringing up a pool of computational resources with extendability and employment of these techniques by the usage of internet. These computational resources are database management system, application software, operating system platforms, hardware and supporting infrastructure and other services deployed in efficient and price profitable computing. The exposure of cloud computing enhances the ownership to pay-per-use based method for getting access to extensible computing resources and services on-request [1]. It provides vast computing capability to big companies which involve in dealing with enormous data produced daily on a pay and use model. Cloud systems are basically pool of computing resources offered as services on a subscription basis. Of the gigantic advantages of cloudcomputing, the datacenters need high amount of energy for their operations. For a data-server, the energy usage cost is directly proportional to service costs. Therefore energy utilization and carbon footage by cloud datacenters is of great environment significance.

2 Overview of Task Scheduling

In cloudcomputing environment taskscheduling procedure is allocating user tasks to appropriate computer resources so as to minimize execution time and cost. The amount of cloud systems are enlarging everyday. Hence the count of tasks to be processed is also growing. In task scheduling the tasks are allocated to the available computing structures. There are a wide variety of tasks scheduling policies. Broadly they are categorized as static and dynamic methods. There are different parameters which influence this scheduling. If the tasks are not scheduled properly the quality of cloud computing may degrade. Therefore taskscheduling algorithms play a crucial role in cloud environment. The amount of client tasks requesting for cloud resources are increasing day by day. This makes scheduling difficult. Hence appropriate algorithm should be selected to satisfy client needs. For developing efficient scheduling algorithms we need to understand the various problems and limitations associated with different scheduling strategies. Different algorithms uses different parameters. The intension of this survey is to study and differentiate scheduling methods and their associated metrics.

3 Parameters for Comparing Scheduling Algorithms

In this section we review different parameters used in scheduling the task of different users of cloud scenario. Several of these parameters are enhanced in the reviewed works. Table 1 summarizes the list of parameters used to compare various scheduling algorithms. The intension of any scheduling method is to minimize makespan, execution time, waiting time, energy consumption, cost and maximize processor and resource utilization, throughput and QoS.

Table 1. Parameters for comparing scheduling algorithms.

Parameter	Description
Makespan/completion time	Total time taken by a task for its complete execution
Execution time	Processing time taken to execute the given task
Processing cost	Cost incurred for using the resources
Throughput	Number of tasks completed per unit time
Resource utilization	Resources utilized by different tasks.
Load balancing	Equally distribution of the work load
Waiting time	Amount of time a task is in queue
Deadline	Maximum time by which it must be completed.
Priority	The order in which task is to be processed
Energy consumption	Amount of power used for doing a task
QoS	Overall achievement of the cloud system

4 Review of Task Scheduling Algorithms

In this section we reviewed some recent literature on taskscheduling methods in cloud environment. The review and analysis reveals that these works can be categorized according to the parameters used to enhance task scheduling. A brief description of reviewed articles are listed below.

In the article [2], authors propose a method for scheduling of tasks in the cloud system. The strategy is a “parallel genetic algorithm-based policy” that considers the priority of tasks. It improves balancing of loads in processors by selecting effective resources to schedule tasks within a short period of time with less task failure rate. In this recent work [3] authors design an effective approach for task scheduler which uses time sharing that effectively does loadbalancing, utilization of resource with better performance than task scheduler with timesharing that currently exists. Using this approach efficient VMs will be assigned with difficult tasks by considering priority of tasks to have minimal execution time for tasks. Taskscheduling plays a crucial role in reducing makespan/completion time of a task. In [4] the authors proposes the Advanced MaxSufferage (AMS) algorithm to enhance the disadvantage of “MaxSufferage algorithm”. The concept of AMS is to dispatch the tasks to the server with the earliest expected time for completion. The role of AMS is refining the loadbalancing and minimization of the completion time.

In [5] nature inspired preemptive task scheduling that follows honey bees foraging behavior for allocating tasks to the VMs. By considering the task priority tasks can be preempted to lower makespan and enhance throughput. The waiting time of the tasks are shortened by considering expected time of completion and order of tasks during preemption. Thus the overall performance of datacenters will be enhanced. The study [6] suggest a method for task scheduling using improved differential evolution for reducing the completion time, energy consumption and maximizing the degree of load balancing. To improve the global and local searching the scheme uses the “adaptive zooming factor mutation policy” and “adaptive crossover factor increasing strategy”. In the work [7] a “two-stage task scheduling framework” and other similar algorithms proposes to achieve scheduling of tasks and enhance service quality of the cloud system. With the previous information of schedulingtasks, an adequate number of virtual machines are pre created. This will reduce vm creation time and also decreases task scheduling failure rate. Suitable vms are selected from pre created vms to task processing. This is done by considering the complexity of tasks.

Recent work [8] authors introduce a “Job spanning time and load balancing genetic algorithm” (JLGA) based on “double-fitness adaptive” algorithm to get taskscheduling with lesser makespan and loadbalancing. The population is initialized by applying greedy method and load of nodes are described using variance. In [9] authors introduce an task scheduling optimization algorithm that uses the contribution of different existing algorithms like Max-min, Min-min and RASA. Proper scheduling will be possible only when the total number of larger and smaller tasks are almost equal. Otherwise makespan increases. RASA implements the advantages of the techniques and the disadvantages are reduced. By scheduling larger tasks before shorter task “Improved Max-min and Enhanced Max-min” accomplishes loadbalancing among

resources. The suggested algorithm gives a superior computational technique with which the system itself operated on the optimized task scheduling method from the current according to the situation.

The article [10] proposes the load balanced task scheduling using the algorithm “Load Balancing Ant Colony Optimization (LBACO)”. By using LBACO algorithm balance the efficient load balancing reduced makespan is achieved. This scheme handles every situations better than FCFS and ACO strategy. This study [11] proposes a new structure for task scheduling depends on “Dynamic Dispatch Queues Algorithm (DDQA) and Particle Swarm Optimization (PSO)” rules. The proposed architecture minimize the waiting time of tasks and reduces the queue length. It also minimizes the makespan and resources utilization is also good. The proposed algorithm also achieve load balancing and is better than FCFS and PSO policies in cloudcomputing scenario. In [12] authors propose a hybrid model called Multi Label Classifier Chains Swarm Intelligence (MLCCSI) and achieves load balancing. The MLCCSI strategy reduces the makespan and the resource utilization is efficient when compared with other standard optimization methods. In this article, they uses the makespan metric for checking the aptness of the scheduling algorithm and the makespan is reduced between 7% and 75%.

The work [13] proposes a method based on “bacteria foraging and genetic algorithm” to do taskscheduling strategy in cloud environment. The situation is interpreted as a “multi objective optimization problem” and a hybrid BFA method is implemented to achieve Pareto solutions which is optimal. This policy reduces makespan and energy consumption. In [14] an enhanced HEFT algorithm tasks are grouped according to a rank and then allocated to a processor. This allocation of the tasks to the differently abled processor will reduce the makespan. When comparing with existing HEFT and CPOP strategy the proposed HEFT algorithm lessen the makespan and load balancing problems. The work [15] reduce makespan and improve resources utilization of the task scheduling algorithm by applying the PSO strategy and fuzzy method. The suggested “Fuzzy strategy Modified Particle Swarm Optimization (FMPSO)” uses fuzzy method for finding the fitness by giving the inputs like tasks length, speed of processor, memory capacity and required execution time. This algorithm applies 4 enhanced velocity modifying policy to explore large search space. The performance is highlighted by combining crossover and mutation with POS algorithm.

In this article [16] a “Multi-Population Genetic Algorithm (MPGA)” based on loadbalancing task scheduling strategy is presented. This scheduling procedure adopts “min-min and max-min” policy for initializing the populations, Local optimum is furnished by the usage of the Metropolis criterion. It is found that the MPGA-based scheduling strategy out perform TCGA, SAGA in terms of price and time for execution and loadbalancing. In [17] authors propose a “Load balancing and task Completion cost Genetic Algorithm (LCCGA)” which reduces task completion cost and reduce load balancing. This algorithm not only uses variance to represent the load among different units but also uses “multi-fitness function”. From the work it seems that this method minimizes overall cost of task completion, and achieves load balancing efficiently.

The article [18] employs a “monkey search” task scheduling method. It provides better Quality of service and reduces cost of task execution efficiently. Using this technique maximum number of tasks can be finished with less execution time and cost

for communication. It seems that most of the static and dynamic algorithms for resource allocation is not take into account communication delay. Therefore they cannot reduce execution time of big tasks. In this work [19], a superior taskscheduling “Multi Criteria Decision Making (MCDM)” policy using VIKOR method has been proposed. The scheduling fulfillment of backfilling strategy is enhanced by solving the conflicts between the similar tasks. The disputes are arbitrates by applying VIKOR scheme as problem solver. The tasks are ranked by taking into account time for execution and tasks deadline. This work improves resource utilization and rejection tasks get reduced.

The article [20] presents a multiobjective “Taskscheduling using Clonal Selection Algorithm (TSCSA)”. In this taskscheduling is achieved using optimization technique when there is adynamic change in data centers and requests. The proposed TSCSA algorithm energy consumption is reduced 10%–30% and the makespan 5%–25% when compared to other task scheduling algorithm. This article [21] proposes a enhanced optimal method for load balancing. This algorithm pays emphasis to higher priority tasks so that they can be executed earlier. For lower priority requests context switching is reduced by finding the difference between threshold value and time for execution. Then a selection is done between shortest job first and round robin. By this method resource utilization is high and tasks get scheduled according to their priority. The work [22] design a job scheduler which gives rank to different jobs. Here the resource utilization is high and a good system performance is achieved. In this method tasks are scheduled according to their priority and high speed processor will be allocated with bigger tasks. The analysis shows that scheduler that uses ranking method results good performance when compared with other space shared and timeshared job scheduler.

In [23] propose a “Multiqueue Interlacing Peak Scheduling Method (MIPSM)”. In this method divide the tasks to different queues are done. The three queues are: processor bound; input/output bound; and storage bound. Second, sort the resources according to processor loads, input and output wait time, and storage needs. Finally scheduling of tasks in the 3 queues are done with resources whose loads for the processor, input-output and storage is smaller. Load balancing is efficient for this policy. Since this procedure taking into consideration both the stay us of tasks and resources rate of rejection of tasks are very small. Hence load balancing and utilization of resources are effective even for big amount of tasks.

The article [24] propose an efficient scheduling of tasks which uses the concept of backfilling and the deadline metric. For scheduling this strategy considers the current time and gap time of each contract. The current time and gap time are used as scheduling criteria. The amount of lease scheduled is used for finding the system efficiency. This policy does not need any tools of the sort AHP for conflict resolution of same type of lease. The authors in this article [25] proposes scheduling algorithms which will schedule virtual machines and tasks concurrently. Context switching and time for waiting is decreased by applying concurrency. Through this technique the energy consumption and switching delay of packets between VMs decreased. The authors [26] proposes an Improved particle swarm optimization algorithm. In this algorithm adaptive weighting method is used. Using this method can prevent the particle swarm algorithm to be trapped in the local minimum. This algorithm improves resource utilization and completion time.

In [27] authors gives anew authentication method with multi-tier authentication. This model is for private cloud systems. The article [28] on Cloud computing analyses different techniques for preserving privacy in cloud environment.

5 Discussion and Summary

As discussed in Sect. 4 different algorithms offer specific solutions. Some articles are single objective while others are multi objective. Table 2 and Fig. 1 show the distribution of task scheduling metrics in the reviewed articles. Reviewed articles 1, 5, 7, 8, 9, 10, 12, 14, 18, 24, 25 enhance multiple metrics while other articles enhance single metric.

Table 2. Distribution of task scheduling metrics in the reviewed articles.

Reference Cited	Execution time	Makespan/completion time	Load balancing	Processing cost	Resource utilization	Energy-consumption	User priority	Waiting time	Deadline
[2]	O					O			
[3]	O								
[4]		O							
[5]		O							
[6]	O		O			O			
[7]		O							
[8]		O	O						
[9]	O		O				O		
[10]	O		O						
[11]	O						O		
[12]	O								
[13]	O		O			O			
[14]	O								
[15]	O				O				
[16]				O					
[17]				O					
[18]				O					
[19]					O			O	
[20]						O			
[21]							O		
[22]							O		
[23]								O	
[24]								O	
[25]						O		O	
[26]		O			O				
Total	2	13	4	4	3	5	2	3	3

Figure 1 shows that 5% of the referenced journals uses execution time and user priority metric, 33% makespan, 13% energy consumption, 10% load balancing and processing cost, 8% resource utilization, waiting time and deadline. It can be seen that most of them have concentrated on the makespan metrics. Makespan is the most important criteria which determines the efficiency of a scheduling algorithm. Since it is the total of the execution time and waiting time, for a specific processor makespan can

be reduced only by reducing the waiting time. Here comes the role of a good scheduling algorithm.

A better algorithm will decrease the makespan along with load balancing. If the task scheduling considers load balancing then neither processor will be overloaded nor underloaded. Load balancing plays an important role in reducing energy consumption too. Environmental issue is a big challenge to the research community. All efforts to address it are important and could lead to constructive results. The overall performance of cloud system depends on makespan, load balancing and energy consumption.

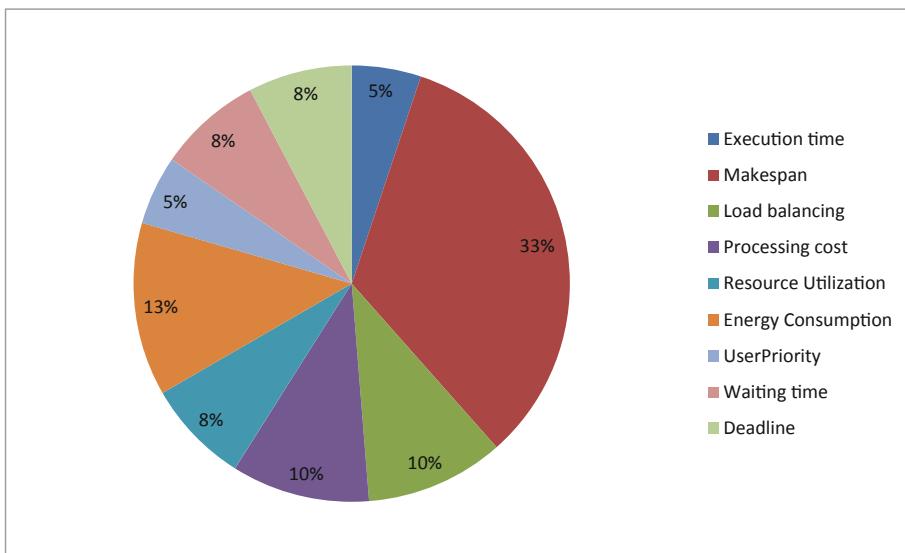


Fig. 1. An overview of metrics addressed by reviewed articles

6 Conclusion

Task scheduling is an essential part of cloudcomputing environment. In this article we reviewed different algorithms for taskscheduling in cloud-environment. We found several metrics for task scheduling algorithms that should be considered in future. Based on our observation, categories of algorithms are summarized in a table. Recently the major concern of computing communities is energy consumption. Software and hardware policies can be found out for minimizing power usage. Therefore future work can be to find efficient techniques to reduce energy consumption.

References

1. Palanivel, K., Kuppuswami, S.: A cloud-oriented green computing architecture for e-learning applications. *Int. J. Recent Innov. Trends Comput. Commun.* **2**(11), 3775–3783 (2014)
2. Ashouraei, M., et al.: A new SLA-aware load balancing method in the cloud using an improved parallel task scheduling algorithm. In: 2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE (2018)
3. Ettikyala, K., Vijayalata, Y., Mohan, M.C.: Efficient time shared task scheduler for cloud computing. In: 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC). IEEE (2017)
4. Chiang, M.-L., et al.: An improved task scheduling and load balancing algorithm under the heterogeneous cloud computing network. In: 2017 IEEE 8th International Conference on Awareness Science and Technology (iCAST). IEEE (2017)
5. Shobana, G., Geetha, M., Suganthe, R.C.: Nature inspired preemptive task scheduling for load balancing in cloud datacenter. In: International Conference on Information Communication and Embedded Systems (ICICES 2014). IEEE (2014)
6. Xue, J., et al.: A study of task scheduling based on differential evolution algorithm in cloud computing. In: 2014 International Conference on Computational Intelligence and Communication Networks. IEEE (2014)
7. Zhang, P.Y., Zhou, M.C.: Dynamic cloud task scheduling based on a two-stage strategy. *IEEE Trans. Autom. Sci. Eng.* **15**(2), 772–783 (2018)
8. Wang, T., et al.: Load balancing task scheduling based on genetic algorithm in cloud computing. In: 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing. IEEE (2014)
9. Mittal, S., Katal, A.: An optimized task scheduling algorithm in cloud computing. In: 2016 IEEE 6th International Conference on Advanced Computing (IACC). IEEE (2016)
10. Li, K., et al.: Cloud task scheduling based on load balancing ant colony optimization. In: 2011 Sixth Annual ChinaGrid Conference. IEEE (2011)
11. Alla, H.B., Alla, S.B., Ezzati, A.: A novel architecture for task scheduling based on dynamic queues and particle swarm optimization in cloud computing. In: 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech). IEEE (2016)
12. Rjoub, G., Bentahar, J.: Cloud task scheduling based on swarm intelligence and machine learning. In: 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE (2017)
13. Srichandan, S., Kumar, T.A., Bibhudatta, S.: Task scheduling for cloud computing using multi-objective hybrid bacteria foraging algorithm. *Future Comput. Inform. J.* **3**(2), 210–230 (2018)
14. Dubey, K., Kumar, M., Sharma, S.C.: Modified HEFT algorithm for task scheduling in cloud environment. *Procedia Comput. Sci.* **125**, 725–732 (2018)
15. Mansouri, N., Zade, B.M.H., Javidi, M.M.: Hybrid task scheduling strategy for cloud computing by modified particle swarm optimization and fuzzy theory. *Comput. Ind. Eng.* **130**, 597–633 (2019)
16. Wang, B., Li, J.: Load balancing task scheduling based on Multi-Population Genetic Algorithm in cloud computing. In: 2016 35th Chinese Control Conference (CCC). IEEE (2016)
17. Yin, S., Ke, P., Tao, L.: An improved genetic algorithm for task scheduling in cloud computing. In: 2018 13th IEEE Conference on Industrial Electronics and Applications (ICIEA). IEEE (2018)

18. Gupta, P., Tewari, P.: "Monkey search algorithm for task scheduling in cloud IaaS. In: 2017 Fourth International Conference on Image Information Processing (ICIIP). IEEE (2017)
19. Nayak, S.C., Tripathy, C.: Deadline based task scheduling using multi-criteria decision-making in cloud environment. *Ain Shams Eng. J.* **9**(4), 3315–3324 (2018)
20. Jena, R.K.: Energy efficient task scheduling in cloud environment. *Energy Procedia* **141**, 222–227 (2017)
21. Tripathi, S., Prajapati, S., Ansari, N.A.: Modified optimal algorithm: for load balancing in cloud computing. In: 2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE (2017)
22. Ettikyala, K., Vijaya Latha, Y.: Rank based efficient task scheduler for cloud computing. In: 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE). IEEE (2016)
23. Zuo, L., et al.: A multiqueue interlacing peak scheduling method based on tasks' classification in cloud computing. *IEEE Syst. J.* **12**(2), 1518–1530 (2016)
24. Nayak, S.C., et al.: An enhanced deadline constraint based task scheduling mechanism for cloud environment. *J. King Saud Univ.-Comput. Inf. Sci.* (2018)
25. Joseph, J., Babu, K.R.: Scheduling to minimize context switches for reduced power consumption and delay in the cloud. In: 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE). IEEE (2016)
26. Luo, F., et al.: An improved particle swarm optimization algorithm based on adaptive weight for task scheduling in cloud computing. In: Proceedings of the 2nd International Conference on Computer Science and Application Engineering. ACM (2018)
27. Sridhar, S., Smys, S.: A hybrid multilevel authentication scheme for private cloud environment. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO). IEEE (2016)
28. Karthiban, K., Smys, S.: Privacy preserving approaches in cloud computing. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE (2018)



Securing Color Image Using Combined Elliptic Curve Crypto-System and Hill Cipher Encryption Along with Least Significant Bit - Steganography

N. Faizal^(✉), S. Sharan, Panchami S. Nair, and Devi S. Sankar

Department of Computer Science, University of Kerala, Kariavattom,
Trivandrum, Kerala, India

faizalnr@gmail.com, sharan956211@gmail.com,
panchunair555@gmail.com, chinnu27oct1996@gmail.com

Abstract. Security of information is becoming main criteria while transferring information through communication networks. Nowadays images are used as information source; therefore its security from unauthorized or unintended access is important. Image encryption play an important role in protecting images from hacking and stealing while sending over an unsecured channel. The proposed method is a combination of encryption using Hill cipher algorithm along with Elliptic curve for enhanced security. Elliptic curve cryptographic method is used to make the system to asymmetric from the less secured symmetric key encryption technique; hill cipher algorithm. In our proposed method we use both grayscale images as well as color images regardless its size. Steganography of actual image with a cover image before encryption is an advantage. The cover image is selected as it mocks like an informative to unauthorized access. Least Significant Bit (LSB) steganography method is used here as it provides more security than any other methods.

Keywords: Image encryption · Visual cryptography · Hill cipher · Steganography · Elliptic curve cryptography

1 Introduction

Nowadays cryptography is done with mathematical principles and computer science practice other than the earlier techniques which was effectively synonymous with encryption. That makes enhancing the security for images from attacks. Encryption and Decryption are the key concepts in cryptography. Image encryption can be defined in such a way that it is the process of encoding secret image using an encryption algorithm so that unauthorized access can be prevented. Decryption is the process of unlocking the encrypted image. The two different encryption techniques are symmetric Key encryption and asymmetric key encryption. In symmetric key encryption uses a single secret key for encryption and decryption process. If you want to share the encrypted data with someone, share the key used for encryption with the receiver. In asymmetric key encryption each person has their own two keys, a public key, which is shared and a

private key. Something encrypted with the public key can be decrypted with the private key of same user, and vice versa.

In our proposed method Encryption and decryption are done to encrypt and decrypt color images as well as grayscale images irrespective of its size while sending it through the internet. Hill cipher along with Elliptic curve cryptography is used for encryption and decryption. As hill cipher is a symmetric key encryption technique, it can be converted into asymmetric one by using elliptic curve function. For providing additional security steganography technique is done with the actual image. A cover image is concealed with the input image. This is done by Least Significant Bit (LSB) steganographic technique which does the substitution of the 4 Most Significant Bits (MSB) of the secret image with the 4 LSBs of the cover image. The stegano-image will be encrypted and send over the network.

2 Proposed Methodology

2.1 Existing System

The existing system is applicable for the grayscale images only. In this the encryption is done for the images that have equal height and width and the multiple of 4, therefore it is not possible to encrypt images with different sizes or a preprocessing of input image to a fixed size is followed. One of the main drawbacks is weak security as the image is encrypted without any modification; the decrypted image will directly gives the secret share.

2.2 Proposed System

The current system is designed to do the encryption and decryption only with pre-fixed size gray scale images. Our proposed system works regardless of sizes or color as well as gray scale images. Here encryption and decryption on image are performed by using elliptic curve and hill cipher technique. Steganography technique improves the security of our system. The combination of the both encryption techniques makes security higher. First we hide the image into a cover image and then convert this resulting stegano-image into encrypted image using cryptography. The resulting image contain secret message will be transmitted over the network without revealing the existence of secret communication. Only the authorized and the valid user can detect the stegano-carrier and read the message.

2.3 Our Methodology

2.3.1 Selection of Input Image and Cover Image

For sending the image securely through the communication channel, we should firstly input the image that user want to send to the receiver. For this select an image which may be color image or gray scale image with any size. After selecting the input image then select a cover image (back ground image). The purpose of selecting the cover image is to increase the security of sending the image through unsecured network. The sample image must be selected from the same field as the input image is selected.

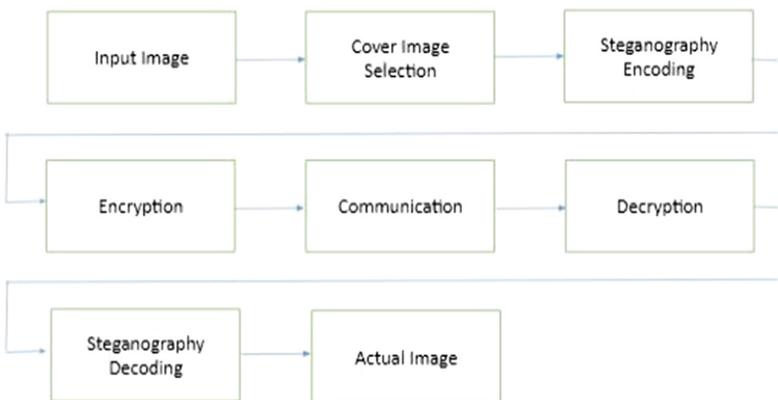


Fig. 1. Basic block diagram for the secure transmission using proposed methodology

2.3.2 Steganography

In image steganography, the image that contains the secret information is called cover image. The secret information may be any digital file. In order to achieve proper steganography communication the secret key should be properly communicated to the receiver while hiding the data into cover image. The steganography empowers information security by embedding secret message inside digital image, altering or modifying the nonessential pixels of the image. Steganography became important application in different areas especially military and intelligence agencies. Steganography differs from cryptography in the way how they exists and feels. Cryptography does to keep the contents of a secret message by modifying the contents or values; but the steganography focuses on hiding the presence of a secret message in an image. Steganography focus on preventing an unintended recipient from suspecting that some hidden data is present in the received image. A combination of steganography and cryptography is used to improve information security.

2.3.2.1. RGB Color Model

Here we will work with RGB color model. The RGB color model represented using the initials of the three primary colors red, green, and blue. Pixels are represented by three 8-bit values (the range is 0–255), each represents Red, Green and Blue values respectively. The pixel value will be the combined intensity of R, G and B values.

2.3.2.2. Least Significant Bit (LSB) Steganography

LSB based technique is most simple and direct approach in which secret message bits are used to store the cover image substituting its Least Significant Bit (LSB) of each pixel. In a digital image each pixels have three values, which can be represented in 8 bit binary code. When working with these binary codes, there will be some bits which are more significant and the remaining will be less significant with the image representation. This can be easily understood from the Fig. 1.

Considering an 8 bit code the significance of values contributed with pixels will be decreasing from MSB to LSB. The Leftmost bit (MSB) will be contributing half of its feature. That means a change in value makes higher impact as we read from right to left.

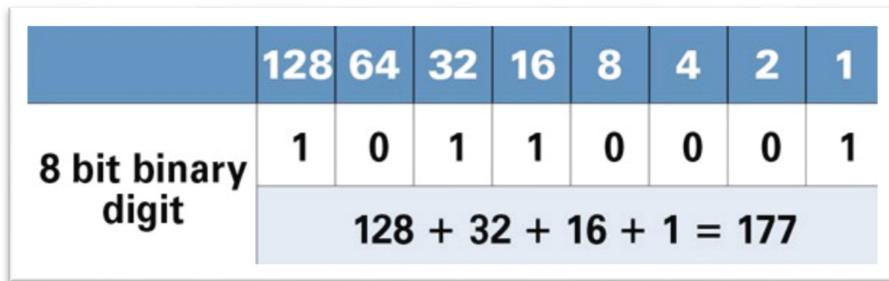


Fig. 2. An 8 bit binary number and its bitwise contribution to the pixel value.

For example, changing leftmost bit from 0 to 1 (01111111 to 11111111); it will change the decimal value from 127 to 255. A change in rightmost bit will make very less impact on the actual value. For example, changing the rightmost bit from 0 to 1 (11111110 to 11111111) will change the decimal value from 254 to 255. Same effect will be applicable to images also. A change in rightmost bits it will have a small visual impact on the actual image. This is the location to hide a data inside another in steganography, replacing least significant bits from an image with most significant bits of secret image (Fig. 2).

2.3.2.3. Least Significant Bit (LSB) Steganography Algorithm

The LSB steganography encryption method follows combining two images in a process of substituting the lower 4 bits of 8 bit pixel value of cover image using the 4 bit higher bits (Most Significant Bits) of consecutive pixel from secret image. This method is a lossy encryption method but have low impact on the actual secret image (Fig. 3).

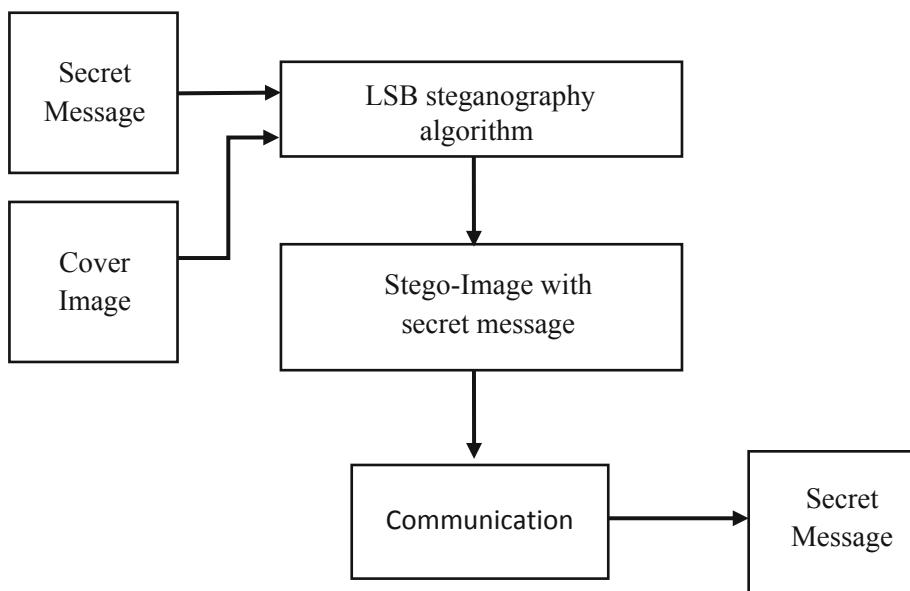


Fig. 3. Steganography block diagram

LSB-based Encoding Algorithm

Step1. Read cover image C & secret image S.

Step2. Equalize size of C & S, say L.

Step3. For i from 0 to (L-1) do,

$$C[5:8] = S[1:4];$$

(repeat for R, G & B values)

Step4. Send stegano-image as C.

LSB-based Extracting Algorithm

Step1. Read stegano- image R.

Step2. Compute size of R as L.

Step3. Initialize sample image with all pixel values as 0.

Step4. For i from 0 to (L-1) do,

$$S[1:4] = R[5:8] \& S[5:4]=0000;$$

(repeat for R, G & B values)

Step4. Retrieved secret image as S.

This steganography method selects the cover image selected suited with the input image for encryption. The cover image will be in same size of secret image. In RGB model, the 4 LSB values of R, G and B components of corresponding pixel from cover image are substituted with the 4 MSB values of R, G and B components of secret image. This can be easily understood from Fig. 4.



Fig. 4. LSB steganography processing for single RGB pixel.

2.3.3 Encryption and Decryption

Steganography encrypted image will be given for encryption and the secret image in encrypted for will be send over the network and the receiver decrypts the image and does the steganography decryption to get the actual data. Here we use Elliptic curve

method for encrypting the data (image here) and the secret key for encryption is secured by using hill cipher standard.

2.3.3.1. Elliptic Curve Cryptosystem

Elliptic curve cryptography (ECC) is an encryption technique most commonly used in embedded systems, portable devices, and mobile devices as it provides better security even with smaller key size, does simple computations with lower power and memory consumptions (Fig. 5).

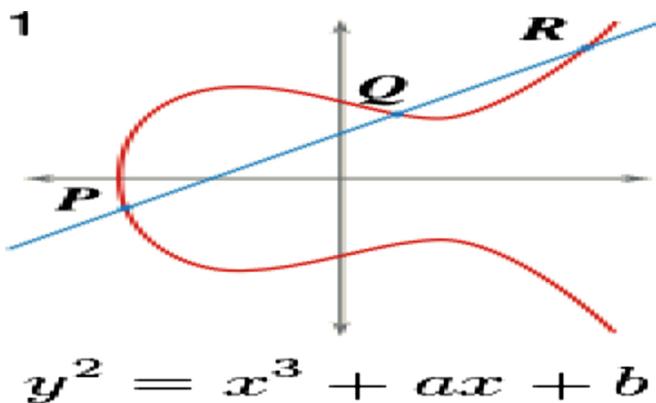


Fig. 5. Elliptic curve model

2.3.3.1.1. Definition

An elliptic curve E over a prime field F_p is defined by $E: y^2 \equiv x^3 + ax + b \pmod{p}$.

Where $a, b \in F_p$, $p \neq 2, 3$ and satisfy the condition $4a^3 + 27b^2 \equiv 0 \pmod{p}$. The elliptic curve group $E(F_p)$ is the collection of all points (x, y) that satisfy the elliptic curve E and pointing at the infinity. Scalar multiplication is the basic operation included in elliptic curve system which utilizes a good portion of encryption and decryption operations; it depends on the point addition and point doubling.

2.3.3.1.2. Point Addition

Consider $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ that lies on the elliptic curve, E . The point R obtained by doubling the point P , which is also a point on the same elliptic curve E and this process is named Point Doubling.

$$R = 2P = P + P = (x_3, y_3)$$

Where $x_3 \equiv (s^2 - 2x_1) \pmod{p}$, $y_3 \equiv (sx_1 - sx_3 - y_1) \pmod{p}$ and $s = \frac{3x_1^2 + a}{2y_1} \pmod{p}$

2.3.3.1.3. Scalar Multiplication

The scalar multiplication of an integer k by the point $P = (x_1, y_1)$ that lies on the curve E can be defined by repeating the addition of the point Q to itself k times. The result point R also lies on the elliptic curve E .

$$Q = kP = P + P + \dots + P \text{ (k-times)}$$

For example, computing $22P$ can be obtained using point addition and scalar multiplication as follows.

$$22P = 2(3(2P + P) + P) + 2P$$

2.3.3.2. Hill Cipher Algorithm

Hill Cipher is a symmetric key encryption technique proposed by the mathematician Lester Hill in 1929. Ciphering and deciphering uses same key matrix by sender and receiver. Hill Cipher technique is working on assigning each character by a numeric value, like, $a = 0, b = 1 \dots z = 25$. The plaintext or secret message is then divided into blocks of size m based on the key matrix of size $m \times n$. For example, for a key matrix of size 2×2 , the block size will be 2, and the encryption will be done to produce cipher text block with two numerical values as follows:

If $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ and $K = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$ then

$$C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \bmod 26 = \begin{bmatrix} (k_{11}p_1 + k_{12}p_2) \bmod 26 \\ (k_{21}p_1 + k_{22}p_2) \bmod 26 \end{bmatrix}$$

The recipient will have a key matrix which is the inverse matrix of encryption key matrix. For an encryption key, K the decryption key will be (K^{-1}) where $K \cdot K^{-1} = I$, the identity matrix. By using the key the deciphering is done to produce the original secret message, P (plaintext) as follows. $P = K^{-1} * C \bmod 26$.

2.3.3.3. Elliptic Curve Cryptosystem and Hill Cipher (ECCHC)

The combination of Elliptic Curve Cryptosystem with Hill Cipher increases the security. This combination improves the system more efficient than the simple Hill cipher technique; also it simplifies the decryption computations because it avoids key matrix inverse computation. Assume the user- M (the sender) needs to transmit an image I to the other party user-N (the receiver) using ECCHC method over an unsecured channel. Initially, the sender and receiver should agree on an elliptic curve function E and share the encryption parameters $\{a, b, p, G\}$, say domain parameters; where p is a large prime number, (a, b) are elliptic function coefficients, and G is the generator point. Then the sender and receiver selects their private key from the interval $[1, p - 1]$; Q_N for user N and Q_M for user M, and generates their public key as follows

$$P_M = Q_M * G \quad P_N = Q_N * G$$

The initial key will be formed by multiplying their own private key with the public key of the other user, say $K_1 = (x, y)$ as follows,

$$K_1 = Q_M * P_N = Q_N * P_M = Q_M * Q_N * G = (x, y)$$

$$\text{Then computes } K_1 = x * G = (k_{11}, k_{12}) \quad K_2 = y * G = (k_{21}, k_{22})$$

The next process is to generate the secret key matrix K by the sender and the receiver. The problem arrives when the key matrix is not invertible; which means inverse of the key matrix does not exist. So the decryption of the cipher text will not be possible for that case. To solve the problem, a matrix which is self-invertible will be selected as key (the K is self-invertible matrix if $K = K^{-1}$), and encryption and decryption can be done with the same key, and it avoids inverse key matrix calculation. So the image is segmented to blocks of size four, each value representing a pixel. Thus the sender as well as receiver produces 4×4 self-invertible matrix key, K_m by using the proposed method.

$$\text{Let } K_m = \begin{pmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{pmatrix}$$

Then the values of the other partitions of the secret matrix key K_m is obtained by solving $K_{12} = I - K_{11}$, $K_{21} = I + K_{11}$, and $K_{11} + K_{22} = 0$, where I is the identity matrix.

Separate the message (pixel values) into blocks of size four, then each block can be converted to a 4×1 vector, say $(P_1, P_2, P_3 \text{ and } P_4)$. Then multiply each of these vector with the self-invertible key matrix, K_m . The ciphered vectors $(C_1; C_2; C_3; C_4)$ can be generated by taking modulo 256 of previous vector result. Repeat the process to all the pixel blocks. The ciphered image C can be formed using the ciphered vectors and transfer over the network.

The following calculations are repeated for each block:

$$\text{The proposed approach assumes that } K_1 = \begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \text{ and } P_1 = \begin{pmatrix} p_{11} \\ p_{12} \\ p_{21} \\ p_{22} \end{pmatrix}.$$

$$C_1 = (K_m * P_1)256 = \begin{pmatrix} (k_{11}p_{11} + k_{12}p_{21} + k_{13}p_{31} + k_{14}p_{41}) \bmod 256 \\ (k_{21}p_{11} + k_{22}p_{21} + k_{23}p_{31} + k_{24}p_{41}) \bmod 256 \\ (k_{31}p_{11} + k_{32}p_{21} + k_{33}p_{31} + k_{34}p_{41}) \bmod 256 \\ (k_{41}p_{11} + k_{42}p_{21} + k_{43}p_{31} + k_{44}p_{41}) \bmod 256 \end{pmatrix} = \begin{pmatrix} c_{11} \\ c_{12} \\ c_{21} \\ c_{22} \end{pmatrix}$$

The decryption process by the recipient on the ciphered image C starts by dividing the image pixel values into blocks of size four then separates each block into four rows column vector. After that, multiplying the self-invertible key matrix K_m by each vector (C_1, C_2, C_3, \dots) and taking modulo 256 to get the plain image vector (P_1, P_2, P_3, \dots) that construct the original image.

2.3.3.4. The Proposed Approach (ECCHC)

2.3.3.4.1. Key Generation (Both Sender and Receiver Side)

- Choose the private key $Q_A \in [1, p - 1]$ and $Q_B \in [1, p - 1]$.
- Compute the public key $P_A = Q_A * G$ and $P_B = Q_B * G$.
- Compute the initial key $K_1 = Q_A * P_B = (x, y)$ and $K_1 = Q_B * P_A = (x, y)$.
- Compute $K_1 = x * G = (k_{11}, k_{12})$ and $K_2 = y * G = (k_{21}, k_{22})$.
- Combine K_i values to form self invertible key K .

2.3.3.4.2. Encryption (User A)

- Segment the pixel values of secret image into blocks of size four.
- Represent each block into single column vector (4×1).
- Multiply each vector (P_1, P_2, P_3 & P_4) with the self-invertible key matrix K_m and take modulo 256 for each value $C_1 = (K_m * P_1) \bmod 256$.
- Combine these vectors (C_1, C_2, C_3, \dots) to form the ciphered image.

2.3.3.4.3. Decryption (User B)

- Segment the pixel values of received image into blocks of size four.
- Represent each block into single column vector (4×1).
- Multiply each vector (C_1, C_2, C_3 & C_4) with the self-invertible key matrix K_m and take modulo 256 for each value $P_1 = (K_m * C_1) \bmod 256$.
- Combine these vectors (P_1, P_2, P_3, \dots) to form the ciphered image.

3 Result Analysis

Here the sender embeds the secret image with cover image using LSB steganography then encrypts using hill cipher and elliptic curve algorithm. The encrypted image will be transmitted over the network. The cover image will be selected as it mocks like actual data. For e.g. Sending a location secretly can embedded with image of some another location, which makes mislead to someone illegally retrieves it. (here in output comparison a rose flower is embedded inside another image of rose flowers). The actual image send and the image retrieved by the receiver will have a maximum variation for each pixel will be 5% loss.

3.1. Sender Side



Input image



Cover image



Stegano- image



Encrypted image

3.2. Receiver Side



4 Conclusion

We conclude our study as the extended version of the “image encryption technique with elliptic curve cryptosystem and hill cipher “which deals with only gray scale images and images of size 4×4 only. But the proposed system will deals with both gray scale images as well as color images regardless of size. Here we perform both encryption and decryption using elliptic curve and hill cipher technique. We added steganography to enhance security. Steganography is used to hide secret image inside another image. The encryption is performed on this stegano-image. The receiver accepts this encrypted image and performs decryption first, then performs steganography decoding to retrieve the original image from the cover image. The advantage of our system is that it doesn’t reveal the existence of a secret image to non-authorized or non-valid user. At the same time the authorized user have the idea of the secret image and he/she can retrieve it from the cover image. We can further improve this system by using more secure cryptographic techniques or their combinations and also by providing more secure mechanism for the transfer of keys.

References

1. Acharya, B., Rath, G.S., Patra, S.K., Panigrahy, S.K.: Novel methods of generating self-invertible matrix for hill cipher algorithm. *Int. J. Secur.* **1**, 14–21 (2007)
2. Acharya, B., Panigrahy, S.K., Patra, S.K., Panda, G.: Image encryption using advanced hill cipher algorithm. *Int. J. Recent Trends Eng.* **1**, 663–667 (2009)
3. Foster, I., Kesselman, C.: *The Grid: Blueprint for a New Computing Infrastructure*. Morgan Kaufmann, San Francisco (1999)
4. Agrawal, K., Gera, A.: Elliptic curve cryptography with hill cipher generation for secure text cryptosystem. *Int. J. Comput. Appl.* (2014)
5. Alese, B.K., Philemon, E.D., Falaki, S.O.: Comparative analysis of public-key encryption schemes. *Int. J. Comput. Appl.* **2**(9), 1552–1568 (2012)
6. Bokhari, M.U., Shallal, Q.M.: A review on symmetric key encryption techniques in cryptography. *Int. J. Comput. Appl.* (2016)
7. Darrel, H., Alfred, M., Scott, V.: *Guide to Elliptic Curve Cryptography*, p. 11. Springer Professional Computing Series. Springer, Heidelberg (2004)
8. Dawahdeh, Z.E., Yaakob, S.N., Othman, R.R.B.: A new modification for Menezes - Vanstone elliptic curve cryptosystem. *J. Theor. Appl. Inf. Technol.* **85**(3), 290 (2016)

9. Diffie, W., Hellman, M.: New directions in cryptography. *IEEE Trans. Inf. Theory* **22**(6), 644–654 (1976)
10. Sateesh, G., Lakshmi, E.S., Ramanamma, M., Jairam, K., Yeswanth, A.: Assured data communication using cryptography and steganography
11. Chikouchen, S.L., Chikouche, N.: An improved approach for LSB-based image-steganography using AES algorithm. Computer Science Department, University of M'sila, Algeria
12. Anurag, Meena, S.: Color image steganography using random key matrix. National Institute of Technology (2018)
13. Mitasha, R.J., Christainbach: Information hiding in images using steganography techniques. University of Zakho, Iraq
14. Cimato, S., Yang, C.-N.: Visual cryptography and secret image sharing. CRC Press. ISBN 978-1-4398-3721-4
15. Yang, C.N., Chen, T.S., Yu, K.H., Wang, C.C.: Improvements of image sharing with steganography and authentication. *J. Syst. Softw.* **80**, 1600–16010 (2007)



Comprehensive Study of Existing Stream Ciphers

S. Chaithanya¹(✉) and V. Anitha²

¹ Department of ECE, Rajarajeswari College of Engineering, Bangalore, India
chaithanya06@gmail.com

² Department of ECE, Dayananda Sagar College of Engineering,
Bangalore, India
anithavijaya@gmail.com

Abstract. Now a day's internet of things is one of the rapidly growing research field in the information technology domain. Offering security for this ever-augmenting technology is still remaining as the challenging task. Cryptographic techniques are used to authenticate and maintain confidentiality of message data. To maintain the security, system cryptographic algorithms and protocols are very essential. The system is mainly categorized into two groups namely stream cipher and block cipher. Stream cipher has its own advantage over block cipher. In this paper, we reviewed some of the stream ciphers. Selection of finest algorithms for the security of internet of things is very difficult in terms of energy and storage. The study aims to summarize some of the existing stream cipher techniques. This paper gives details on fundamental knowledge about encryption algorithms and its comparison. We also describe the design considerations of stream ciphers.

Keywords: Cryptography · Security · Stream cipher · Block cipher · Internet of things · Encryption algorithms

1 Introduction

Over the most recent couple of years, Internet of Things (IoT) is quickly making progress in the region of remote interchanges and systems administration. The essential thought is the interconnection of heterogeneous objects such RFID labels, sensors, cell phones, wearable, and so on. These heterogeneous objects communicate to achieve shared objectives. Each associated objects has its own identity on the Internet. Wireless Sensor Networks are considered as one of genuine and best IoT applications network. They cover a wide application area for the IoT, for example, Home automation, smart transport, business, industrial applications, military, healthcare, power management and so on.

Currently Most of the IoT implementations have unique security challenges. IoT device and service protection is the main challenge. The customer's belief these gadgets and associated services are secure from Fragility. The unsecured IoT devices and services are the doorway to the cyber attack. So it requires a strong and reliable authentication algorithm to prevent this. It is important to use cryptography in countless

regions in technology to secure the data. One of the most important region it includes internet of things.

The message data being transmitted with confidentiality will constitute as an idea of security. Cryptography is one of the scientific based ways to deal with information security. Likewise it is a learning of technique for guarantee the privacy and security aspects such as confidentiality, data integrity, and authentication of the information. Encryption and decryption are the two major part of cryptography. Encryption is going to convert input message to scribbled form and decryption is converting back this in to original form.

Mainly our cryptosystem is divided in to two types of Encryption form based on the number of keys employed, they are one is symmetric key ciphers and the other is asymmetric key ciphers.

Symmetric key cipher:- The algorithm uses identical key for both encryption and Decryption.

Asymmetric key cipher:- The algorithm uses two un identical keys called public key and private key for encryption and decryption.

There are two kinds of symmetric key ciphers, stream cipher and block cipher.

Stream cipher encryption algorithm which encrypts one bit or byte at a time. Plain-text bits or byte combined with keystream sequence with exclusive-or operation. It encrypts plain text digit one at a time. Simplicity of execution and Lack of error propagation are the advantage of stream cipher. The encryption and decryption process of stream cipher shown in Fig. 1.

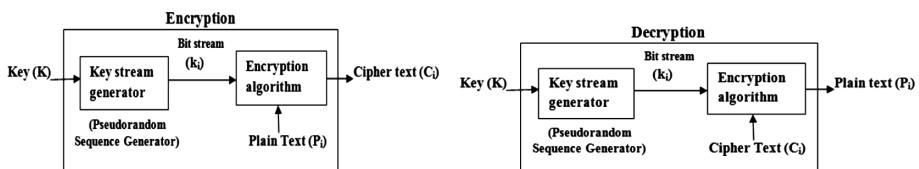


Fig. 1. Encryption and decryption of stream cipher.

Block cipher is an encryption algorithm which encrypts group of data bits at a time. It operates on blocks of fixed lengths. The input message is broken down in to blocks and these blocks encrypted individually with the same key. Since same key is used, it produces same cipher text for the repeated input message this is one of the drawback of this cipher. The encryption and decryption of Block cipher is shown in the Fig. 2.

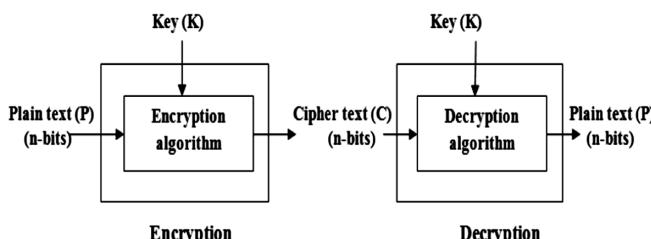


Fig. 2. Encryption and decryption of block cipher

Some of the comparison between Stream cipher and Block cipher is listed down in Table 1.

Table 1. Comparision between stream and block cipher

Stream cipher	Block cipher
Encrypts single bit or byte at a time	Encrypts one block at a time (group of n bits)
Suitable for hard ware implementation	Easy to implement in software
Produces distinguishable cipher for repeated plaintext since like parts of Message vector are encrypted with different parts of the key streams	Produces same cipher text block for the repeated plain text since same key is used in encryption of blocks
Transmission error in one block affect more than one block	Transmission errors only affect that particular block
Compare to block cipher it is somewhat slow	Faster than stream cipher
Key stream generation is dependent on message stream	Key is independent of message stream

Cryptanalysis:

Cryptanalysis is technique of obtaining a plain text by the study of ciphertext, without access to the secret information. cryptanalysis is having an intention to defeat the system by analyzing the ciphers and the cryptosystem without knowledge of encryption key, plaintext source or encryption algorithm. Some of the cryptanalysis techniques for stream cipher are listed down.

Correlation Attacks, Time-Memory Tradeoff Attack, Algebraic Attack, Divide & Conquer Attack, Distinguishing Attack, Dedicated Attacks, The Slide Attack, Statistical Attacks, Linearization Attacks, Re-Synchronization Attacks, Trade-Off Attacks, Guess and Determine Attacks, Linear Approximation Attacks, Related-Key Attacks, Cube Attacks, Fault Attacks, Exhaustive Key Search Attack, Side Channel Analysis Attack etc.

2 Design Considerations

From the definition we know that Stream cipher will encrypt byte by byte. Some of the design considerations for stream cipher is given below.

- Generation of a pseudorandom sequence based on encryption key is the primary scheme in the process of stream cipher.
- Cipher text will be obtained just by XORing the plain text with the pseudorandom stream bytes in the process of encryption.
- Continuously a new stream of pseudorandom sequence should be generating for the encryption of every plain text bytes.

- In decryption the plain text is obtained by XORing cipher text with the pseudo-random sequence byte. But same pseudorandom sequence should be generated as that we used in the process of encryption.
- Different encryption keys will produce different pseudorandom sequences. But same pseudorandom sequence will be used at both encryption and decryption end.
- At some particular point pseudorandom sequence generator will repeats the numbers. To increase the security of the stream cipher, the period of the pseudorandom sequence must be as long as possible.
- the encryption key should be as long as possible, with respect to practical limitations. Longer the key size makes the stronger encryption but the more extended key size also results in complex encryption process.
- With a well designed pseudorandom sequence generator, the Stream cipher will be considered as secure as block cipher with the same key size.

The simple logic is that we would get same ciphertext for the identical plaintext. If we want to reuse the key it may leads to an information leakage about the plaintext. To avoid this An IV is required for any symmetric cipher if you want to reuse the key. That to in stream ciphers encryption was done just by XORing the key stream with the plaintext. If an identical message found an cryptanalyst can easily break the code even though the key should still be secure. Therefore for most stream ciphers it is enough to supply a nonce. the IV is this nonce. As long as a unique nonce is given the key stream will be indistinguishable from random.

Some ciphers [20] such as RC4 do not accept an IV. In that case a unique key must be generated. In most cases it is then possible to simply concatenate key and IV as to generate a key stream indistinguishable from random.

Guessing one bit of one message automatically reveals the bit in the same position in the other message. The remedy is to ensure that the same keystream is never used twice. This can be done by ensuring that the key is only ever used once, or by incorporating a nonce (an IV) in the way the keystream is derived from the key.

3 Literature Review

The idea to build an infinite pseudorandom sequence using a finite-length random sequence, Ashouri [1] proposed a new stream cipher PALS designed as a clock-controlled combination generator with memory. The initial vector of 1600 bits is generated by combining the 256 bit main key with the message key. LFSR with the length of 32 bits is used to generate a message key. A 32 bit message key undergone stream-5 function eight times to achieve 256-bit sequence. The session key is obtained by bitwise XORing the resulting 256-bit sequence with the main key. The main key changeover period in this structure is up to 4.25 years. Keystream generation in PALS algorithm is based on system theory and complete random sequences. PALS is resistant to various types attack.

Ali et al. [2] designed Oppel-2 is a small and fast stream ciphers. It outturn the pseudorandom keystream by concoction of FCSR and output function. In many applications the Individuals from this group is comfortable to give an appropriate

security within the margin. It is applicable to restricted source implementation of hardware and rapid programming oriented operations. This is established on GFCSR with larger length to generate l-sequence pseudorandom generator and function F to conceal the numerical properties of l-sequences. security of 2^{64} , 2^{80} and 2^{128} primitive operations are achieved by the associates of this group.

For hardware applications Berbain et al. [3] designed DECIM with limited resources. DECIM comes under, a synchronous stream cipher, DECIM structure use Key and IV of 80 and 64 bit respectively with 192 bit internal state. Binary addition of input message and keystream gives output. The system consisting of LFSR, non-linear Boolean function and an irregular decimation mechanism ABSG which is similar to SG (Shrinking Generator) and SSG (Self-Shrinking Generator). It operates at a rate of 1/3 with one input sequence. The buffer is required to regulate the constant throughput because of the uneven rate of ABSG mechanism. This mechanism begins at the start of the round and empty buffer. When the buffer full, The keystream generation process will starts.

Ghafari et al. [5] designed Fruit-80 is obtained as a improved or concluding version of the Fruit stream cipher, to obtain a security level of 80 bits. Fruit-80 is going to employ LFSR and NFSR of size 80 bits. The inner position of cipher consist of 43 bit LFSR, 37 bit NFSR and 7 bit counter. The structure includes a secret key size of 80 bits and an initial value of 70 bits. One key and IV pair can produce keystream sequence with a upper limit of 2^{43} . It is not good enough to reuse IV. To overcome the drawbacks associated in fruit stream cipher, fruit 80 encounter the two measures in the design of fruit 80 such as Weaving of IV forever and beneath every key designing finite number of keystream bits.

Lizard is a recent lightweight stream cipher introduced for power-constrained devices like passive RFID tags to overcome the security limitation of many classical stream ciphers due to TMDTO attacks. This is designed by Hamann et al. [6] The motivation for the design is Grain ciphers. The internal state of Lizard consist of two interconnected feedback shift registers. Whereas grain uses one LFSR and one NLFSR of similar length but Lizard uses two NFSRs of different lengths. By combining the Grain-like design with the FP(1)-mode it achieves hardware efficiency. 128 bit key, 64 bit IV and an internal state of 121 bits length were used by this cipher to achieve 80-bit security against key recovery attacks. it permits to create up to 2^{18} keystream bits for each key/IV pair which would be adequate for some current communication situations like Bluetooth, WLAN or HTTPS. One of the important problem with this cipher is that a large guaranteed period of the internal state is necessary but not sufficient for a large guaranteed period of the keystream.

Predominantly in web SSL/TLS, WEP an RC4 is used because of its simplicity efficiency and speed designed by Mantin [20]. It has two main functional blocks. Firstly by jumble the input vector with a random key produces IV of 256 byte in Key Scheduling Algorithm. The transformed internal state keystream are created in Pseudo Random Generation Algorithm. This produces ciphertext by XOR with the plaintext. One of its drawbacks includes that first byte produced by RC4 spills data about individual key bytes. Since RC4 is a byte oriented hence it is futile overload for present processors. Hence the Paul et al. [21] made Quad-RC4 with some modifications to RC4

destroying the conventional RC4 structure to meet the security requirement of present day scenario.

Hell et al. [7] designed and implemented Grain Cipher with little hardware usage. This structure consisting of three basic building blocks, are nonlinear output function, LFSR and NFSR. Output is obtained by 64 bit initialization vector and 80 bit key usage. It is a stream cipher of bit align in its easiest usage it produce 1 bit/clock. By using some additional hardware increase the rate up to 16 bits/clock. Since the key size of 80 bits are not sufficient in secure applications because the TMDT attack would have a computational complexity $O(2^{40})$. To overcome this drawback by retaining the advantages of grain Hell et al. [8] propose a new stream cipher named Grain-128 with a IV of 96 bits and a key of 128 bits. The unique feature of this family of cipher is that easy to implement in hardware, and simple to enhance the speed with additional hardware. The 128 bit key is loaded to NFSR elements and the early 96 bits of LFSR are filled with IV and the next followed 32 bits filled with unit vector. Without creating any keystream the system is clocked 256 times.

Biryukov et al. [9] describes the idea of leak extraction from block cipher to make stream cipher. He thought to generate the output key stream by extracting the some portion at the inner state at some particular rounds. LEX is using AES cipher in simple manner. The key stream of 128 bits and an initialization vector of 128 bits is initially encrypted by a single AES, $S = \text{AESK}(IV)$. The 128 bit S and secret key K makes the 256 bit secret state. The output and its frequency will depend on proper location of the four bytes. Just with little changes of AES implementation can be reused.

By exploiting the fundamental design structure from stream cipher SNOW 2.0, Kuznetsov et al. [10] designed STRUMOK cipher to improve security and the proficiency perspectives of SNOW2.0. The 512 and 1024 bits are most conceivable key sizes to portray the system. It is an additive cipher using words. The construction speed of pseudo-random sequence can lift by the use of vigorous 64-bit processing frameworks. The creative keystream generation process is used without any complex calculations. Realization of LFSR with pre-computation table is increase the speed of the system.

ABC is a synchronous stream cipher designed by Anashin et al. [11] with high speed adaptable features for software applications. It has a key of 128 bit and IV of 128 bit with 32 bit non-linear filter, adaptable key extension, adaptable and quick IV setup methods. It present a security level of 2^{128} . This cipher make use of some thoughts of p-adic dynamical systems theory which were introduced as a T-functions in cryptosystem. ABC have state transition function as well as output function is being adapted while encrypting. High flexibility, high performance with good security assets are the advantages of this cipher.

Ping pong-128 is derived from the same tribe of ciphers by Lee and Chen [12]. LM-type summation generator is used by the keystream generator of this class with a mutual clock- control mechanism. It has L_a and L_b , two LFSRs having a length of 127 and 129 bits with collective clocking and one bit memory C. To get the uncertain output the functions f_a and f_b give numerous clocks to farther LFSRs. It achieves a security of 128 bits by a key size and an initialization vector of size 128 bits with an internal state of 257 bits. Security analysis in terms of keystream properties and mutual clocking is shown in this paper and it prevents known security attacks.

Achterbahn is a binary additive stream cipher proposed by Gammel et al. [13]. The cipher text Ct is obtained by adding the plaintext Pt with the binary pseudo-random sequence as a keystream. This keystream generator is designed by 8 binary nonlinear feedback shift registers of size 22 to 31 and a 4th order Boolean function R: $F_2^8 \rightarrow F_2$ of degree 3. The NLFSR's are gifted with adjective linear feed forward functions. Group of 2^{64} different paraphrase binary sequence can be deliver from the keystream generator, its period is more than 2^{207} having a linear complexity greater than 2^{85} . Keystream generator allows high-speed implementation Because of quick equipment of fundamental feedback shift registers in which one byte of keystream is generated per clock cycle that cycle can be used to encrypt all eight lines of a bus in real time.

Salsa 20 is designed by Bernstein [14] to encrypt the data efficiently by using Salsa20 encryption function by using the strong cryptographic function Salsa20 hash function. The salsa 20 hash functions have addition, XORing and constant-distance rotation of 32 bits. 64 byte is taken as an input and 64 byte as an output. The encryption procedure employing the expansion function. Nonce, key and the block numbers are the basic contributions to this function. Then the XOR operation is used to get the output.

Chacha8 is derived from salsa20 family of stream ciphers [15]. It is a 256-bit stream cipher with 8 rounds. Chacha8 follows has fundamental tasks like Salsa20 with an alternate request to improve the measure of diffusion in each round. Addition, XORing and constant distance rotation of 32-bit words for 16 times. In correlate with salsa20, four addition, XOR and rotations are used to update four 32-bit state words different order. ChaCha accomplishes a similar programming speed as Salsa20 and still better in some other platforms.

To get the adjustable balance between speed and area De Cannière [16, 17] designed Trivium. Since speed and area are the important factors in the design of a system. It is a synchronous stream cipher mainly designed for hardware applications, to produce up to 264 key stream bits the structure uses The secret key of 80 bit length and an initialization vector of 80 bit length. This procedure comprises of two stages, by employing the key and IV initially the internal state of the system is initialized. The next state is periodical refreshing to produce the keystream bits. Second state is repeatedly updated and used to generate key stream bits. To produce the desired number of keystream bits the system comprises of 288-bit internal state shift register. To process 1 bit of key stream it requires to update 3 bits by removing the 15 specific state bits of this state finally the rotation of the state bits are done and the process will repeats.

To achieve the haphazardness in the formation of keystream to attempt a powerful security Nawaz et al. [18] designed a new synchronous stream cipher called WG cipher established using Welch-Gong transformations. The output produced by WG keystream generator acquires the different properties randomness includes period, balance, 2-level autocorrelation, t-tuple distribution, Linear Complexity etc. The size of the initialization vector may be 32 bit or 64 bit. Secret key of different key lengths are incorporated with this cipher such as 80 bits, 96 bits, 112 bits and 128 bits. The plaintext is added with the output of WG keystream generator to get the cipher text. The speed of more than 100 Mbps was achieved almost with a little hardware. In 2003 at Fast Software Encryption workshop a synchronous stream cipher Rabbit was first

presented by Boesgaard et al. [19]. It takes a 128 bit secret key and 64 bit initialization vector along with 513 bits of internal state. The internal state is reserved for eight counters of 32 bit each; counter carry of one bit and a eight state variables of 32 bit each. The state variables are updated by eight connected non-linear functions. With the support of 128 bit key size the algorithm gives a better speed by encrypting up to 2^{64} blocks of plaintext. From the perfect random generator it is very complicated to identify up to 2^{64} blocks of cipher output from a complete keysearch over 2^{128} keys with a few functions. It provides a solid non-linear integration of the inner state between two iterations. Some of the features of above described stream ciphers are tabulated in Table 2.

Table 2. Features of stream ciphers

Name of cipher	Author	Year of publication	Key length	IV length	Basic primitives used	Internal state (bits)	Attacks described
LEX	Biryukov [9]	2008	128 bits	128 bits	AES Boolean functions	256 bits	Tradeoff Attacks Algebraic Attacks Differential, Linear, or Multiset Resynchronization Attacks Dedicated Attacks The Slide Attack
Oppel-2	Ali [2]	2014	128 bits	128 bits	GFCSR Boolean functions	–	Statistical Attacks Linearisation Attacks Re-synchronisation Attacks Trade-off Attacks
DECIM	Berbain et al. [3]	2005	80 bits	64 bits	LFSR, non-linear Boolean function, ABSG Buffer mechanism	192 bits	TMDTO attacks Guess-and-determine attack on the ABSG Guess-and-determine attack focusing on y Distinguishing attack Side channel attacks
Fruit 80	Ghafari, Hu [5]	2018	80 bits	70 bits	NFSR LFSR Counter	167 bits	TMDTO Attacks Guess and Determine Attacks Linear Approximation Attacks Related-Key Attacks Cube Attacks Algebraic Attacks Fault Attacks

(continued)

Table 2. (*continued*)

Name of cipher	Author	Year of publication	Key length	IV length	Basic primitives used	Internal state (bits)	Attacks described
Lizard	Hamann et al. [6]	2016	120 bit	64 bit	NFSR Output function α	121 bits	TMDTO Attacks Correlation Attacks, Linear Approximations Algebraic Attacks Guess-and-determine Attacks Conditional Differentials, Cube distinguishers IV Collisions
PLAS	Ashouri [1]	2018	256 bit	1600bits	LFSR, Stream-5, Boolean functions	-	Correlation attacks Time-memory tradeoff attack Algebraic attack Divide & conquer attack Distinguishing attack AIDA/cube attack
Grain	Hell et al. [7]	2007	80 bits	64 bits	LFSR NFSR Non linear output function	160	Algebraic Attack, Correlations, TMDTO Attack, Chosen-IV Attack, Fault Attack,
Grain-128	Hell et al. [8]	2006	128 bits	96 bits	LFSR NFSR Non linear output function	256 bits	Linear Approximations, Algebraic Attacks, TMDTO Attack, Fault Attacks
STRUMOK	Kuznetsov et al. [10]	2016	512 bits or 1024 bits	256 bits or 512 bits	LFSR Pre-computations table Boolean functions S-boxes	1024 bits	
ABC	Anashin et al. [11]	2005	128 bits	128 bits	LFSR Single cycle function Filter function	-	TMDTO attacks Related-key and resynchronization attacks Algebraic attacks Resistance to side-channel attacks
Ping-Pong	Lee and Chen [12]	2007	128 bits	128 bits	Summation Generator LM Generator LFSR	257 bits	Divide and conquer attack Time Memory Tradeoff Attack Correlation attacks

(continued)

Table 2. (*continued*)

Name of cipher	Author	Year of publication	Key length	IV length	Basic primitives used	Internal state (bits)	Attacks described
Achterbahn	Gammel et al. [13]	2005	80bits	0–64 bits	KSG NLFSR	275 bits	Side-channel attacks Correlation attack
Salsa 20	Bernstein [14]	2007	256 bits	128 bit (nonce and block counter)	Salsa20 hash function Boolean functions	512 bits	Side-channel attacks Differential attacks Algebraic attacks Weak-key attacks Equivalent-key attacks Related-key attacks
ChaCha	Bernstein [15]	2008	256 bits	128 bit (nonce and block counter)	Boolean functions	512 bits	–
Trivium	De Cannière [16]	2005	80 bits	80 bits	Non linear feedback Shift registers	288 bits	Guess and Determine attacks Algebraic attacks Resynchronization attacks Distinguishing attacks
RC4	Mantin [20]	2001	8 to 2048 bits	–	KSA PRGA	2064 bits	Known IV attack Choosen IV attack A Related-Key Attack Improving Tradeo Attacks
WG	Nawaz et al. [18]	2005	80, 96, 112 and 128 bits	32 or 64 bits	WG Keystream generator WG Transformation LFSR	161bits	Time/Memory/Data tradeoff attacks Algebraic attacks Correlation attacks
Rabbit	Boesgaard et al. [19]	2003	128 bits	64 bits	State function Counter function	513 bits	Guess-and-Verify Attack Guess-and-Determine Attack Algebraic Attacks Correlation Attacks

4 Research Direction

From the review of different stream ciphers it is found that there is a need of design of a stream ciphers with bellowed listed points in the mind.

- Efficient techniques to discover low-degree conditions.
- Key and IV should be distinctive and for every round it should be altered.

- Fast algorithms to solve system of equations.
- Criteria to avoid the presence of low-degree conditions over many clocks i.e. minimal execution time.

5 Conclusion

As recent trend expecting to embed smart devices into common objects. Since these devices have constrained resources, there is a need to innovate and develop a light-weight cryptographic algorithm. Both block ciphers and stream ciphers are perform good enough in this field. Stream ciphers are preferable in such a system where the plaintext length is either unknown or continuous.

We reviewed some of the stream ciphers described in the literature. The design concerns of stream ciphers are described. Some of the silent features of these ciphers are tabulated such as basic building blocks, size of secret key, attacks described in literature etc. These ciphers can be implemented in hardware, software or both. Security of most of the stream ciphers are depends on Randomness and size of key and IV. The security algorithms having less energy, stumpy storage with high throughput are crucial for IoT. In the present situation the optimization of security level is essential.

References

1. Ashouri, M.: Design of a New Stream Cipher: PALS (2018)
2. Ali, A.: Oppel-2: a new family of FCSR-based stream ciphers. In: 2014 International Conference on Emerging Technologies (ICET), pp. 75–80, Islamabad (2014). <https://doi.org/10.1109/icet.2014.7021020>
3. Berbain, C., et al.: DECIM, a new stream cipher for hardware applications (2005)
4. Ghafari, V.A., Hu, H.: Fruit: ultra-lightweight stream cipher with shorter internal state. IACR Cryptology ePrint Archive 2016/355 (2016)
5. Ghafari, A.V., Hu, H.: Fruit-80: a secure ultra-lightweight stream cipher for constrained environments. Entropy **20**, 180 (2018)
6. Hamann, M., et al.: LIZARD - a lightweight stream cipher for power-constrained devices. IACR Trans. Symmetric Cryptol. **2017**, 45–79 (2016)
7. Hell, M., Johansson, T., Meier, W.: Grain: a stream cipher for constrained environments. IJWMC **2**, 86–93 (2007). <https://doi.org/10.1504/IJWMC.2007.013798>
8. Hell, M., Johansson, T., Maximov, A., Meier, W.: A stream cipher proposal: grain-128. In: 2006 IEEE International Symposium on Information Theory, pp. 1614–1618, Seattle (2006). <https://doi.org/10.1109/isit.2006.261549>
9. Biryukov, A.: Design of a new stream cipher—LEX. In: Robshaw, M., Billet, O. (eds.) New Stream Cipher Designs. LNCS, vol. 4986. Springer, Heidelberg (2008)
10. Kuznetsov, O., Lutsenko, M., Ivanenko, D.: Strumok stream cipher: specification and basic properties. In: 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), pp. 59–62, Kharkiv (2016). <https://doi.org/10.1109/infocommst.2016.7905335>
11. Anashin, V., Bogdanov, A., Kizhvatov, I.: ABC: A New Fast Flexible Stream Cipher—eSTREAM, ECRYPT Stream Cipher Project, Report 2005/050 (2005)

12. Lee, H., Chen, K.: PingPong-128, a new stream cipher for ubiquitous application. In: 2007 International Conference on Convergence Information Technology (ICCIT 2007), pp. 1893–1899, Gyeongju (2007). <https://doi.org/10.1109/iccit.2007.375>
13. Gammel, B., Göttfert, R., Kniffler, O.: The Achterbahn stream cipher (2005)
14. Bernstein, D.J.: The Salsa20 family of stream ciphers (2007)
15. Bernstein, D.J.: ChaCha, a variant of Salsa20. In: Workshop Record of SASC (2008)
16. De Cannière, C.: Trivium: a stream cipher construction inspired by block cipher design principles. In: Katsikas, S.K., López, J., Backes, M., Gritzalis, S., Preneel, B. (eds.) Information Security, ISC 2006. LNCS, vol. 4176. Springer, Heidelberg (2006)
17. De Cannière, C., Preneel, B.: TRIVIUM — specifications. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/030 (2005). <http://www.ecrypt.eu.org/stream>
18. Nawaz, Y., Gong, G.: The WG stream cipher (2005)
19. Boesgaard, M., Vesterager, M., Pedersen, T., Christiansen, J., Scavenius, O.: Rabbit: a high-performance stream cipher. In: Proceedings of FSE 2003. LNCS, vol. 2887, pp. 307–329, Springer (2003)
20. Mantin, I.: Analysis of the Stream Cipher RC4 (2001)
21. Paul, G., Maitra, S., Chattopadhyay, A.: Quad-RC4: Merging Four RC4 States towards a 32-bit Stream Cipher.. IACR Cryptology ePrint Archive. 2013:572 (2013)
22. Stallings, W.: Cryptography And Network Security Principles And Practice. 4th edn. Pearson Education (2017)
23. Stallings, W.: Network Security Essentials: Applications and Standards. Prentice Hall (2003)



An Analysis of Scheduling Algorithms in Real-Time Operating System

Jayna Donga¹(✉) and M. S. Holia²

¹ Gujarat Technological University, Ahmedabad, Gujarat, India
jdonga@mbict.ac.in

² BVM Engineering College, Anand, Gujarat, India
msholia@bvmengineering.ac.in

Abstract. The real-time systems are those in which the correctness of output does not depend only on logical results of the computations, but also on the time at which output is produced. It means that result must be produced within stipulated time. The time constraint in which the system needs to respond is called the deadline. Meeting the deadline is an important parameter in any real time system. The real time operating system helps to real-time applications for meeting its deadline using the mechanism of scheduling. The scheduling technique is the heart of any real-time system which is responsible for making decision about execution order of tasks in the system so any kind of overlapping can be avoided. In this paper, the classification of several scheduling techniques have been done based on different parameters. We have also analyzed different schedulers used for real-time system and comparison between various scheduling techniques have been done. There are various scenarios represented on which further work for improvement can be done.

Keywords: Deadline · Laxity · Utilization · Priority · Context switching · Schedulability · Preemption

1 Introduction

In Real Time Systems, the integrity of the outcome depends on the analytical outcome of the computations as well as on the time instant at which the outcome gets generated [5]. The system has been called Real Time System if at least one task in the system is having demarcated timing constraints i.e.; action should be taken in stipulated time. Meeting a deadline is first and foremost requirement of any real-time system and Deadline is defined as the instant of time at which the action must be performed otherwise RTS is said to be failed [9]. The Real-Time Systems can be categorized into three different types: Hard Real-Time Systems, Firm Real-Time Systems and Soft Real-Time Systems. **Hard Real-Time System:** the whole organization will be failed if the deadline miss occurs; some of them are safety critical. Anti-missile system is the example for the same. **Soft Real-Time System:** if the Deadline miss occurs, the system will not fail but the utility of result will be reduced over the period of time. System performance will be degraded. All the interactive applications are the example of soft real-time system. **Firm Real-Time System:** it is almost similar to soft RTS, the

deadline miss will not destroy whole system but the result produced after the deadline having zero utility. Very rare deadline misses are bearable. A video conferencing application comes under this category. Any computing system is full of resources and these common resources are shared between multiple tasks running simultaneously to meet the multiple goals. Taking decision regarding execution order of the tasks on currently available processors is called scheduling and the part of operating system which is responsible for taking decision is called the scheduler. In any multitasking and real-time operating system scheduling is a fundamental design issue. It is the process of decision making which performs the distribution of various system resources to different processes as per their demand during their execution to obtain required outcomes. For any real-time application meeting the dead-line is a crucial task and real-time operating system helps to them to meet its deadline by using the various scheduling mechanisms.

Scheduling mechanism can be categories as follow:

The major categories of Real-Time scheduling approaches are: (1) Static approach (2) Dynamic approach. The priorities of the processes is kept fixed and it is allocated at the time of desining algorithm as well as it will remain constant during whole life cycle of the task. While in case of dynamic algorithms the priority of task will be assigned at run time based on different parameters and also can be changed during its execution period. Further classification of Dynamic scheduling (As shown in Fig. 1) is also possible like scheduling with fixed priority and scheduling with dynamic priority. The dynamic scheduling with static priority approach can be represented by Rate Monotonic (RM) and Deadline Monotonic (DM) approach [6] while the Earliest Deadline First (EDF), Least Laxity First (LLF) are the examples for the dynamic scheduling approach with dynamic priority [7]. The optimal task scheduling approaches for uniprocessor system are EDF and LLF/LSF with specific condition like jobs should be preemptive in nature and if the system is not overloaded [6, 7]. The performance of these algorithms poor under the transient overload condition is the main disadvantage of them [8].

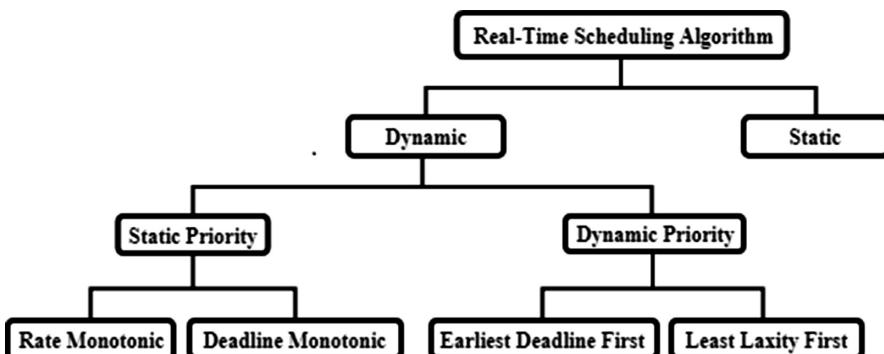


Fig. 1. Different categories of real-time scheduling algorithms

2 Literature Survey

The subsequent segments represent the research has been done in the area of Real-Time Operating System specifically for real-time task scheduling by the different researchers.

Lee et al. [1] presented EDF Scheduling of Uniprocessor Systems with new pre-emption policy in terms of meeting deadline in 2014. Earliest Dead line first algorithm broadly analysed to schedule the real-time processes as EDF is the simplest and effective approach for uniprocessor system. But the additional delay in execution of jobs are generated due to pre-emption and hence the efficiency of EDF getting exaggerated significantly with the currently available pre-emption mechanism which takes decisions about when a high priority task should be permitted to pre-empt the presently running less priority task. So in the paper researcher presents the novel and superior pre-emption policy where the performance metric is deadline miss ratio. This new mechanism is applying Earliest Deadline First with controlled pre-emption (CP) and defined a new policy called CP-EDF which enhance schedulability of EDF approach is 7.4% more than the current policy. This mechanism will work for the Uniprocessor system only. The researchers had proved that the proposed approach(CP-EDF) will give extra task sets which are schedulable and they were not found schedulable under EDF's currently existing pre-emption policies.

In 2016 Keerthanaa et al. [2] has presented enhanced Real-time scheduling algorithm which is priority based approach. It has been observed that major class of scheduling algorithms for real-time systems are desired with the support of priorities. The deadline miss ratio is going to increase if the real-time tasks are not scheduled precisely. When a higher priority task will be permitted to preempt forcefully the lower priority task then it causes the context switching in Real-Time Operating System. The context switch causes the wastage of CPU-Time and Power consumption which is extra overhead to the system. These troubles can be prevented by the proposed approach CP-EDF(Controlled Preemptive EDF) in which the number of preemptions are restricted. The main goal is to minimize the number of context switching so it can prevent the wastage of CPU-Time as well as CPU-power Consumption. It aims to solve the troubles of higher priority processes missing their deadlines and lower priority processes suffering from starvation. CP-EDF compared with two existing Fixed priority Earliest Deadline First and Non-Preemptive Earliest Deadline First approaches. They observed that CP-EDF (Controlled Priority Earliest Deadline First) performs better than existing two in terms of reduce context switching overhead, Deadline meeting ratio, Deadline miss rate and CPU-Utilization. EDF performs well only in under loaded condition.

In 2014 Mottaghi et al. [3] presented the fault tolerant policy for scheduling real-time tasks in multiprocessors system which is dynamic. Goal of this algorithm is to increase scheduling possibility as well as increase the performance by reducing the all over duration for running the jobs.

Techniques for fault tolerant is redundancy

1. Hard ware based redundancy (multiple copies of a task on different hardware)
Drawback: extra hardware costing and power usage overhead

2. Software based redundancy (rollback recovery by check pointing and re-run on same h/w) Drawback: extra execution time overhead (for long duration, serial executions)
3. This paper use task utilization and defines criticality of each task. Tasks divided in two groups (1) critical (2) non-critical

As per the types of task whether it is critical task or non-critical task and suitable fault tolerance policy is going to be exploited at execution time dynamically.

- a. Non critical jobs are scheduled on a Uniprocessor system and rollback recovery by the check pointing is to be applied for them.
- b. The critical tasks are copied onto the different processors to improve the possibility of task completion within deadline if any fault appears into the system.

In 2014 Kalpana et al. [4] has proposed an improved Non-Preemptive soft real-time scheduling policy with the DC-Group EDF.

DC-gEDF algorithm use the non-pre-emptive policy so there will be Zero switching overhead. Hybrid algorithm will creates clusters of the tasks based on its domain description and also according to their deadline requirements then it will schedule the processes belongs to that group. The Deadline missing ratio of group EDF and DC-Group EDG is taken into consideration as performance parameters for various standard deadline values. The results show the enhancement in the deadline missing ratio for the newly designed algorithm Domain Cluster-gEDF.

3 Algorithms for Scheduling Real-Time Tasks

There are important programs which are used for allocation of numerous resources like CPU time, bandwidth etc. are called scheduling algorithms. Scheduling is done by allocation of computation workload between multiple processors in such a way so that we can achieve maximum CPU utilization, minimum response time, maximum throughput and maximize Schedulability [10]. Any scheduling approach is designed with the aim to accomplish the following conditions. A. There must not be the situation of starvation means that any process will not be put waiting for indefinite time. Distribution of resources should be in such a way so that every tasks get processor time in order to prevent starvation. B. There must be fairness in any preemption policy means that in case of priority based algorithm the lower priority tasks must not be put waiting indefinitely by the higher priority tasks. Every tasks should get fair share of cpu time.

Some notorious scheduling approaches for Real-Time Tasks are as following:

3.1 Rate Monotonic Scheduling Algorithm (RM)

The Rate Monotonic algorithm (RM) has been presented by Liu and Layland in 1973 [14]. RM is the dynamic approach for hard real time tasks which is based on static priority. In this algorithm priorities are fixed can't be changed during execution. To schedule a task set using this algorithm the following assumptions are made [9, 10].

- a. All the real-time tasks in task set having hard deadline should be periodic tasks.
- b. There should not be any kind of dependency between tasks and there should not be any constraints like priority constraints or mutual exclusion constraints among any set of tasks.
- c. for every tasks the deadline interval and its period should be equal.
- d. The maximum CPU time requirement should be constant and known in advance.
- e. Time spent in context switching is assumed as zero.
- f. $U = \sum(c_i/p_i) \leq n(2^{1/n} - 1)$ represents the sum of utilization of n tasks with period p . The increment in number of tasks will cause decrement in the utilization factor over the period of time and with one task highest utilization factor 1 will be achieved. As n goes to the infinity, the term $n(2^{1/n} - 1)$ reaches up to $\ln 2$ (around 0.7). In this algorithm the task priorities are calculated based on task's *period*. The Rate of task is inversely proportional to task's period. Thus, the processes having small period contains high rate and hence its priority is high. The process with higher rate will be executed first. With all the above assumptions this algorithm guarantees to meet deadline of every processes in the process set. RM is an optimal algorithm for Uniprocessor system.

3.2 Deadline Monotonic Scheduling Algorithm (DM)

Leung and Whiteland has proposed Deadline Monotonic Scheduling Algorithm in 1982 [9]. Proposed real-time task scheduling approach is an extension of Rate Monotonic (RM) technique. This technique is a dynamic algorithm with static priority having full pre-emption concept [9]. One of the assumption in Rate Monotonic algorithm is that there must be every tasks in task set with same deadline interval and its period. This condition has been made flexible in case of dead-line monotonic algorithm. The task have relative deadline rather than absolute deadline; relative deadline could be less than or equal to its period (Fig. 2).

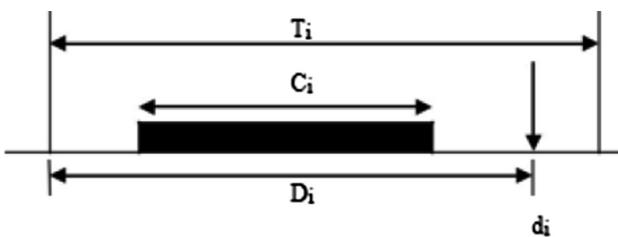


Fig. 2. Task parameters in deadline monotonic scheduling [10]

C_i : Worst case execution time of task i

D_i : Relative Deadline of task i

T_i : Period of a task i

Absolute deadline is starting from 0 to deadline and Relative deadline is from occurrence of task to the deadline. Every task has assigned a static priority which is

inversely proportional to its relative deadline D_i . Thus, the task with shortest deadline will be executed first at any instant of time. DM is said a static priority assignment technique as the relative deadlines are constant.

3.3 Earliest Deadline First Scheduling Algorithm (EDF)

Earliest Deadline First Algorithm has been presented by Lui and Leyland. [11]. EDF is designed with preemptive policy having dynamic priority assignment for uniprocessor system. EDF algorithm gives optimum result than any other presently available methods with dynamic priority. In this algorithm scheduling of task is done base on its deadline as its name suggests the task having earliest deadline will be scheduled first among all the available ready tasks in the queue. A task set is said to be schedulable only when the utilization factor is less than or equals to one that is $U \leq 1$.

The steps for EDF scheduling algorithm is as following: [11]

OR

- 1: Set arrival and competition time, time which is left and targeted time for all the tasks in task set.
- 2: If node is free then add task to schedule and goto 4
- 3: if newly arrived task's targeted time is earlier than executing task's targeted time then update executing g task's remaining time and swap tasks else change new task's arrival time
- 4: if all available task have not been scheduled then goto 2 else stop.

3.4 Least Laxity First Scheduling Algorithm (LLF)

LLF scheduling approach for real-time tasks has been presented by Stewart and Khosla [12]. It is an optimal dynamic algorithm with dynamic priority for single core system which is enhanced version of EDF. In this algorithm, first the laxity for each task in a system will be calculated, after that the task which is having minimum slack time will be selected for the next execution. That is why the algorithm is known with the name Least Laxity First (LLF). The LAXITY of a task can be represented with the following formula:

$$\text{Laxity} = \text{deadline} - \text{current_time} - \text{CPU_time_still_required}$$

The difference between the Deadline and Remaining-Execution-Time defines the LAXITY of any task.

Laxity also known as Slack time and hence this algorithm is said to be Least-Slack Time-First (LSF). Laxity can be used to measure the flexibility of a task for scheduling. The task with the laxity t_L indicates that it can meet its deadline even though it is delayed by t_L . In other words a process is allowed to complete its execution within its deadline even if it is having delay of t_L time units where t_L is the laxity of that process. When the laxity of a job seems zero represents that the process must be executed at present else there is a highest possibility of missing the deadline. LLF allots the highest priority level to the ready job which is having least slack time [13] and the job which is

having highest priority will be executed first. If a task T₁ is in execution and the laxity of another task T_i gets reduced than the running task then the task T₁ can be preempted by T_i as now it is having least laxity among them. In this policy the problem arise when more than one tasks having similar slack time. One task get CPU for particular time slot and then it will be preempted by the other process, in this way the processor switches back and forth from one task to another task. Thus, it increases context switching count during the lifecycle of the tasks and it is costly in terms of time In the Real-Time Systems the Large class of the tasks are periodic in addition to that the systems having periodic real-time tasks can use LLF algorithm and it gets optimal result. At every new arrival of a task the task is added into the ready queue, calculated its laxity and then priority is assigned based on its laxity.

4 Conclusion and Future Scope

By performing the literature survey of different real-time scheduling techniques, the conclusion is that the scheduling approaches for Real-Time Tasks are being categories in two parts; the algorithm with fixed priority and the algorithms with dynamic priority. We have done study of familiar real-time scheduling approaches like Rate Monotonic, Deadline Monotonic, EDF, Least Laxity First etc. and tried to analyze its advantages and limitations. The algorithms with dynamic priorities are having higher CPU utilization than static priority algorithms but the number of context switches are also higher than static priority algorithms. Dynamic priority algorithms performs better than static priority algorithm if the system is not with transient overload condition. Most of the algorithms we have discussed that provides optimal solution for uniprocessor system so in future one can try to design more generalized and effective multiprocessor real-time scheduling algorithm.

References

1. Lee, J., Shin, K.G.: Preempt a job or not in EDF scheduling of uniprocessor systems. *IEEE Trans. Comput.* **63**(5), 1197–1205 (2014)
2. Keerthanaa, C., Poongothai, M.: Improved priority based scheduling algorithm for real time embedded systems. In: *IEEE xplore for International Conference on Circuit, Power and Computing Technologies [ICCPCT]* (2016)
3. Mottaghi, M.H., Zarandi, H.R.: DFTS: a dynamic fault-tolerant scheduling for real-time tasks in multicore processors. *Microprocess. Microsyst.* **38**, 88–97 (2014)
4. Kalpana, R., Keerthika, S.: An efficient non-preemptive algorithm for soft real-time systems using domain cluster-group EDF. *Int. J. Comput. Appl.* **93**(20), 0975–8887 (2014)
5. Liu, J.W.S.: *Real-Time Systems*. Pearson Education, pp. 121–126, India (2001)
6. Liu, J.: *Real-Time Systems*. Pearson Education (2000)
7. Kotecha, K., Shah, A.: ACO based dynamic scheduling algorithm for real-time operating system. In: *Sent to AIPR-2008*, Florida (2008)
8. Saini, G.: Application of fuzzy logic to real-time scheduling. In: *14th IEEE-NPSS Real Time Conference* (2005)
9. Brucker, P.: *Scheduling Algorithms*. 5th edn. Springer

10. Buttazzo, G.C.: Hard Real Time Computing Systems: Predictable Scheduling Algorithms and Applications. 3rd edn. Springer (2011)
11. Yoo, M., Gen, M.: Study on scheduling for real-time task by hybrid multiobjective genetic algorithm, Thesis (2006)
12. Stewart, D.B., Khosla, P.: Real-Time Scheduling of Sensor-Based Control Systems (1991)
13. Mohammadi, A., Akl, S.G.: Scheduling algorithms for real-time systems, Technical report No. 499 2005, 15 July 2005
14. Liu, C.L., Layland, J.W.: Scheduling algorithms for multiprogramming in a hard real time environment. *J. Assoc. Comput. Mach.* **20**(1), 46–61 (1973)



A Novel Approach for Cluster Head Selection By Applying Fuzzy Logic in Wireless Sensor Networks with Maintaining Connectivity

Aaditya Jain^(✉) and Bhuwnesh Sharma

Department of CSE, R. N. Modi Engineering College,
Rajasthan Technical University, Kota, Rajasthan, India
aadityajain58@gmail.com, bsharma.it@gmail.com

Abstract. The problem of increasing network lifetime by reducing energy consumption becomes more significant as the topology of the wireless sensor network is not fixed and sensor nodes are located randomly within the networks. This paper focuses on maintaining the network connectivity as long as possible. A clustering method that checks connectivity during topology formation is proposed. A fuzzy inference system is proposed with a specific consideration on the node energy, distance from base station and number of alive neighbours to decide the probability of a node, which has to be appointed a cluster head and also decides the size of cluster it may have.

Keywords: Cluster head selection · Fuzzy inference system · CUCF · WSN · Energy efficient protocol

1 Introduction

In the present age, Wireless Sensor Networks (WSN) is considered as a new model for real time applications. Wireless sensor nodes are not rechargeable and have very limited and less energy resources. These nodes are spread over a hostile environment with the aim of analyzing and monitoring physical characteristics. So in such cases it is very difficult to replace battery. Thus it motivates the research in the direction of lifetime enhancement of WSN by using cluster based design that allows only some nodes i.e. cluster heads (CH) to communicate with base station (BS) [1]. CHs collect the data sent by each node in that cluster, compressing it and then transmitting the aggregated data to the BS. Clustering minimizes the need for central organization but the problems associated with clustering in WSNs are: proper selection of CHs and hot-spot problem. A clustering method that checks connectivity during topology formation is proposed in this paper. Also The leader election to appoint CHs takes place through fuzzy inference system.

1.1 Role of Fuzzy Logic and Connectivity

Fuzzy logic (FL) control is capable to work in real time even when incomplete information is present. Fuzzy approach is suitable for WSN where the degree of uncertainty is

higher. FL mainly consists of four significant parts: fuzzifier, inference system, rule base and defuzzifier over the geographical region of interest (RoI). The existing protocols that use a fuzzy inference system (FIS) to facilitate proper CH election and hence uniform distribution of energy load rarely consider the connectivity of network. Hence, this paper is aimed at filling this research gap. Communication protocol for WSN is design that adopts clustering topology through dynamic CH election using a FIS. The protocol maintains connectivity of the network at all times under assumption that a disconnected network is equivalent to dead network.

Paper organised as follows, Sect. 2 describe literature search. Section 3 describes proposed fuzzy system and clustering topology protocol. Results and performance evaluation done in Sect. 4, at last paper conclude in Sect. 5.

2 Literature Search

The research for topology control, efficient distribution of load, uses of fuzzy logic for CH selection and life till connected in WSNs has been active in recent years and ample literature exists some of them mentioned here:

Heinzelman et al. in [1] proposed a Low Energy Adaptive Clustering Hierarchy (LEACH) approach. In this scheme CH are rotated periodically to balance energy depletion. TDMA/CDMA mechanism used to reduce collision. LEACH-C (centralized version) [2], D-LEACH (Density Based) [3], T-LEACH (Time period Based) [4] etc. are the modification of LEACH. Ye et al. in [5] proposed energy efficient clustering scheme that produce clusters of unequal size in single hop network. Zu et al. in [6] proposed distributed version of [5] for heterogeneous networks but scalability is the prime issue.

Xu et al. in [7] proposed game theory based algorithm, in which as a clustering it uses game theory. Also introduced utility function based on node's density and residual energy. Gupta et al. in [8] proposed first scheme that uses fuzzy logic for clustering and define 27 rules for fuzzy rule base. Author represent fuzzy set by using triangle membership function. Kim et al. in [9] uses two fuzzy sets and fuzzy if then rule with two fuzzy variables namely, Energy and Local Distance.

Bagci et al. in [10] focuses on reducing the internal work of CHs that are near to BS or have very low battery power. Author use residual energy as an additional parameter with distance to the base station for the calculation of competition radius. Santhi et al. in [11] proposed DUCF-a distributed load balancing scheme in which cluster of unequal size are produced to balance load in the network.

Logambigai et al. in [12] proposed fuzzy based unequal clustering FBUC as improved version of EAUCF. It uses probabilistic threshold value, for electing cluster head. Its main advantage is that when node degree increases the competition radius is decreased. Multi-objective fuzzy clustering algorithm (MOFCA) proposed in [13] in which first tentative CHs are elected using a probabilistic model. Shoukohifar et al. in [14] proposed LEACH-SF algorithm that based on Sugeno fuzzy system that gives balanced clusters and then elect a valid CH.

Wang et al. [15] have provided a formal treatment to connectivity and coverage problems in WSNs. Goratti et al. [16] proposed a protocol to automatically restore connectivity if communication between access point to sensor nodes break. Very recently, Jain et al. in [17] proposed a tracing based solution for long term connectivity in mobile nodes. Mekkis et al. in [18] have suggested analytical models for connectivity for both unicast and broadcast transmission schemes of WSNs.

Mostly all existing methods consider energy of a node as a criterion but in its absolute quantity. Instead one must note that a CH should have higher energy as compared to all its neighbours. This in itself automatically ensures a local CH election. We propose a measure called energy factor instead of using residual energy of a node directly as a property of node in CH election.

3 Proposed Fuzzy System and Clustering Topology Protocol

We present a fuzzy inference based approach that directly outputs the node selection probability and cluster size bound. The 1-hop neighbour nodes towards and away from BS are named as TBS-neighbours and ABS-neighbours respectively. A node with many ABS-neighbours is expected to receive heavy traffic, and is termed as a **crucial** node in multi hop communication models. In the case of single hop communication a node will be considered as crucial if it has zero or few ABS neighbours. Try to avoid such node to become a CH and if it is not possible then decreasing the load of the crucial nodes.

3.1 Proposed Fuzzy Inference System (FIS)

The proposed fuzzy system as shown in Fig. 1, takes three inputs:

- Criticality – The criticality of a sensor node can be understood as an estimate of expected traffic that it would receive to forward towards BS.
- Energy-factor – This indicates the ratio of its residual energy to the average residual energy of the nodes within its communication range.
- Distance from BS – Necessary to decide the number of members a CH should have in its cluster. The nodes near to BS have higher priority to select as CH.

We use Mamdani method for fuzzy inference. It uses fuzzy rule base of 27 rules to compute output as:

- Chance of Election (CoE) – This value shows the eligibility of the nodes to elect as CH.
- Cluster Member Limit (CML) – Value that limits the node to join a cluster according to distance.

3.2 Proposed Protocol

A topology formation, communication and routing protocol is proposed in Fig. 2 named as “Connectivity based unequal clustering using fuzzy logic (CUCF)” protocol. It progresses in rounds, each round having two phases with following processes:

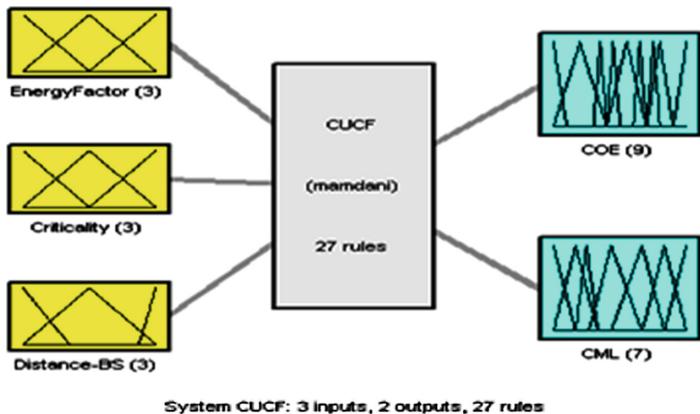


Fig. 1. The fuzzy inference system of CUCF: block diagram

CUCF Algorithm:

```

For very node do
    this.State = probabitory CH
    this = pointer to current node
    this.ND = number of nodes within communication radius 'r'
    this.DBS = distance of the node with BS
    this.RE =residual energy of the node
    this.ABS=number of nodes within communication radius 'r' and away
from BS
    this.TBS= number of nodes within communication radius 'r' and towards
BS
    COE, CML = calculateFuzzy(this.ND, this.DBS, this.RE)
    If this.ABS>this.TBS
        Limitsize(this.CSB)
    end
    for m=1:N
        Send CH_CANDIDATE to all neighbor nodes
        x=list of all CH_CANDIDATE from neighbor nodes
        if (this.COE > COE(x))
            advertise CH_WON
            this.State = Final_CH
        end
    end
    if this.state ==Final_CH
        Receive requests from other nodes
        for every request do
            if this.CML>count(current members)
                Send CM_ACCEPTANCE
            else
                Send CM_REJECTION
            end
        end
    else
        for every received CH_WON
            send CM_JOIN to nearest CH in sequence
            if received CM_ACCEPTANCE
                Join CH which issued CH_WON
                this.State=Member_Node
                break
            end
        end
        if not joined any CH
            this.state=Final_CH
        end
    end
end

```

Fig. 2. Proposed CUCF method

- Cluster Formation Phase
 - Fuzzy computations
 - Local CH election
 - Joining of members

4 Experimental Evaluation and Comparative Results

It is assumed that sensor nodes are homogeneous, randomly dispersed and stationary once deployed. We perform simulation in MATLAB. To estimate the energy consumption of nodes radio model as adopted by [19] is considered. Performance of the proposed CUCF protocol is compared with the Non-fuzzy simple baseline, CHEF [9] and popular fuzzy approach EAUCF [10].

Comparison parameters are (a) Life till connected, (b) Average energy consumption per round, (c) Average number of CHs appointed and (d) Standard deviation in number of CHs elected. In each simulation the BS is stationary at any one of the following positions as (a) Corner of RoI, (b) Middle of RoI.

4.1 Comparison of Life till Connected of CUCF with Other Algorithms

It is clearly justifying Figs. 3 and 4 that proposed algorithm runs longer even when BS is placed at corner and middle of RoI. Also it is able to identify the crucial nodes properly compare to other algorithms and manages the energy load accordingly.

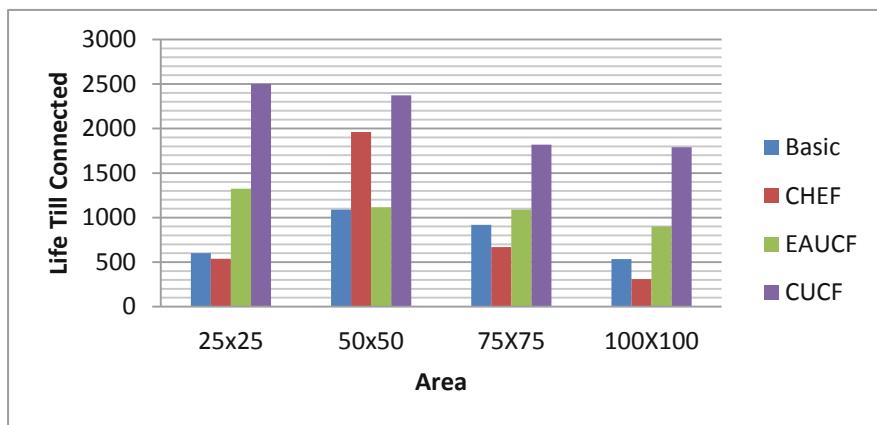


Fig. 3. When BS located in corner of RoI

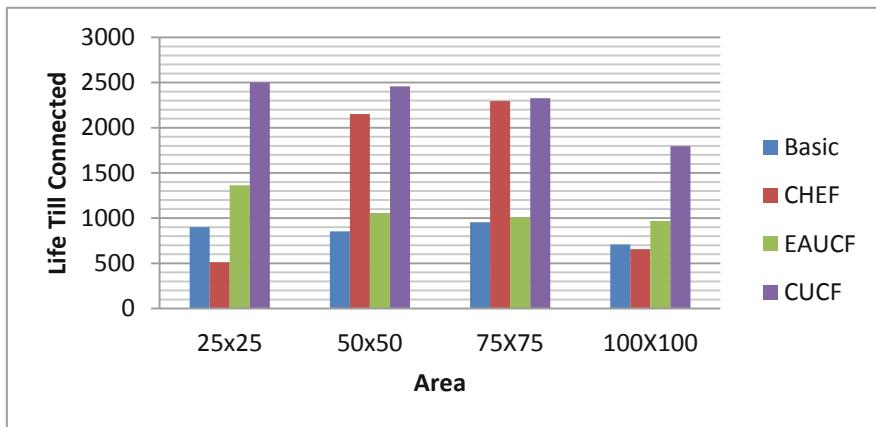


Fig. 4. When BS located in middle of RoI

4.2 Comparison of Energy Consumption of CUCF with Other Algorithms

The energy consumption of a clustering method should be low. The comparison of four algorithms is shown in Figs. 5 and 6, respectively for BS at corner and middle of the RoI. CUCF gives better results among all.

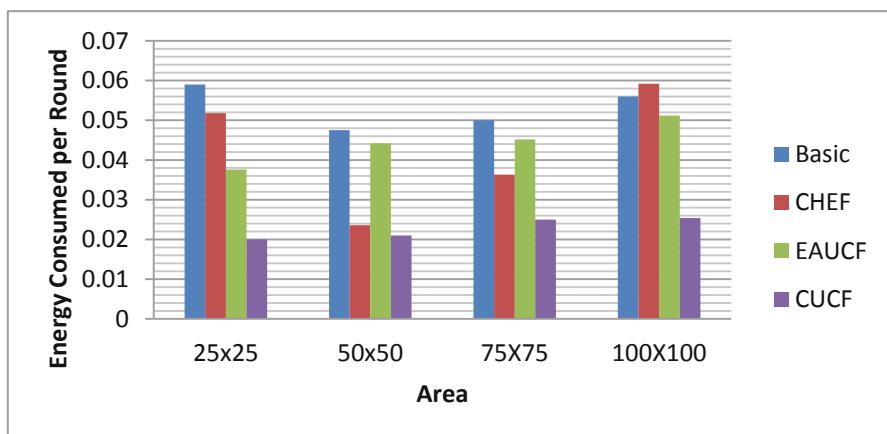


Fig. 5. When BS located in corner of RoI

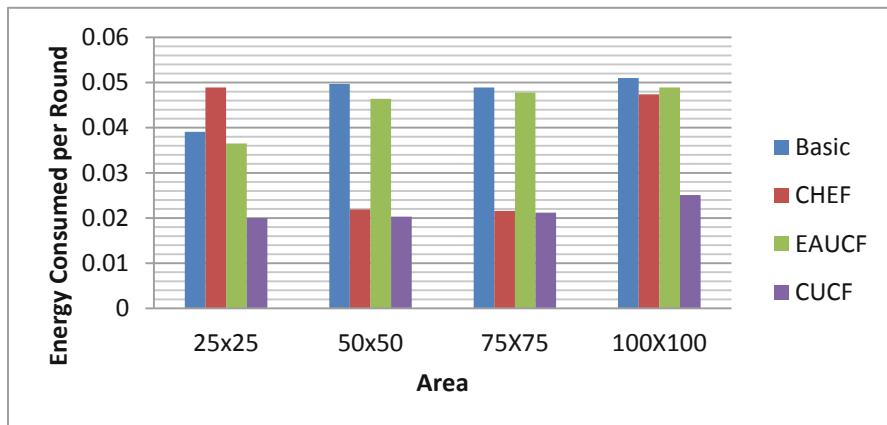


Fig. 6. When BS located in middle of RoI

4.3 Comparison of Average Number of CHs Elected by CUCF with Other Algorithms

We record the number of CHs appointed at each round and then compute its average. The average obtained in two different scenarios as shown in Figs. 7 and 8 respectively.

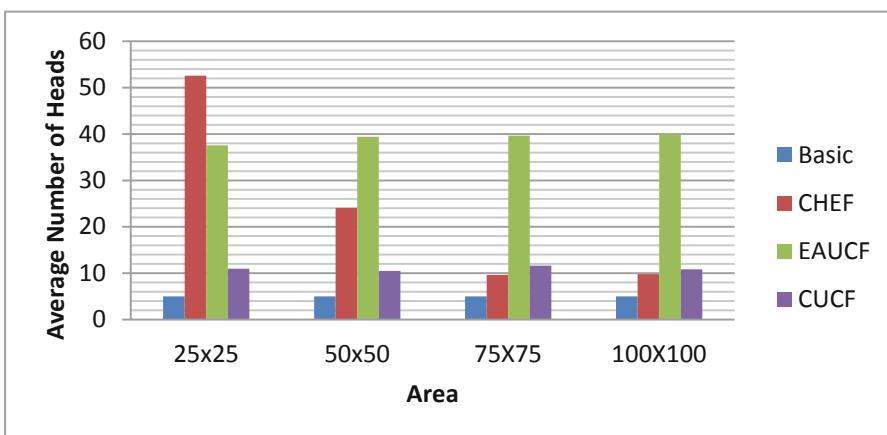


Fig. 7. When BS located in corner of RoI

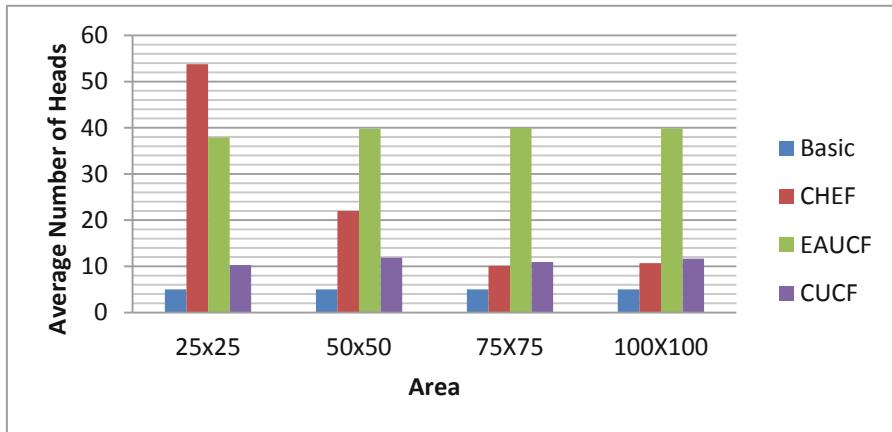


Fig. 8. When BS located in middle of RoI

4.4 Comparison of Standard Deviation in Number of CHs Elected by CUCF and Other Algorithms

We also compute the standard deviation (SD) in the number of CHs elected at every round by all four algorithms as shown in Figs. 9 and 10 for both scenarios. A low value of SD of CUCF will indicate that the algorithm has a predictable behaviour and topology control. The near-to-zero values are not visible as the bar. Deviation in number of CHs is high in Basic, despite the regulation it involves through probability. Its probabilistic nature makes it very unpredictable.

Thus, it is more readily accepted for suitable applications as compared to those algorithms that may elect arbitrary number of CHs.

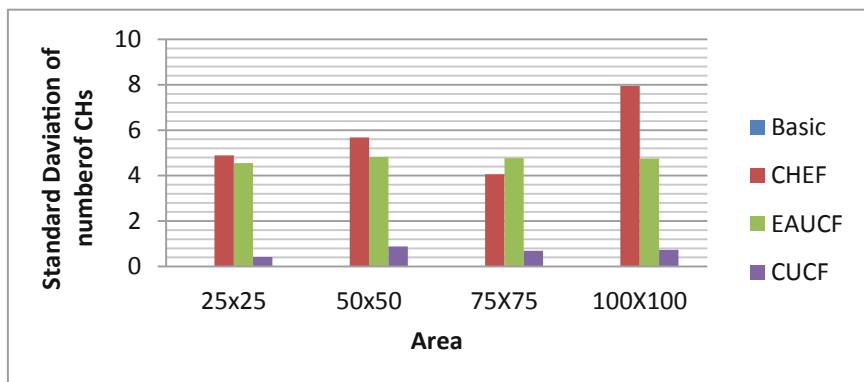


Fig. 9. When BS located in corner of RoI

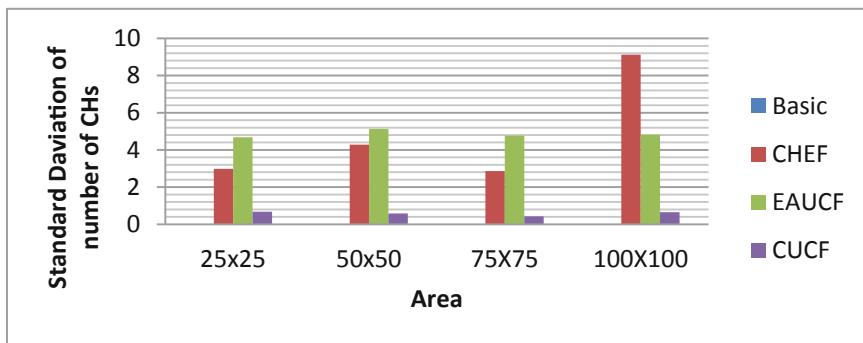


Fig. 10. When BS located in middle of RoI

5 Conclusion

This work analyzes the protocols especially for connectivity. Also, a new protocol is proposed that uses fuzzy logic computations. The fuzzy inferences are used for cluster head election and cluster formation. The comparison with other fuzzy logic based methods is done through simulation experiments in variety of settings by changing position of BS and density of nodes in RoI. In all experiments, the proposed method maintains connectivity of the network for longer duration. There is uniform distribution of energy consumption among nodes and average number of CHs elected is also in proportion to number of nodes that are alive.

At present, the work assumes a homogenous WSN having all nodes identical to each other. Health service applications generally deal with heterogeneous networks, hence the proposed method can be modified to such applications in future. The fuzzy logic can be extended to have mobility also as a factor.

References

- Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Hawaii International Conference on System Sciences, vol. 8, pp. 8020 (2000)
- Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. *IEEE Trans. Wirel. Commun.* **1**(4), 660–670 (2002)
- Kim, J., Byun, T.: A density-based clustering scheme for wireless sensor networks. In: Advanced Computer Science and Information Technology, pp. 267–276 (2011)
- Hong, J., Kook, J., Lee, S., Kwon, D., Yi, S.: T-LEACH: the method of threshold-based cluster head replacement for wireless sensor networks. *Inf. Systems Front.* **11**, 513–521 (2009)
- Ye, M., Li, C., Chen, G., Wu, J.: EECS: an energy efficient clustering scheme in wireless sensor networks. In: Proceedings of the 24th IEEE International Performance, Computing and Communications Conference (IPCCC), pp. 535–540 (2005)

6. Qing, L., Zhu, Q., Wang, M.: Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. *Comput. Commun.* **29**, 2230–2237 (2006)
7. Xu, Z., Yin, Y., Wang, J.: A density-based energy-efficient routing algorithm in wireless sensor networks using game theory. *Int. J. Future Gener. Commun. Netw.* **5**(4), 62–70 (2012)
8. Gupta, I., Riordan, D., Sampalli, S.: Cluster-head election using fuzzy logic for wireless sensor networks. In: Proceedings of the 3rd Annual Communication Networks and Services Research Conference 2005, pp. 255–260 (2005)
9. Kim, J.M., Park, S.H., Han, Y.J., Chung, T.M.: CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks. In: Proceedings of the ICACT, pp. 654–659 (2008)
10. Bagci, H., Yazici, A.: An energy aware fuzzy approach to unequal clustering in wireless sensor networks. *Appl. Soft Comput. Sci. Publishers* **13**(4), 1741–1749 (2013)
11. Baranidharan, B., Santhi, B.: DUCF: distributed load balancing Unequal Clustering in wireless sensor networks using Fuzzy approach. *Appl. Soft Comput.* **40**, 495–506 (2016)
12. Logambigai, R., Kannan, A.: Fuzzy logic based unequal clustering for wireless sensor networks. *Wirel. Netw.* **22**(3), 945–957 (2015)
13. Sert, S.A., Bagci, H., Yazici, A.: MOFCA: multi-objective fuzzy clustering algorithm for wireless sensor networks. *Appl. Soft Comput.* **30**, 151–165 (2015)
14. Shokouhifar, M., Jalali, A.: Optimized sugeno fuzzy clustering algorithm for wireless sensor networks. *Eng. Appl. Artif. Intell.* **16**, 16–25 (2017)
15. Wang, Y., Zhang, Y., Liu, J., Bhandari, R.: Coverage, connectivity, and deployment in wireless sensor networks. In: Patnaik, S., et al. (eds.) Recent Development in Wireless Sensor and Ad-hoc Networks, Signals and Communication Technology. Springer (2015)
16. Goratti, L., Baykas, T., Rasheed, T., Kato, S.: NACRP: a connectivity protocol for star topology wireless sensor networks. *IEEE Wirel. Commun. Lett.* **5**(2), 120–123 (2016)
17. Jain, A., Pardikar, V., Pratihast, S.R.: Tracing based solution for ubiquitous connectivity of mobile nodes for NDN: a RA kite. In: 8th IEEE International Conference on Computing, Communication and Networking Technologies, IIT, Delhi, PP. 1–7, 3–5 July. <https://doi.org/10.1109/icccnt.2017.8204191>
18. Mekkis, P.-V., Kartsakli, E., Antonopoulos, A., Alonso, L., Verikoukis, C.: Connectivity analysis in clustered wireless sensor networks powered by solar energy. *IEEE Trans. Wirel. Commun.* **17**(4), 2389–2401 (2018)
19. Kuhn, F., Moscibroda, T., Wattenhofer, R.: Initializing newly deployed ad hoc and sensor networks. In: Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, PP. 260–274 (2004)



Simple and Coverage Path Planning for Robots: A Survey

R. S. D. Pragnavi^(✉), Akhileshwar Maurya, Bharath N. Rao, Akash Krishnan, Srijan Agarwal, and Maya Menon

Department of Computer Science and Engineering, Amrita Vishwa Vidyapeetham,
Amritapuri, Kollam, India

pragnavi1398@gmail.com, akhileshwarmaurya007@gmail.com,

bharathrao696@gmail.com, akashkrishnan705@gmail.com,

srijanagarwal.cse@gmail.com, mayamenon@am.amrita.edu

Abstract. Path planning plays a significant role in most of the applications in the field of robotics. Path planning ensures that the robot follows a planned and efficient path in the environment. This paper discusses the types of path planning, i.e., simple and coverage path planning. It explores the advancements made in the research and development of various algorithms and approaches under the two types. It also discusses the application of these path planning strategies in real-life scenarios. The final section describes the application of path planning in search and rescue operations in a disaster environment. Based on the study, some algorithms and approaches are suggested for the most efficient use of the robot in this scenario.

Keywords: Robotics · Simple Path Planning · Coverage Path Planning · Search operation

1 Introduction

The World Disaster Report released by The International Federation of Red Cross and Red Crescent Societies (IFRC) in 2016, between 2006 and 2016 shows that the total count of people outlined killed and affected by natural disasters are respectively 771,911 and 1,917,557 [1]. The government, NGOs, and aid organizations are all working to keep these tragic deaths as low as possible. The stats mentioned above include both casualties and rescuers who lost their own lives in the rescue of victims stuck in debris. Replacing human rescuers with search and rescue robots reduce the deaths to some extent.

Robots provide several benefits during disasters. They often fit into and operate in areas where humans cannot. Also, they can operate continuously without pause. Robots are capable of performing better than humans in many tasks. And the added advantage is that they can be replaced. Robots can be deployed in spaces which are too risky for rescue workers.

The first set of Search and Rescue robots were used to traverse the damage caused by the terrorist attacks in 2001 at New York, where the twin towers of World Trade Center were demolished. Starting then, the Center for Robot-Assisted Search and Rescue (CRASAR) deployed around fifty aerial and ground robots in different disaster scenarios. The major contributions of CRASAR include deployments in La Conchita Mudslides, La Conchita, California (USA) in the year 2005, Berkman Plaza II Collapse, Jacksonville, Florida (USA) in the year 2007, Fukushima Daiichi Nuclear Event, Fukushima (Japan), and Tohoku Earthquake and Tsunami (Japan) in the year 2011 [2].

There are many challenges in using robots for search operations. Some of the challenges are:

- Information processing of the robot
- Mobility/navigation of the robot
- Manipulation of the robot
- As the robots are not fully autonomous, critical decisions need to be taken in real-time by the controller teams, which operate remotely

Among these challenges, this paper addresses the autonomous navigation of the robot in a disaster environment. For a robot to navigate autonomously in a given environment, the following steps are required:

- Mapping - Initially, the robot must map the environment
- Sensing and Localization - The robot has to sense its surroundings and localize itself in the generated map
- Navigation - Identify an effective path from the source position to the target position and navigate autonomously

Most of the time, a team of robots involving both Unmanned Aerial Vehicles (UAV) and Unmanned Terrestrial Vehicles (UTV), is employed in SAR operations to perform search and rescue operations effectively. In such scenarios, UAVs survey the disaster environment simultaneously mapping it and also locate the probable victim presence on the map using PR sensors or camera imagery. UTVs use the map with probable victim presence and to go to the victim, validate the victim presence and detect whether the victim is alive or dead using thermal sensors. UTV has to navigate from the start node to the goal node efficiently by avoiding all the obstacles, considering its current position on the map to be the start node and one of the probable victim presence points to be the goal node. Thus UTV has to identify an optimal path from the start node to the target node in reasonably less time. This can be achieved by using different Simple Path Planning strategies which are discussed in the tailing sections of the paper.

Unlike natural disasters, there are some hindrances to use robots for search and rescue operations in case of human-instigated disasters such as terrorist attacks and explosions. Today, only about one fourths of the world's countries allow the use of robots in such situations. The major limitation is that, most of the time, it is difficult to differentiate between the SAR robots and the combat drones used for destruction. The SAR robots are often misunderstood for the

combat drones used for destruction. In such cases, only UTVs are employed in performing SAR operations. Assuming that UTVs map the entire environment, to detect both alive and dead victims, the UTV has to navigate to each and every node or grid in the map at least once. Unlike the previous case, this can be achieved by using different Coverage Path Planning strategies.

This paper talks about some of the popular simple path planning and coverage path planning strategies that are currently available in the literature.

2 Related Works

Path planning algorithms available today basically use either of the two approaches i.e Heuristics and Exact methods. One of the best comparisons done between the two is by Randria et al. In this study, 6 different algorithms (BFS, DFS, A*, Moore–Dijkstra, neural approach and GA) were taken for comparison based on 3 parameters: distance traveled by the mobile robot, the number of visited points and the computational time for each algorithm. A simulation environment was created and the algorithms were put to test. The simulation results showed that GA outperformed others when distance and execution time are taken into account. The simulation results obtained were for a small scale environment, thus there was a need for it to be tested in a large-scale environment [3].

The analysis performed by Zaremba and Kodors compares a couple of exact simple path planning algorithms with some popular heuristic simple path planning algorithms. The comparison was based on the execution times of the algorithms in grid environments. BFS and Dijkstra's were the chosen exact methods, while A*, LPA* and HPA* filled in the heuristic portion. From the results, it is evident that heuristic methods are faster than exact methods in terms of execution time. Among exact methods, Dijkstra's outperformed BFS, while HPA* outperformed the other two heuristic methods [4].

The heuristic function added to the cost function makes the heuristic algorithms outperform exact approaches in most of the cases. The heuristic approaches differ from each other based on their respective definition of the heuristic function. Thus choosing an appropriate heuristic function that best suits the search and rescue applications is also important. Xiang Liu and Diaxiong Gong from Beijing University of Technology compared three versions of A* algorithms intended for search and rescue operations. The three versions have three different definitions of heuristic functions. The performance of each version of the A* algorithm [5] is compared to one of the exact approaches namely Depth First Search. From the results, it is evident that all three heuristic methods outperformed the exact method in most of the cases. Of the three definitions of the heuristic function, the heuristic approach which adopts Euclidean distance to approximate the distance between the present node and the target node performed best [6].

A* algorithm is one of the popular heuristic approaches used for path planning in search and rescue operations. In one of the recent competitions involving

rescue robotics, a simulated urban disaster environment was given to the teams competing. ROS and Gazebo were used to tackle the situation. As a simulation environment is used, so the cost factor is not taken account and the best sensors and equipment are used so as to increase the efficiency of correctly finding a victim. Two types of robots were used: a wheeled Pioneer robot and an aerial robot. Sensors used: GPS, laser scanner, an ultrasound sensor, and an RGB camera. It's multi-robot cooperation where land-based agents were used for undertaking a more low-level search, and a joint map was built up firstly using UAVs and land-based vehicles to allow a more rapid rescue after which the land-based robots were dispatched to the victims. The land-based robots were navigated in the disaster environment using ROS Navigation Stack. Laser-based SLAM provided by the gmapping ROS package was used for mapping and the move-base package took care of the path planning. For more effective path planning the Dijkstra's algorithm implemented by the move-base package was replaced by another more efficient searching algorithm called A* searching algorithm for navigating between two points generated on the map [7].

Heuristic path planning approaches most likely give a near-optimal path, while exact approaches give an optimal path. In SAR operations it is important to find a near-optimal path which is close to the optimal path in reasonably less time. Considering the above requirement for SAR operations, Andel Ammar et al. proposed a Relaxed version of A* algorithm which runs in linear time. The Relaxed A*(RA*) algorithm finds a near-efficient path which is very close to the optimal path faster than A* algorithm. The results validate that RA* gives a better planned path in less time compared to the regular A* algorithm [8].

Coverage Path Planning is an approach which aims to find a path by exploring the entire environment efficiently. Considering efficiency, the robot is expected to visit all the nodes in the environment without overlapping with the path that is already visited. In 2001, Howie Choset published a survey on the coverage path planning techniques available to date. In his study, he classified coverage path planning algorithms into four types namely, heuristic, approximate, partial-approximate, and exact cellular decomposition [9].

In 2013, Enric Galceran et al. published an updated survey on the coverage path planning techniques including the advancements occurred after the previous survey. Apart from considering the classification made by Choset in his study, they further classified the algorithms into two types namely, off-line algorithms and on-line algorithms. The off-line algorithms best suited for applications where the environment is well-known and the obstacles are not dynamic. But in the case of disaster search operations, the robots are expected to navigate in a partially known environment where the obstacles are dynamic. The off-line coverage path planning algorithms do not serve the purpose in such cases. This is where the on-line coverage algorithms come into play. The on-line algorithms deal with the coverage path planning in unknown or partially known environments with dynamic obstacles [10].

The tailing sections of the paper detail some of the Simple and Coverage Path Planning algorithms and classify them accordingly considering advantages, disadvantages, and applications of the algorithms.

3 Simple Path Planning

Simple path planning requires to find a route from the current position to target position. This can be achieved by 2 different approaches, they are:

- Exact approach
- Heuristic approach

3.1 Exact Approach

Exact Approach is the one which gives an optimal path without any approximations involved in it. Dijkstra's algorithm, Breadth First Search (BFS) and Depth First Search (DFS) are some of the famous algorithms which come under the exact approach. Extensive research has already been done to explain the working of these algorithms.

BFS: It is one of the most widely used search algorithms. This algorithm when searching the environment expands the root node first and then all the successors of it are expanded. This function is repeated until the target node is found. At every expansion, the node is checked if it is the target node or not. The function used for the expansion of nodes for a BFS is

$$f_n = g_n \quad (1)$$

where $g(n)$ is determined by a FIFO queue. This algorithm always finds the shortest path on its first run with time complexity of $O(N+E)$, N being the node and E being the edge [11].

DFS: This algorithm uses a slightly different approach than BFS. It continues on the same path until it finds a dead end. This means that the descendants of the first sibling are checked before moving onto check the descendants of the other sibling. DFS uses the same function for expansion as a BFS i.e.,

$$f_n = g_n \quad (2)$$

But here it uses a LIFO stack for expansion. The stack contains the list of expanded nodes. DFS is most optimal when we have many possible solutions for a problem and we need to choose one among them. It has the same time complexity $O(n+e)$ as the BFS algorithm [12].

Dijkstra's Algorithm: Dijkstra's performs an uninformed search. Thus it does not need to know the goal node beforehand. Because of this, it's efficient in problems where we don't have any previous knowledge of the graph. This algorithm also uses the same function for expansion as BFS and DFS i.e.,

$$f_n = g_n \quad (3)$$

But here it expands the node with the least path cost. This is done by implementing a priority queue. The nodes are inserted and sorted in the priority queue with their path cost. This takes $O(\log Q)$ time, Q is the measure of nodes in the queue. The total time complexity being $O(n^2)$. One of the problems here is that since it does a blind search it takes more computation time [13].

3.2 Heuristic Approach

The heuristic approach includes approximations, unlike the exact approach. The heuristic approach gives a near-optimal path. A heuristic path planning approach is further classified into two sub-classes namely, Static Path Planning and Dynamic Path Planning.

Static Path Planning: It is a path planning approach that gives a one-time near-optimal path between the source node and the target node avoiding all obstacles. The application of Simple Path Planning is mostly in environments with static obstacles. A* algorithm is one of the most used algorithms in this category.

A Algorithm:* Unlike Dijkstra's algorithm, A* algorithm is an informed algorithm which considers the distance from the target node at every point. It is a combination of both the actual cost from the source node and the evaluated approximate cost to the target node. Thus the cost function here is modified to

$$f_n = g_n + h_n \quad (4)$$

where g_n is the distance between start node and the present node, while h_n is the approximate distance from the present node to the target node. The heuristic distance can be estimated using various distance measures. The most popular and basic techniques that are generally used in the A* algorithm are Manhattan distance and Euclidean distance. The heuristic nature of the algorithm contributes to a better speed-accuracy trade-off. The algorithm can lead us either to finding a near-optimal path in less time or finding an optimal path in reasonably greater time by gauging the heuristic cost accordingly. The time complexity of A* algorithm is $O(n^2)$.

Relaxed A Algorithm:* The basic version of the A* algorithm is a quadratic time algorithm. Time is a major influential factor in SAR operations. The faster the robot identifies the victims, more is the number of lives can be saved. Relaxed A*

algorithm reduces the time complexity of regular A* algorithm from quadratic to linear. The RA* (Relaxed A*) algorithm works similar to the A* algorithm while making sure that the robot is not visiting any grid more than once. The heuristic function is modified to

$$f_n = g_n + t_break * h_n \quad (5)$$

Where g_n is the cost required by the robot to reach the present grid from the source grid, h_n is the approximate cost required for the robot to reach the target grid and t_break is the tiebreaker. The value of the t_break is equal to $1 + \epsilon$, where ϵ is $1/(\text{length of the grid} + \text{width of the grid})$ [14].

Improved A Algorithm with Least Turns:* As discussed above, A* algorithm is a heuristic approach. The Relaxed A* (RA*) algorithm reduces the complexity by reducing the number of computations. The RA* algorithm strictly makes sure that no grid is visited more than once. The output given by the A* algorithm is not the same always. The algorithm generates different paths with the same path length after each pass. But the count of rotations the robot takes is different for all the paths. Although RA* algorithm reduces the complexity of the A* algorithm it still does not consider to optimize the rotation cost of the robot. Ashok M Choudary et al. introduced the Improved A* algorithm with least turns which optimizes the rotation cost of the robot. The cost function is modified to

$$f_n = g_n + h_n + R \quad (6)$$

Where h_n is the cost required by the robot to reach the present grid from the source grid, h_n is the approximate cost the robot takes to reach the target grid, and R is the rotation cost of the robot [15].

Dynamic Path Planning: It is the path planning approach that gives a dynamic or variable path between the start node and the target node, which adjusts itself with the dynamic obstacles in the given environment. Dynamic Path Planning generally suits best for real-life scenarios like search and rescue in a disaster environment where the obstacles are dynamic and unpredictable. The D* algorithm is a conventional Dynamic Path Planning Algorithm.

D* Lite Algorithm: D* lite can easily be used to navigate in an unknown terrain where the prime goal is to reach any particular node. It is a revised version of LPA*(Lifelong Planning A*) algorithm, which in turn is a revised version of A* algorithm. Since it is dynamic it considers the path which is already traversed. It does this with the help of the data structure heap and the process of heap reordering. D* lite efficiently computes the shortest path from goal to starting node. Computing shortest path in D* lite is similar to LPA*(Lifelong Planning A*) and guarantees that the shortest path is found correctly, if present and it terminates. Sven Koenig has proved that D* Lite performs better than both D* algorithm and A* algorithm involving no heuristic search. D* Lite also stands a tier apart from the other two algorithms when it comes to grid mapping.

Table 1. Simple path planning algorithms - pros and cons

Algorithm	Pros	Cons
Dijkstra's	<ul style="list-style-type: none"> Optimal in cases where there is no prior knowledge of the graph Useful when there are multiple nodes but the immediate closest node is not known 	<ul style="list-style-type: none"> Blind search is done where lot of time is wasted in processing Negative edges cannot be handled
BFS	<ul style="list-style-type: none"> Never fails in finding an optimal solution 	<ul style="list-style-type: none"> All the connected vertices must be stored in memory, so memory consumption is more
DFS	<ul style="list-style-type: none"> Less consumption of memory 	<ul style="list-style-type: none"> Optimal solution may not be found
A*	<ul style="list-style-type: none"> The focus here is to arrive at the target node as fast as possible, not to go around every other node 	<ul style="list-style-type: none"> Not optimal if the problem has many target nodes
RA*	<ul style="list-style-type: none"> With a better trade-off between the optimality of the solution and the time required, a major portion of the solution space is covered. Also, the execution time is remarkably reduced 	<ul style="list-style-type: none"> RA* does not assure an optimal solution. The obtained solution is near-optimal in most of the cases

Table 2. Simple path planning algorithms - complexities

Algorithm	Time complexity	Space complexity
Dijkstra's	$O(n^2)$	$O(n^2)$
	Grid Size: nxn	Grid Size: nxn
BFS	$O(m * n)$	$O(m + n)$
	Grid Size: mxn	Grid Size: mxn
DFS	$O(m * n)$	$O(m * n)$
	Grid Size: mxn	Grid Size: mxn
A*	$O(n^2)$	$O(n^2)$
	Grid Size: nxn	Grid Size: nxn
RA*	$O(n)$	$O(n)$
	Grid Size: nxn	Grid Size: nxn

D* Lite is better than D* as the former is built on LPA and the latter on A*. Also given that LPA is efficient than A* since it does not expand on vertices whose g-values are equal to goal distance. Thus D* Lite is a better Dynamic path planning algorithm [16] (Tables 1 and 2).

4 Coverage Path Planning

Coverage Path Planning (CPP) involves that a mobile robot should visit all available points in the enclosed area while avoiding obstacles using sensor information. This is an integral part of various real-life applications like cleaning

robots [17], painter robots [18], underwater vehicles [19] and lawn mowers [20]. CPP algorithms mostly use grid maps, where the value of each cell provides the probability of an obstacle. The CPP is similar to the covering salesman problem. The algorithms in this part can be divided as one among heuristic or complete based on whether or not they ensure full coverage of the environment. To achieve some form of provable assurance, many algorithms either directly or indirectly use cellular decomposition to ensure coverage. It focuses on breaking down the area into cells so that coverage in each cell is “simple”. The various approaches used are discussed below.

4.1 Heuristic and Randomized Approach

First and one of the basic approaches available is to randomize. This is commonly seen in cleaning robots. If the robot sweeps the surface randomly for sufficiently long time, the surface is assumed to be cleaned. One of the advantages is that we don’t need sensors for localization. Only one sensor is needed so as to prevent the robot from hitting the boundaries of the area. Also, no complex algorithms are necessary onboard. Hence, it is cost-efficient and easier to implement. One of the heuristics, repulsion from other robots, makes sure that the agents spread out during the search phase, and thus cover the area more uniformly. This heuristic, and others, like obstacle avoidance, are combined to provide the overall behavior of the robot. The robots in this approach do not plan search paths, instead select directions at random until they encounter an object for retrieval.

4.2 Approximate Cellular Decompositions

In this the area is approximated with a fine representation of the free space that covers the area, and the algorithm is implemented in the grid [21]. Here, it is assumed that once the robot enters a cell, it has covered the cell. When the robot goes through each cell in the decomposition, coverage is complete. Zelinsky et al. used the distance transform to find a coverage path. The algorithm initially marks 0 to the target and then a 1 to all nearby cells. After this, all unmarked cells near the marked 1 are then marked with a 2. This procedure goes on until it goes past the start. Once this happens, the robot uses gradient descent on this numeric potential function to find a path. The main problem here is that it does not look into kinematic constraints [22].

4.3 Semi-approximate

This focuses on partial discretization of the area where the cells have a fixed width but the top and bottom can be of any shape. Hert et al. presented an algorithm which applies to this kind of decomposition. The algorithm applies to a 3D planar space by extending a 2D terrain-covering algorithm. The algorithm is recursive in nature [23]. Robots using this algorithm may start at any point in the area and will zigzag along parallel straight lines to cover the given area.

Portions that either would not be covered or would be covered twice are called inlets. These inlets are covered as soon as they are detected and inlets within inlets are treated in the same way. Due to this the inlets are covered in depth-first order. The robot is to remember the points at which it enters and exits every inlet it covers. This makes sure that every inlet is covered only once. One advantage of this approach is that the algorithm can be implemented on-line [24].

4.4 Exact Cellular Decompositions

This approach breaks the free space down into simple regions called cells. The union of these gives us the free space. The free space is “easy” to cover and can be done by the robot using simple motions- simple back and forth motions. A popular technique in this approach is the trapezoidal decomposition, in which the free space is decomposed into cells having shape like a trapezoid. Coverage in each cell can be done again by simple motions. Coverage of the region is achieved by going through each cell in the adjacency graph. An upgrade to this was provided by VanderHeide and Rao [25], which proposed a sensor-based version of this technique.

5 Conclusion

In this section, we talk about the use of robots in search and rescue operations and propose an efficient way to approach such situations based on the research done above. In search and rescue operations in a disaster-affected environment, time is the most important factor. As time passes, there will be an increase in the loss of human life and property. The region will be damaged and it will be difficult for disaster relief teams to go in certain places or under debris. Thus, robots play an important part in this [26]. So, instead of the relief teams going all around the area and rescuing people, the mobile robots will be used for this. The robot will go around the area and identify if a human is alive and dead and inform the same to a remote control room. It will also give an efficient path to reach the victim in minimum time. From the literature analysis, it is clear that among all the available Simple Path Planning algorithms, the Relaxed A* algorithm, which works in linear time is more efficient for the purpose of Search and Rescue operations where time is a major constraint. Also, the Improved A* algorithm with least turns reduces the rotation cost which indirectly contributes to optimizing the time required by the robot. Further research can be made to verify the feasibility of a hybrid approach which combines Relaxed A* algorithm with the Improved A* algorithm with least turns which might increase the efficiency of the Relaxed A* algorithm by optimizing the time required. Coming to Coverage path planning, not much research has been done on the approaches available and their application in search and rescue operation. So, we conclude that more research has to be done in the coverage path planning approaches and their various applications and RA* is the most efficient algorithm in case of search and rescue operation involving mobile robots.

References

1. Chester, D.: International federation of red cross and red crescent societies, world disasters report 1994 (book review). *Third World Plann. Rev.* **17**(3), 357 (1995)
2. Murphy, R.R.: A decade of rescue robots. In: 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 5448–5449. IEEE (2012)
3. Randria, I., Khelifa, M.M.B., Bouchouicha, M., Abellard, P.: A comparative study of six basic approaches for path planning towards an autonomous navigation. In: IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society, pp. 2730–2735. IEEE (2007)
4. Zaremba, I., Kodors, S., et al.: Pathfinding algorithm efficiency analysis in 2D grid. In: Proceedings of the 9th International Scientific and Practical Conference, vol. 1 (2013)
5. Chaudhari, A.M., Apsangi, M.R., Kudale, A.B.: Improved a-star algorithm with least turn for robotic rescue operations. In: International Conference on Computational Intelligence, Communications, and Business Analytics, pp. 614–627. Springer (2017)
6. Liu, X., Gong, D.: A comparative study of a-star algorithms for search and rescue in perfect maze. In: 2011 International Conference on Electric Information and Control Engineering, pp. 24–27. IEEE (2011)
7. Cheah, M., Gilday, K., Hughes, J.: Cambridge robotics robocup virtual rescue simulation
8. Ammar, A., Bennaceur, H., Chaari, I., Koubaa, A., Alajlan, M.: Relaxed Dijkstra and A* with linear complexity for robot path planning problems in large-scale grid environments. *Soft. Comput.* **20**(10), 4149–4171 (2016)
9. Choset, H.: Coverage for robotics-a survey of recent results. *Ann. Math. Artif. Intell.* **31**(1–4), 113–126 (2001)
10. Galceran, E., Carreras, M.: A survey on coverage path planning for robotics. *Robot. Auton. Syst.* **61**(12), 1258–1276 (2013)
11. Coenen, S., Steinbuch, M.M.: Motion planning for mobile robots a guide. *Control Syst. Technol.* **79** (2012)
12. Giesbrecht, J.: Global path planning for unmanned ground vehicles. Technical report, defence research and development suffield (alberta) (2004)
13. Soltani, S., Tawfik, H., Goulermas, J., Fernando, T.: Path planning in construction sites: performance evaluation of the dijkstra, A, and GU search algorithms. *Adv. Eng. Inf.* **16**(4), 291–303 (2002). <http://www.sciencedirect.com/science/article/pii/S1474034603000181>
14. Yang, S.X., Luo, C.: A neural network approach to complete coverage path planning. *IEEE Trans. Syst. Man Cybern. Part B (Cybern.)* **34**(1), 718–724 (2004)
15. Atkar, P.N., Greenfield, A., Conner, D.C., Choset, H., Rizzi, A.A.: Uniform coverage of automotive surface patches. *Int. J. Robot. Res.* **24**(11), 883–898 (2005). <https://doi.org/10.1177/0278364905059058>
16. Hert, S., Tiwari, S., Lumelsky, V.: A Terrain-Covering Algorithm for an AUV, pp. 17–45. Springer, Boston (1996)
17. Cao, Z.L., Huang, Y., Hall, E.L.: Region filling operations with random obstacle avoidance for mobile robots. *J. Robot. Syst.* **5**(2), 87–102 (1988). <https://doi.org/10.1002/rob.4620050202>
18. Spires, S.V., Goldsmith, S.Y.: Exhaustive geographic search with mobile robots along space-filling curves. In: Drogoul, A., Tambe, M., Fukuda, T., (eds.) *Collective Robotics*, pp. 1–12. Springer, Heidelberg (1998)

19. Choi, Y., Lee, T., Baek, S., Oh, S.: Online complete coverage path planning for mobile robots based on linked spiral paths using constrained inverse distance transform. In: 2009 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 5788–5793, October 2009
20. Latombe, J.: Boston, Kluwer Academic (1991). <https://doi.org/10.1007/978-1-4615-4022-9>
21. Galceran, E., Carreras, M.: Efficient seabed coverage path planning for ASVs and AUVs. In: 2012 IEEE/RSJ International Conference on Intelligent Robots and Systems (2012)
22. Devi, A., Vanualailai, J., Kumar, S.A., Sharma, B.: A cohesive and well-spaced swarm with application to unmanned aerial vehicles. In: 2017 International Conference on Unmanned Aircraft Systems (ICUAS), pp. 698–705, Miami (2017). <https://doi.org/10.1109/ICUAS.2017.7991342>
23. Geedhu, K.V., Ramachandran, K.I., Adarsh, S.; Canfis based robotic navigation. In: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1660–1664, Udupi (2017). <https://doi.org/10.1109/ICACCI.2017.8126081>
24. Gopalapillai, R., Gupta, D., Sudarshan, T.S.B.: Experimentation and analysis of time series data for rescue robotics. In: Thampi, S.M., Abraham, A., Pal, S.K., Rodriguez, J.M.C. (eds.) Recent Advances in Intelligent Informatics, pp. 443–453. Springer, Cham (2014)
25. VanderHeide, J.: Terrain coverage of an unknown room by an autonomous mobile robot, December 1995
26. Suresh, A., Ajithkumar, N., Kalathil, S.T., Simon, A., Unnikrishnan, V.J., Mathew, D.P., Basil, P., Dutt, K., Udupa, G., Hariprasad, C.M., Menon, M., Balakrishnan, A., Ramachandran, R., Murali, A., Shankar, B.: An advanced spider-like rocker-bogie suspension system for mars exploration rovers. In: Robot Intelligence Technology and Applications 4, Part of the Advances in Intelligent Systems and Computing book series, vol. 447, pp. 423–447. Springer, Cham (2017)



Secrecy Capacity of Symmetric Keys Generated by Quantising Channel Metrics Over a Fading Channel

L. Srividya¹(✉) and P. N. Sudha²

¹ Department of ECE, Dayananda Sagar College of Engineering,
Bangalore 560078, India

lsrividya@gmail.com

² Department of ECE, K.S. Institute of Technology, Bangalore 560109, India
pnsudha@gmail.com

Abstract. Physical layer security has become the cornerstone of the wireless communication system. Key generation by channel estimation enables legitimate users to generate keys in a decentralised manner than sharing secret information in open wireless mediums. In this paper we propose secrecy evaluation of symmetric keys which are, generated by channel metrics estimated over the Rayleigh fading channel, encrypted and transmitted over a fading channel in the presence of an eavesdropper. The results are obtained in terms of secrecy capacity and outage probability for various key sizes, different position of eavesdroppers from the source. It is seen that as key size increases and distance of eavesdropper increases from the source the secrecy capacity increases. Also the performance of keys derived from various channel metrics such as complex channel path gains, EVM rms and complex phase difference are discussed in this paper.

Keywords: Physical layer security · Key generation · One time pad encryption · Channel metrics · Secrecy capacity · Quantisation · Outage probability

1 Introduction

Physical layer security has become the cornerstone of the communication system as loss of physical layer security results in the total exposure while other layer results without the catastrophic effect. Hence it has become a prime research area of the recent times. In the information theoretic approach, many works are being carried on implementing cryptographic algorithms at physical layer level [1]. Symmetric key encryption has become attractive due to its simplicity in implementation particularly in restricted environment where memory, processing capacity, power is a constraint. However strong the encryption algorithm might be but if the key is compromised while sharing it, results in data exposure. Hence, now a days there is a shift in the paradigm from developing computationally more complex encryption algorithm to securely generating and sharing symmetric key algorithms. Similarly however strong the key

might be it is always prone to malicious attacks as it is shared over a common wireless channel which are open medium and easily accessible [2].

Hence decentralisation of key generation is the solution for this problem. The reciprocity property of the channel between the two legitimate users and its decorrelation in space, makes it secure with respect to possible illegitimate users, is used [8]. The physical layer security is predominantly focused in random time varying component of wireless channel. The physical layer measurements are the typical source of information for two legitimate users and therefore can be processed in order to obtain common bits. Key generation chain consists of channel probing, randomness extraction, quantization, information reconciliation and privacy amplification [6]. Using simple data acquisition process we can probe the channel and get time varying random metrics such as RSSI, CIR, complex channel gains, complex phase difference, EVMrms and so on. Quantization is done on the absolute scales and convert it in processable binary bit sequences [8, 9, 13]. Information reconciliation is essential as imperfect reciprocity and random noise results in mismatch of bits, reconciliation corrects and deletes these using minimum channel data. Privacy amplification is done to select number of secret bits to avoid illegitimate user to deduce the secret bit sequence.

In this paper we focus on the first part of the key generation chain that is channel probing, quantization as we generate a random symmetric key from channel metrics, encrypt, pass it to a fading channel and measure its secrecy capacity and outage probability. Here we have used One time pad encryption scheme as it is proven to achieve Shannon perfect secrecy [13]. Also it is the simplest algorithm which consumes less memory, less computation, perfect for restricted environments [11]. But requires key to be of the same size of the input. Hence we also examine secrecy capacity of the generated symmetric keys from the channel metrics over different key sizes over practical Rayleigh fading.

The rest of the paper is organised this way. Key Generation Phase, Channel Threat Model, Proposed System Model, Simulation Results and Analysis, Conclusion and Future Work.

2 Key Generation Phase

We have implemented simple data acquisition of Rayleigh channel metrics in Simulink model. We have passed an reference binary data from a discrete memory less Bernoulli generator into a 16-QAM modulator and Rayleigh channel and acquired three metrics simultaneously in order to compare the results, the acquired random complex data is further processed for quantisation in order to obtain sequence of binary bits of same size of input data as one time pad encryption scheme requirement.

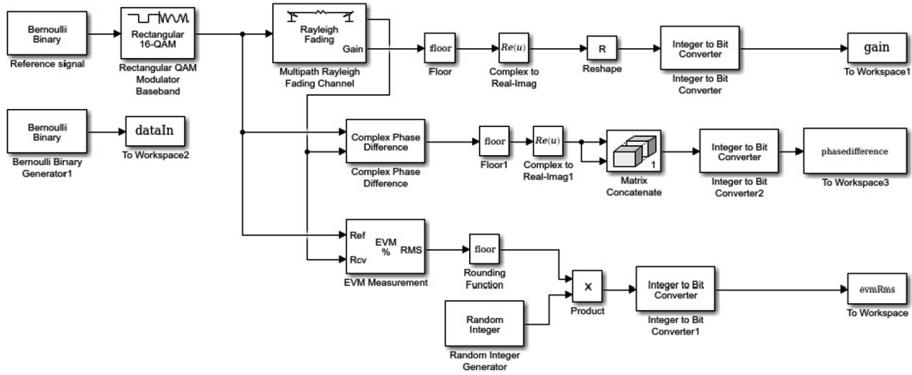


Fig. 1. Key generation from channel metrics.

Figure 1 shows the Simulink model of the proposed key generation scheme, gain port of the Rayleigh channel block outputs the complex path gain for each path, Complex phase difference block outputs the phase difference between the two complex input signals. This we have measured before and after passing values to the channel. Its range is $-\pi$ to π . EVMrms estimates the RMS Error Vector Magnitude (EVM) between two signals; one is reference signal and a corrupted received signal of the input frame. Power values are expressed in Watts with respect to 1Ω .

Obtained complex values is quantised on absolute scales and processed to get binary output form. This generated binary bit sequence whose length is equal to the input data of the encryptor is taken as the input to the for OTP encryption as cryptographic symmetric key.

The simulated output is saved in the workspace of the MATLAB which is considered during the execution of the encryption and channel secrecy estimation.

3 Channel Threat Model

Figure 2 depicts the two hop decode and forward Wyner's wiretap channel model where the information from source to destination reaches in two hops via legitimate relay. Eavesdropper is assumed to be located at a distance d_{se} from the source. Two legitimate nodes have been assumed to establish a secure link by one time pad encryption [9]. The secrecy conditions are measured at one stop relay node which is located at a distance d_{sr} . Source is assumed to generate output which is the encrypted output of key generated by channel metrics and input data source. The two hop channel is assumed to be a fading wireless channel where each node has decode and forward capability. The eavesdropper channel is assumed to be degraded by a factor a .

Using this Wyner's wiretap channel model we try to evaluate the secrecy capacity by fixing the distance between legitimate relay node, d_{sr} , as 500 m and varying the distance between the eavesdropper and the source, d_{se} , 50 m, 500, and 1000 m respectively. The secrecy capacity is further calculated from the received SNR at relay and eavesdropper.

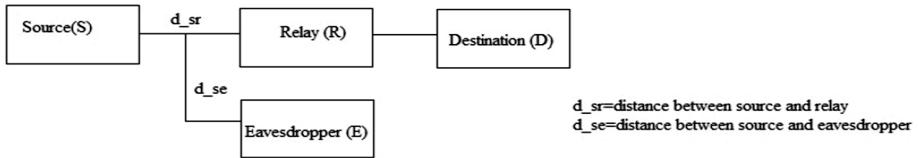


Fig. 2. Two hop DF Wyner's Wiretap Channel Threat Model

4 Proposed System Model

An input data is generated from a random generator, the key generation model is stimulated and three keys are obtained (derived from Complex path gain (gain), complex phase difference (phase difference) and EVM rms (evmRms)). The data with key (Anyone key) is encrypted. A fading legitimate channel with path loss coefficient alpha = 3.5, Secrecy Rate $Rs = 0.1$, noise variance -60 dBm over various global transmit powers ranging from -5 dBm to 35 dBm is stimulated and SNR_SR at first hop relay at a distance of d_{sr} from the source is measured. We have assumed it to be 500 m. Similarly a fading eavesdropper channel with path loss coefficient alpha = 3.5, Secrecy Rate $Rs = 0.1$, noise variance -60 dBm over various global transmit powers ranging from -5 dBm to 35 dBm is stimulated and SNR_SE at first hop relay at a distance of d_{se} from the source is measured. We have obtained for 50 m, 500 m, 1000 m and estimated total received at eavesdroppers SNR_E_linear . The secrecy capacity of two hop DF relying system is estimated using the formula [5]

$$P(Cs) = (1/2) * \log 2((1 + SNR_SR)/(1 + SNR_E_linear)). \quad (1)$$

The outage probability is estimated using the formula [3]

$$P(outage) = (1 - (SNR_SR/(SNR_SR + (2^Rs) * (SNR_SE))) * \exp(-((2^Rs) - 1)/SNR_SR)). \quad (2)$$

The graph $P(Cs)$ Vs Global transmit power in dBm is plotted. Also the graph $P(Outage)$ Vs Global transmit power in dBm is plotted. The above steps, for various key sizes (64, 128, 256, 1000), channel metrics (gain, phase difference, evmRms), d_{se} (50 m, 500 m, 1000 m), are repeated.

Here we have to remind that both sides of communication link are running algorithm at the same time but independently, we believe on the channel coherence time to slower transmission time to ensure both ends observe the same fading effects [10].

Secrecy capacity is defined as the maximum transmission rate from the source to the destination where the malicious eavesdropper is not able to access the information [12]. According to the information theory to achieve this, the mutual information must satisfy the condition $I[x:y] > I[x:z]$ where x = input, y = legitimate output, z = output at the eavesdropper.

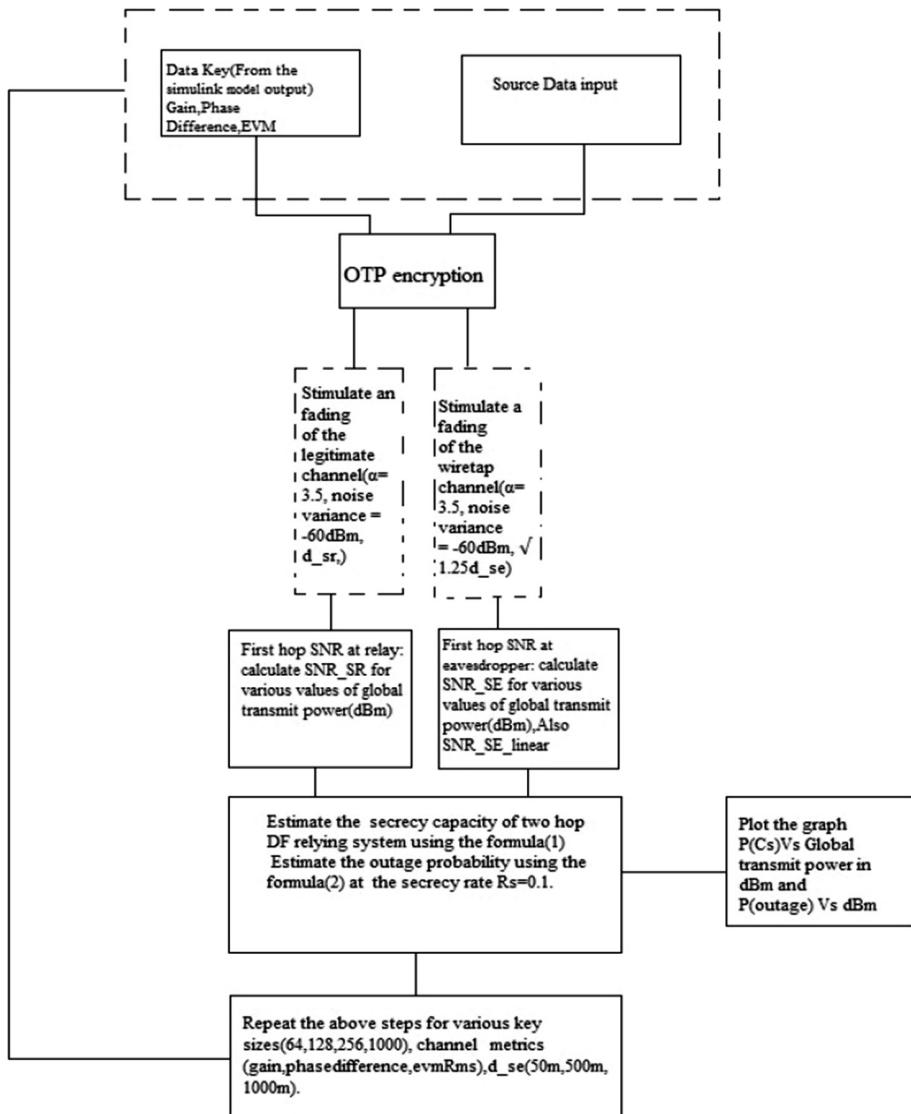


Fig. 3. Flow chart of the proposed system model

Secrecy capacity(C_s) is the difference of capacity through the legitimate link(C_r) and eavesdropper link(C_e), which implies that the system is secure if the values of C_s are positive. [5]

$$C_s = [C_r - C_e] + . \quad (3)$$

C_s is a random variable as it is a function of random channel gains. Therefore we study outage probability [14]. It is the probability that the instantaneous secrecy capacity is less than a target secrecy rate $R_s > 0$. Source assumes that eavesdroppers capacity $C_e' = Cr - R_s$. As long as the secrecy rate $R_s < C_s$ the Eavesdropper channel capacity C_e will be worse than source estimate C_e' that is $C_e < C_e'$. So the wiretap codes used by the source will ensure perfect secrecy. Else if $R_s > C_s$ then $C_e > C_e'$ and information theoretic security is compromised.

$$\text{When } SNR_{SR} \gg SNR_{SE}; \text{ outage probability is} \\ = (1 - \exp(-((2^R_s) - 1)/SNR_{SR}))). \quad (4)$$

While $SNR_{SE} \gg SNR_{SR}$; outage probability approaches unity [3, 15].

In our proposed model we try to analyse the effect of key size and complexity on the secrecy of the channel. whether we are able to achieve secure transmission still with the trade off of key size and complexity. Also we try to analyse the effect of position of eavesdropper, in this situation, on the secrecy capacity of the channel (Fig. 3).

5 Stimulation Results and Analysis

5.1 Stimulation Results for Secrecy Capacity Versus Global Transmit Power

Figure 4 shows the simulation results of the secrecy capacity versus global transmit power (dBm) taking evmRms as input for key. Also each graph contains four plotting with respect to different key sizes 64 bits, 128 bits, 256 bits, 1000 bits. Graph (a) shows that secrecy capacity is negative irrespective of power level hence secrecy is lost. Graph (b) and (c) graph shows that as the eavesdropper moves away and number of bits increases the secrecy capacity increases.

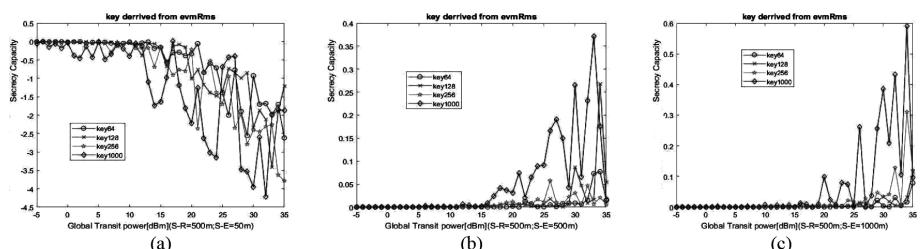


Fig. 4. C_s vs Global transmit power (dBm) while evmRms taken as input for key. The graphs a, b, c, shows the variation of C_s with respect distance from source to the eavesdropper at 50 m, 500 m and 1000 m respectively.

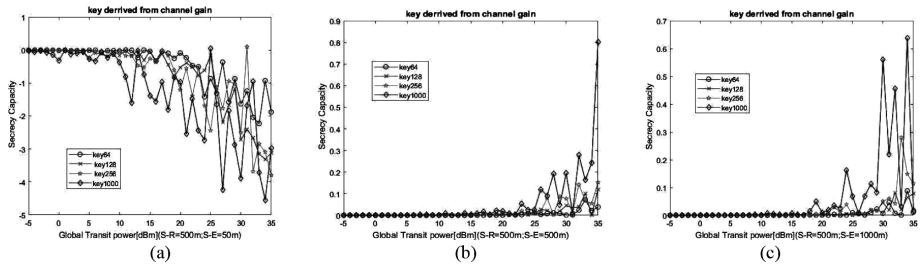


Fig. 5. C_s vs Global transmit power (dBm) while channel gain taken as input for key. The graphs a, b, c, shows the variation of C_s with respect distance from source to the eavesdropper at 50 m, 500 m and 1000 m respectively.

Figure 5 shows the simulation results of the secrecy capacity versus global transmit power (dBm) taking the complex channel path gains as input for key. Also each graph contains four plotting with respect to different key sizes 64 bits, 128 bits, 256 bits, 1000 bits. Graph (a) shows that secrecy capacity is negative irrespective of power level hence secrecy is lost. Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the secrecy capacity increases.

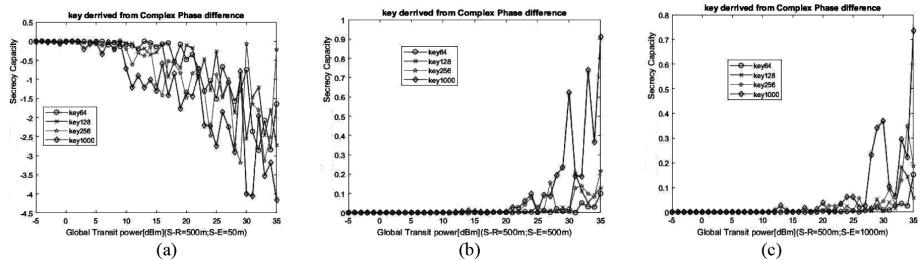


Fig. 6. C_s vs Global transmit power (dBm) while complex phase difference taken as input for key. The graphs a, b, c, shows the variation of C_s with respect distance from source to the eavesdropper at 50 m, 500 m and 1000 m respectively.

Figure 6 shows the simulation results of the secrecy capacity versus global transmit power (dBm) taking the complex phase difference as input for key. Also each graph contains four plotting with respect to different key sizes 64 bits, 128 bits, 256 bits, 1000 bits. Graph (a) shows that secrecy capacity is negative irrespective of power level hence secrecy is lost. Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the secrecy capacity increases.

Analysis for effect of channel metrics on secrecy capacity

As key size increases the secrecy capacity is becoming more positive. At lower transmit powers, secrecy capacity increase above R_s when channel gain is taken as input for key. Similarly at higher transmit powers gain and phase difference as the input for key achieves high C_s values.

5.2 Stimulation Results for Outage Probability Versus Global Transmit Power

Figure 7 shows the simulation results of the outage probability versus global transmit power (dBm) taking the evmRms as input for key. Also each graph contains four plotting with respect to different key sizes 64 bits, 128 bits, 256 bits, 1000 bits. Graph (a) shows that outage probability is unity as theoretical values but dips at higher power level and key sizes. Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the outage probability decreases hence giving more probability of high secrecy capacity at the given secrecy rate which is taken as 0.1. The spikes in between is due to the random function introduced in fading.

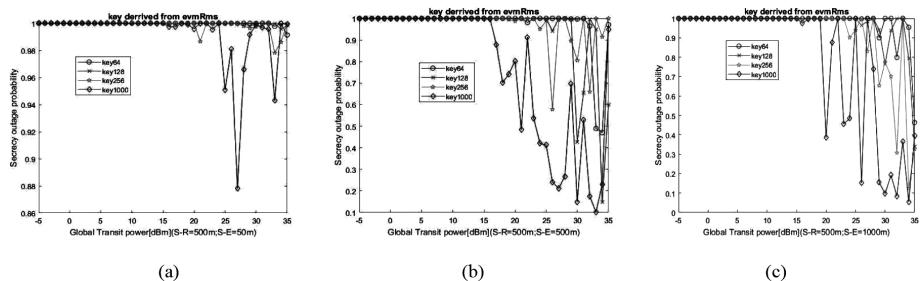


Fig. 7. Outage Probability vs Global transmit power (dBm) while evmRms taken as input for key. The graphs a, b, c, shows the variation of $P(\text{outage})$ with respect distance from source to the eavesdropper at 50 m, 500 m and 1000 m respectively.

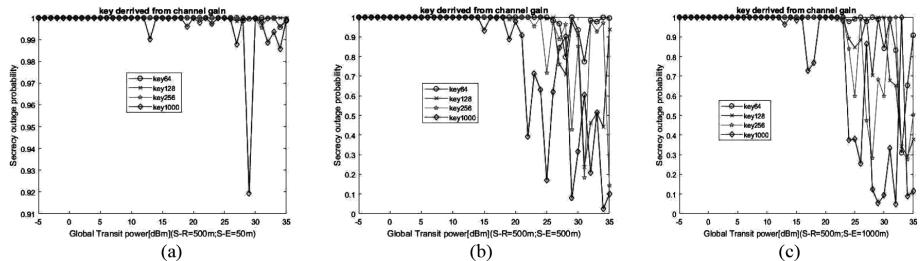


Fig. 8. Outage Probability vs Global transmit power (dBm) while complex phase difference taken as input for key. The graphs a, b, c, shows the variation of $P(\text{outage})$ with respect distance from source to the eavesdropper at 50 m, 500 m and 1000 m respectively.

Figure 8 shows the simulation results of the outage probability versus global transmit power (dBm) taking the complex channel path gains as input for key. Also each graph contains four plotting with respect to different key sizes 64 bits, 128 bits, 256 bits, 1000 bits. Graph (a) shows that outage probability is unity as theoretical values but dips at higher power level and large key sizes. Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the outage probability decreases hence giving more probability of high secrecy capacity at the given secrecy rate which is taken as 0.1. The spikes in between is due to the random function introduced in fading.

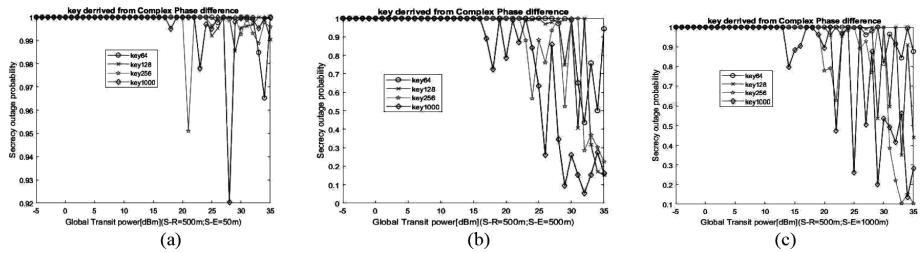


Fig. 9. Outage Probability vs Global transmit power (dBm) while complex phase difference taken as input for key. The graphs a, b, c, shows the variation of $P(\text{outage})$ with respect distance from source to the eavesdropper at 50 m, 500 m and 1000 m respectively

Figure 9 shows the simulation results of the outage probability versus global transmit power (dBm) taking the complex phase difference as input for key. Also each graph contains four plotting with respect to different key sizes 64 bits, 128 bits, 256 bits, 1000 bits. Graph (a) shows that outage probability is unity as theoretical values but dips at higher power level and large key sizes. Graph (b) and (c) shows that as the eavesdropper moves away and number of bits increases the outage probability decreases hence giving more probability of high secrecy capacity at the given secrecy rate which is taken as 0.1. The spikes in between is due to the random function introduced in fading.

Analysis for effect of channel metrics on outage probability

As key size increases the outage probability dips at the earliest compared to lower key sizes, which means that even at low power levels and $\text{SNR}_{SE} > \text{SNR}_{SR}$ we are able to achieve transmission rate greater than secrecy rate hence achieving secrecy with larger key sizes. The performance while taking phase difference as input for key at lower transmit powers (around 15 dBm) and evmRms, gain at relatively high transmit power(around 20 dBm) is at its best comparatively.

6 Conclusion and Future Work

A key generation scheme was proposed using channel metrics which was acquired by stimulating Rayleigh fading channel and encrypted with the information data and transmitted over an fading channel. The performance evaluation of various keys sizes, channel metrics and d_se were conducted and analysed under various global transmit powers.

Higher key sizes resulted in better secrecy capacity compared to low sized keys and also in case of outage probability it resulted in better performances. It is affirmed that as the distance between eavesdropper and source increases secrecy capacity increases and outage probability decreases.

The performances as various channel metrics as a key input were evaluated and each proved better at various combination of transmit power levels and d_se. The performance while taking phase difference as key input at lower transmit powers (around 15 dBm) and evmRms, gain at relatively high transmit power (around

20 dBm) was having better secrecy capacity. In case of outage probability, phase difference as key input had less outage probability at lower power levels (around 15 dBm) while gain, evmRms had better performance at 20 dBm.

Further this work can be improvised by information reconciliation and privacy amplification. Also can be extended by improvising its BER performances over fading channels by error control coding mechanisms [7].

References

1. Srividya, L., Sudha, P.N.: Literature survey on recent audio encryption techniques. *Int. J. Electron. Commun. Eng. Technol. (IJECE)* **7**(6), 91–95 (2016). Article ID: IJECE_07_06_013
2. Srividya, L., Sudha, P.N.: Physical layer secret symmetric key generation and management techniques for wireless systems-a study. *JASC: J. Appl. Sci. Comput.* **VI**(II) (2019). ISSN NO 1076-5131
3. Bloch, M., Barros, J., Rodrigues, M., McLaughlin, S.: Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **54**(6), 2515–2534 (2008)
4. Barros, J., Rodrigues, M.: Secrecy capacity of wireless channels. *IEEE Trans*
5. Nosrati, E., Wang, X., Khabbazibasmenj, A.: Secrecy capacity enhancement in two-hop DF relaying systems in the presence of eavesdropper. In: *IEEE ICC - Communication and Information Systems Security Symposium*, pp. 7365–7369 (2015)
6. Tunaru, I.: Physical layer secret key generation for decentralized wireless networks, signal and image processing, Université Rennes 1, Europe (2015)
7. Sudha, P.N.: Speech compression and error correction for mobile communication, JNTU, Anantapur, India (2012)
8. Wang, T., Liu, Y., Vasilakos, A.: Survey on channel reciprocity based key establishment techniques for wireless systems, 13 January 2015. Springer, New York (2015)
9. Sahin, C., Katz, B., Dandekar, K.: Secure and robust symmetric key generation using physical layer techniques under various wireless environments, pp. 211–214. IEEE (2016)
10. Kostov, N.: Mobile radio channels modeling in MATLAB, n. kostov, mobile radio channels modeling in MATLAB
11. Harrison, W.: *Physical-layer security: practical aspects of channel coding and cryptography*, Georgia Institute of Technology (2012)
12. Padala, A., Kommana, K.: Performance of physical layer security with different service integrity parameters, Blekinge Institute of Technology SE-37179 Karlskrona, Sweden
13. Limmanee, A., Henkel, W.: Secure physical-layer key generation protocol and key encoding in wireless communications. In: *IEEE Globecom Workshop on Heterogeneous, Multi-hop Wireless and Mobile Networks* (2010)
14. Goel, S., Negi, R.: Obtaining secrecy through intentional uncertainty. In: Liu, R., Trappe, W., (eds.) *Securing Wireless Communications at the Physical Layer*, vol. 2, Springer (2010). <https://doi.org/10.1007/978-1-4419-1385-2>
15. Gungor, O., Tan, J., Koksal, C., El-Gamal, H., Shroff, N.: *Secrecy Outage Capacity of Fading Channels*, vol. 43210. The Ohio State University, Columbus



Orthogonal Frequency Division Multiplexing-Multiple Input Multiple Output Channel Estimation for Rayleigh and Rician Channel Models

R. B. Hussana Johar^(✉) and B. R. Sujatha

Department of ECE, Malnad College of Engineering, Hassan, Karnataka, India
husnavais@gmail.com, brshsn61@gmail.com

Abstract. Mobile users experience the effect of change involved in channel characteristics. System delay leads the outdated channel state information (CSI) and that will be used for adaptive modulation techniques. By using adapt modulation techniques can predict the future CSI with the help of channel prediction approaches. The primary contribution of this paper is a low complexity channel prediction method using polynomial approximation. In this paper, orthogonal frequency division multiplexing (OFDM) is designed for radio band communication to moderate inter symbol interference and thus increase the system capacity. A comparison of MIMO-OFDM using BPSK and QAM on Rayleigh and Rician channels, by designing the STCP estimators through a 2×2 multi antenna system using MATLAB is done.

Keywords: Orthogonal frequency division multiplexing (OFDM) · Additive white gaussian noise (AWGN) · Minimum mean square estimator (MMSE) · Spatial Temporal channel prediction (STCP)

1 Introduction

Wireless communication has endorsed an excellent gain in prime users, bit rate demands and has been used for broadcasting for several decades. As the requirement for bit rate and system capacity increases, researchers and system engineers must evolve capable techniques. A familiar method is to enhance the radio bandwidth and bandwidth usage expending to a wideband frequency selective channel. Explicit familiarity of time-fluctuating radio channel aspects is necessary for present and future communication systems where the channel power may differ by many forms of amplitude over a very precise range explored by wireless station. Scattered transmission, however, yet confines perhaps attained from enlarged bandwidth.

To ensure huge data rates at improved Quality of Service in wireless conditions is a specific major issue of the next generation cellular systems [1], in addition to enhanced spectral capability. One of the techniques employed is OFDM-MIMO is a sequence of multiplexing and antenna diversity. Linking the two methods can ensure higher data rate, distance and accuracy without demanding added bandwidth. It utilizes non-overlapping neighbor channels to improve radio spectrum accuracy and permit many

carriers be used to propagate distinct symbols with spectral fold over while assuring conjunction of overlapping signals as a result of orthogonality.

In recent days several transmission techniques, including modulation, power control and channel coding and antenna diversity is being applied to fast, time variant fading channel environments. Prediction of the channel coefficients-tens-to-hundreds of symbols is needed to realize these processes in practice.

Finally, outcome of diverse simulations are correlated to wind up that STCP algorithm afford analogously finer outputs with the realization of OFDM-MIMO system. He et al. [2] have used linear and Gaussian interpolation algorithm to reduce the feedback overhead caused by beam forming on every subcarrier in MIMO-OFDM system. However, the actual model that describes the relation between BER and SNR with limited feedback has not been developed.

Duel-Hallen et al. [3] have described long-range fading channel prediction algorithm for simulating stationary fading models and tested with measured data and with data produced by physical channel model. We make use of the approximate formula developed by them to evaluate the average BER for the given SNR.

The rest of the paper has the proposed system in Sect. 2 followed by the schematic representation, related work in Sect. 2 and results in Sect. 3 and conclusion in Sect. 4.

2 Proposed System

The flow diagram of implemented OFDM-MIMO system is as shown in Fig. 1.

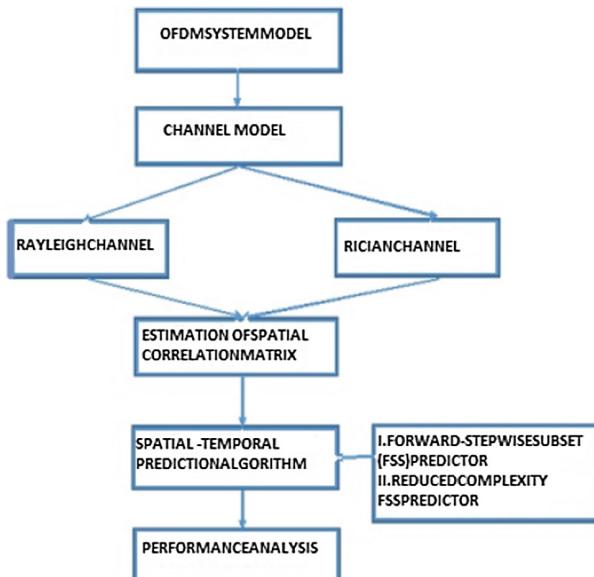


Fig. 1. Flow Diagram of OFDM-MIMO System

2.1 Schematic Representation

OFDM-MIMO system is having M transmit and N receive antennas, and K subcarriers on the transmission side. The transmitted symbol $X_m(i, k)$ is converted into the time domain signal at the m-th transmit antenna, i-th symbol time using the k-th subcarrier using IFFT. Then, a cyclic prefix is added to reduce inter-symbol interference [4].

At the destination, to begin with the cyclic prefix is eliminated by the FFT system. The cyclic prefix is larger than maximum delay spread of the channel, and frequency, time integration is efficient. The conventional signal received at receiver antenna is given by,

$$Y_n(i, k) = \sum_{m=1}^M H_{n,m}(i, k)X_m(i, k) + Z_n(i, k), \quad (1)$$

In Eq. (1) Z_n denotes AWGN and $H_{n,m}$ is the channel gain between the mth receive and nth transmit antenna pair. The wireless channel has its impulse response expressed as,

$$h_{n,m}(t, \tau) = \sum_{l=0}^{L_{n,m}-1} h_{n,m}(t, l)\delta(\tau - \tau_{n,m}(l)), \quad (2)$$

At the pilot positions, least square (LS) channel estimation utilizes the received symbol $Y_n(i, k)$ and noted pilot symbol $X_m(i, k)$ given by,

$$\begin{aligned} \hat{H}_{n,m}(i, k_m, j) &= Y_n(i, k_m, j)/X_m(i, k_m, j) \\ &= H_{n,m}(i, k_m, j) + Z'_{n,m}(i, k_m, j) \end{aligned} \quad (3)$$

2.2 Spatial Correlation Matrix Estimation

The wireless communication system performance can be improved by maintaining distinct antennas at the transmitter and receiver. The phenomenon is that if the transmission channels surrounded by each combo of transmit and receive antennas are statistically independent and distinct, then free channels with proper features can be found by pre coding and be utilized for transmitting more input symbols.

In MIMO, with N_t transmit and N_r receive antennas in a narrow band flat fading channel, the communication channel is modeled as

$$y = Hx + n \quad (4)$$

Variables x and y are $N_t \times 1$ transmit and $N_r \times 1$ receive angles cojointly. The noise vector for $N_r \times 1$ is denoted as n. The $N_r \times N_t$ is an ijth antenna having channel matrix H that defines the channel from the jth transmitting antenna to the ith receiving antenna.

When creating spatial correlation it is suitable to exploit the Kronecker illustrative, where the interconnection among transmit and receive antennas are arranged as autonomous and detachable. This model is feasible when the primary reflection emerges nearest to the antenna arrays and is approved by a couple of indoor and outdoor analysis.

The Kronecker model with Rayleigh fading describes the channel matrix H as,

$$H = R_R^{1/2} H_w \left(R_T^{1/2} \right)^T \quad (5)$$

Where the components of H_w are nonaligned and uniformly distributed as spheroid proportional composite Gaussian with null-mean and unit variance. The essential element of the model is that H_w is post-multiplied by transmit-side spatial correlation matrix R_T and pre-multiplied by the receive-side spatial correlation matrix R_R .

2.3 Spatial Temporal Channel Prediction Algorithm

To do the frequency-time conversion, the K-points IFFT can be represented as,

$$\begin{aligned} \hat{h}_{n,m}(i, l) &= \frac{1}{K} \sum_{k=0}^{k-1} \hat{h}_{n,m}(i, k) e^{j2\pi lk} / K \\ &= \begin{cases} h_{n,m}(i, l) + Z_{n,m}(i, l) & l = 0, \dots, L - 1 \\ Z_{n,m}(i, l) & l = L, \dots, K - 1 \end{cases} \end{aligned} \quad (6)$$

For each channel path, p is defined as the prognosis length Q . Present and past evaluated coefficients of the channel are given by,

$$\hat{h}_{n,m}(i, l) = [\hat{h}_{n,m}(i, l), \hat{h}_{n,m}(i - 1, l), \dots, \hat{h}_{n,m}(i - Q + 1, l)]^T \quad (7)$$

To predict $\hat{h}_{n,m}^{pre}(i + p, l)$, the data set \hat{h} is utilized

$$\begin{aligned} \hat{h} &= [\hat{h}_{1,1}(i, l)^T, \hat{h}_{1,2}(i, l)^T, \dots, \hat{h}_{1,M}(i, l)^T, \\ &\quad \hat{h}_{2,1}(i, l)^T, \dots, \hat{h}_{N,1}(i, l)^T, \dots, \hat{h}_{N,M}(i, l)^T]^T \end{aligned} \quad (8)$$

2.4 Forward-Stepwise Subset (FSS) Predictor

A condensed form of auto regressive predictor is implemented to reduce the estimation load of the all correlation predictor. If a datum is independent with the predicted datum, then the datum has no help for prediction. The prediction AR model is given by,

$$\hat{h}_{n,m}^{pre}(i + p, l) = w_B^H \tilde{h} \quad (9)$$

From the MMSE criterion we get,

$$W_B = \arg_{WB} \min E \left\{ \| h_{n,m}(i + p, l) - w_B^H \tilde{h} \|^2 \right\} \quad (10)$$

Conferring to auto regressive model and MMSE paradigm $\hat{h}_{pren,m}(i + p, l) = wR\tilde{h}$, we get wR , where $\tilde{h} = [\tilde{h}_1, \dots, \tilde{h}_{k-1}]^T$. Define $residual = h_{pren,m}(i + p, l) - wR\tilde{h}$, the \tilde{h}_k is the selected data which is most correlated with the *residual*.

2.5 Rayleigh Channel

Rayleigh fading is an analytical model that defines the propagation condition for a transmitted signal, being used by wireless devices. It is explored as a feasible model for tropospheric and ionospheric wave generation and for densely develop urban environments. It is suitable only when there is no effective communication along a line of sight within transmitter and receiver. It is a exceptional case of two-wave with diffuse power (TWDP) fading [5]. Rayleigh fading is a acceptable model when there are more entities in the domain that diverge the transmission signal. This is explained using the central limit theory that states, if there is adequately more spreads, the channel impulse response will be better modeled as a Gaussian process regardless of the partition of the particular factors. If there is no leading segments to the spread, then such mechanisms will have null mean and phase uniformly assigned among $(0, 2\pi)$ radians. The performance of the channel response will be Rayleigh dispersion. Usually, the factors such as gain and phase of channel are defined as a complex number. Here, Rayleigh fading is presented by the hypothesis that the real and complex elements of the feedback are modeled by nonaligned and uniformly allotted null-mean Gaussian systems so that the magnitude of the response is the summation of two said systems. The probability density function (PDF) of the received signal envelope $f(r)$, can be shown to be relay given by

$$f(r) = \frac{r}{\sigma^2} e^{-\frac{r^2}{2\sigma^2}} \quad (11)$$

Where σ^2 is the time-average power of the received signal before the envelope detection.

2.6 Rician Channel

Rician fading is a probabilistic model for wireless communication deviation produced by fractional elimination of a transmit signal with the signal reaching the receiver by numerous distinct paths and at most one of them being is unstable. It arises when one of the signals frequently a line of sight signal or any active reflection signals is dominant over others. Here, the magnitude gain is featured by a rician spreading and this itself is a specific part of two-wave with diffuse power (TWDP) fading. There are three distinct techniques for evaluating the specifications of the Rician scattering- method of moments, method of maximum likelihood and method of least squares. In the first two

techniques, the importance is to find specifications of distribution v and σ from an element of information. This might be fulfilled by adopting the method of moment's i.e., sample mean and standard deviation. Assuming the channel as a two port network, the sample mean is an evaluation of μ_1' and standard deviation is an evaluation of $\mu_{21}/2$. The probability density function of Rayleigh fading is,

$$f(r) = \frac{r}{\sigma^2} e^{-\left\{\frac{r^2 + \kappa^2 d}{2\sigma^2}\right\} + \left\{\frac{rk}{\sigma^2}\right\}} \quad (12)$$

Where $I_0(0)$ the 0th order is modified Bessel function of the first kind.

3 Results

The system working is simulated using MATLAB. BPSK and QAM modulation is used along with OFDM assuming Rayleigh and Rician channels. A Rayleigh context accepts NLOS (no line-of-sight) whereas if there is a line-of-sight then it can be evaluated by Rician fading. Simulation experiments have been conducted for the different specifications given in Table 1 using basic OFDM system.

Table 1. Simulation criterion

Criterions	Specifications
FFT size (n)	64
Constellation	QAM/QPSK/BPSK
Channel model	Rayleigh/Rician
No. of taps	5
Cyclic prefix (N_{cp})	n/4
No. of used subcarrier (K)	52
No. of symbols per frame	3

The Fig. 2(a) and (b) shows comparison of BER with distinct SNR for BPSK and QAM modulations using two separate channel models i.e. Rayleigh and Rician fading channels. It is seen that for low values of SNR, the computed BER is quite high due to nominally large noise power.

The Fig. 3(a), (b) and (c) shows the comparison of BER with SNR for distinct transmit and receive antennas values using two channel models - Rayleigh and Rician fading channels. For nTx and nRx values (3 × 2), the calculated BER is 10^{-9} as compared with (1 × 1) having 10^{-3} .

Figure 4(a) and (b) shows the comparison of channel capacity for different SNR that uses BPSK and QAM modulations for Rayleigh and Rician fading channels. Even for high values of SNR = 10, the channel capacity = 9, which is quite high in case of QAM as compared to BPSK due to relatively large noise power.

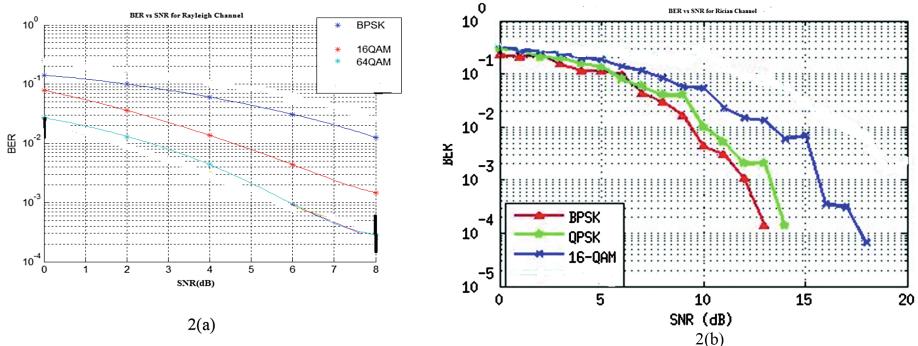


Fig. 2. BER graph for STCP (a) QAM & BPSK in Rayleigh fading with OFDM (b) QAM& BPSK in Rician fading with OFDM

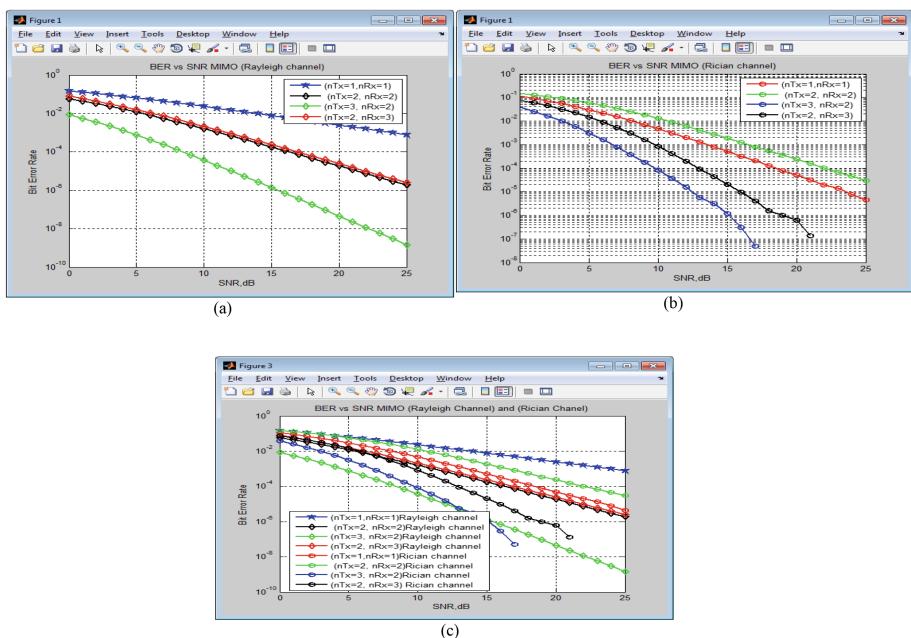


Fig. 3. BER graph (a) $n_{Tx} = 1, 2, 3$ $n_{Rx} = 1, 2, 2$ in Rayleigh fading with OFDM-MIMO (b) $n_{Tx} = 1, 2, 3$ $n_{Rx} = 1, 2, 2$ in Rician fading with OFDM-MIMO (c) $n_{Tx} = 1, 2, 3$ $n_{Rx} = 1, 2, 2$ in Rayleigh and Rician fading with OFDM-MIMO

The Fig. 5(a) and (b) shows the comparison of channel capacity with SNR for distinct transmit and receive antennas values for Rayleigh and Rician fading channels. For n_{Tx} and n_{Rx} values (4×4) in Rician channel, the channel capacity is 24, which is high as compared with values of ‘n’ in Rayleigh channel.

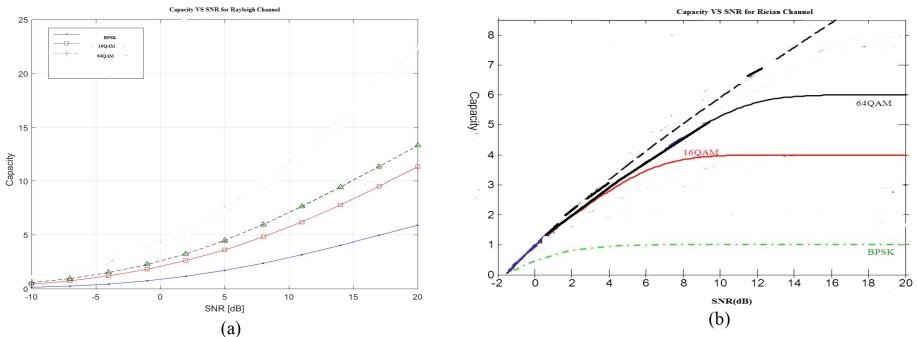


Fig. 4. Capacity graph for STCP (a) QAM & BPSK in Rayleigh fading with OFDM (b) QAM & BPSK in Rician fading with OFDM

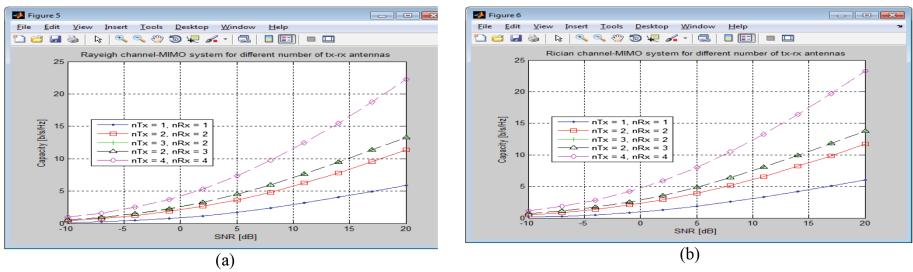


Fig. 5. Capacity graph (a) $n_{Tx} = 1, 2, 3, 4$ $n_{Rx} = 1, 2, 2, 4$ in Rayleigh fading with OFDM-MIMO (b) $n_{Tx} = 1, 2, 3$ $n_{Rx} = 1, 2, 2$ in Rician fading with OFDM-MIMO

4 Conclusion

BER and channel capacity computation has been done for two wireless channel models. Simulated experiments indicate that BER is low for QAM modulation. Therefore this is the best modulation technique for data transmission on Rayleigh and Rician channel models. Spatial-Temporal channel prediction algorithm was used to upgrade the received computed signal. Simulated experiments for distinct specifications were tested to inspect the reflex on the obtained BER values. In particular, QAM broadcast more symbols than BPSK. This improvement is an outcome of both inter-antenna and inter-subcarrier interference. It can be summarized that QAM with Rayleigh fading gives better performance when OFDM is implemented with prediction algorithm.

References

1. Sampath, H., Talwar, S., Tellado, J., Erceg, V., Paulraj, A.: A fourth generation MIMO-OFDM broadband wireless system design, performance, and field trial results. *IEEE Commun. Mag.* **40**(9), 143–149 (2005)
2. He, H., Zeng, Y.: Transmit Beamforming Interpolation algorithm for MIMO-OFDM system in limited feedback scenario. *IEEE J. Sel. Areas Commun.* **26**(6), 958–959 (2012)
3. Du-Hallen, A., Hu, S., Hallen, H.: Long-range prediction of fading signals: enabling adaptive transmission for mobile radio channels. *IEEE Signal Process. Mag.* **17**(3), 62–75 (2014)
4. Wang, X., Giannakis, G.B.: Resource allocation for wireless multiuser OFDM networks. *IEEE Trans. Inf. Theory* **57**(7), 4359–4372 (2011)
5. Joham, M., Castro, P.M., Utschick, W., Castedo, L.: Robust precoding with limited feedback design based on predcoding MSE for MU-MISO systems. *IEEE Trans. Signal Process.* **60**(6), 3101–3111 (2012)
6. Prakash, S., McLoughlin, I.: Predictive transmit antenna selection with maximal ratio combining. In: Proceedings of 2013 IEEE GLOBECOM, pp. 1–6 (2013)
7. Duel-Hallen, A.: Fading channel prediction for mobile radio adaptive transmission systems. *Proc. IEEE* **95**, 2299–2313 (2013)
8. Hallen, H., Duel-Hallen, A., Hu, T.S.Y.S., Lei, M.: A physical model for wireless channels to provide insights for long range prediction. In: Proceedings of 2011 MILCOM, vol. 1, pp. 627–631 (2011)
9. Heidari, A., Khandani, A.K., McAvoy, D.: Adaptive modelling and long-range prediction of mobile fading channels. *IET Commun.* **4**, 39–50 (2010)
10. Hwang, J.K., Winters, J.H.: Sinusoidal modeling and prediction of fast fading processes. In: Proceedings of 2012 IEEE GLOBECOM, pp. 892–897 (2012)
11. Chen, M., Ekman, T., Viberg, M.: New approaches for channel prediction based on sinusoidal modeling. *EURASIP J. Adv. Signal Process.* **2007**(1), 04933 (2006)
12. Semmelrodt, S., Kattenbach, R.: Investigation of different fading forecast schemes for flat fading radio channels. In: Proceedings of 2013 IEEE VTC – Fall, vol. 1, pp. 149–153 (2013)
13. Schafhuber, D., Matz, G.: MMSE and adaptive prediction of time varying channels for OFDM systems. *IEEE Trans. Wirel. Commun.* **4**(2), 593–602 (2005)
14. Wong, I.C., Forenza, A., Heath, R.W., Evans, B.L.: Long range channel prediction for adaptive OFDM systems. In: Proceedings of 2014 IEEE ACSSC, vol. 1, pp. 732–736 (2014)
15. Li, Y., Cimini, L.J., Sollenberger, N.R.: Robust channel estimation for OFDM systems with rapid dispersive fading channels. *IEEE Trans. Commun.* **46**, 902–915 (2009)
16. Semmelrodt, S., Kattenbach, R.: A 2-D fading forecast of time variant channels based on parametric modeling techniques. In: Proceedings of 2016 IEEE PIMRC, pp. 1640–1644 (2016)
17. Wong, I.C., Evans, B.L.: Sinusoidal modeling and adaptive channel prediction in mobile OFDM systems. *IEEE Trans. Signal Process.* **56**(41), 1601–1615 (2015)
18. Park, S., Choi, J.W., Seol, J.Y., Shim, B.: Expectation maximization-based channel estimation for multiuser MIMO systems. *IEEE Trans. Commun.* **65**, 2397–2410 (2017)
19. Zhou, Z., Fang, J., Yang, L., Li, H., Chen, Z., Blum, R.S.: Low-rank tensor decomposition-aided channel estimation for millimeter wave MIMO-OFDM systems. *IEEE J. Sel. Areas Commun.* **35**, 1524–1538 (2017)
20. Thomas, T., Charishma, G., Veeraswamy, K.: MIMO antenna system with high gain and low HF of 5G operating at MM wave design. In: 10th International Conference on Information Communications and Signal Processing (ICICS) (2015)



An Efficient Training Strategy for a Temporal Difference Learning Based Tic-Tac-Toe Automatic Player

Jesús Fernández-Conde^(✉), Pedro Cuenca-Jiménez,
and José María Cañas

GSyC Department (ETSIT), Universidad Rey Juan Carlos,
28943 Fuenlabrada, Madrid, Spain
{jesus.fernandez, pedro.cuenca,
josemaria.plaza}@urjc.es

Abstract. Temporal Difference (TD) learning is a well-known technique used to train automatic players by self-play, in board games in which the number of possible states is relatively small. TD learning has been widely used due to its simplicity, but there are important issues that need to be addressed. Training the AI agent against a random player is not effective, as several millions of games are needed until the automatic player starts to play intelligently. On the other hand, training it against a perfect player is not an acceptable option due to exploratory concerns. In this paper we present an efficient training strategy for a TD-based automatic game player, which proves to outperform other techniques, needing only roughly two hundred thousand games of training to behave like a perfect player. We present the results obtained by simulation for the classic Tic-Tac-Toe game.

Keywords: Reinforcement Learning · Temporal difference learning · Computer board games · AI efficient training

1 Introduction

Reinforcement Learning (RL) studies how Artificial Intelligence (AI) agents can learn what to do in the absence of labeled examples of what to do [1]. RL uses observed rewards to learn an optimal (or nearly optimal) policy for the environment, without any prior knowledge of the environment or the reward function. RL might be considered to be an archetypical AI problem: an agent is placed in an unknown environment and must learn to behave successfully therein.

When applied to board games, the RL agent learns how to play by getting feedback (reward, reinforcement) at the end of each game, knowing that something good has occurred when it wins or something bad when it loses, without possessing any kind of previous familiarity with the game rules.

During board game playing, it is very hard for a human to provide accurate and consistent evaluations of large numbers of positions, which would be needed to discover an evaluation function directly from examples. Nevertheless, an RL agent can be told whether it has won or lost every game played, so it can use this information to learn an evaluation function that gives reasonably accurate estimates of the probability of winning from any given position.

Temporal Difference Learning (TD), a special form of Reinforcement Learning (RL) has been widely used to train automatic game players successfully [2–6], due to its simplicity and low computational requirements. The TD agent uses a state-based representation of a fully observable environment. The agent’s policy is fixed and its task is to learn the utility values of the different states. The TD agent does not know the transition model, which specifies the probability of reaching a given state from another state after performing a given action; nor does it know the reward function, which specifies the reward for each state.

TD learning does not need a transition model to perform its updates. The environment supplies the connection between neighboring states in the form of observed transitions. The TD approach tries to make local adjustments to the utility estimates in order to make each state “agree” with its successors. As a simplification, TD adjusts a state to agree only with its observed successor (according to the TD update rule equation [7]), instead of adjusting the state to agree with all of the successors that might occur, weighted by their probabilities. This approximation turns out to be adequate when the effects of TD adjustments are averaged over a large number of transitions, because the frequency of each successor in the set of transitions is approximately proportional to its probability.

In TD, the major issue to address is exploration: an agent must experience as much as possible of its environment in order to learn how to behave in it. Due to this fact, some previous research works have exhibited discouraging results [8, 9], needing several million games until the agent starts to play intelligently.

Some modifications and extensions of the original TD algorithm have also been proposed [10–13], even including the combination of TD with deep learning [14]. These works demonstrate successful results at the expense of losing focus in the main two advantages of TD learning: its extreme simplicity and reduced computational cost.

In this paper we present an effective technique to train a TD learning agent for the Tic-Tac-Toe classic game, needing only roughly two hundred thousand games of training to behave like a perfect player. The TD agent presented here uses the original TD algorithm without any extension, hence preserving the easiness and low processing needs of TD implementation.

The remainder of this paper is organized as follows: In Sect. 2, we discuss the main characteristics of the TD agent used to learn how to play the Tic-Tac-Toe classic board game. The Sect. 3 describes the experiments performed and the results obtained. Interpretation of the results is detailed in Sect. 4. Finally, Sect. 5 draws the main conclusions of this work.

2 TD Learning Agent for the Tic-Tac-Toe Game

Tic-Tac-Toe [15] is a classic two-player (X and O) board game, in which players take turns marking the spaces in a 3×3 grid. The player who succeeds in placing three of their marks in a horizontal, vertical, or diagonal row wins the game. In Fig. 1 we can observe a typical Tic-Tac-Toe game, won by the first player (X):

A TD learning agent has been implemented in C language, in order to evaluate different training strategies. Considering the straightforwardness of the TD algorithm,

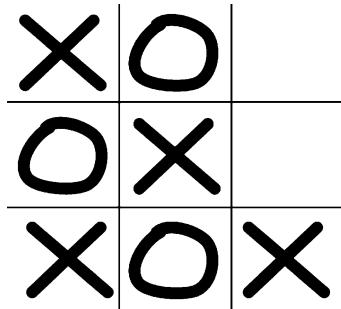


Fig. 1. A finished game of Tic-Tac-Toe, won by player X

the developed C program barely accounts for 300 non-commented lines of code, including the different training strategies evaluated.

In our implementation of TD agent, regular Tic-Tac-Toe game rules are assumed. The opponent of the TD agent always plays first (player X), in order to give some advantage to the opponent. In the Tic-Tac-Toe game, due to its inherent asymmetry, the player that initiates the game (player X) has approximately twice the probability of winning than the second player (player O).

The different game states are identified by a nine-digit number with possible digits 0 (empty position), 1 (position occupied by opponent) and 2 (position occupied by TD agent). In principle, this would mean that there are $3^9 (=19683)$ possible states, but some of them are not reachable, due to game restrictions. It can be proved by combinatorial analysis that the number of reachable states is 5478.

In each game played, the TD agent always tries to move from a given state to the state with the maximum estimated utility, of all the reachable states. If all the reachable states have the same estimated utility, it will make a random move.

When the game is over, the TD agent updates its utility estimates for all the states traversed during the game in the following way: for the last state of the game (terminal state), the utility function will be: -1 (opponent won), +1 (TD agent won) or 0.1 (game tied up). Note that a small positive reward is given to the game ties, considering the special nature of Tic-Tac-Toe, as the game will end in a tie if played properly. For the rest of the states visited during the game, utilities are updated backwards using the following code:

```

if (TD_agent_won) {
    U[current_state] = 1.0;
}
else if (opponent_won) {
    U[current_state] = -1.0;
}
else { /* tied up */
    U[current_state] = 0.1;
}
for (i = 1; i <= n_moves; i++) {
    /* this is the TD update rule equation */
    /* ALPHA -> learning rate; DF -> discount factor */
    U[seq[n_moves-i]] += ALPHA*(DF*U[current_state]-U[seq[n_moves-i]]);
    current_state = seq[n_moves-i];
}

```

2.1 TD Agent Training Strategies

The learning capabilities of the Tic-Tac-Toe TD learning agent will be evaluated after being trained against the following different players:

1. **Random player:** completely random moves.
2. **Attack-only player:** the player will check first if there is the immediate possibility to win, and will do so in that case. In any other case, it will perform a random move.
3. **Defense-only player:** the player will check first if the TD agent has the immediate possibility to win, and will impede it in that case. In any other case, it will perform a random move.
4. **Attack-then-Defense player:** combination of Attack and Defense players. This player will try to win first; if it cannot win, it will then check if the TD agent may win in the next move, impeding it in that case. Otherwise it will perform a random move.
5. **Defense-then-Attack player:** combination of Defense and Attack players. This player will first check if the TD agent may win in the next move, impeding it in that case. If it is not the case, it will try to win immediately if possible. Otherwise it will perform a random move.

It is worth mentioning that the perfect player has not been considered as a training opponent. By definition, the perfect player will perform the best possible move in any situation, in order to win the game (or at least tie up if the game cannot be won). Therefore, its absence of randomness makes it completely inadequate for the TD learning agent training process.

3 Experiments Performed and Results Obtained

We have developed a TD learning agent for the Tic-Tac-Toe game, following the learning process and rules detailed in previous sections. The experiments carried out have the following characteristics:

- The opponent player used for training the TD agent always moves first. It will play one of the 5 strategies presented in the previous section. The first move in each game will always be random.
- The number of training games is set to 200000.
- After the training games are finished, the TD agent will play a number of post-training games against a completely random player. During these post-training games, the TD agent will fine-adjust its utilities.
- The number of post-training games is set to 20000 (10% of the training games).
- After the post-training games are finished, the training process is considered complete. The TD agent will then play a number of test games. In these test games, the values of the utilities estimated by the TD agent are constant.
- The number of test games against a completely random player is set to 1 million.
- The number of test games against a perfect player is set to 9 games, as the moves made by the perfect player are invariant for each game situation, and therefore the only variable parameter is the first move, that can be made in any of the 9 positions of the grid.

- The value of learning rate α parameter in TD update rule equation is set to 0.25.
- The value of discount factor γ parameter in TD update rule equation is set to 1.
- Utilities are initially set to zero for all possible game states.

Figures 2 and 3 below show the results of the experiments during the training phase. There are 5 different curves in each figure, corresponding to the different training alternatives stated in the previous section.

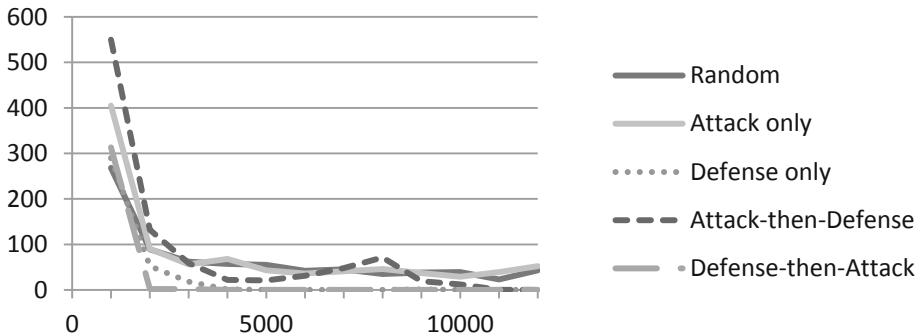


Fig. 2. TD agent rate of learning during the training phase as a function of the number of games played

In Fig. 2 we can observe the rate of learning for the TD agent when trained using different strategies, for the first 12 thousand games (after that period, values are practically stable). The rate of learning is computed as the number of games lost during the last 1000 games interval.

Figure 3 depicts the total number of games lost by the TD learning agent during the training phase, for the first 12 thousand games.

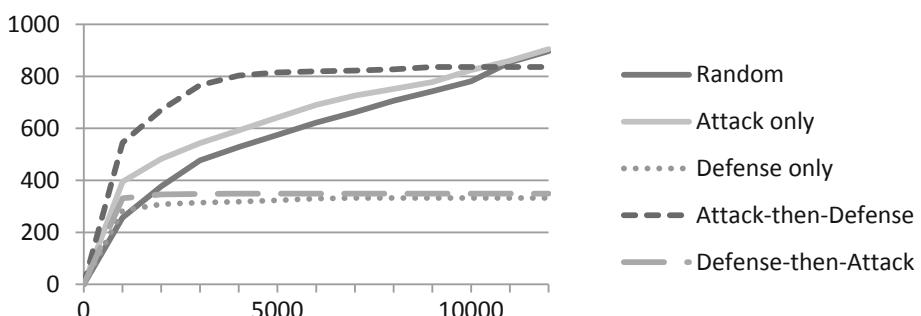


Fig. 3. Games lost by TD agent during the training phase as a function of the number of games played

Figure 4 illustrates the number of games lost by the TD agent against a completely random player during the test phase, after having completed the training and post-training phases. It is reminded that the number of games played by the TD agent against a random player in the test phase is 1 million.

Test games lost vs. random opponent

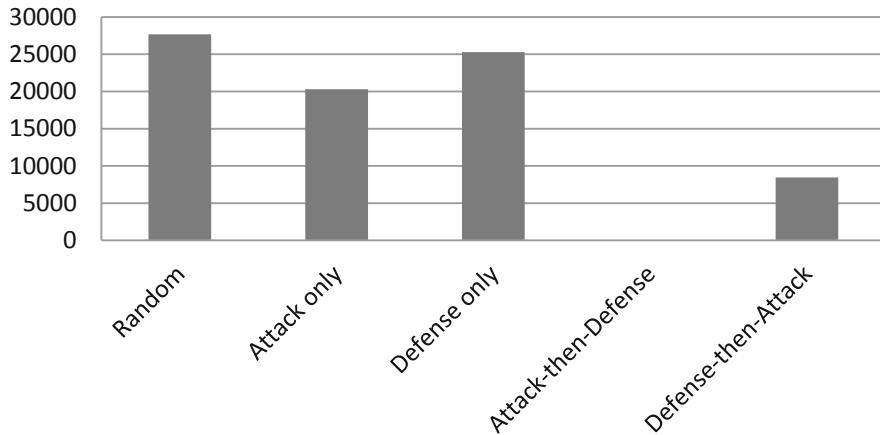


Fig. 4. Games lost by TD agent against a random player for different training strategies

Figure 5 shows the number of games lost and tied by the TD agent against a perfect player. In this case, as explained before, only 9 games are played, as perfect player moves are invariable.

Test games vs. perfect opponent

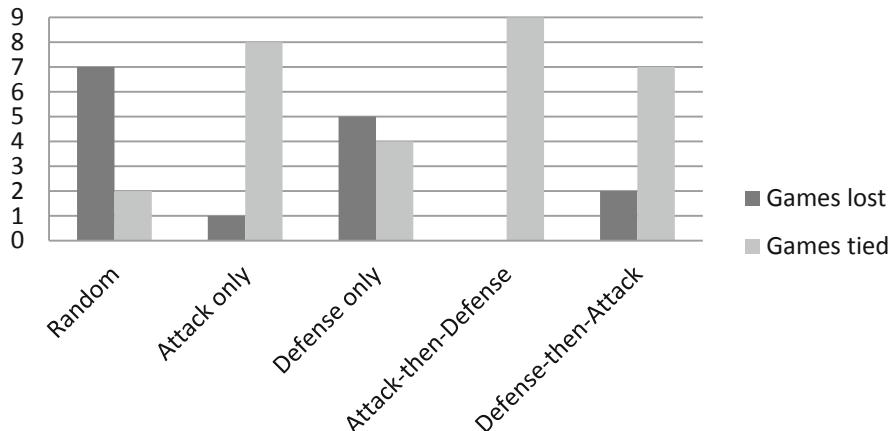


Fig. 5. Games lost/tied by TD agent against a perfect player for different training strategies

4 Discussion of Results

Interpretation of the experiments performed leads to the following discussion of results:

1. Regarding the rate of learning and the number of games lost during the training phase, it is noticed that the strategies Random and Attack are losing games at a constant rate after the first thousands of games, whereas the rest of strategies (all containing Defense tactics in the opponent) basically stop losing games after playing a few thousand games.

The circumstance of losing zero games after the initial period is not necessarily positive, since it may be due to a lack of randomness in the opponent. It is valuable to recall that the most important statistic is the number of games lost during the test phase.

In fact, as we observe in Figs. 2 and 3, the rate of learning and number of games lost by the Attack-then-Defense technique are worse than the corresponding ones for Defense-only and Defense-then-Attack. Nevertheless, as we will point out below, Attack-then-Defense experiments a better behavior during the test phase.

2. With respect to the number of games lost during the test phase, Random and Defense-only strategies perform poorly against both random and perfect opponents. Those strategies including the “Attack” part in the first place, namely Attack-only and Attack-then-Defense perform much better against the perfect player.
3. The **Attack-then-Defense** method clearly outperforms the other proposed strategies in number of test games lost by the TD agent (check Figs. 4 and 5). In fact, we observe that the TD agent trained using this technique does not lose a single game out of 1 million games played against a random player. Furthermore, it behaves like a perfect player, attaining ties in all games played against a perfect opponent.

5 Conclusions

In this paper we have proposed, described, developed and evaluated several training strategies for a Temporal Difference learning agent, implemented as simulated opponent players with different rules.

We have shown that convergence of TD algorithm can be vastly improved if the proper training strategy is selected. In this case, the expert level is attained in the classic Tic-Tac-Toe board game with only roughly two hundred thousand games of training. In previous research works, several million games were needed to reach comparable standings.

The Attack-then-Defense training strategy presented (try to win, if not possible try not to lose, otherwise perform a random move), in spite of being notably simple to implement and having a low computational cost, has proven to be highly effective in our experiments, outperforming the rest of options considered. Moreover, the TD agent trained using this strategy can be considered as a perfect Tic-Tac-Toe player, not losing a single game when confronted with the perfect opponent.

Future work includes examination of the efficiency of Attack-then-Defense training strategy in other board games, (e.g., Connect Four), in which the number of states is considerably larger.

References

1. Sutton, R., Barto, A.: Reinforcement Learning: An Introduction, vol. 156, pp. 10–15. MIT Press, Cambridge (1998)
2. Samuel, A.: Some studies in machine learning using the game of checkers. IBM J. Res. Dev. **3**(3), 210–229 (1959)
3. Tesauro G.: Temporal difference learning of backgammon strategy. In: Proceedings of the 9th International Workshop on Machine learning, pp. 451–457. Morgan Kaufmann Publishers Inc. (1992)
4. Tesauro, G.: Practical issues in temporal difference learning: Reinforcement Learning, pp. 33–53. Springer (1992)
5. Konen, W.: Reinforcement Learning for Board Games: The Temporal Difference Algorithm (2015). <https://doi.org/10.13140/rg.2.1.1965.2329>
6. Gatti, C.J., Embrechts, M.J., Linton, J.D.: Reinforcement learning and the effects of parameter settings in the game of Chung Toi. In: 2011 IEEE International Conference on Systems, Man, and Cybernetics, pp. 3530–3535, Anchorage, AK (2011). <https://doi.org/10.1109/icsmc.2011.6084216>
7. Russell, S., Norvig, P.: Artificial Intelligence: A Modern Approach, 3rd edn. Prentice Hall Press, Upper Saddle River (2009). 0136042597 9780136042594
8. Gherrity, M.: A game-learning machine. Ph.D. Dissertation, University of California, San Diego (1993)
9. Schraudolph, N., Dayan, P., Sejnowski, T.: Using the TD(λ) algorithm to learn an evaluation function for the game of go. In: Advances in Neural Information Processing Systems, vol. 6 (1994)
10. Szubert, M., Jaskowski, W., Krawiec, K.: Coevolutionary temporal difference learning for Othello. In: Proceedings of 5th International Conference on Computational Intelligence and Games (CIG 2009), pp. 104–111. IEEE Press, Piscataway (2009)
11. Krawiec, K., Szubert, M.: Learning n-tuple networks for Othello by coevolutionary gradient search. In: Proceedings of GECCO 2011, Dublin, pp. 355–362. ACM, New York (2011)
12. Lucas, S.M.: Learning to play Othello with n-tuple systems. Aust. J. Intell. Inf. Process. **4**, 1–20 (2008)
13. Thill, M., Bagheri, S., Koch, P., Konen, W.: Temporal difference learning with eligibility traces for the game connect-4. In: IEEE Conference on Computational Intelligence and Games (CIG), Dortmund (2014)
14. Van De Steeg, M., Drugan, M.M., Wiering, M.: Temporal difference learning for the game Tic-Tac-Toe 3D: applying structure to neural networks. In: 2015 IEEE Symposium Series on Computational Intelligence Cape Town, pp. 564–570 (2015). <https://doi.org/10.1109/ssci.2015.89>
15. Baum, P.: Tic-Tac-Toe, Thesis for the Master of Science Degree, Computer Science Department, Southern Illinois University (1975)



Detection of Causative Attack and Prevention Using CAP Algorithm on Training Datasets

D. Suja Mary^{1(✉)} and M. Suriakala²

¹ Department of Computer Applications, J.H.A Agarsen College,
University of Madras, Chennai 600060, India

dsuja2004@yahoo.com

² Department of Computer Science, Government Arts College for Men,
Nandanam, Chennai 600035, India
suryasubash@gmail.com

Abstract. Machine learning is the scientific study of algorithms, which has been widely used for making automated decisions. The attackers change the training datasets by using their knowledge, it cause impulses to implement the malicious results and models. Causative attack in adversarial machine learning explores certain security threat against carefully executed poisonous data points into the training datasets. This type of attacks are caused when the malicious data gets injected on training data to efficiently train the model. Defense techniques have leveraged robust training datasets and prevents accuracy on evaluating the machine learning algorithms. The novel algorithm CAP is explained to substitute trusted data instead of the untrusted data, which improves the reliability of machine learning algorithms.

Keywords: Causative attack · Poisoning attack · Causative Attack Protection (CAP) algorithm · Adversary

1 Introduction

In Causative or Poisoning attack the adversary Provides incorrect information to the machine learning algorithm [1]. The training set datas are assumed to be easy accessible unprotected in physical manner. A machine learning adversary may take advance to access the training set data and manipulate physical attacks on training datasets. The intent of adversary is to retrieve information from data source and eventually sneak secrets. This adversary attack is to inject invalid data to the classification system, in turn forcing the system to make wrong decisions. An attacker can intrude, modify, replay, and inject datas [2]. The modified training datas are feed into the legitimate training phase play an important role in establishing a high performance machine learning mode. Accordingly, many adversaries target the training data, resulting in a significant decrease of the overall performance of the machine learning model [4]. The misleading classification performance lead to provide wrong data driven insights, decisions, and predictions [8, 9]. We proposed to explain the causative attacks or poisoning attack which affect the training datasets and to reduce the learning algorithms classification accuracy.

In this paper, described that the causative attacker known the details about training datasets, working strategy of machine learning Algorithms and expected output. In real-world situation an assumption is unfeasible, an attacker could insert malicious sample data in the training set drawn from the same class distribution. Our approach is to prove a worst case analysis of the attacker's talent capabilities. We use the algorithm to detect the attacked datas and displayed it to the user view. The proposed algorithm Causative Attack Protection (CAP) compares the machine learning datasets and adversarial affected datasets and replaces the affected data with legitimate data. We consider that our adversarial attacker well known about the training datasets and made an attack in the used sample training Electricity Board dataset. We have to find the worst case modification of attacker's challenges using detection algorithm implemented in python programming. The CAP algorithm to change the attackers affected training datasets into trusted datasets.

2 Adversarial Machine Learning

Machine learning algorithms used the training datasets as the learning classifiers and the algorithms operate it, then the algorithms classifieds the datasets as the same type class distribution. In this moment, in adversarial frameworks of the training datasets, knowledgeable and technical adversaries may purposely attack the datasets to handle existing harmed machine learning algorithms. It will be damage the entire machine learning system classification algorithms. This manipulation raises several security open issues on machine-learning algorithms classification techniques, the training dataset may require defense techniques and reverse engineering for this purpose. To identify main open issues are: The adversary to analyze the existing classification learning algorithms and modify their sample training dataset to evade detection [21]. The classifiers designer reacts by analyzing modified dataset and to produce the updated new classification performances.

The adversaries use different algorithms, for example gradient-ascent or mimicry attack, where the attacker is initialized the attack vector at the cloning arbitrary point of the attacked training dataset class and marked its label. The point of attack vector on the training datasets initialized T_0 . In the dataset T_0 can be choose any point which deeply needed within the attacked training dataset class's boundary. We assume, the dataset's prior class only manipulated by the attacker and attack point's of distribution in prior class T by essentially adding into the training data, one at a time and can alter the feature values of the attack sample within some lower and upper bounds. In particular, we limited the attack point to lie within a box that is $T_{lb} \leq T \leq T_{ub}$. The security risk caused in the classification algorithms based on the attack quality made in the training dataset by the adversaries.

3 Related Works

The machine learning attacked datasets affected different discipline accuracy measurements. An image detection classification problem by applying a certain undetectable perturbations is not a random experiment of machine learning: the same perturbation can cause a different algorithm that was trained on a different models of the dataset, to misclassify the same input [6]. For example the Breast Cancer training dataset applied different machine learning algorithms, the experiments show that the effectiveness of the attacks is 8-10% higher when comparing with some machine learning algorithm [7]. During document classification, it analyst an unsupervised maliciously labels, which can be in fact very hard to detect [10]. In deep learning, the classification algorithm input crafted by the adversarial sample, hence learning algorithms to misclassify [11]. Figure 1 shows how to adversary inject malicious data to training datasets.

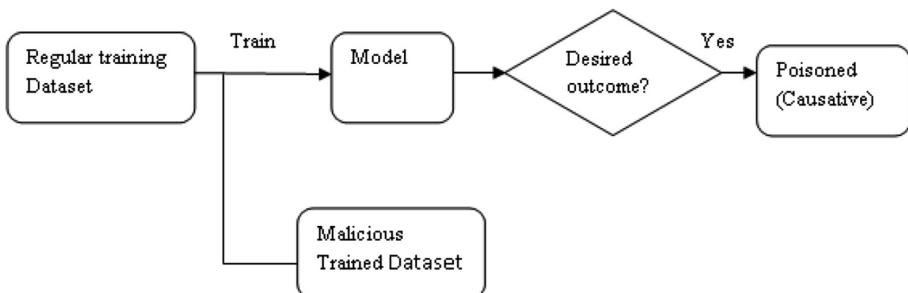


Fig. 1. Causative attack block diagram

Security problems against causative attack training datasets as a adversaries reactive arms race, the adversaries has prior knowledge about the dataset framework design and they attempt to achieve their attacking goals and success by reacting to the challenging behavior of the opponent [12], that is learning problem from the adversaries prior work.

4 Defense System Description

The machine learning causative attack problem is considered as a supervised manner based on the supervised training dataset input from a data stream. After receiving an initial training data set from the relevant source, the causative attack model is created based on this data and a set of metrics evaluated to determine how well machine learning algorithms performing on the attacked dataset, including prediction, test accuracy, and empirical security risk. A simple defense mechanism is enforced by the

learning system to stop this attack it happening and it help to prevent attacks from occurring [5]. The two prior defense methods are RONI and PS.

4.1 Reject on Negative Impact (RONI)

The quality of Machine Learning systems from causative attack's misleading caused by an arms race, will be prevent using the data Provence defense methods. RONI was implemented against training dataset's poisoning or causative attacks [18]. The RONI [19] defense was to increase adversarial costs when find out the attacks and forcing attackers to improve skill that show accurate result must be a small metrics loss difference. For that reason, they implicitly assumed that causative attack stand out from the remaining attacks, and they negatively affect the victim classifier.

The approach of RONI determines effectively identify causative attack on training set samples and to decrease the performance of the machine learning algorithms which one fit for the selected training dataset. The defense method to prevent the learning performance, it required a sizable well frame structured clean set of testing datasets for trained the classifier. However, RONI has the drawback; it remains computationally inefficient as the number of trained classification algorithms scales linearly with the large training set [20].

4.2 Probability of Sufficiency (PS)

The PS method by take the similarities of RONI for detecting causative or poison data by evaluating the effect of individual data points on the classification performance of the trained model [3]. In the PS method's Causative attack detection process is more scalable comparing to other defense methods because it reduces the number of times retrained the training datasets. The model needs in the machine learning for retrained to a fraction of the total number of untrusted training datasets.

5 Evaluation of Causative Attacked on Training Datasets

In this section explains the experiments conducted on training set datas evaluated in machine learning algorithms. To detect targeted causative attacks using the attack detect causative algorithm and to describe how the algorithm will be works. The attack and detection experiments conducted on the training set data and testing data, and then the followed results are explained.

The experiments applied on EB training dataset on machine learning using python programming language. The datasets evaluated on various machine learning algorithms. The decision classification problems on training datasets allowing practically execute a well defined type of supervised learning algorithm.

5.1 Machine Learning Algorithms Evaluation on Causative Attack Datasets

A causative attack on the training datasets becomes a more powerful attacking model when the adversary plays the role in training datasets [5]. All the datasets has a structured framework. An adversarial attacker unknown about the training datasets model structure, but they interested unlimited access to evaluate the training model and willing to learn how to decrease the machine learning algorithms performance score [16]. The evaluation of classification algorithm indicates that, which algorithms would be fit or over fit on the selected training datasets or what structure of configurations used on the datasets. The experiments of evaluating machine learning algorithms we use 6 different algorithms on the training dataset.

1. Logistic Regression (LR)
2. Linear Discriminant Analysis (LDA)
3. K-Nearest Neighbors (KNN)
4. Classification and Regression Trees (CART)
5. Gaussian Naive Bayes (NB)
6. Support Vector Machines (SVM)

To load the EB datasets to our system, then split the loaded datasets into two parts. The 80% of datasets considered to use train our classification models and 20% of datasets that stored back for a validation dataset. Execute both datasets in the python programming language. Finally, to compare each algorithm evaluation results and select which one is most accurate.

Table 1. Comparison of accuracy on different algorithms

Algorithm	Accuracy before attack	Accuracy after attack
LR	0.063326	0.063326
LDA	0.167130	0.166954
KNN	0.999956	0.994034
CART	0.999912	0.989792
NB	0.724159	0.687392
SVM	0.999956	0.989836

The Table 1 shows the result, the causative attack to decrease the accuracy level of original dataset. From the table Support Vector Machines (SVM) has comparing with other classification algorithms; it is the largest estimated 99% accuracy score. But the datasets affected to causative attack SVM algorithms accuracy score decreased 99% to 98%. According to the result, machine learning algorithms loss their original preference and gives misleading results.

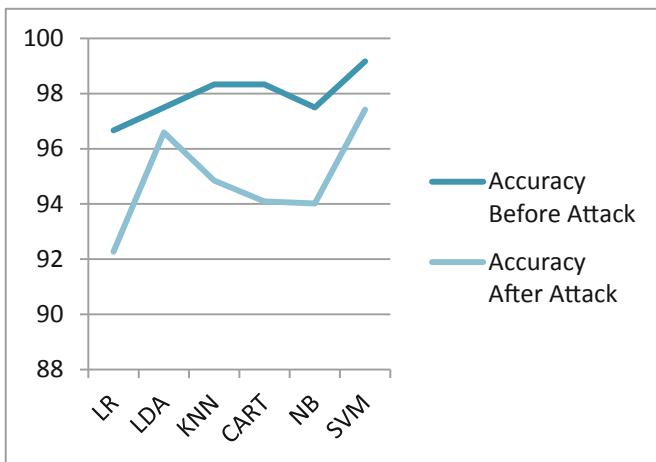


Fig. 2. The machine learning algorithms accuracy comparison before and after attack

The Fig. 2 explained the causative attack affected the accuracy of six different kinds of machine learning algorithms.

6 Algorithm to Detect Attacked Data Sets

A defense provenance based causative or poison detection mechanism that works on data collected adversarial samples make a re-training is untrusted [3]. Assume that URL downloaded datasets are legitimate and adversary made the attack in the training set data. The algorithm used to detect the affected datasets from adversarial datasets.

Algorithm1. Detect Causative attack

Input: URL datasets in U

Adversarial Datasets in A

Output: Display Attacked datasets

1. U <- URL Read
2. A <- Adversary Read
3. For all U_i in U
4. If U_i not equal to A_i
5. CA <- A_i
6. Write CA
7. End if
8. End for

In algorithm 1 the URL datasets marked as U and Adversarial datasets marked as A. Each and every data from URL and Adversarial compared to each other ($U_i \neq A_i$). The compared datas are not equal to write affected datas in the file CA. The adversarial attacked datasets are displayed on the output screen. The algorithm implementation and outputs are shown in the following Fig. 3.

The figure shows two side-by-side Jupyter Notebook cells. Both cells have a title 'Run: EB_Causative' and a status bar at the bottom indicating 'Process finished with exit code 0'. The left cell displays a table of classification metrics for various industries. The right cell shows the same table but with significantly lower precision, recall, f1-score, and support values across all categories, indicating a successful causative attack.

		precision	recall	f1-score	support
	AutomobileIndustry	1.00	1.00	1.00	664
	Bank	1.00	1.00	1.00	711
	BpoIndustry	1.00	1.00	1.00	687
	CementIndustry	1.00	1.00	1.00	667
	ChemicalIndustry	1.00	1.00	1.00	1456
	Farmers1	1.00	1.00	1.00	714
	Farmers2	1.00	1.00	1.00	707
	FertilizerIndustry	1.00	1.00	1.00	1946
	FoodIndustry	1.00	1.00	1.00	1435
	Hospital	1.00	1.00	1.00	2717
	HealthCareResources	1.00	1.00	1.00	659
	PoultryIndustry	1.00	1.00	1.00	1463
	Residential(Apartments)	1.00	1.00	1.00	1451
	Residential(individual)	1.00	1.00	1.00	1473
	Supermarket	1.00	1.00	1.00	1433
	TextileIndustry	1.00	1.00	1.00	654
	Theatre	1.00	1.00	1.00	1464
	University	1.00	1.00	1.00	1428
	micro avg	1.00	1.00	1.00	22629
	macro avg	1.00	1.00	1.00	22629
	weighted avg	1.00	1.00	1.00	22629

		precision	recall	f1-score	support
	AutomobileIndustry	1.00	1.00	1.00	664
	Bank	0.86	0.96	0.91	614
	BpoIndustry	0.16	0.05	0.08	57
	CementIndustry	1.00	1.00	1.00	667
	ChemicalIndustry	1.00	1.00	1.00	1456
	Farmers1	1.00	1.00	1.00	714
	Farmers2	1.00	1.00	1.00	707
	FertilizerIndustry	1.00	1.00	1.00	1946
	FoodIndustry	1.00	1.00	1.00	1435
	Hospital	1.00	1.00	1.00	2717
	HealthCareResources	1.00	1.00	1.00	659
	PoultryIndustry	1.00	1.00	1.00	1463
	Residential(Apartments)	1.00	1.00	1.00	1451
	Residential(individual)	1.00	1.00	1.00	1473
	School	0.00	0.00	0.00	9
	Supermarket	1.00	1.00	1.00	1435
	TextileIndustry	1.00	1.00	1.00	654
	Theatre	1.00	1.00	1.00	1464
	University	0.99	1.00	1.00	1419
	micro avg	0.99	0.99	0.99	22629
	macro avg	0.91	0.91	0.90	22629
	weighted avg	0.99	0.99	0.99	22629

Fig. 3. Before and after causative attacked result

The causative detection python program can be applied all causative attacked training datasets which stores in CSV file format. The program detected the adversarial affected datas against from the legitimate training dataset.

7 CAP Algorithm Recover Trusted Datasets

The security problems of machine learning algorithms under adversarial attacks that manipulate the learning system, the defense strategies make a counter measures on these attacks [13]. The framework of empirical security evaluation [12] to protect training datasets from causative attack. Security problems in the training datasets often lead to risk reactive arms race between the ML adversary and the ML classifiers designer [14, 15].

The datasets collected are assumed as legitimate, that is not a causative attacked. The machine learners obtaining the datasets partially trusted training can be achieved through manual curation of the collected data or through well trusted sources of data for training [17]. To use the partial trusted data in machine learning algorithms evaluation, it is difficult for manual verification due to cost associated and real-time requirements. Hence, in our protection method, evaluate and replaced the causative attacked data with fully trusted datasets.

The existing algorithm find Poison Data Fully Untrusted (DU, F) [3] is a defense provenance based causative or poison attack detection mechanism that works on

machine learning even if all data collected for untrusted datasets. It evaluates both training dataset and adversarial dataset models and remove corresponding attacked data from adversarial dataset.

Algorithm 2. Causative Attack Protection (CAP)

Input: CU := all data are untrusted, P := Trusted data

Output: Set of datas that are suspected from causative attack and replace it.

```

1: Cattack ← x
2: P ← DatasetByProvenanceFeature(CU , P )
3: Ptrain ← x, Peval ← x
4: for all <Ci , Ei> ∈ P do
5: Learner randomly assign half of the data in Ci to Ptrain and Ei half to Peval
6: end for
7: for all Di ∈ P do
8: set row in P=1
9: for Ci_row in CU
10: Reprow = Prow
11: if Ci_row not equal to Prow
12: DetecedFile ← trainModel(Ctrain \ Ci)
13: ReplaceFile ← trainModel(Prow)
14: getdata (ReplaceFile )
15: end if
16: CU ← Remove the validation set with trusted data
17: end for

```

The CAP algorithm to compare both the trusted and untrusted datasets line by line and replaced the untrusted data with trusted data. The condition applied to read each row P_{row} and C_i_row from the datasets and compare both rows equal or not. If the row equal to each other, the trusted dataset placed in the Replaced File. The condition not equals the attacked data C_i replaced with P_{row} and placed the trusted data in the Replaced File.

8 Conclusion and Future Work

In machine learning algorithms, the classification systems do not take into account of changing the framework settings, they can shows their talent on attack vulnerabilities on the training datasets to several potential attacks and allowing their effectiveness through undermine learning algorithms. In this paper discussed different algorithms accuracy rate compared by using original and attacked training datasets. Also presented how to detect attacked the training datasets and secure these datasets using CAP algorithm through substitution method.

As future work state that the study of learning algorithms make interesting to the learner, they should be well-known about multiple different training datasets that may collaborate to perform causative attack on the machine learning model. Also our work assigned in future will be loyal to develop various security techniques to pretend attacks on different applications.

References

1. Shi, Y., Sagduyu, Y.E.: Evasion and causative attacks with adversarial deep learning. In: Milcom 2017 Track 3 - Cyber Security and Trusted Computing (2017)
2. Aman, M.N., Chua, K.C., Sikdar, B.: Secure data provenance for the Internet of Things. In: Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security (IoTPTS 2017), pp. 11–14. ACM, New York (2017)
3. Baracaldo, N., Chen, B., Ludwig, H., Safavi, J.A.: Mitigating poisoning attacks on machine learning models: a data provenance based approach. In: Defense Against Poisoning AISec 2017, 3 November 2017, Dallas (2017)
4. Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., Leung, V.C.M.: A survey on security threats and defensive techniques of machine learning: a data driven view, vol. 4, pp. 2169–3536. IEEE (2018)
5. Burkard, C., Lagesse, B.: Analysis of causative attacks against SVMs learning from data streams. In: IWSPA 2017, 24 March 2017, Scottsdale (2017)
6. Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., Fergus, R.: Intriguing properties of neural networks
7. Mozaffari-Kermani, M., Sur-Kolay, S., Raghunathan, A.: Systematic poisoning attacks on and defenses for machine learning in healthcare. IEEE J. Biomed. Health Inf. **19**(6), 1893–1905 (2013)
8. Rouse, J.M.: Machine learning definition. <http://whatis.techtarget.com/definition/machine-learning>
9. L'heureux, A., Grolinger, K., Elyamany, H.F., Capretz, M.A.M.: Machine learning with big data: challenges and approaches, vol. 5. IEEE Access (2017)
10. Pi, L., Lu, Z., Sagduyu, Y., Chen, S.: Defending active learning against adversarial inputs in automated document classification. In: IEEE Global Conference on Signal and Information Processing (GlobalSIP), December 2016
11. Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z.B., Swami, A.: The limitations of deep learning in adversarial settings. In: 1st IEEE European Symposium on Security & Privacy, Saarbrucken, Germany. IEEE (2016)
12. Asharani, V., Veerappa, B.N., Rafi, M.: Security evaluation of pattern classifiers in adversarial environments. IJCSMC, **4**(4), 768–774 (2015)

13. Fawzi, A., Fawzi, O., Frossard, P.: Analysis of classifiers' robustness to adversarial perturbations. *Mach. Learn.* **107**, 481–508 (2018). <https://doi.org/10.1007/s10994-017-5663-3>
14. Gnana Pavani, P., Venkatesh, K., Rajesh, V.: Security evaluation of pattern classifiers under attack. *IJDCAST* V-5, I-5, SW-39 (2017)
15. Biggio, B., Fumera, G., Fabio Roli, F.: Security evaluation of pattern classifiers under attack. *IEEE Trans. Knowl. Data Eng.* **26**(4), 984–996 (2014)
16. Anderson, H.S., Kharkar, A., Filar, B.: Evading machine learning malware detection. In: *Black Hat*, USA, July 2017, pp. 22–27, Las Vegas (2017)
17. Baracaldo, N., Chen, b., Ludwig, H., Safavi, A., Zhang, R.: Detecting poisoning attacks on machine learning in IoT environments. In: *IEEE International Congress on Internet of Things* (2018)
18. Barreno, M., Nelson, B., Joseph, A.D., Tygar, J.D.: The security of machine learning. *Mach. Learn.* **81**, 121–148 (2010)
19. Li, H., Chan, P.P.K.: An improved reject on negative impact defense. Springer, Heidelberg (2014)
20. Lin, X., Chan, P.P.K.: Causative attack to incremental support vector machine. In: *International Conference on Machine Learning and Cybernetics*, Lanzhou, 13–16 July 2014
21. Biggio, B., Corona, I., Nelson, B., Rubinstein, B.I.P., Maiorca, D., Fumera, G., Giacinto, G., Roli, F.: Security evaluation of support vector machines in adversarial environments. In: *Support Vector Machines Applications* (2014)



Discrete Wavelet Transform Based Multiple Watermarking for Digital Images Using Back-Propagation Neural Network

C. Ananth¹(✉), M. Karthikeyan¹, and N. Mohananthini²

¹ Department of Computer and Information Science,
Annamalai University, Chidambaram, India

ananth.prog@gmail.com, karthiaucse@gmail.com

² Department of Electrical and Electronics Engineering,
Muthayammal Engineering College, Rasipuram, India
mohananthini@yahoo.co.in

Abstract. A Discrete Wavelet Transform (DWT) based multiple watermarking technique for images using Back-Propagation neural networks (BPNN) are proposed. The successive/re-watermarking is one of the best method in multiple watermarking techniques. In successive/re-watermarking method, the various watermarks are embedded and extracted one by one. The wavelet coefficient is selected based on the weight factor by using Human Visual System (HVS). The BPNN is incredibly well-liked in neural networks and its variety of supervised learning neural networks. The two watermarks are embedding into the original image using improved BPNN, which can advance the speed of the erudition, reduce error and the trained neural networks be capable of extracting the two watermarks from the embedded images. The simulation results show that the proposed work achieves good quality on the embedded images and more robustness on extracted two watermarks.

Keywords: Discrete Wavelet Transform · Digital watermarking · BPNN · Human visual system and successive watermarking

1 Introduction

The development of the Internet alongside with the increasing convenience of multi-media system applications has generated a variety of copyright issues. One amongst the areas that this enlargement has increased is that of digital watermarking. The digital watermarking is that the general procedure of embedding a splotch of data within the original file, such that a changed files are obtained. The advances to watermarking are diverse and might be largely classified supported their fragility, robustness or visibility. Their uses are versatile, as they'll be applied to text, audio, images or video. Jaishri guru et al. [1] discussed various algorithms of watermarking for digital image.

An superior method to enhance the strength of embedded information is analyzed in [2]. Their proposed results express that the watermark may be efficiently improved when attacks. The digital watermarking with attacks and evaluation methods are introduced in [3–6]. The three major classes of multiple watermarking methods like,

composite, segmented and successive watermarking are elaborated in [7–9]. Their method is optimized to maximize the performance of Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC).

Mark et al. [10] confirmed the watermark boundary may be a risk to dependable uncovering in multiple re-watermarking situations. A unique image watermarking emerge supported in the HVS model with neural network technique is proposed in [11, 12]. Their experiments for every dissimilar image the watermark can be accustomed to present an utmost and appropriate potency focus to the imperceptibility constriction. Nagai et al. [13] proposed a digital image watermarking intended for ownership authorization of bottomless neural networks. Their experiments show to make known the possible of watermarking bottomless neural networks. Namba and Sakuma [14] presented a unique watermarking technique, exponential weight. Their experimentally demonstrate that their watermarking method attains higher presentation of watermark even below a wicked attempt of unauthorized service suppliers.

2 Related Works

The related work focuses on DWT based successive watermarking technique using neural network. The proposed methodology are discussed as follows,

2.1 Discrete Wavelet Transform (DWT)

DWT is that the decomposition of an image into diverse secondary images of dissimilar dimension resolution level. The DWT is considered lofty frequencies, to present deprived frequency resolution as well as superior time resolution. The DWT is planned at short frequencies, poor time, frequency declaration and high frequency declaration. The benefits of wavelets are that they offer localization in frequency domain and able to separate the fine details in a Signal. This can be used to isolate the fine and coarse details in a signal.

2.2 Multiple Watermarking

In re-watermarking, the various watermarks are inserted one by one and then the various watermarks are extracted from one by one from the watermarked images.

2.3 Human Visual System (HVS)

The coefficients of wavelet are chosen accords to the HVS characteristics. The HVS can explained in conditions of three dissimilar properties such as frequency sensitivity, texture sensitivity and luminance sensitivity. Estimate the power features for wavelet coefficient of original image by use the model of Barni [15].

$$q_i(i,j) = a(l, \theta) b(l, i, j) c(l, i, j)^{0.2} \quad (1)$$

Where θ , l , stands for the orientation along with declaration level of wavelet transform of the image, (i, j) is DWT coefficient's position. The initial expression obtains interested in relation of the human eye sensitivity to noise transforms depends on the band.

$$a(l, \theta) = \begin{cases} \sqrt{2}, & \text{if } \theta = 1 \\ 1, & \text{otherwise} \end{cases} \cdot \begin{cases} 1.00, & \text{if } I = 0 \\ 0.32, & \text{if } I = 1 \\ 0.16, & \text{if } I = 2 \\ 0.10, & \text{if } I = 1 \end{cases} \quad (2)$$

The second term obtains confined clarity of the image can calculated as in Eq. (3). It takes into account that the eye is less sensitive to noise in regions of the image wherever the clarity is extremely high or extremely low.

$$b(l, i, j) = 1 + \frac{1}{256} I_3^3 \left(1 + \left[\frac{i}{2^{3-l}} \right], 1 + \left[\frac{j}{2^{3-l}} \right] \right) \quad (3)$$

Finally, the local texture activity can be calculated as in Eq. (4). Measure takes into account that the human being eye is fewer sensitive to regions of the image with strong texture, more specifically, to areas near the edges.

$$c(l, i, j) = \sum_{k=0}^{3-l} \frac{1}{16^k} \sum_{\theta=0}^2 \sum_{x=0}^1 \sum_{y=0}^1 \left[I_k^\theta (y + \frac{i}{2^k}, x + \frac{j}{2^k}) \right]^2 \cdot \text{Var} \left\{ I_3^3 \left(1 + y + \frac{i}{2^{3-l}}, 1 + x + \frac{j}{2^{3-l}} \right) \right\}_{x=0,1} \quad (4)$$

The $q_i(i, j)$ is equivalent to the quantization of coefficient to that the watermarking ciphers have to be additionally new. The watermark cipher is binary; the emerge allows addition to every DWT coefficient the highest insignificant watermark intensity.

2.4 Back Propagation Neural Network (BPNN)

The BPNN are one type of supervised learning neural networks and mainly used learning techniques in neural networks. To achieve least mean squared error (MSE) among expected outputs as well as actual outputs through feed-forward and then the BPNN preserve fix the network weights with using gradient descent methods along with MSE. Figure 1 shows, BP network architecture has three layers, which is input layer, hidden layer as well as output layer. The wavelet coefficient $q_i(i, j)$ is selected based on the weight factor. The production of the equation Round $q_i(i, j)|Q|$, which is signified as x , is used like an input rate for the BPN. Q represented as Quantization value. The primary weights of back propagation neural network are initialised at x values. Compute the output unit (a_k) and production of hidden unit (h_j) the by using activation functions.

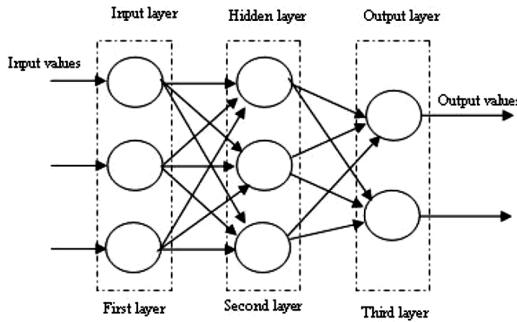


Fig. 1. Structural design of back propagation neural network

$$h_j = f\left(\sum_i x_i g_{ij}\right) \quad (5)$$

$$a_k = f\left(\sum_{j=1}^p h_j m_{jk}\right) \quad (6)$$

Here g_{ij} and m_{jk} are weights in neural network. Evaluate the error (e_k) is

$$e_k = (d_k - a_k)f'\left(\sum_{j=1}^p h_j m_{jk}\right) \quad (7)$$

Determine the error correction term, update the weight among the output layer along with hidden layer is measured by using equation

$$\Delta(m_{jk}) = \alpha e_k h_j \quad (8)$$

The modified weight is obtained as follows

$$m_{jk}(new) = m_{jk}(old) + \Delta(m_{jk}) \quad (9)$$

The error information term (e_j) is calculated as follows

$$e_j = \sum_{k=1}^m e_k m_{jk} f'\left(\sum_i x_i g_{ij}\right) \quad (10)$$

On the strength of e_j , renew the weight among the hidden layer along with input layer is measured by using equation

$$\Delta(g_{ij}) = \alpha e_j x_i \quad (11)$$

The modified weight can be obtained as follows

$$g_{ij}(\text{new}) = g_{ij}(\text{old}) + \Delta(g_{ij}) \quad (12)$$

After change the weight, check reaches the closure output. Otherwise repeat the step until actual output equal the desired output.

3 Proposed Method

The watermark embedding and extracting process are described as bellow:

3.1 Watermark Embedding Process

The watermarks embedding procedure is shown in Fig. 2 as followed by,

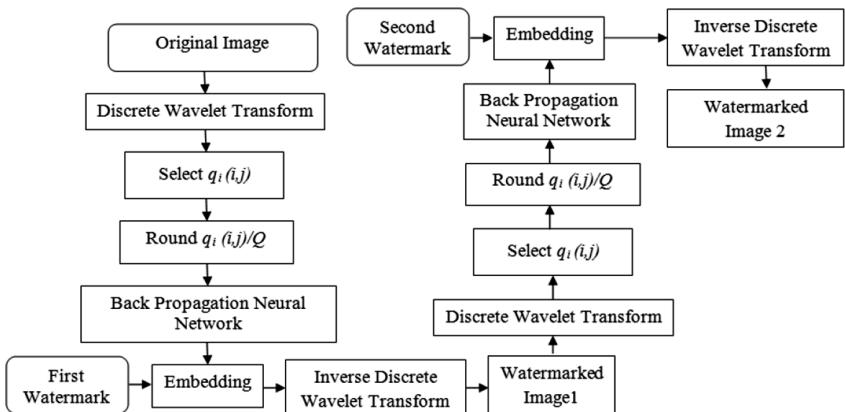


Fig. 2. Watermark embedding process

1. The novel image is decomposed with DWT.
2. Get the weight factors $q_l^0(i,j)$ in favor of wavelet coefficients seeing that certain in Eq. (1).
3. The location of watermark embedding coefficient are calculated based on their weight factors, then quantize the DWT coefficient $q_l^0(i,j)$ through Q, in addition to employ that value as the input of BPN, production values can be achieved. Training BPNN using production values, and the first watermark can be embedded into the wavelet domain use the trained BPN.
4. The IDWT can be presented to obtain watermarked image-1.

5. Likewise, the next watermark is inserted to the watermarked image-1 to obtain the watermarked image-2.

3.2 Watermarking Extraction Process

The watermarks extraction process is shown in Fig. 3 as followed by,

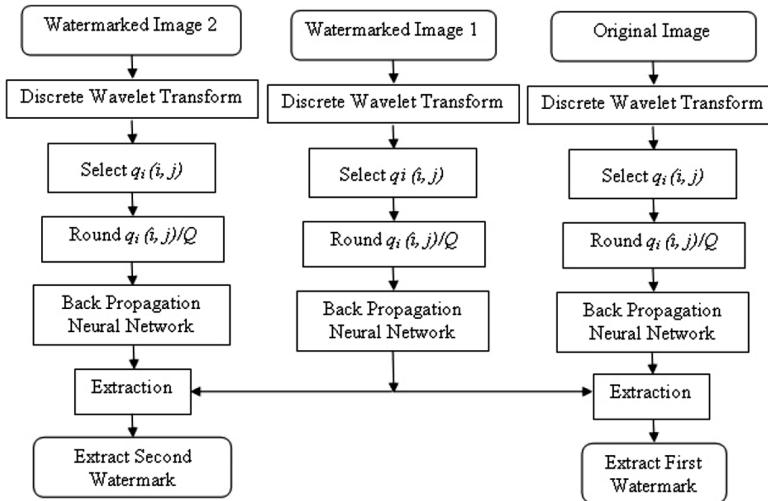


Fig. 3. Watermark extracting process

1. The watermarked image 2 as well as watermarked image 1 are decomposed with DWT.
2. The position of coefficient are find based on weight factors, Quantize the DWT coefficient $q_i(i,j)$ with Q, and use that value as the input of BPN, use back propagation algorithm, the production values can be obtained.
3. Extract the second watermark, by using the watermarked image 2 and watermarked image 1.
4. Likewise, the initial watermark can be extracted from the watermarked image-1 and original image.

4 Experimental Results

The performance of the successive watermarking technique along with number of experimentations are executed on dissimilar images of dimension 512×512 . The logos of size 48×48 are used as multiple watermarks are shown in Fig. 4.

Table 1 shows the imperceptibility and robustness value on successive watermarking technique exclusive of attacks. Table 2 shows the PSNR, NC values on successive watermarking technique for the Lena image with attacks.

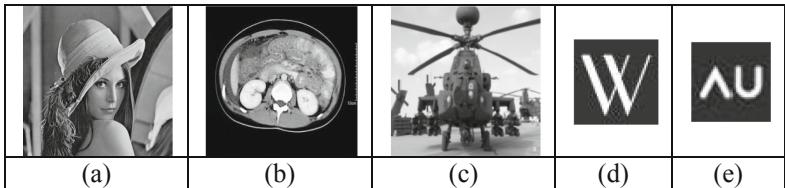


Fig. 4. Common, medical, military (a–c) and watermark images (d–e)

Table 1. Tested values on successive watermarking technique exclusive of attacks

Images	Successive watermarking		
	PSNR (dB)	NC1	NC2
Lena	45.0177	1	1
Medical	44.9961	1	1
Military	44.7831	1	1

Table 2. PSNR values on successive watermarking technique with attacks

Attacks	Successive watermarking PSNR (dB)	Extracted watermark	
		1	2
Rotation (60°)	10.8067	0.1364	0.9736
Row & column blanking	12.7619	0.0125	1
Row & column copying	18.6990	0.8358	0.9956
Median filtering (3×3)	33.4053	0.9916	1
JPEG compression (20)	35.3364	1	0.9652
Gaussian noise (1%)	20.2283	0.7891	0.9906
Sharpening	25.3802	0.8000	1
Smoothing	37.0359	0.9989	1
Cropping	18.7839	0.3360	0.9970

From the results, it is evident that, in the second watermark attains high robustness for various attacks.

5 Performance Comparison with Existing Method

To demonstrate the efficiency of the proposed method, the PSNR results can be contrasted with existing method [9]. Their method single watermark is embedded into Lena image, but our technique is embedded with two watermarks. The PSNR value can be showed in Table 3 and it is obvious that the imperceptibility presentation of the projected method can be greater than the offered method [9].

Table 3. Comparison of PSNR values to existing method

Lena image	Existing method [9]	Proposed method
PSNR (dB)	43.02	45.01

6 Conclusion

The successive multiple watermarking method supported on BP Neural Network and HVS have been offered in this work. The original image is decomposed using wavelet domain and the weight factors are calculated using HVS. The improved BPNN, which is develop the pace of the learning and decrease the error the trained neural networks can extract the two watermarks since the watermarked images. The presented watermarking algorithms have been tested with different images. The developments of watermarking algorithms are improved imperceptibility on the watermarked image as well as the robustness of extracted watermark against attacks.

References

1. Guru, J., Damecha, H.: A review of watermarking algorithms for digital image. *Int. J. Innov. Res. Comput. Commu. Eng.*, **2**, 5701–5798 (2014)
2. Zhou, X., Cao, C., Ma, J., Wang, L.: Adaptive digital watermarking scheme based on support vector machines and optimized genetic algorithm. *Math. Prob. Eng.*, **2018**, 1–10 (2018)
3. Lin, L.: Research on digital watermarking algorithm for anti-geometric attack. In: AASRI International Conference on Intelligent Systems and Control, vol. 267 (2019)
4. Ananth, C., Karthikeyan, M., Mohananthini, N.: A secured healthcare system using private blockchain technology. *J. Eng. Technol.*, **6**, 42–54 (2018)
5. Patel, M., Swati, A.C.: The study of various attacks on digital watermarking technique. *Int. J. Adv. Res. Comput. Eng. Technol.*, **3**, 1567–1570 (2014)
6. Sunesh, H.K.: Watermark attacks and applications in watermarking. *Int. J. Comput. Appl.* 8–10 (2011)
7. Sheppard, N.P., Shafavi Naini, R., Ogunbona, P.: On multiple watermarking. In: Proceedings of the ACM Multimedia and Security Workshop (MMSW), pp. 3–6, New York (2001)
8. Mohananthini, N., Yamuna, G.: Comparison of multiple watermarking techniques using genetic algorithm. *J. Electr. Syst. Inf. Technol.*, **3**, 68–80 (2016)
9. Mohananthini, N., Yamuna, G.: Performance comparison of single and multiple watermarking techniques. *Int. J. Comput. Netw. Inf. Secur.*, **6**, 28–34 (2014)
10. Mark, D., Uhl, A., Wernisch, H.: Experimental study on watermark interference in multiple re-watermarking. In: Proceedings of SPIE, Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505 (2007)
11. Lou, D.-C., Liu, J.-L., Hu, M.-C.: Adaptive digital watermarking using neural network technique. In: IEEE 37th Annual 2003 International Carnahan Conference on Security Technology (2003)

12. Mohananthini, N., Yamuna, G.: Watermarking for images using wavelet domain in back-propagation neural network. In: International Conference on Advances in Engineering, Science and Management (ICAESM-2012), pp. 100–105. IEEE (2012)
13. Nagai, Y., Uchida, Y., Sakazawa, S., Satoh, S.: Digital watermarking for deep neural networks. *Comput. Vis. Pattern Recogn.* **7**(1), 3–16 (2018)
14. Namba, R., Sakuma, J.: Robust watermarking of neural network with exponential weighting, cryptography and security (2019)
15. Barni, M., Bartolini, F., Piva, A.: Improved wavelet based watermarking through pixel-wise masking. *IEEE Trans. Image Process.* **10**, 783–791 (2001)



Multilevel Converter for Renewable Energy System

Vishal Anand^(✉) and Varsha Singh

National Institute of Technology, Raipur, Raipur, India
vishal240294@gmail.com, vsingh.ele@nitrr.ac.in

Abstract. Multilevel converters are very much involved in application which is high as well as medium voltage applications. They are utilised to inject voltages into grid, which is considered as an example of infinite voltage application, where the reliability of converters plays a significant role. More the level of multilevel converter has, more the chances of sinusoidal output voltages. Hybrid topologies of MLIs, which are capable of handling switching stresses, utilisation of DC sources, capacitor balancing and capacitor current ripple and losses are discussed. In order to maintain the reliable network, auxiliary switches are used. These are usually comprised of diodes, bridges or bi-directional switches. This paper also focuses on the full utilisation of DC link capacitor for multilevel inverter and few new topologies along with its mode of operations.

Keywords: Multilevel converter · DC link capacitor · Auxillary switch · DC sources · Active bus voltage utilization · Advanced multilevel inverter topologies

1 Introduction

The reliability of multilevel inverter is important as it is used mostly in SVCs, VFDs, HVDC transmission lines, DTC of induction machine drives, minimisation of current ripple distortion, to attain sinusoidal current rectifiers, frequency response for renewable energy interfacing with grid. In modern power system, MLIs find its appliaction in Power factor correction and HVDCT by increasing the back-to-back configurations [1].

Most of the two-level inverters (VSIs) are limited to low voltage applications as power grades of power switches are specified. Moreover, the operating frequency for these power switches are also specific, which means it can handle limited stresses. Other problems are suffering high switching losses when power switches are operated at higher switching frequencies. The three kinds of multilevel inverters were proposed named as CHB-MLI, NPC-MLI, FC-MLI, which are also known as orthodox topologies for MLI [2]. Even though all three have its own recompenses and its restriction, researchers used CHB-MLI the most due to its simple structures. The most important advantage of CHB-MLI is active utilization of each power switches and DC supplies, but this can act to be disadvantageous also because they require isolated DC supplies which is costly, substantial. In modern day these DC supplies are replaced by either PV panels or regulated rectifiers. Coming to the NPC-MLI, it primarily suffers

from absence of segment, usage of large number of clamping diodes to get midpoint voltages. Other problems are unequal potential, unequal utilization of each power switches and DC supplies, due to which there is unequal power and associated power losses from each segment, when there is increase in voltage levels. In case of FC-MLI, there is a requirement of large capacitors, which is difficult to come to be. Other problems are capacitor balancing problem and problems associated with switching frequencies (ESR values changes). Due to these problems, the conventional MLI topologies suffered from unequal voltage stresses, power losses and found out to be uneconomical structure. Thus, researchers started moving towards hybrid topologies [11–15].

In order to increase the voltage levels for MLIs, researches incorporated usage of unequal voltage sources instead of equal voltage sources, which is also known as asymmetrical configuration for DC sources [3]. The usage of asymmetrical DC sources had problems of voltage balancing. Peng (2001) introduced his topology which had self-voltage balancing capabilities [4]. Barbosa (2005) made MLI which combines traits of both clamp diodes i.e. NPC and clamp capacitors i.e. FC, which he named as active neutral point clamped (ANPC) [5]. Later many works were presented on high frequency operation for power switches, replacing DC supplies with cheaper constant DC sources, half bridge topology, full-bridge topology. Topologies with reduced number of power devices, DC sources, capacitors etc. [6]. These topologies got suitable nobility from industrialists as the failure rates were significantly reduced. In this decade, researchers emphasized on the power quality, making topology fault-tolerant, active DC bus utilisation, grid-tie applications using renewable energy sources [7]. The Sect. 2 describes types causes of fault in multilevel inverter along with some fault-tolerance structures. The Sect. 3 describes some hybrid topologies which involves active utilisation of DC bus voltage, switched capacitors, usage of bi-directional switches to make fault tolerant structure.

2 Making Multilevel Inverters Fault-Tolerant

This section mainly pacts on fault tolerant-topologies, which is necessary to make system robust, reliable configurations. Most of the reliability failures are due to capacitors, poor soldering, PCBs, connectors etc. These failures may be due to electrical over stresses, electro-statistics discharges that develops in capacitors also known as ESDs, parasitic have also major role in large dv/dt stress which occurs due to poor soldering, electro-migration and induced migration are probable causes for stresses across switches. Lastly, external radiations always lead to substantial failure in topology [8]. Cost factor, modularity, control algorithms and its complexity are factor impacting design. Most of the recent hybrid topologies for MLIs focuses on level generation and polarity generation. The main advantage of this type of configuration is polarity generation is simply a bridge structure that takes care of polarity across the load terminal, whereas the level generation takes care of attaining maximum levels with usage of least number of power switches. Several research articles show the usage of bidirectional switch comprises of two IGBTs, this configuration reduces the ON state voltage drop significantly which is shown in configuration below (Fig. 1).

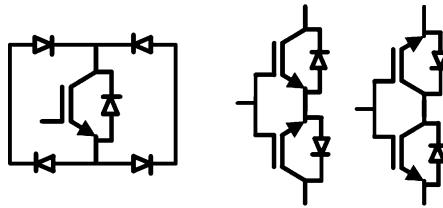


Fig. 1. Types of bidirectional IGBTs

These configurations of bidirectional switches can make circuit to be open circuit fault tolerant, which is attained further by applying several modulations and switching strategies. These bi-directional switches require only one gate driver circuit which reduces the cost and power density.

Most of the multilevel converter utilizes maximum of 50% of the DC link voltage. For active utilization of DC link voltage Kolar proposed T-type inverter which comprises of combination of two transistors across the DC link and bidirectional switches which gives 100% utilization of DC link voltage [9]. The advantages of this method are that lower conduction losses across the switch, the life cycle of load also gets increased due to lesser fluctuations. Another advantage is these switches can be operated at high frequencies, which improves the power density of converter and reduces the EMI losses and filter size.

To enhance the switching capability of device, bidirectional switches are used, which reduces the switching stresses by half. In literature T type inverters, which is configured by using bidirectional switches enhance the reliability of the system by reducing the switching stresses. The bidirectional switches can operate in either common collector configuration or common emitter configuration. The shaded region depicts that bidirectional switch low voltage stress [10].

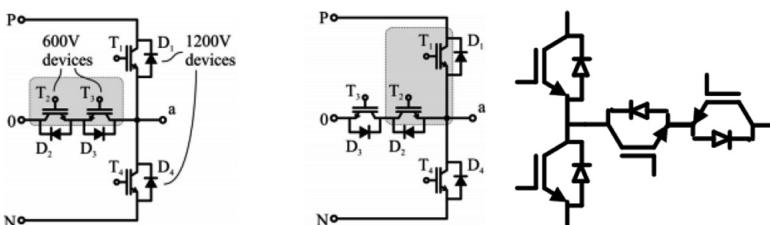


Fig. 2. Bidirectional switches for MLI topology with common-emitter configuration and common-collector configuration [9, 10]

These switching topologies are enhancing the reliability as the antiparallel diodes comes into operation whenever there is junction failure, and potential across the load is maintained without much variation across AC load.

DC link capacitors are key element in distribution of voltage levels across several switched capacitor multilevel inverters. In order to achieve full utilization of DC-link

voltage across multilevel inverters another T-type inverter is proposed in literature shown Fig. 2 [9, 10]. This topology offers better DC bus voltage utilization and enhanced efficiency, reliability as well as power density is improved.

In literature presented recently, kite type multilevel inverter is described with two asymmetrical DC sources with capacity of V_{DC} and $2V_{DC}$ to generate 13 output levels [11]. This circuit is capable of preventing short circuit as none positive of DC links makes anti-parallel diodes to conduct (Fig. 3 and Table 1).

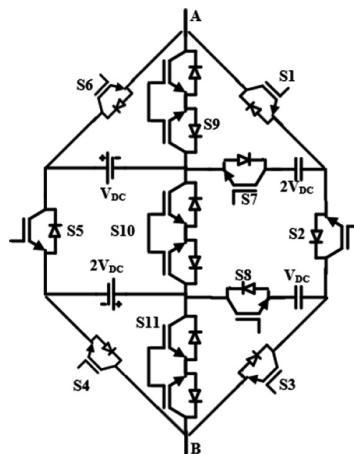


Fig. 3. Kite-type multilevel inverter for 13 output levels [11]

Table 1. Switching States to attain 13 output levels

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11
$6V_{DC}$	0	1	0	1	0	1	1	1	0	0	0
$5V_{DC}$	0	1	0	1	0	0	1	1	1	0	0
$4V_{DC}$	0	1	0	0	0	1	1	1	0	0	1
$3V_{DC}$	0	0	0	1	0	1	0	0	0	1	0
$2V_{DC}$	0	0	0	1	0	0	0	0	1	1	0
V_{DC}	0	0	0	0	0	1	0	0	0	1	1
0	0	0	0	0	0	0	0	0	1	1	1
$-V_{DC}$	0	0	0	1	1	0	0	0	1	0	0
$-2V_{DC}$	0	0	0	0	1	1	0	0	0	0	1
$-3V_{DC}$	0	0	0	0	1	0	0	0	1	0	1
$-4V_{DC}$	0	0	1	0	1	0	0	1	1	0	0
$-5V_{DC}$	1	0	0	0	1	0	1	0	0	0	1
$-6V_{DC}$	1	0	1	0	1	0	1	1	0	0	0

This topology is having PIV (peak inverse voltage) same for all the configurations. The capacitor charging, discharging rate and capacitor ripple current is constant, ripples can be reduced with usage of higher capacitance values [11]. This topology has inherent characteristics to produce negative levels with using H-bridge structure. Switches plays leading role in the inverter design, so, inverter with least switching stresses, and minimum number of turn on and turn off will have more longevity. If there is equal switching stress across the switches then chances of failure of one switch decrease and life of inverter increases.

3 Hybrid Topologies

In recent decade, hybrid topologies have gained importance, which gets further classified on low voltage applications and high voltage applications.

This topology describes single DC sources and three symmetrical capacitors to attain the 7-levels shown in Fig. 4 [12]. Capacitor charging and discharging is discussed.

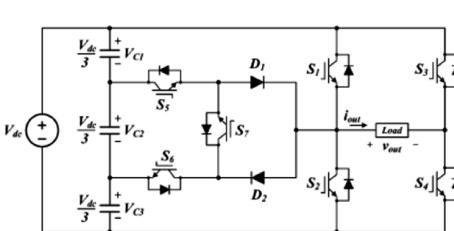


Fig. 4. Configuration of 7-level inverter [12]

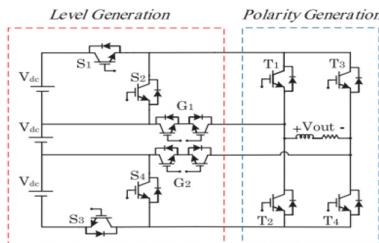


Fig. 5. Fault tolerant topology for 7-level inverter [13]

Charging of Symmetrical Capacitors for Fig. 4

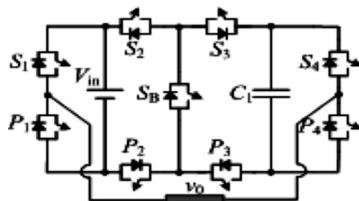
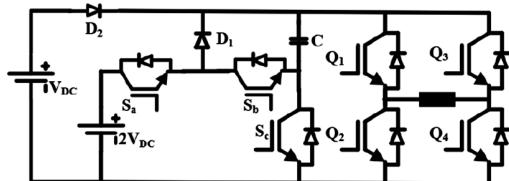
From Fig. 4 to generate V_{DC} all the capacitors (C_1, C_2, C_3) are charged and S_1 and S_4 operates, to generate $V_{DC}/3$ capacitor C_3 is charged and antiparallel diode for S_6, S_7, D_1 and S_4 is operates, to generate $2V_{DC}/3$. For zero level antiparallel diode of S_2 and S_4 operates. For $-V_{DC}$ C_1, C_2, C_3, S_3 and S_2 operates, to generate $-V_{DC}/3$ C_1, S_3, D_2, S_7 , and antiparallel diode of S_5 operates, to generate $-2V_{DC}/3$ C_2, C_1, S_3, D_2 and S_6 operates. similarly, by reversing the current flow, we can discharge the capacitors to generate levels.

Figure 5 topology has level generation and polarity generation along with fault-tolerance using bidirectional switches. The modes of operation to attain 7 levels is discussed in Table 2.

Table 2. Switching table for fault tolerant 7-level inverter

Output levels	Switches									
	S ₁	S ₂	S ₃	S ₄	G ₁	G ₂	T ₁	T ₂	T ₃	T ₄
3V _{dc}	1	0	1	0	0	0	1	0	0	1
2V _{dc}	0	1	1	0	0	0	1	0	0	1
V _{dc}	0	1	0	1	0	0	1	0	0	1
0	0	1	0	1	0	0	1	0	1	0
-V _{dc}	0	1	0	1	0	0	0	1	1	0
-2V _{dc}	0	1	1	0	0	0	0	1	1	0
-3V _{dc}	1	0	1	0	0	0	0	1	1	0

In Fig. 6 describes the improved packed U cell whose capacitor charging and discharging is described in Table 3.

**Fig. 6.** IPUC 7-level inverter [14]**Fig. 7.** Switched capacitor topology for 7-level inverter [15]**Table 3.** Modes of operation for 7 level improved packed U cell

Output levels	Switches									
	S ₁	S ₂	S ₃	S ₄	S _B	P ₁	P ₂	P ₃	P ₄	C ₁
1.5V _{in}	0	1	0	1	1	1	0	1	0	↑
V _{in}	0	1	1	1	0	1	0	0	0	-
0.5V _{in}	0	1	1	0	0	1	0	0	1	↑
0	1	1	1	1	0	0	0	0	0	-
0	0	0	0	0	0	1	1	1	1	-
-0.5V _{in}	1	0	0	1	0	0	1	1	0	↓
-V _{in}	1	0	0	0	0	0	0	0	1	-
-1.5V _{in}	1	0	1	0	1	0	1	0	1	↓

This topology has lesser switching stresses which is attained by advanced modulation method, it also reduces THD. The capacitor charging and discharging gives voltage boosting capabilities. The total blocking voltage of switch is good to handle inductive loads and dynamic loading conditions.

In Fig. 7 a topology for switched capacitor is discussed which aims to provide voltage boosting with the help of capacitors. This asymmetrical topology has couple of redundant states for zero level. The mode of circuit operation state is for $\pm V_{DC}$ uses transistors S_a , S_b and D_a is OFF while C is charged by V_{DC} through D_b and S_c . Similarly, when $\pm 2V_{DC}$ operates S_a is ON whereas S_b and S_c are OFF. When $2V_{DC}$ is operating, C powers the load. In this stage only $2V_{DC} > V_{DC}$, the diode D_b behaves as reverse biased and blocks all voltage from V_{DC} . When all the sources i.e. $\pm 3V_{DC}$ are in operation S_a and S_b is ON and D_b is reverse biased and block source voltage V_{DC} . Thus, the DC link voltage is $3V_{DC}$. The modes of operation are described in Table 4.

Table 4. Modes of operation for 7-level inverter using switched capacitor

Output levels	S_a	S_b	S_c	Q_1	Q_2	Q_3	Q_4
$3V_{DC}$	1	1	0	1	0	0	1
$2V_{DC}$	1	0	0	1	0	0	1
V_{DC}	0	0	1	1	0	0	1
0	0	0	1	1	0	0	0
	0	0	1	0	1	0	0
$-V_{DC}$	0	0	1	0	1	1	0
$-2V_{DC}$	1	0	0	0	1	1	0
$-3V_{DC}$	1	1	0	0	1	1	0

4 Conclusion

In multilevel inverter, the cost optimization and reliability are an important aspect, which is attained by reducing number of switches, equal stress across switches, less capacitor current ripples in case of switched capacitor multilevel inverter. Another important aspect in switched capacitor multilevel inverter design is ESR value of capacitor. Fault tolerant topologies can help reliable operation of multilevel inverter with proper bypass across switches and a fault tolerant algorithm for using the alternate bypass switches. Renewable energy-based grid tied switched capacitors multilevel inverters have high current ripples. The current ripple can be optimised and reduced with the help of equal switching stresses for positive and negative level generation. Thus, capacitor current ripples are essential parameter for grid tied switched capacitor based multilevel inverters design.

References

1. Samuel, P., Gupta, R., Chandra, D.: Grid Interface of wind power with large split-winding alternator using cascaded multilevel inverter. *IEEE Trans. Energy Convers.* **26**(1), 299–309 (2011)
2. Rodriguez, J., Lai, J.S., Peng, F.Z.: Multilevel inverters: a survey of topologies, controls, and applications. *IEEE Trans. Ind. Electron.* **49**(4), 724–738 (2002)
3. Mekhilef, S., Kadir, M.N.A.: Voltage control of three-stage hybrid multilevel inverter using vector transformation. *IEEE Trans. Power Electron.* **25**(10), 2599–2606 (2010)
4. Peng, F.Z.: A generalized multilevel inverter topology with self-voltage balancing. *IEEE Trans. Ind. Appl.* **37**(2), 611–618 (2001)
5. Barbosa, P., Steimer, P., Steinke, J., Meysenc, L., Winkelkemper, M., Celanovic, N.: Active neutral-point-clamped multilevel converters. In: IEEE 36th power electronics specialists Conference PESC 2005, pp. 2296–301 (2005)
6. Kala, P., Arora, S.: A comprehensive study of classical and hybrid multilevel inverter topologies for renewable energy applications. *Renew. Sustain. Energy Rev.* **76**, 905–993 (2017)
7. Sivakumar, K.: A fault-tolerant single-phase five-level inverter for grid-independent PV systems. In: IEEE Transactions on Industrial Electronics, vol. 62, no. 12, pp. 7569–7577, December 2015
8. Richardieu, F., Pham, T.T.L.: Reliability calculation of multilevel converters: theory and applications. *IEEE Trans. Ind. Electron.* **60**(10), 4225–4233 (2013)
9. Siwakoti, Y.P., Mahajan, A., Liese, S.: Active utilization of a full DC-link voltage in multilevel converter. In: 2018 IEEE International Telecommunications Energy Conference (INTELEC), Turin, pp. 1–5 (2018)
10. Katebi, R., He, J., Weise, N.: Investigation of fault-tolerant capabilities in an advanced three-level active T-type converter. *IEEE J. Emerg. Sel. Top. Power Electron.* **7**(1), 446–457 (2019)
11. Samadaei, E., Kaviani, M., Bertilsson, K.: A 13-levels module (K-Type) with two DC sources for multilevel inverters. *IEEE Trans. Ind. Electron.* **66**(7), 5186–5196 (2019)
12. Choi, J., Kang, F.: Seven-Level PWM inverter employing series-connected capacitors paralleled to a single DC voltage source. *IEEE Trans. Ind. Electron.* **62**(6), 3448–3459 (2015)
13. Choupan, R., Golshannavaz, S., Nazarpour, D., Barmala, M.: A new structure for multilevel inverters with fault-tolerant capability against open circuit faults. *Electr. Power Syst. Res.* **168**, 105–116 (2019)
14. Sathik, M.J., Bhatnagar, K., Sandeep, N., Blaabjerg, F.: An improved seven-level PUC inverter topology with voltage boosting. *IEEE Trans. Circ. Syst. II Express Briefs* (2019)
15. Raman, S.R., Cheng, K.W.E., Ye, Y.: Multi-input switched-capacitor multilevel inverter for high-frequency AC power distribution. *IEEE Trans. Power Electron.* **33**(7), 5937–5948 (2018)



Comprehensive Study on Methods that Helps to Increase the Life of the Wireless Sensor Networks

Aaditya Jain^(✉), Akanksha Dubey, and Bhuwnesh Sharma

CSE Department, R. N. Modi Engineering College, Rajasthan Technical University, Kota, Rajasthan, India

aadityajain5@gmail.com, dubeyakanksha92@gmail.com,
bsharma.it@gmail.com

Abstract. Wireless communication between sensors allows the formation of flexible sensor networks, which can be deployed rapidly on inaccessible areas. Energy management remains as the tedious challenge in these networks. Collection of data by sensors in a clustered topology and aggregating data at intermediate level remains as the good solution to save energy. The research for topology control and efficient distribution of load in wireless sensor networks (WSNs) has been active in recent years and ample literature exists. This paper discusses some important works in this direction. Overall analysis is based on the following categories: Clustering without cluster size restriction, Unequal clustering methods, Cluster head selection using fuzzy logic and protocol that maintain connectivity.

Keywords: WSN · Cluster head selection · Energy efficient protocol · unequal clustering

1 Introduction

Wireless Sensor Networks (WSNs) are eligible to work in those environment where infrastructure based networks are not easy to deploy. WSNs are easy to install and the cost of installment is very less and decreases as territory increases. Such networks have widespread applications like security surveillance, environmental monitoring, habitat monitoring, hazard and disaster monitoring, health field applications and home applications. Analysis and monitoring physical characteristics of the environment is the key idea behind deployment of sensor nodes in the hostile area[1–3]. These nodes are not rechargeable but play vital role in data transmission. So overall motivation switch to increase the life of these nodes. Efficient clustering techniques that distribute load evenly among the nodes and prolong network life are constantly appearing in literature. But very few works consider the maintenance of connectivity of the network. Coverage and connectivity should be taken as constraints within the clustering process. Connectivity ensures that all alive nodes in the network are able to send their sensed data to the base station. This paper is the analytical study of the works that proposed in recent

years in order to increase network life time and to select proper cluster head (CH) in clustering topologies. Paper also focus on the protocols that maintain connectivity.

Paper arrange as follows, Sect. 2 gives detail of LEACH protocols. Section 3 summarize the protocols in with their are no restriction on cluster size, Sect. 4 Unequal clustering methos. Section 5 defines fuzzy logic based method for cluster head selection. Section 6 focuses on protocols that maintain connectivity during topology formation. Section 7 gives comparision between protocols. Work conclude in Sect. 8.

2 LEACH and Futher Extensions

The first work to establish that clustering may help in reducing energy consumption and increase network lifetime is “Low Energy Adaptive Clustering Hierarchy (LEACH)” [4]. It is a very popular scheme.

2.1 Leach

Heinzelman et al. [4] proposed this scheme in 2000. In this scheme Cluster Heads (CHs) are rotated periodically to balance energy depeletion.CH election is based on probabilistic model. Working process of the scheme is divided into various rounds and having two phases in every round: Set up phase and the Steady state phase. Clusters are organized in first phase whereas data is delivered to the Base Station (BS) in second phase. For reducing the collisions inside and between the clusters this protocol used time base approach. Dynamic clustering in LEACH performs election at every round of the protocol. Broadcasting so many messages may consume more energy.

2.2 LEACH-C

Heinzelman et al. [5] in 2002 proposed a centralized version of LEACH. It assumes BS to be a very powerful processor. All nodes report their location and and status of available energy to the BS. Only those nodes which have more energy compare to average energy of the network, are eligible to take part in CH election process. The load distribution is guaranteed. In smaller networks or the networks where BS is located very near to the nodes, the energy that LEACH spend in inter-node communication for CH election is saved. BS are generally situated far, and such centralized algorithm that require communication with nodes at every round of the protocol will not prove to be energy-efficient.

2.3 D-LEACH

Kim et al. [6] in 2011 proposed a density based LEACH scheme called D-LEACH. Density around the CH is consider as a main criteria for the node to join any CH in the network. If local density of any CH is less than estimated density of the network, then a non-CH node may join it as member. Else, this non-CH will not join a CH in the current round. The density of network is estimated as ratio of total nodes to the desired number of clusters.

2.4 T-LEACH

Hong et al. [7] in 2009 proposed a scheme called T-LEACH. In this scheme instead of performing CH election at every round of execution of the protocol, the CHs are only elected during certain periods. They call re-election of CH as replacement of CHs. This saves the energy spent in inter-node communication at every round.

3 Clustering without Restriction on Cluster Size

In this section we discuss the clustering techniques that do not decide the size of clusters by bias or any criteria. Rather the size of cluster is automatically decided by the members that join a cluster.

3.1 HEED

Younis et al. [8] in 2004 proposed a hybrid fully distributed clustering method, that supports multi-hop transmission. HEED is a modified version of LEACH. This scheme introduced transmission range limit and the information about the cost of communication inside the clusters. The cost of nodes is the estimate by the cost of communication between the cluster and a function of power level of a node. It is called average minimum reachability power (AMRP). Multi hop behaviour promotes scalability and save energy.

3.2 DWEHC

Ding et al. [9] in 2005 gives the upgrade of HEED. Author consider this as a distributed weighted scheme to enhance network life. It has multi-hop communication between the clusters. Clusters are balanced in size. DWEHC has same assumptions as HEED like no restriction on network size and density. Due to location awareness, a node itself can then decide whether to communicate with its CH using 1-hop or h-hops. It then becomes h-level member. At intra-cluster level, aggregation may be performed at every parent node and forwarded towards the CH. At inter-cluster level, the CHs poll their first-level children and add necessary information then transmit it to the BS.

4 Unequal Clustering Methods

In these methods there is no restrictions on cluster size. Usually clusters which located near to BS are smaller compare to clusters located far away.

4.1 EECS and DEEC

Ye et al. [10] in 2006 gives a clustering scheme whose aim is to save battery power. It assumes single hop routing for transmission from CHs to BS and produce unequal size clusters. A localized competition based on residual energy is conducted for CH election. Any node that has no neighbors with higher residual energy than elects itself as

CH. The cost function and the associated functions are so designed that a node may join its nearest CH and the CH that is also nearer to BS, thus decreasing the burden of the CHs that are farther from BS. Qing et al. [11] in 2006 gives proposal for heterogeneous networks and nodes with high energy get chance to elect as CH.

4.2 EEUC

Li et al. [12] in 2005, introduced Energy Efficient Unequal Clustering with multihop routing. A competition range is given for each node for CHs election. Within the computed competition radius, a tentative CH node competes to become CH on the basis of residual energy. When node's distance to base station decreases then node range also decrease. All the cluster which are close enough to BS are generally small in size. This scheme preserve more energy comparatively.

4.3 DEGRA

Xu et al. [13] in 2012 describes clustering and routing method based on node density. Author uses game theory for clustering and define a utility function whose value depends on various parameter like node's residual energy, density, and energy consumption of nearby nodes. From game theoretic point of view, all nodes are players that are interested in transmitting their data to BS. And Density can be understood as number of nodes with in a certain distance with itself.

5 Fuzzy Approaches for Cluster Head Selection

Electing proper CHs is the main concern in the clustering based algorithms. Fuzzy logic may be used to decide size of cluster to obtain an unequal clustering.

5.1 CEFL

Gupta et al. [14] in 2005 proposed a method with the name Cluster Head Election using Fuzzy Logic. Basically 27 rules and two membership functions are used. Trangular membership function define medium and adequate fuzzy set where as trapezoidal functions define fuzzy sets which are close and far. Main focus is on maximizing life of a network. When one node elected as CHs then each node associate itself to the CHs and Data transmission begin. Besides energy, the other two inputs to the fuzzy inference base remain same in value unless a few nodes die. Energy will play as a prominent decision factor. A major factor of distance of a CH from the BS has not been considered.

5.2 CHEF

Kim et al. [15] in 2008 proposed a algorithm with the similar aim as in CEFL. It is distributed algorithm and cluster head election is performed locally. In round process any node become a tentative cluster head (TCH) if it generates a value which is less

than predefined threshold. Author define two fuzzy sets and fuzzy if then rule with two fuzzy variables namely, Energy and Local Distance. Output will be a chance and if chance of TCH is higher compare to other TCH then it will consider as a actual CH within predefined redius r.

5.3 EAUCF

Bagci et al. [16] gives a fuzzy approach based solution for unequal clustering in 2010. It works in the direction of reducing the intra cluster work of the CH whos life time is low or near to the BS. This approach is used for handling uncertainties in the estimation of cluster head radius. Competition radius is calculated by considering residual energy in addition with distance to the BS. The idea behind the concept of competition radius is that no CH occurs within competition radius of a CH. So unequal cluster structure produced automatically.

5.4 DUCF

Baranidharan et al. [17] in 2016, proposed a distributed approach that uses fuzzy logic to produce balance load in networks. Cluster formation and data collection are two key process in this method. Mamdani method is used as fuzzy if then rule base and centroid method is used for defuzzification. By considering three input parameters DUCF decides the limit on the number of member nodes for any cluster head.

5.5 FBUC

Logambigai et al. [18] in 2015 uses probabilistic threshold value and fuzzy logic for electing cluster head. This scheme uses node degree for the computation of competition radius. Main considerable point is enhancement in the node degree will result in decrement of competition redius. All the nodes that are not elected as CH can join clusters by using two parameters: distance to the CH and CH degree. Use of fuzzy logic increases the life of CHs close to the BS. Mamdani inference system is used.

5.6 MOFCA

Sert et al. [19] in 2015 suggest a multi objective based method with the aim of CHs election. In this scheme first tentative CHs are elected using a probabilistic model and then node uses fuzzy system to participate in competition. Residual energy, node density, and distance are the basic inputs parameters in this scheme. Multiple outputs of the fuzzy system are reflected in the name of the protocol.

5.7 LEACH-SF

Shoukohifar et al. [20] proposed LEACH-SF in 2017. This protocol is based on Sugeno fuzzy system and uses inverse approach to form a cluster. This scheme initially try to find balanced clusters and then focus on selecting suitable CH in the network. Based on

this strategy author get advantage to limit the CHs election. The fuzzy rules are not defined manually but can be optimized according to application specifications.

6 Protocols that Maintain Connectivity

Wang et al. [21] in 2015 have provided a formal treatment to connectivity and coverage problems in WSNs. The deployment being static lattice-like or random has been dealt with separately. If a direct or multihop transmission possible between WSN nodes to BS than nodes are consider as connected. Goratti et al. [22] in 2016 proposed a protocol that consider connectivity issues. If communication breaks due to obstructions this protocol restore connection in star topology WSNs.

Oladimeji et al. [23] in 2016 introduced a clustering approach that uses iterated local search as a key concept to resolve problem of CHs selection. This approach also consider coverage effect and try to save node's energy.

Very recently, Mekkis et al. [24] in 2018 have suggested analytical models for connectivity for both unicast and broadcast transmission schemes of WSNs. The energy tradeoffs with other performance parameters are studied through simulations extensively and the paper identifies the conditions under which connectivity of the network can be maintained for long. Though the models are for solar powered sensors that do not have energy issue of the sensors that are battery-powered, yet it signifies that even when energy issue has been resolved, connectivity still remains a reason for premature death or failure of a WSN.

7 Comparative Analysis

(See Table 1.)

Table 1. Comparison of different protocols

Sr. No	Protocol	Key point	Weak point
1	LEACH [4]	Periodic cluster head rotation to balance energy. Used TDMA for division	Certain regions of the network do not have any CH. Not applicable to large region networks
2	LEACH-C [5]	Centralized in nature and BS act as a very powerful processor	It does not go well with ad-hoc topologies of WSNs
3	D-LEACH [6]	Density is the key point to join any CH. Try to produce cluster of equal member nodes	Creates certain extra CH nodes which may not have the desired energy saving effect in all cases
4	T-LEACH [7]	CHs are only elected during certain periods and save energy	Not scalable.

(continued)

Table 1. (continued)

Sr. No	Protocol	Key point	Weak point
5	HEED [8]	Fully distributed. Proper CH distribution and load balancing to promote scalability	Unbalanced energy consumption Computational overhead
6	DWEHC [9]	It is a multi hop at intra network level. It achieves more balanced CHs distribution than HEED	It is not energy efficient for large region networks. Due to iterative nature it produces high message overhead
7	EECS [10]	Produce unequal size cluster by assuming single hop communication	High energy consumption and decision making cost
8	DEEC [11]	Distributed clustering algorithm for heterogeneous networks Node with higher residual energy get chance to being CH	Lack of scalability due to its communication model. Only theoretical approach
9	EEUC [12]	Each node has a competition range and have multihop routing	Only the nodes that generate a random number greater than a threshold compete
10	DEGRA [13]	Use of game theory and utility function for clustering and routing	More energy consumption due to all nodes act as players
11	CEFL [14]	Use of fuzzy logic for CHs selection Use of triangle and trapezoidal member function to define fuzzy set	It has a centralized operation and not produce the load distribution as expected Major factor distance of CH from BS not considered
12	CHEF [15]	CHs election perform locally. Local distance and node's energy are considerable parameters	Output of the fuzzy system is chance, not easy to calculate
13	EAUCF [16]	CHs radius introduced to handle uncertainties. No CH occurs within competition radius of a CH	It is not applicable to multi-hop communication model. Scalability issue
14	DUCF [15]	It gives assurance of balancing the load among the clusters by changing the cluster size of its CH node	Suitable for homogeneous nodes only
15	FBUC [16]	Use node and when node degree increases the competition radius is decreased	Scalability Issue and more attention required for CH selection
16	MOFCA [17]	Multi objective fuzzy clustering, that takes three inputs for computation	Multiple outputs need to take in consideration
17	LAECH-SF [18]	Inverse cluster formation method used to control Number of CHs. Suitable for time critical applications	Fuzzy rule not defined manually

8 Conclusion

Wireless sensor networks are an important part of many applications. Energy efficiency with long time connectivity is a primary concern in these networks. This paper shows comprehensive study of various protocols proposed till date. We receive the conclusion that most of the protocols consider energy consumption as a primary concern and focuses only on the strategy that prolong the network life. But very few authors switch in the direction of maintaining connectivity. So in future it is necessary to develop a clustering method that reduce energy consumption and checks connectivity during topology formation.

References

1. Jain, A., Pardikar, V., Pratihast, S.R.: Tracing based solution for ubiquitous connectivity of mobile nodes for NDN: A RA kite. In: 8th IEEE International Conference on Computing, Communication and Networking Technologies, Organized at IIT, Delhi, 3–5 July 2017, pp. 1–7 (2017). <https://doi.org/10.1109/icccnt.2017.8204191>
2. Jain, A., Buksh, B.: Solutions for secure routing in mobile ad hoc network (MANET): a survey. Imp. J. Interdiscip. Res. (IJIR) **2**(4), 5–8 (2016). ISSN:2454-1362
3. Jain, A., Sharma, S., Buksh, B.: Detection and prevention of wormhole attack in wireless sensor network. Int. J. Appl. Innov. Eng. Manag. (IJAIEM) **5**(2), 138–142 (2016)
4. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Hawaii International Conference on System Sciences, vol. 8, p. 8020 (2000)
5. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. **1**(4), 660–670 (2002)
6. Kim, J.-S., Byun, T.-Y.: A density-based clustering scheme for wireless sensor networks. In: Kim, T.-h., Adeli, H., Robles, R.J., Balitanas, M. (eds.) AST 2011. CCIS, vol. 195, pp. 267–276. Springer, Heidelberg (2011)
7. Hong, J., Kook, J., Lee, S., Kwon, D., Yi, S.: T-LEACH: the method of threshold-based cluster head replacement for wireless sensor networks. Inf. Syst. Front. **11**, 513–521 (2009)
8. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mob. Comput. **3**(4), 366–379 (2004)
9. Ding, P., Holliday, J., Celik, A.: Distributed energy efficient hierarchical clustering for wireless sensor networks. In: Proceedings of the 8th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 322–339, June 2005
10. Ye, M., Li, C., Chen, G., Wu, J.: EECS: an energy efficient clustering scheme in wireless sensor networks. In: Proceedings of the 24th IEEE International Performance, Computing and Communications Conference (IPCCC), pp. 535–540 (2005)
11. Qing, L., Zhu, Q., Wang, M.: Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. Comput. Commun. **29**, 2230–2237 (2006)
12. Li, C., Ye, M., Chen, G., Wu, J.: An energy-efficient unequal clustering mechanism for wireless sensor networks. In :Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems Conference (MASS), pp. 596–604 (2005)
13. Xu, Z., Yin, Y., Wang, J.: A density-based energy-efficient routing algorithm in wireless sensor networks using game theory. Int. J. Fut. Gener. Commun. Netw. **5**(4), 62–70 (2012)

14. Gupta, I., Riordan, D., Sampalli, S.: Cluster-head election using fuzzy logic for wireless sensor networks. In: 2005. Proceedings of the 3rd Annual Communication Networks and Services Research Conference, pp. 255–260 (2005)
15. Kim, J.M., Park, S.H., Han, Y.J., Chung, T.M.: CHEF: cluster head election mechanism using fuzzy logic in wireless sensor networks. In Proceedings of the ICACT, pp. 654–659 (2008)
16. Bagci, H., Yazici, A.: An energy aware fuzzy approach to unequal clustering in wireless sensor networks. *Appl. Soft Comput.* **13**(4), 1741–1749 (2013). Elsevier Science Publishers
17. Baranidharan, B., Santhi, B.: DUCF: distributed load balancing unequal clustering in wireless sensor networks using Fuzzy approach. *Appl. Soft Comput.* **40**, 495–506 (2016)
18. Logambigai, R., Kannan, A.: Fuzzy logic based unequal clustering for wireless sensor networks. *Wirel. Netw.* **22**(4), 945–957 (2015)
19. Sert, S.A., Bagci, H., Yazici, A.: MOFCA: multi-objective fuzzy clustering algorithm for wireless sensor networks. *Appl. Soft Comput.* **30**, 151–165 (2015)
20. Shokouhifar, M., Jalali, A.: Optimized sugeno fuzzy clustering algorithm for wireless sensor networks. *Eng. Appl. Artif. Intell.* **16**, 16–25 (2017)
21. Wang, Y., Zhang, Y., Liu, J., Bhandari, R.: Coverage, connectivity, and deployment in wireless sensor networks. In: Patnaik, S., Li, X., Yang, Y.-M. (eds.) Recent Development in Wireless Sensor and Ad-hoc Networks. SCT, pp. 25–44. Springer, New Delhi (2015)
22. Goratti, L., Baykas, T., Rasheed, T., Kato, S.: NACRP: a connectivity protocol for star topology wireless sensor networks. *IEEE Wirel. Commun. Lett.* **5**(2), 120–123 (2016)
23. Oladimeji, M.O., Turkey, M., Dudley, S.: Iterated local search algorithm for clustering wireless sensor networks. In: IEEE Congress on Evolutionary Computation (CEC) (2016)
24. Mekkis, P.-V., Kartsakli, E., Antonopoulos, A., Alonso, L., Verikoukis, C.: Connectivity analysis in clustered wireless sensor networks powered by solar energy. *IEEE Trans. Wirel. Commun.* **17**(4), 2389–2401 (2018)
25. Smys, S., Bala, G.J., Raj, J.S.: Self organizing hierarchical structure for wireless networks. In: IEEE International Conference on Advances in Computer Engineering, pp. 268–270, June 2010
26. Jyothirmai, P., Raj, J.S., Smys, S.: Secured self organizing network architecture in wireless personal networks. *Wireless Personal Communications.* **96**(4), 5603–5620 (2017)



Implementation of IDS Within a Crew Using ID3Algorithm in Wireless Sensor Local Area Network

K. Raja^{1(✉)} and M. Lilly Florence²

¹ Bharathiar University, Coimbatore, Tamil Nadu, India
raja.ktkm@gmail.com

² Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India
lilly_swamy@yahoo.co.in

Abstract. Mobile and Pervasive Computing was introduced by the technological vision of Mark Weiser. With the ideology of Urban Development, it is considered that the world will be composed of interconnected devices and system models of networks, which allows the accessibility of information present across the globe. A U-City characterized by the information and computing technologies is gradually becoming indistinguishable and unviable from daily life. In that regard, this article provides an in-depth evaluation of Mobile and Pervasive Computing considered as an evolutionary framework applicable in electric motors, which are invisible hence forming a pervasive environment. Mobile technology will play an essential role in urban development. This signifies that the mobility initiatives are applicable for many telecommunication aspects used in our daily lives. The article starts by illustrating the significant mobile technologies in the urban areas, thereby elaborating on the planning format of pervasive computing, which is meant for urban development. To effective plan for the establishment or expansion of urban centers, the article calls for planners to concentrate on the formation of pervasive computing areas that define the correlations between people, places, objects, buildings and infrastructure. Mobile Crowd Sourcing Technologies for smart environments calls for planners to concentrate on revolutionizing the globe by aligning technological functions and enhance the integration and coordination of various services involved in technological intelligence.

Keywords: Mobile computing · Pervasive Computing · Urban development · Virtual reality · Mobile Crowd Sourcing Technologies

1 Introduction

Mobile World is connected with the interconnected wireless sensor network. A Small organization, industries, a crew or even vehicle is connected with wireless into the internet. Wireless Sensor Network [1] mainly focused on a distributed wireless network system which connected with n number of sensors at the lower cost for industries or organization or even a crew. Each sensor node has its own attributes such as memory, capacity, the flow of data, and data rate per seconds which is connected to unreliable

and unauthorized networks. Number of Usage of Sensor had been rapidly increased in the past five years which made a revolution in the latest technologies. Since the Number of Sensor and Usage increases rapidly, security threats become one of the major issues in the **Wireless Network**.

Security issues can be overcome with new technology is called the **Intrusion Detection System**. Intrusion Detection System [2] is the key process of extracting the information from the large huge amount of information to monitor and detect the intruder in the network. In another word, the Intrusion Detection System mainly used to monitor, identify the information and predict the results which can be used for future actions. Classification is one of the major key roles in the Intrusion Detection System. IDS Can be Classified into two categories: [3] (a) **Network Intrusion Detection System** which is used to monitor and detect the packet of data, which is entering or leaving the wireless network. This NIDS [4] are broadly divided into two categories: (i) **Misuse detection**, digital signatures or any patterns of an existing person or customer in the appropriate network which analyzes and report the attacks of an intruder. (ii) **Anomaly Detection** acts as a defender to the unauthorized profile from the particular network traffic and either blocked or report to authorized personnel. Offline data are represented by Misuse Detection whereas online data are mainly focused on Anomaly Detection. A Machine Learning Algorithm is mainly focused for Anomaly Detection. (b) **Host Based Intrusion Detection System** [5], which is used to provide the information via the operating system or information gathered or provided by a particular operating system. HIDS mainly used to monitor or detect a particular operating system or system. This paper, simulation example to demonstrate, security mechanisms against the intruder in the wireless sensor network.

2 Preliminary of Proposed IDS

The topology for Proposed IDS is the Decision Tree Algorithm. This algorithm represents diagrammatically in terms of data and elements. This Algorithm is classified into three categories (a) root, (b) parent node and (C) leaf node of particular elements in the crew. The main goal of this algorithm is used to classify the given data set and leads to information gain. This process is called ID3 Iterative Dichotomiser 3(ID3). Founder of ID3 is Ross Quinlan, Who generates a dataset from the decision tree. This algorithm used in Machine Learning and Natural Language Processing. ID3 Categorized into two parts (a) Entropy and (b) Information Gain [6].

2.1 Entropy and Information Gain

Entropy is the process of constructing dataset into decision tree and Information gain is a process of optimization from the decision trees. Let S_r be the Set which consists of a Cluster of Sensor used in the Organization or within crew such as Sr_1, Sr_2, \dots, Sr_n . Let S be the Collection of Data Set which consists of different attributes such as s_1, s_2, \dots, S_n . Entropy $H(S)$ which is used to select an appropriate attribute with least values from the given attributes Whereas Information Gain $IG(S)$ which is used to optimize the value from the Entropy and predict the appropriate result for future work which acts as an

Iterative Process using ID3 algorithm. This Iterative Process May stratifies any one of these cases.

Type 1: Every Element in Subset Contains Superset, where each element as a leaf node

Type 2: Every Element in Subset partially belongs to Superset, where each element as a leaf node

Type 3: No elements are matched, each element act as a common class of parent set.

2.2 Decision Tree

The main objective of this decision tree to detect the intruder from the database is called a decision tree. These decision tree algorithms are as follows.

- (1) Consider the Set S which consist of a set of attributes and R be the Given Set of particular organization or crew
- (2) Let S_r be the Set of Sensor user in the Wireless Local Area Network.
- (3) To Calculate Entropy: R can be classified into two category, P_{yes} which contains the attributes with yes value and P_{No} which contains the attributes with No values.
- (4) Calculate P_{yes} and P_{No} , Process should be iterative for the given all attributes
- (5) Calculate the Information Gain from step 3 and Step 4.
- (6) Construct Matrix with Entropy and Information Gain and Optimize maximum value from the attributes based on the given set.
- (7) Stop the Process.

3 Designing of Proposed IDS

The Communication between the Sensor and Each Wireless device via mobile or lab connected to a wireless network can be subjected to cybercrime attack by unauthorized devices. An Intruder can access the wireless local area network and possible to transmit the content from one device to another. The attack can be classified into three categories: [7] (A) Dos attack, where the attackers can block the information from one device to another device. (B) Reply attack, can attackers can record the information send by some other device and delay the reply of information. (C) Bias injection, where the attacker can append some more information to the transmitted message which changes the entire content of the information.

The main process of the proposed IDS is to detect the intruder from Wireless Local Area Network. The sensor used to monitor the thread of each and every device in the appropriate network [8]. Each device hostname, host address, and port number are retrieved from the device and pass this three parameter to the server. In Server, these attributes are monitored from the database. If authorized Hostname, Host address and port number then the user can access the device within the network. If unauthorized hostname, hosts address and port number which is not available in the database, then these details will be blocked and appropriate details will be stored in the blocked list and the corresponding message will be sent to the administrator via SMS and email (Fig. 1).

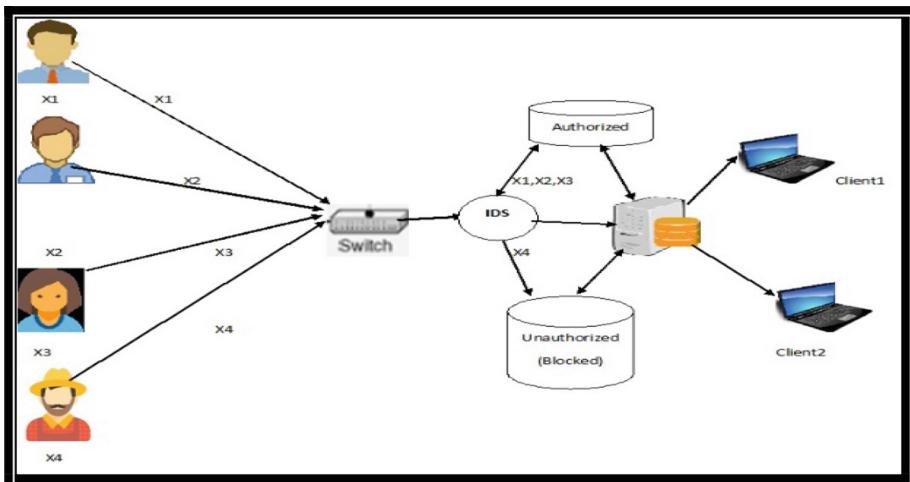


Fig. 1. Architecture diagram for proposed IDS

The following Fig. 2 illustrates the process of Proposed IDS as User is classified as Authorized and Unauthorized Person Who Access the Sensor used within an organization.

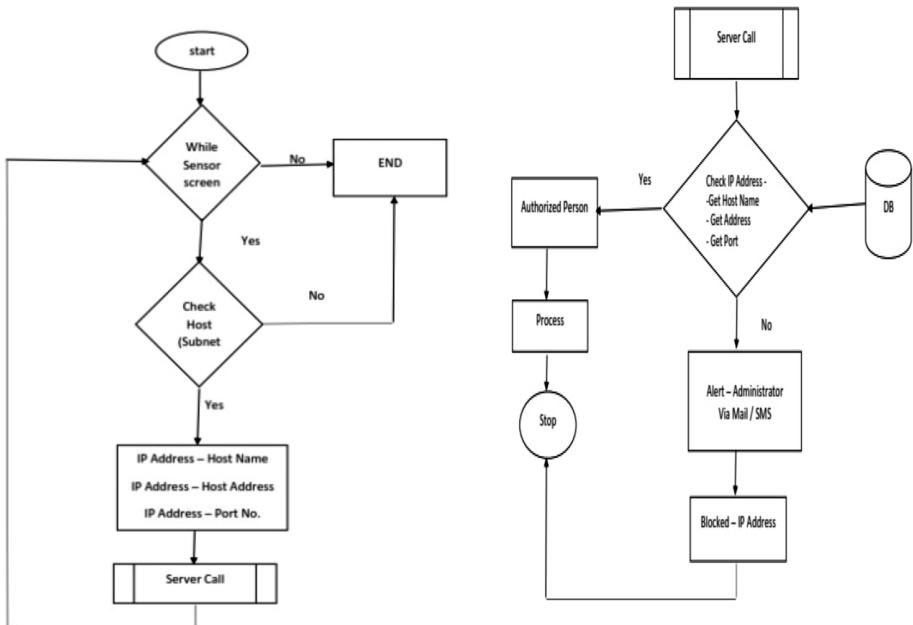


Fig. 2. Flow diagram for proposed IDS

IDS is used to monitor or detect the intruder from the sensor used in the organization. A proposed algorithm is used to detect the Unauthorized user and block the appropriate unauthorized user with the help of their hostname, host address and port number which are entered as an intruder. The Next section of this paper will clearly explain the process of the proposed algorithm to detect the attackers or an intruder in the wireless Sensor network [9].

4 The Algorithm of Proposed IDS

The algorithm for the proposed IDS are as follows:

- Let S_r be the Set of Sensor = { $s_{r_1}, s_{r_2}, \dots, s_{r_n}$ } for all 1 to “n” sensor device in the wireless sensor network.
- Let D be the Set of the mobile device such as a laptop, mobile within organization = { d_1, d_2, \dots, d_n } an authorized device which is connected to the sensor network.
- Let S be the Set of Attributes of particular device d_i , Such that each device has its own set of attributes named as { s_1, s_2, \dots, s_n } where s_i represents host-name, host-address and port number for 1 to 3 respectively.
- Assume the Sensor S_r will scan the device from the Set D such that $D \subseteq S_r$, Set D can be classified into two categories: Authorized Device d_i , which is stored in the database, d_x un-authorized device connected to sensor network

```
If ( $d_x \notin \text{Set}(D)$ ) {
    Intruder =  $d_x$ ;
} else
    {authorized User =  $d_i = d_x$ ;
```

- Consider d_x is un-authorized device or intruders, then attributes of the Set S such as host-name, host-address, and port number are passed as a parameter to server function.
- Server function will block the d_x device from the wireless sensor local area network and passed to information to the administrator via SMS or email [10].
- This process used to protect the intruder in the wireless sensor area network in a particular organization.

5 Experimental Result

The Sample Data used in the proposed application, which mainly focused to estimate the information gain from the decision tree algorithm using ID3. This ID3 algorithm implemented in the proposed application. A Device which is connected to the wireless sensor network is considered with their host address, hostname, and port number (Table 1).

Table 1. Experimental result

Sl no	Host address	Host name	Port number	Intruder
1	192.168.44.81	CS3	110	No
2	192.168.46.38	IT23	8009	Yes
3	191.168.44.75	CS56	6891	Yes
4	192.168.49.24	BME18	25	No
5	192.168.46.89	IT44	8080	No
6	192.168.44.66	CSI4	443	Yes
7	192.168.49.87	BME67	8009	Yes
8	192.168.46.44	IT98	8080	Yes
0	192.168.44.101	CS74	6891	No
10	192.168.49.128	BMEI23	25	No

The proposed IDS experiment via Waikato Environment for Knowledge Analysis (WEKA) and the KDD Cup 99 dataset are tested. The WEKA Tool is a Collection of Java Class Libraries which is used to execute the Machine Learning and Data mining concept at various level in the form of state of art.

Consider KDD CUP 99 dataset used as experimental data, which is retrieved from DARPA 98 intrusion detection evaluation at MIT, handled by Lincoln Laboratory [11]. This data set is a collection of test set which is widely used in the detection of the instruction data.

It includes about nearly 4.9 Million simulative attack record with 22 types of attack. It also provides a very large amount of data. The KDD Cup 99 data set of 10% alone are to be considered for Training and Testing with proposed research work.

This training data set and Testing done with two types of attacks such as (a) DoS (b) U2R (user to Root).

KDD Cup99 is an audited set of the standard dataset which includes training and testing set. Data has the following two major groups of attacks:

- (a) Denial-of-Service (DoS): A some of the services which are accessible through the network are unavailable to the legitimate user, this kind of attacks are termed as DoS. like Neptune, smurf, land etc.
- (b) Remote-to-Local (R2L): A Attacker who had no privileges to access a private network from outside like Sendmail, guess password, spy etc. over the internet.

Attacks of an intruder can be determined with four types of metrics.

- False Positive (F_P): Which equals to the number of attacks detected, which is considered to be a normal fact.
- False Negative (F_N): this is mainly focused on the intrusion detection system, which means the actual number of attacks detected with normal instances.
- True Positive(T_P): number of fact attack which is equal to the detected attacks.
- True Negative(T_N): equals to detected normal instances are to be considered.

5.1 Performance Measures

The Performance measure is used to evaluate the proposed ID3 with existing ID3 as follows:

- (a) The rate of Detection: The Percentage of the detected attacks among all other attack data, given as

$$\text{Rate of Detection} = (T_P / (T_P + T_N)) * 100 \quad (1)$$

By applying Eq. 1, to both existing and proposed ID3 which observed that the results of the detection rate for the different type of attacks are shown in Fig. 3. From the result of KDD Cup Dataset 99, its observed the detection rate of existing ID3 is approximately 49.51 and 99.31 for the Proposed ID3 [12]. Similarly, detection of proposed ID3 is comparatively more than the existing ID3.

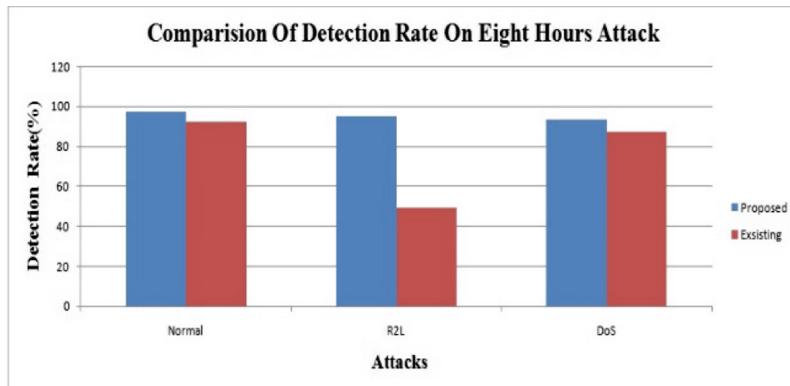


Fig. 3. Rate of Detection

- (b) The rate of False Alarm: the normal data which is wrongly determined as the attack of the intruder is defined as follows:

$$\text{Rate of False Alarm} = (F_P / (F_P + F_N)) * 100 \quad (2)$$

By applying Eq. 2, to both existing and proposed ID3, which observed the result of the false alarm rate as shown in Fig. 4. Form the result its observer that the false alarm rate for proposed ID3 is better than existing ID3 compare with all types of attacks.

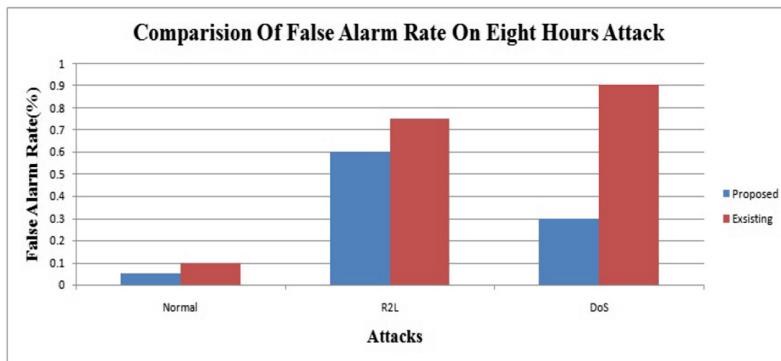


Fig. 4. Rate of False Alarm

6 Simulation

The proposed application implemented PHP5, Java 1.7, JASON, MySQL. Simulations of the proposed application are as follows (Fig. 5).

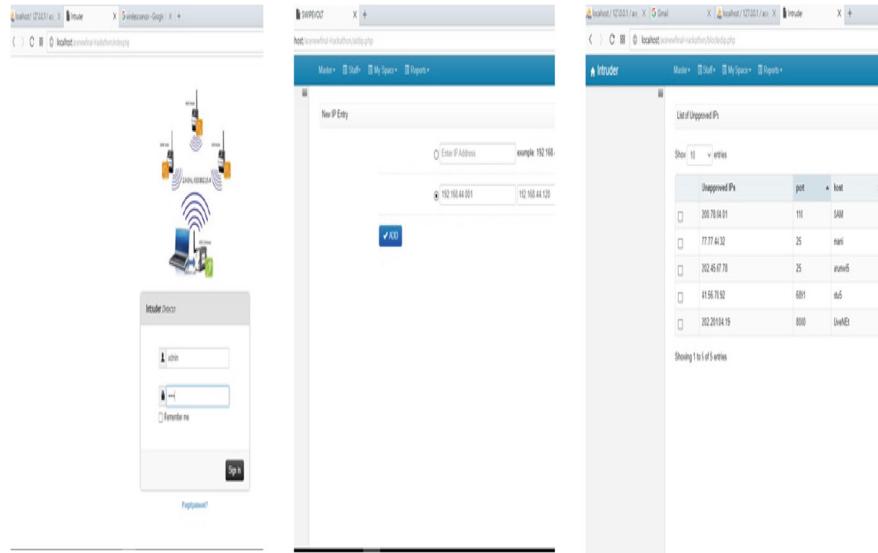


Fig. 5. Proposed application to detect the intruder

7 Conclusion

In this paper, we conclude that a proposed application to monitor and detect the intruder in terms of a mobile device such as laptop or mobile connected to the wireless sensor local area network in a more effective and efficient manner. This proposed application is used to estimate entropy and information gain from the decision tree algorithm to detect the intruder using the ID3 algorithm. This proposed application can be extended to the mobile application with cloud security in the future work.

References

1. Sun, Z., Xu, Y., Liang, G., Zhou, Z.: An intrusion detection model for wireless sensor networks with an improved V-detector algorithm. IEEE Publication, 1558–1748, pp. 567–580 (2017)
2. Sultana, A., Jabbar, M.A.: Intelligent network intrusion detection system using data mining techniques. In: IEEE Publication, pp. 85–89 (2016)
3. Raja, K., Florence, M.L.: Tracking of intruder in local area network using decision tree learning algorithms. Asian J. Appl. Sci. **05**(01), 46–49 (2017). ISSN:2321–0893
4. Verma, A., Ranga, V.: Statistical analysis of cidds-001 dataset for network intrusion detection system using distance-based machine learning. In: 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7–8 December 2017, pp. 709–716. Elsevier Publication (2017)
5. Mageswari, G., Karthikeyan, M.: Intrusion detection using data mining techniques. Int. J. Eng. Sci. Invent. (IJESI) (2018). ISSN (Online):2319–6734, ISSN (Print):2319–6726
6. Goliwale, P., Gupta, V., Johre, A., Bendale, S.: Intrusion detection system using data mining. Int. Res. J. Eng. Technol. (IRJET) **05**(03), 234–238 (2018)
7. Al-Dabbagh, A.W., Li, Y., Chen, T.: An intrusion detection system for cyber attacks in wireless networked control systems. IEEE Publication, 1549–7747, pp 789–799 (2016)
8. Moosavi, H., Bui, F.M.: A game –theoretic framework for robust optimal intrusion detection in wireless sensor networks. IEEE Trans. Inf. Forensics Secur. **9**, 524–529 (2014)
9. Zhang, Z., Zhu, H., Luo, S., Xin, Y., Liu, X.: Intrusion detection based on state context and hierarchical trust in wireless sensor networks. IEEE Publication, pp 457–462 (2017)
10. Mehmood, A., Khan, A., Umar, M.M., Abdullah, S., Ariffin, K.A.Z., Song, H.: Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. IEEE Publication, 2169–3536, pp 309–314 (2017)
11. Jaiganesh, V., Rutravigneshwaran, P., Sumathi, P.: An efficient algorithm for network intrusion detection system. Int. J. Comput. Appl. **90**(12), 894–896 (2014). (0975–8887)
12. Gupta, A., Jha, R.K., Gandotra, P., Jain, S.: Bandwidth spoofing and intrusion detection system for multistage 5G wireless communication network. IEEE Trans. Veh. Technol. **67** (1), 128–134 (2018)



A Hybrid Technique for Unsupervised Dimensionality Reduction by Utilizing Enriched Kernel Based PCA and DBSCAN Clustering Algorithm

D. Hemavathi^(✉), H. Srimathi, and K. Sornalakshmi

Department of Information Technology, School of Computing,

SRM Institute of Science and Technology, Chennai, India

{hemavathi.d, sornalakshmi.k}@ktr.srmuniv.ac.in,
srimathi.h@srmuniv.ac.in

Abstract. Selection of relevant features is a significant technique in the real time applications. It constitutes a number of data related to the ever-augmenting domains like financial organization, education etc. For recognition of relevant features, the results should be determined accurately. In the developed work Terry dataset is considered for unsupervised learning. Whereas significant features are selected by embedded method and the selected features are processed with enriched kernel based Principal component Analysis (PCA) for dimensionality reduction, which is further evaluated with Density-based spatial clustering of applications in the noise (DBSCAN) algorithm for developing a better performance.

Keywords: Embedded · DBSCAN · Terry data · Kernel based PCA

1 Introduction

In information industry humongous data is present. At present scenario humans are living in the age which is known as information age. Information forefront to humans to success, power and many other mandatory things. Humans are very grateful to electrical technologies like computers, Satellites etc. from where data are received. In the beginning information are gathered form computers and it is utilized for all types of data storage. Unluckily these huge data collections stored in the systems are overwhelming. This laid a path to the discovery of database structures and database management systems. Managing database efficiently has become a significant asset for managing huge amount of data. Mainly it is utilized for efficient and effective retrieval of a particular data from the whole collection data. The multiplication and growth of database structures are responsible for massive collection of all kinds of data. At present scenario we are provided with vast data transactions in business. Scientific data, satellite pictures etc. Countless amounts of data have been collected from text documents and other sources. Unless these available data in the industry is transformed into useful data it is of no use. Hence it is significant to evaluate the vast data and extricate the required data from it.

For extrication of the required data from the mining of information have to be performed. Mining of data includes some other process like Data cleaning, Data integration, Data transformation, pattern evaluation etc. Knowledge discovery in database (KDD) is also called as Data mining. Mining of data is a post of knowledge discovery process. Extraction of feature is a significant process in mining of data. Extraction of feature and selection methods is utilized to increase the accuracy, visualization of the data. Extraction of feature includes the quantity of data required to explain the vast set of information. Traditionally features are distinguished as relevant, irrelevant or redundant. Datas have numerous numbers of features. Feature extraction plays a vital role in recognition and extraction of most useful data from the collection of data. It is utilized for extricating useful information and reducing the complexity in data processing. Feature extraction is done by utilizing machine learning methods.

Learning represents either gaining or improvising the knowledge. Machine learning is utilized for monitoring the transformations made in the data for effective & efficient output. Machine learning is classified into supervised and unsupervised learning. In supervised learning data sample is gained from source with the classification assigned. And not efficient accuracy and evaluation. In unsupervised learning the hidden patterns learn and recognise the unlabelled data. Supervised learning refers to the capability of learning and organising signal. Discriminative features can be discovered for object identification.

Traditionally these are two major categories in dimensionality reduction. They are feature selection and feature extraction. Methodology which utilizes feature selection finds the smallest subsets with similar features. In feature extraction the dataset dimensionality is reduced by gathering the features. This unique technique reduces the data loss but in feature selection the originality of data will be remain the same. Hence features selection is utilized in the work where as among all dataset number of instances and dimensions and attributes numbers are gradually increasing day by day. In these datasets many dissimilar attributes will also be available by distributing knowledge and discovery to avoid this irrelevant disturbances dimensionally reduction is utilized. After the selection of subsets and processing of subsets unsupervised learning is utilized for clustering datasets.

In the developed work the input datasets with large number of attributes is processed. The significant features are selected through feature subset selection with embedded method. This selected features are given to enriched kernel based PCA for reduction in dimensionality. Thus reduced subsets are grouped by attribution grouping. Grouped attributes are clustered by DBSCAN Algorithm, fuzzy k means and k means algorithm. The clustering accuracy is calculated.

2 Related Work

Feature extraction and feature selection of data with unsupervised learning needs inartistic analysis and constituter a number of complication. A number of researchers have researched on this area for data mining in Information technology. In this section

numerous work and study related to features extracting with unsupervised learning is discussed.

Kale et al. [1] presented a principal component analysis for selection of feature by utilizing fuzzy learning machine. Fuzzy subset selection makes use of optimal feature order for data subsets. Anoop et al. [2] utilized a efficient and sealable technique for extraction of feature from large texts. The complete process is made by unsupervised learning method. Wang et al. [4] developed a feature selection method and used for big data informatics. Implemented the technique by utilizing filter, wrapper and embedded approaches in selection of feature.

Sridhar et al. [5] implemented a supervised system for domain specific normalisation in data. Utilised lexical similarity between noisy and canonical form of data for better representation. Tutz et al. [6] exhibited a signal regression for extraction of feature from data. Pavlenko et al. [7] developed a technique for feature selection data set. And utilized discretization for preprocessing by PSO search techniques for continuous attributes. Sathyam et al. [13] presented a comparative analysis for supervised and unsupervised learning method by utilizing pattern recognition for classification of data. El Ferchichi et al. [16] manipulated data by using supervised learning for extracting features. Dimensionally reduction is used for extracting original features from the redundant data set.

Jasmina et al. [18] evaluated a feature ranking method by using two data set. Data sets are evaluated. Four supervised learning algorithms are evaluated with RBF network. Jayalakshmi et al. [12] presented a modified ANN technique by utilizing non linear classifier. The datas are trained with back propagation method for better accuracy. Suneetha et al. [15] presented a technique for predicting data subset. Gini index is utilized by biases multivariable attributes. Jaba Sheela et al. [14] analysed approach for finding data with continuous valued attributes by utilizing discretization. Kwak et al. [17] proposed a new methodology for regression of feature extraction. For classification a modified linear discriminant analysis technique is utilized. Salappa et al. [9] presented a pattern recognition technique for selection of feature and utilized wrapper technique for accuracy in classification. Pavlenko et al. [7] presented a discriminant function by utilizing inclusion and exclusion factor of data and irrelevant feature sets are eliminated.

Chavez et al. [8] presented a proximity search for high dimensional data. Liu et al. [11] presented a new methodology for discretization of data. Chakroborty et al. [19] developed a unsupervised learning methodology for multidimensional data based on similarly of data samples. Bullman et al. [10] investigated an optimal rate for convergence of data regression. Bolon canedo et al. [3] developed a feature selection technique to minimize the complexity in high dimensional data.

Existing Methodology

Principal Component Analysis (PCA) based kernel technique have been implemented for Senseval-2 data and differentiated with SVM for supervised learning mechanism. Whereas the accuracy of the system not appropriate and implemented with difficulty in

dimensionality reduction. Hence forth a new technique has been developed for unsupervised learning technique.

Proposed Methodology

A unique methodology has been developed for unsupervised learning methodology for terry dataset. For selection of feature subsets embedded technique is utilized. Thus selected subsets with significant features are processed for reduction in dimensionality by using enriched kernel based PCA algorithm. The above work minimises the maximum dimension (irrelevant) in the dataset. The reduced dataset is grouped by attribution while grouping forms a new group of data. From the newly formed data the significant features are clustered by DBSCAN, K means, Fuzzy k means algorithms for evaluating clustering accuracy of the algorithms (Fig. 1).

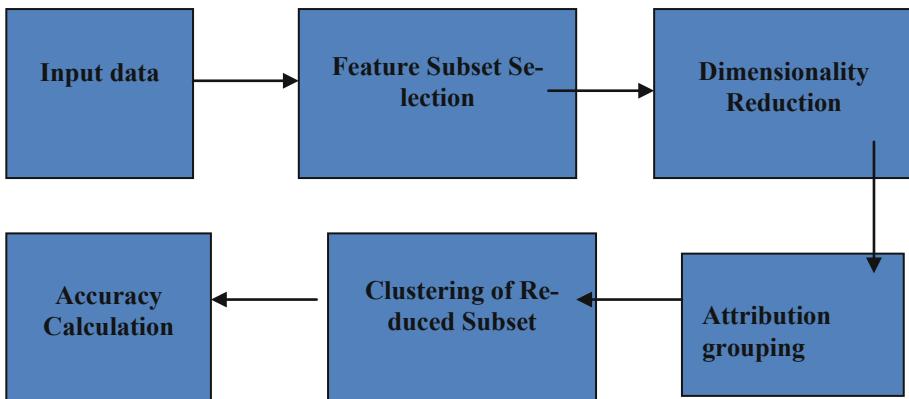


Fig. 1. Block diagram of proposed work

Input Data

In the developed methodology Terry dataset utilized as it is a text recognition dataset. Terry dataset is mainly used for unsupervised learning. A set of 200 subsets are utilized from Terry RCV1- V2 collection of data. These input terry dataset are further processed to next level of subset selection.

Feature Subset Selection

The procedure of feature selection has become a mandatory past in the past few years in the field of machine learning. In supervised learning for classification of dataset into its relevant subsets. It is indeed to remove the irrelevant, recurring, noisy data from the database. All the features in database have a significant function in evaluating the subset (Fig. 2).

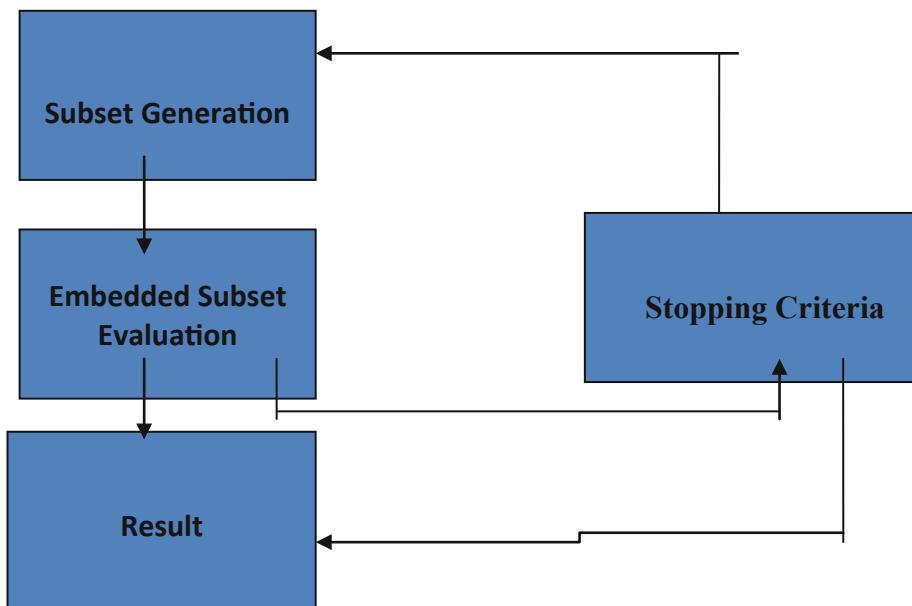


Fig. 2. Process of feature subset selection

Subset Generation

For subset generation, complete search methodology is utilized for optional subset generation without missing a single subset for evaluation of adopted criterion. Dissimilar heuristic function is involved to neglect the search space in dataset without disturbing optimal subset searching.

Subset Evaluation

For evaluation of subset embedded technique is utilized due to its unsupervised learning and lower cost when distinguished with filter and wrapper technique. This technique contributes the best features for accuracy in subset evaluation. The common traditional type of embedded feature selection techniques are regularization techniques. This is also known as Penalization methodology. It introduces an extra constraint for optimization of terry datasets which leads to reduced complexity. Thus evaluated subsets are fed to the dimensionality reduction.

Stopping Criteria

The deciding factor of a process is commonly known as stopping criterion of feature selection. Generally stopping criteria is attained when the search ends, required number of features is obtained. Thus obtained criterion is evaluated in the result by reducing the subset terry data into 110 subsets.

Dimensionality reduction

Reduction in dimension is a significant aspect in machine learning. Dimensionality reduction is an effective technique for reducing the size of data. Many of the unsupervised and data mining methodologies are not effective for data with high dimensionality.

Minimising the quantity of data features helps in developing unsupervised learning procedure.

Dimensionality reduction is a unique technique for collecting information from high dimensional data. Dimensionality reduction can be classified into many approaches among them feature extraction and feature selection is very significant of all. Usually feature extraction is utilised for higher dimensional data. An alternate distinction of reduction in dimensionality is feature selection is linear and non linear techniques. Linear technique utilizes a original feature combination with linearity. It includes many techniques like PCA, Singular Value Decomposition, and LDA etc.

The techniques are literally low in efficiency and evaluation of dataset hence a non linear dimensional reduction is utilized. Evaluation of feature selection is generally done by information measures such as

Entropy of variable X

$$H(X) = - \sum_j P(x_i) \log_2(P(x_i)) \quad (1)$$

Entropy of X after observing Y

$$H(X|Y) = - \sum_j P(y_i) \sum_i P(x_i|y_i) \log_2(P(x_i|y_i)) \quad (2)$$

Information gain

$$IG(X|Y) = H(X) - H(X|Y) \quad (3)$$

In the developed technique nonlinear unsupervised dimensionality reduction is utilized with enriched kernel based PCA methodology. Enriched kernel based PCA is evaluated via a feature space which is in relationship with input space.

Enriched Kernel Based PCA

Enriched kernel based PCA is a unique non linear dimensionality reduction kernel technique for selection of principal components from vector sets. Input vectors with n dimension are mapped nonlinearly from the original space to a feature space (F) with maximum dimension is evaluated by creating a transformation of which the input vectors are mapped with nonlinearity to a new vector set. A significant adage of enriched KPCA is it is not like other evaluating methodologies, it makes use of predictive features with new set of combinations into evaluation when optimization is in need in reduction of dimensionality.

For evaluation of nonlinear PCA enriched kernel methodology is utilized for the Terry dataset. The feature selected subsets are evaluated by this technique by feature map $x \mapsto \Phi(x)$ and the empirical covariance matrix is defined as

$$C_\Phi = \frac{1}{n} \sum_{i=1}^n \Phi(x_i) \Phi(x_i)^T \quad (4)$$

Eigen vectors with linear feature combination of vectors

$$\begin{aligned}\lambda v &= C_\Phi v = \frac{1}{n} \sum_{i=1}^n \Phi(x_i) \Phi(x_i)^T v \\ &= \frac{1}{n} \sum_{i=1}^n \langle \Phi(x_i), v \rangle \Phi(x_i) = \sum_{i=1}^n \alpha_i \Phi(x_i)\end{aligned}\quad (5)$$

Where

$$\alpha_i = \frac{1}{n} (\Phi(x_i), v) = \frac{1}{n\lambda} \langle \Phi(x_i), v \rangle = \frac{1}{n\lambda} \langle \Phi(x_i), C_\Phi v \rangle$$

Now

$$\lambda \sum_{i=1}^n \alpha_i \langle \Phi(x_k), \Phi(x_i) \rangle = \lambda \langle \Phi(x_k), C_v \rangle \quad (6)$$

For kernel matrix ($K = K_{ij}$)

$$\begin{aligned}K_{ij} &= [\Phi(x_i), \Phi(x_j)] \\ \lambda n K \alpha &= K^2 \alpha\end{aligned}\quad (7)$$

For evaluation of kernel Eigen value

$$K \alpha = n \lambda \alpha \quad (8)$$

Above equation is diagnosed by $n * n$ system. For computing enriched kernel based PCA projection of test point x , feature vector is mandatory onto principal direction v_m

$$\begin{aligned}\langle v, \Phi(x) \rangle &= \sum_{i=1}^n \alpha_i \langle \Phi(x_i), \Phi(x) \rangle \\ \langle v, \Phi(x) \rangle &= \sum_{i=1}^n \alpha_i K(x_i, x)\end{aligned}\quad (9)$$

This entire technique utilized any evaluation of enriched kernels $K(x, x_i)$ and actual feature vector manipulation is not mandatory. For first K vectors arbitrary data point is calculated by projecting $\Phi(x)$, hence the feature space is approximated. The complete evaluation of enriched KPCA algorithm is mandatory for detailing feature space centring by utilizing enriched kernel operations. The kernel operations are given below.

$$\tilde{K}_{ij} = (K - 1_n K - K 1_n + 1_n K 1_n)_{ij} \quad (10)$$

Where

$$\mathbf{1}_n = \frac{1}{n} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} = \frac{1}{n} \mathbf{1} \mathbf{1}^T$$

$\mathbf{1}$ = Vector of all ones

Enriched Kernel PCA Algorithm

1. Kernel is centralised.
2. Computation of $K_{ij} = K(X_i, X_j)$
3. Diagonalization of K
4. Normalization of Eigen vector $\alpha^{(m)}$
Hence $[\alpha^{(m)}, \alpha^{(m)}] = \frac{1}{\lambda_m}$
5. Test point x is projection for computation of Eigen vector v_m

$$\text{By } [v_m, \Phi(x)] = \sum_{i=1}^n \alpha_i^{(m)} K(X_i, x)$$

Thus the dimension of the terry dataset got reduced to 27 attributes from the selected subset features by utilizing enriched kernel based PCA technique the reduced features are fed to attribution grouping.

Attribution Grouping

Attribution grouping is a well known method for grouping significant data from the database in data mining. Irrelevant attributes tend to minimise the efficiency and performance of the dataset. Attribution grouping is the prior process of dataset. Similar types of attributes are grouped together by eliminating the irrelevant and redundant attributes. There are three major types of attributes they are numeric, binary, ordinal and nominace. These are grouped according to the relevancy in subset features and this data is further processed with clustering techniques.

Clustering of Subset Features

Clustering is partitioning of data into a set of unique nature. In unsupervised machine learning Destiny based spatial clustering of application with Noise. Hierarchical clustering algorithm generates clusters gradually whereas partitioning algorithm learns clustering directly. Hierarchical clustering either recognised cluster by iteratively relocating point between subsets or tries to identify clusters with high populated data partitioning algorithms identify data components which are connected with density. These density based algorithms are flexible in terms of their shape. Density based clusters are less responsive to outliers and able to recognise clusters with irregular shape. It also concentrates on numerical attributes called as spatial data in text mining. DBSCAN recognises the dense point in datasets and starts to search for the dense arbitrarily shaped clusters. In DBSCAN algorithm density reach ability and density connectivity.

Density Reachability

From point “q” to point “p” is said to be density reach ability within the limit of ϵ distance from “q”. Point “q” constitutes enough number of points in neighbours within the distances.

Density Connectivity

Two points “p” and “q” are connected with respect to density. Another point “r” is considered which constitutes the needful number of point in its neighbourhood and point “p” and “q” lies within the range of ϵ distance.

DBSCAN algorithm requires two essential parameters for calculation of clustering. They are epsilon (EPS) and minimum points (Minpts). The process is initiated with a starting data from arbitrary which haven't been visited yet. And it searches for neighbourhood data within the limit of ϵ distance from the initial point. The quality of neighbouring data is higher or equal to minimum data the cluster is formed. The initial data and its neighbours are coupled to the cluster and the initial point is marked as visited. Thus process is been repeated for evaluation of all neighbours recursively.

3 DBSCAN Algorithm

Step1. Initiated from arbitrary starting data which is not visited at all.

Step2. Each and every data within ϵ neighbourhood of data is extricated.

Step3. Evaluates the neighbourhood points if the required data are available the clustering process is initiated. Hence the data is marked as visited.

Step4. If a data is identified as a part of cluster its neighbouring data will also be part of the cluster. Hence step2 is repeated for all ϵ data in the neighbourhood. Reaped till all the data points in cluster is evaluated.

Step5. A new unvisited data point is found and processed which leads to the formation of cluster.

Step6. Step5 continues until all the data points are marked as visited.

From the DBSCAN algorithm the above steps are evaluated and the clusters are formed with relevant data and irrelevant data with noise are removed. Thus formed clusters are evaluated by accuracy parameters for K means and Fuzzy K means algorithms (Figs. 3 and 4).

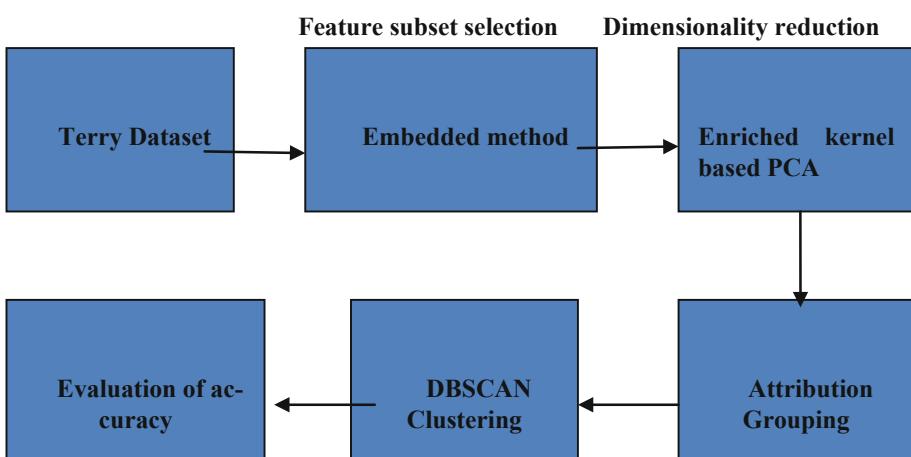


Fig. 3. Proposed methodology for dimensionality reduction

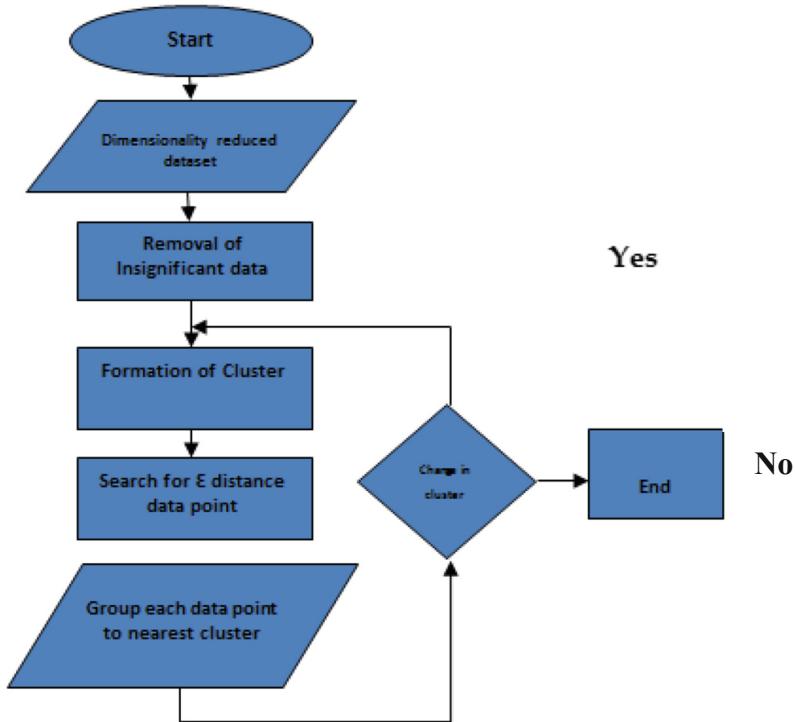


Fig. 4. Flowchart of DBSCAN algorithm

4 Accuracy Calculation

The accuracy of the clustering algorithm utilized for the unsupervised learning in the proposed methodology is evaluated with K means and Fuzzy K means algorithms for performance evaluation of DBSCAN.

5 Root Mean Square Deviation

The root mean square deviation is utilized to measure the dissimilarity in between two data points.

$$RMSD = \sqrt{\frac{\sum_{i=1}^n (p - q)^2}{n}} \quad (11)$$

Where p, q are data points.

6 Dunn Index

Dunn index is utilized for evaluating the spacing in between the clusters.

$$D = \frac{\min_{1 \leq i < j \leq n} d(i, j)}{\max_{1 \leq k \leq n} d'(k)} \quad (12)$$

Where I, j, k cluster indices

d = inter cluster distance.

7 Davis Bouldin Index

Davis Bouldin index calculates the cluster values which is far away from the centre region.

$$DB = \frac{1}{n} \sum_{i=1}^n \max_{j \neq i} \left(\frac{\sigma_i + \sigma_j}{d(c_i, c_j)} \right) \quad (13)$$

Where n = number of clusters

σ_i = average distance of clusters

c_i, c_j = distance of all points from centre.

8 Result and Discussion

The proposed methodology is evaluated by Terry datasets. It is mainly utilized for unsupervised learning. A set of data with 200 attributes is of RCV1-V2 data is evaluated. For performance evaluation of dataset DBSCAN, K means and Fuzzy K means algorithms are utilized.

9 Experimental Result

From the Table 1 it is observed that the DBSCAN clustering algorithm performs better than Fuzzy K means and K means algorithm.

Table 1. Performance analysis of clustering algorithms

Clustering algorithm	No of attributes	Cluster formation	Noise
DBSCAN	27	38	9
Fuzzy K means	54	84	28
K means	68	103	46

Table 2. Accuracy comparison of proposed methodology

Algorithms	Performance		
	RMSD	Dunn index	Davis Bouldin index
DBSCAN	0.9324	0.9641	0.9321
Fuzzy K means	0.7401	0.7891	0.8101
K means	0.6841	0.6932	0.6600

From Table 2 it is represented that the DBSCAN algorithm performs with better accuracy than the other methods.

10 Conclusion

Data mining plays a vital role in the information industry. Data mining is carried out by supervised and unsupervised machine learning techniques, Whereas unsupervised machine learning plays a prominent role in data mining. In unsupervised machine learning feature subset selection is utilized due to its simplified nature. In the developed method terry dataset is utilized. Feature subsets are selected by embedded method. Thus selected features are processed with enriched KPCA for dimensionality reduction. From the reduced subsets attributes are grouped and clustered by DBSCAN algorithm and compared with fuzzy k means and k means clustering for accuracy classification. Performance of the system is evaluated using the clustering algorithms and concluded that DBSCAN clustering performs better than other techniques when processed with enriched KPCA for dimensionality reduction. Thus the datasets are reduced and irrelevant data are removed with high accuracy.

References

1. Kale, A.P., Sonavane, S.: PF-FELM: a Robust pca feature selection for fuzzy extreme learning machine. *IEEE J. Sel. Topics Signal Process.* **12**(6), 1303–1312 (2018)
2. Anoop, V.S., Ashraf, S., Deepak, P.: Unsupervised concept hierarchy learning: a topic modeling guided approach. *Procedia Comput. Sci.* **89**, 386–394 (2016)
3. Bolón-Canedo, V., Sánchez-Marcano, N., Alonso Betanzos, A.: Recent advances and emerging challenges of feature selection in the context of big data. *Knowl. Based Syst.* **86**, 33–45 (2015)
4. Wang, L., Wang, Y., Chang, Q.: Feature selection methods for big data bioinformatics: a survey from the search perspective. *Elsevier* **6**(2), 2–31 (2016)
5. Sridhar, V.K.R.: Unsupervised text normalization using distributed representations of words and phrases. In: *Proceedings of NAACL*, vol. 6, pp. 8–16 (2015)
6. Tutz, G., Gertheiss, J.: Feature extraction in signal regression: a boosting technique for functional data regression. *J. Comput. Gr. Stat.* **19**(1), 154–174 (2011)
7. Pavlenko, T.: On feature selection, curse-of-dimensionality and error probability in discriminant analysis. *J. Stat. Plann. Infer.* **115**(2), 565–584 (2003)

8. Chávez, E., Navarro, G.: Probabilistic proximity search: fighting the curse of dimensionality in metric spaces. *Inf. Process. Lett.* **85**(1), 39–46 (2003)
9. Salappa, A., Doumpas, M., Zopounidis, C.: Feature selection algorithms in classification problems: an experimental evaluation. *J. Optim. Methods Softw.* **22**(1), 199–214 (2007)
10. Bühlmann, P., Yu, B.: Boosting with the L2 loss: regression and classification. *J. Am. Stat. Assoc.* **98**, 324–339 (2003). [158, 159, 161]
11. Liu, H., Hussain, F., Tan, C.L., Dash, M.: Discretization: an enabling technique. *Data Min. Knowl. Disc.* **6**(4), 393–423 (2002)
12. Jayalakshmi, T., Santhakumaran, A.: Statistical normalization and back propagation for classification. *Int. J. Comput. Theory Eng.* **3**(1), 1793–8201 (2011)
13. Sathy, R., Abraham, A.: Comparison of supervised and unsupervised learning algorithms for pattern classification. *Int. J. Adv. Res. Artif. Intell.* **2**(2), 34–38 (2013)
14. Jaba Sheela, L., Shanthi, V.: An approach for discretization and feature selection of continuous-valued attributes in medical images for classification learning. *Int. J. Comput. Electric. Eng.* **1**(2), 1793–8163 (2009)
15. Suneeta, N., Hari, M.K., Kumar, S.: Modified gini index classification: a case study of heart disease dataset. *Int. J. Comput. Sci. Eng.* **02**(06), 1959–1965 (2010)
16. El Ferchichi, S., Zidi, S., Lille, L., Laabidi, K.: A new unsupervised clustering-based feature extraction method. *Int. J. Comput. Appl.* **57**(6), 43–49 (2012)
17. Kwak, N., Choi, S., Choi, C.H.: Feature extraction for regression problems and an example application for pose estimation of a face. *Int. J. Comput. Theory Eng.* **3**(1), 1793–8201 (2011)
18. Jasmina, N., Perica, S., Dusan, B.: Toward optimal feature selection using ranking methods and classification algorithms. *Yugoslav J. Oper. Res.* **21**(1), 119–135 (2011)
19. Chakraborty, G., Chakraborty, B.: A novel normalization technique for unsupervised learning in ANN. *IEEE Trans. Neural Netw.* **11**(1), 253–257 (2000)



A Survey on Quality of Service Metrics Using Cross Layer Optimization Technique

Amutha R¹⁽ , Sivasankari H², and Venugopal K R³

¹ VTU, AMC Engineering College, Bangalore, India
amutha.shruthi@gmail.com

² Department of CSE, AMC Engineering College, Bangalore, India
shivashankarigg@gmail.com

³ Bangalore University, Bangalore, India
venugopalkr@gmail.com

Abstract. Wireless Sensor Network (WSN) is group of sensor nodes connected in a network to monitor the physical situations and collect the information to communicate to sink node. The low-cost feature of WSN is a significant advantage over the conventional networks. The successful implementation of WSN requires to adapt a strict QoS metrics. Each application demands a specific QoS such as throughput, latency, reliability bandwidth etc. The cross-layer algorithm optimizes the overall performance. The efficient design of routing algorithm and cross layer optimization technique improves the performance of WSNs. This paper depicts the comparison of various optimization techniques on WSNs with their strengths and limitations. The cross-layer optimization techniques of previously proposed methods highlighting its merits and demerits to develop optimized cross layer technique.

Keywords: Cross layer · Energy consumption · Latency · QoS · Reliability · Scalability · Throughput · WSN

1 Introduction

The wireless sensor network consists of low power, tiny sensors which consume low energy and computation at low cost that notice the area of sense and communicate data by multi hop so as to meet the requirement of applications that may be precise or more complicated. In wireless networks of same kind all devices has equal transmission radius. The communication link between two nodes will exist only if the distance from each other lies within the transmission radius or by mediator devices through relaying.

The technological advancement of WSN reformed the sensor nodes with multi-functional and as small as possible. For any decision making, finding out location of the sensor nodes is very important. A GPS may be used but consumption of more power and high cost of components makes it impossible to install GPS on every sensor. Many Localization algorithms used for optimizing the location tracing problems.

In multi hop wireless network different sensors have different requirements on workload and energy sources. Since the performance of network depends on energy management at the different network layers some attempts on cross-layer optimization of energy is applied to design an adaptive transmission mechanism for wireless sensor networks with re-charging capability of system to maximize the utility and stability of the system.

Cross layer communication encourages interaction of layers with other layers in the transmission protocol. Conventionally the network layers are segmented into independent layers. The communication among each layer is done through an interface. The benefit of layered approach is flexibility in architecture. In wireless communication the variable nature of links makes use of cross layer scheme. The poor resource availability of the wireless devices motivated several researches that are made to enhance the transmission performance by utilizing cross layer design in wireless systems. More attention is given to cross layer approach because of service quality, consumption of energy, wireless coupling versatility, packet loss and delay problems.

Figure 1 shows the cross-layer architecture for WSNs.

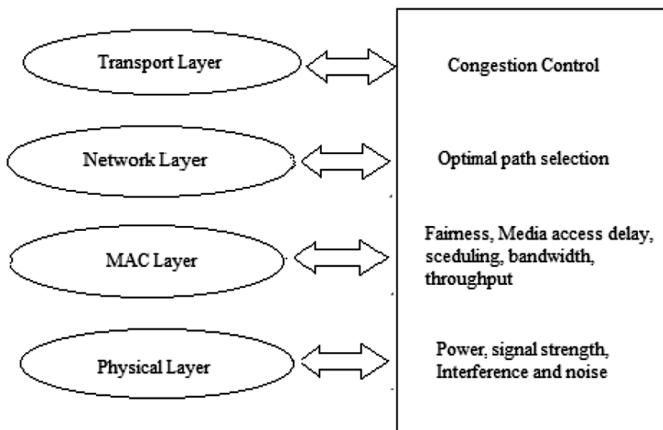


Fig. 1. Cross layer architecture

The cross-layer approach enables the communication between different nonadjacent layers as well. The cross-layer approaches help to minimize the consumption of energy of wireless sensor networks. When the networks function with the parameters acquired by combined design and optimization mechanism, the consumption of energy is reduced. However, it is not easy to obtain the network information such as network topology and sensor's residual energy for the design of cross layer in wireless networks. To design and optimize the cross layer the transmission of signal between the sensor and the receiver consumes some energy and bandwidth.

2 Related Works

Lahane *et al.* [1] proposed cross layer design mechanism to optimize routing in WSN. The interaction between different layers improves the performance of WSN by selecting the best path. Choosing the optimal route is a much challenging task in the wireless sensor network. The optimized design network function produces the energy consumption. However, it is hard to obtain network topology and residual energy in sensor nodes for cross-layer communication.

The improvement in efficiency and performance enhancement of WSN by utilizing different parameters of multilayer promotes the requisite to implement cross layer protocol for wireless sensor networks.

Zhang *et al.* [2] introduced an Intermittent Energy Aware (IEA) Energy Harvesting in Wireless Sensor Network platform. This method uses double stage capacitor for node synchronization without energy consumption. An Integrator is used for measuring very low power. The complete design of the IEA platform and the energy management mechanism is discussed. The node synchronization in different energy environments at different time and measurement of the energy in real time is achieved. The IEA platform consumes low power with high accuracy for energy measurement and prediction.

An optimized energy management scheme for intermittent function is realized in both prototype model and in simulation software. Experiments are done to validate the performance of IEA such as validity and reliability in real environment.

Yang *et al.* [3] proposed energy efficient cross layer model to mitigate the problem of high energy consumption of sensors and passive devices in multimedia wireless sensor network. This cross-layer approach has three layers which uses the location information of nodes in network layer, full duplex interface in physical layer and medium access control protocol in MAC layer. When compared to existing models, Cross-layer Energy Efficiency (CEE) models has advantages of low delay and high-power control, improvement in throughput with high energy efficiency. Hence the proposed model reduces consumption of energy and improves performance of transmission.

In future this transmission model is utilized as Internet of Things (IOT) in real time multimedia WSNs.

Ezdiiani *et al.* [4] developed a conceptual architecture based on adaptive QoS. This architectural system provides communication between a physical server network and virtual remote environments. An adaptive QoS algorithm is implemented to enhance the performance of QoS by identifying the adjustments required for physical server network. The virtualization concept is illustrated as the performance of network by showing the similarity between the simulation model and the physical server network experiment. The interoperability between pairing system encourages the proposed system to be utilized as a model for experiments that involves custom adaptive QoS parameters and performance analysis of real time network. The simulation function between network simulator and MATLAB is working successful and hence future researches were possible when complexity exist at the business intelligence level.

The performance of the adaptive QoS is compared with other work in this paper. The repetition of adjustment calculation is overcome by the approach for the adaptive

QoS, thereby system latency is reduced. Producing incremental outcome from the standard organization and a complete automated system is achieved.

Singh *et al.* [5] presented a Low Delay Cross Layer Algorithm (LDCMAC) to drive events in wireless sensor networks. This protocol allocates data reception segment for all node in its scheduling window to send data transfer request (FSP) or retrieve FSP based on next hop of receiver node. It allows a node to process its data segment for deploying the unused portion of data reception segment of the neighborhood hop when a node failed to setup data packet transfer flow in the scheduling window. These characteristics extend the number of nodes that move ahead their data segment at the same cycle when multiple nodes in queue to forward data segment that lies in the communication range.

From the result observed that both end to end delay and packets reliability were found to be improved with increase in the average energy consumption than existing cross layer approach.

Sun *et al.* [6] developed a routing algorithm on the basis of ant colony algorithm to know the optimal transmission route for data in WSNs. To update route information this algorithm combines the local and global phenomenon by introducing the penalty function and dynamic weight factor. This algorithm also considers the transmission path of different nodes and residual energy of individual nodes. A new route updating rule is established by enhancing the heuristic function and gave importance to transmission length in node communication, direction of transmission, energy and distance of the receiver node. This rule produces a relatively more average residual energy and a least minimal residual energy.

By comparing Ant and OARA with EEABR, the proposed algorithm minimizes the consumption of energy and increases the life time of the network.

Han *et al.* [7] developed a green routing scheme for multimedia applications. The protocols are compared by their energy efficiency, multi-path capability, path latency, reliability, location awareness, a whole bypassing and data delivery model. It was practically impossible to conclude the best routing protocol because each protocol has its own merits and demerits. The WMSNs field was rapidly developing and there are still many research challenges that need to be solved.

Future work is to investigate the available solutions and try to propose new approaches to solve these challenges.

Shahzad *et al.* [8] presented an improved pioneer distance vector algorithm to calculate estimation of localization to improve the accuracy and efficiency. The proposed protocol gives importance on improving the accuracy of localization with no efficiency consideration in communication. He formulated the objective optimization functions for localizing the problems. Improved localization accuracy is achieved in anisotropic and isotropic wireless networks with efficient performance of much fast convergence with minimum communication and energy overheads.

It was planned to analyze the effect of complex distribution of anchor and signal fading during process of localization.

Dobslaw *et al.* [9] introduced an integrated cross-layer framework for identifying the network configurations that satisfy the process requirements such as the data rates, delay, service differentiation and reliability of specific application. The configuration of network consists of routing decision and scheduling. It is not possible to identify a

perfect configuration due to the environmental conditions for many topologies. Therefore, converging algorithm is introduced to build a gateway background on framework top which configures a topology by positioning of sink that ensures the specific constraints of all application. The results showed that a backbone with multiple end terminals is needed for the required topology to maintain a high reliability with the minimum delay combination for all stages in a network for all specific application. The analysis tools and optimization schemes are developed to help the humans to find valid network configurations.

The shortcoming of this framework is modeled for periodic traffic and not suitable for variable data flow and time.

Boubiche *et al.* [10] proposed a watermarking based security mechanism to provide the integrity of data aggregation in heterogeneous WSNs. This scheme depends on dynamic embedded cross layer strategy and providing authentic data integration and security are critical in data aggregation. The traditional encryption and decryption techniques produces high computation overload and hence not suitable for secure aggregation but the watermarking protocol without overload establishes communication. This watermarking scheme decreases the end to end latency established by the conventional algorithm as well.

Xu *et al.* [11] proposed a model for WSN by considering multiple energy consumptions, transmission, reception and energy supplied from renewable energy, multi-dimensional stochastic nature. The optimization problem of discrete stochastic cross layer is developed to obtain the maximum tradeoff between the time average utility rate and electric cost.

By using the shortest path algorithm and modifying the disciplines of queuing, the end to end delay is reduced.

Lin *et al.* [12] present a cross-layer mechanism to reduce the consumption of energy and to obtain reliability by integrating a multipath routing and a data interleaving. The selection of transmission path of sensor is a rucksack problem and the work is formulated to solve it by greedy algorithm. With multipath routing technique in the proposed algorithm, the sensors were enabled to choose the multiple transmission paths. The paths created by this method have different edges for each node to reduce the energy consumption and network lifetime also prolonged. The data interleaving technique is utilized for reliable data transmission based on multiple transmission paths by employing Reed Solomon code.

From the simulation result it is revealed that the performance of proposed scheme such as network lifetime, energy consumption and reliable communication is improved than the conventional multipath routing technique.

Demigha *et al.* [13] proposed binary integer linear programming model to collect correlates data in WSNs with low energy consumption and high precision. This model helps in data processing of each round such as sensing, relaying and processing. This model useful for the successful correlated data collection based in dynamic clustering on environment.

Yetgin *et al.* [14] improved the lifetime of network by formulating the modeling effect of the physical layer and processing power of signal on the network layer. The network lifetime enhancement problem is framed with the help of a lower bounded signal to noise ratio value fall links to characterize QoS to depend on bit error ratio

(BER) by considering the effect of the physical layer parameters. Coding affects the energy consumption of modulation scheme and the transfer range of the communication system. Increasing the level of signal to noise ratio to the acceptable level in physical layer which reduces energy consumption in WSNs.

Fu *et al.* [15] developed a cross layer approach to eliminate the imbalance of data encapsulation between layers in transmission control protocol. Even though encapsulation improves network standard, still it compromises delay and other QoS parameters etc. In cross layer approach information is shared between the five layers to increase the functionality of network, reliability and QoS with scalability. Cross layer is classified as manager and non-manager method based on the data and information shared between the layers. On the other hand, cross layer is organized as centralized and decentralized structure based on the network organization.

The drawbacks in the cross-layer approach are coexistence, signaling, lack of a common cross layer and the elimination of the layered architecture.

Cheng *et al.* [16] proposed the design of cross layer approaches to minimize the transmission delay in multi hop wireless networks. An optimization models had been established to consider the effect of wireless interference. A linear programming model is created to reduce interference in routing with a necessary condition such that no two links can use the same slot if they interfere with each other. A conflict free transmission is established using this condition as a constraint. The condition is utilized in a global optimization and also used for dynamic scheduling locally where the condition required being satisfied within the two hop neighborhood of a link.

In future, it is utilized in wireless networks for reservation of resource and admission control.

Wang *et al.* [17] analyzed the stochastic queuing probabilistic model of cross layer scheme to study the end to end latency of wireless sensor network. The proposed approach is generic and described the various routing protocols parameters. CSMA protocol is used to analyze the developed model and predicts the end to end latency. A Markov process-based problem formulation is utilized to develop the communication model of a network. The proposed model is validated for various network configurations.

From the result it is observed that the accurate model of the cross-layer distribution for end to end latency is developed. Proposed work is utilized to develop the QoS based scheduling and communication solutions for WSNs.

Ehsan *et al.* [18] presented elaborately the research challenges and the energy efficient routing techniques of WMSNs. The QoS requirements are varying for different multimedia applications. The basic QoS requirements are latency or delay, bandwidth, jitter and reliability. This work highlights each routing protocol and algorithm with the benefits and performance issues. An open issue is provided in the unexplored areas to enhance more interests on research. WMSNs may become a powerful technology by the increasing advancement of technology in hardware.

Babulal *et al.* [19] proposed cross layer approach to estimate optimal path based on link distance reliability cost. Link distance, reliability and cost analysis are used to minimize latency, enhance throughput and minimize energy consumption. Link distance is varied with respect to the network load.

The proposed approach monitors the node even located at far distance by considering capacity of battery and reliability. LRC takes the decision depends on the battery capacity and reliability factor.

Figure 2 describes the graph between data delivery ratio with sensor nodes with different location. Table 1 shows the relationship between energy, reliability and its value:

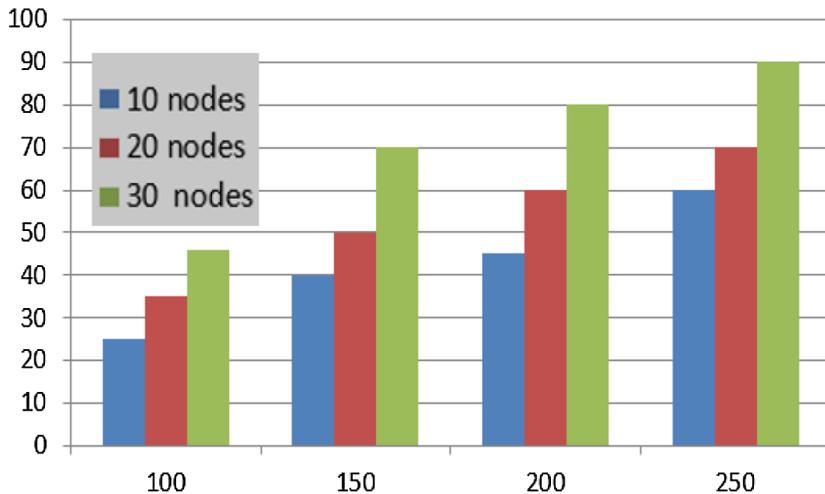


Fig. 2. Data delivery ratio with different locations

Table 1. Relation between energy, reliability and its value

Residual energy in %	Reliability (R)	Reliability value
80 to 100	More	1
79 to 50	Medium	.6
49 to 30	Less	.2
<30	Very less	0

Liu *et al.* [20] proposed a reliability-based transmission service in WSNs. A proliferation routing scheme is implemented to execute the end to end recovery scheme. Proliferation routing consist of three independent parts each concentrating at one specific problem. A more flexible and more freedom end to end transmission quality are granted by proliferation routing by carefully designing system parameters.

Di Francesco *et al.* [21] proposed an adaptive cross layer mechanism to improve reliability and reduce energy in wireless sensor network. The proposed scheme has an adaptation module setup the MAC layer automatically based on network configuration and traffic constraints to reduce the power consumption and meet the reliability and energy aware requirements of application. A low complexity distributed ADaptive

Access Parameters Tuning (ADAPT) algorithm is proposed to achieve reliability for specific application under different operating conditions for both single hop and multi hop networks. Figure 3 shows the setup of cross layer adaptation.

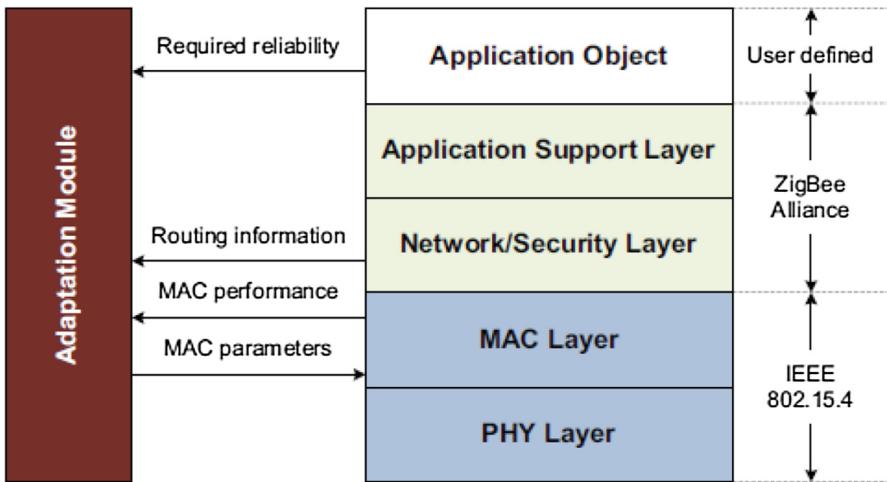


Fig. 3. Cross layer adaption setup

Simulation output showed that ADAPT algorithm performs well and the reliability specified by the application is guaranteed with efficient reduction in energy consumption.

Jing *et al.* [22] presented a coverage algorithm for multimedia WSN by altering the position of sensors and reducing the overlap of coverage area of active sensors on the basis of virtual centripetal force. The lifetime of networks is increased by turning off maximum sensors which are not in use based on the grid theory and waking up the sensors depending on correlation degree. This algorithm uses the visual approach to improve the coverage area to control the rotating of sensors after the random deployment and turned off sensors to increase the network lifespan. The proposed scheme has high coverage ratio and extension of it takes minimum processing time since the overlap area among sensors was decreased by decreasing the sensors mass. The equiangular rotation is changed as centripetal motion under virtual centripetal force, the reciprocating oscillation was eliminated. The future work focused on building model of sense to all practical applications of wireless networks.

Cho *et al.* [23] discussed a robust regression estimator using computational aspects for the measurement of wireless ad-hoc sensor network. It uses decomposition procedure to calculate the minimum bound of measurement redundancy and model of sub calibration reduces the computation in solving the LTS estimation. This method gives much accurate distance that estimate the variables connected with sensor nodes.

The current version is not fast enough in practical even though this algorithm improves the computation aspects for robust calibration.

Yi et al. [24] introduced an analytic tool called minimum scan statistics for wireless sensor network. Three asymptotic of minimum scan statistics are derived to boundary conditions. The results are applied to the ad-hoc and wireless sensor networks. Analyses are directed on some points of transmission radii in previous works. On contrast, this paper expels full line evolution of neighbor network topology, instead of applying toroidal metrics to eliminate effects of boundary.

In future more works are needed even minimum scan statistics gave a maximum view of network topology evolution.

Wang et al. [25] designed a cross layer scheme for reducing the consumption of energy and extending the lifetime of network of a wireless sensor network with multi source and single sink terminal. An optimization problem is formulated by integer convex problem with TDMA in MAC layer and by maintaining the integer on time slots. Routing, link access and data rate, the network topologies such as linear and planar are considered for increasing the network lifetime. When all nodes are completely used up simultaneously Karush Kuhn Tucker optimality condition is used to derive the optimal network lifetime expression theoretically.

Liu et al. [26] presented a scheduling algorithm at the MAC layer for multiple connections with diverse QoS requirements. A priority is assigned to all the link based on the channel quality and qos parameters. Priority for the link is dynamically updated, links which is having highest priority is scheduled first. Thus, the proposed scheduling algorithm provides ideal time delay based on traffic.

The bandwidth is efficiently utilized by having diverse connection for multiple users with various services. Further the scheduling algorithm provides malleability, scalability and low complexity during implementation.

Kozat et al. [27] developed a cross layer mechanism to satisfy the requirements of QoS for various applications. This paper addresses power consumption issue in wireless communication with scheduled access channel and solved to ensure end to end reliability at low bit error rate. Heuristic algorithms with top down and bottom up strategy based on graph theory is proposed to solve the scheduling issue and to minimize transmission power of communication channel.

The Table 2 depicts the cross-layer approaches used in literature survey and describes the performance of the previous works in terms of QoS measures with its advantages and disadvantages.

Figure 4 shows the energy consumption at various nodes for different protocols and Fig. 5 shows delay produced by different protocols at different nodes. Figure 6 shows the throughput for different protocols at several nodes and Fig. 7 shows the delivery ratio for various protocols at different nodes.

Table 2. Performance of Previous Works in terms of Qos Metrics

Author	Protocol	Energy efficiency	Bounded latency	Throughput	Reliability	Scalability	Network lifetime	Advantages	Disadvantages
Lahane [1]	Cross layer protocol	✓		✓			✓	Efficiency and performance improved	More overhead
Zhang [2]	Intermittent energy aware energy harvesting (IEAEH-WSN)	✓		✓	✓			Low power consumption and high accuracy	Network efficiency reduced
Yang [3]	Cross-layer energy efficiency (CEE) model	✓	✓		✓			Energy consumption reduced with improvement in transmission parameters	Less effective for less number of nodes
Ezdiari [4]	Virtualization	✓		✓		✓		A flexible system that react to dynamic changes	Challenges in learning and reconfiguration latency was not addressed
Singh [5]	Cross layer contention-based SYNCHRONOUSMAC protocol	✓	✓	✓				End to end delay reduced	DRS is not assigned to source node
Sun [6]	Ant colony optimization algorithm	✓			✓	✓		Prolonged network lifetime with reduced energy consumption	Energy balance of the network is not considered
Han [7]	Green routing protocol	✓		✓				Trade-off between network lifetime and	Ultimate solution not yet met to conclude and

(continued)

Table 2. (continued)

Author	Protocol	Energy efficiency	Bounded latency	Throughput	Reliability	Scalability	Network lifetime	Advantages	Disadvantages
Shahzad [8]	DV-Max Hop algorithm	✓	✓	✓				qos requirements is balanced	select the best protocol in WMSN
Dobslaw [9]	Converging algorithm	✓	✓					Accurate and efficient	Performance decay with increased network density
Boubiche [10]	Watermarking based data aggregation	✓			✓			Multi-channel utilization and aggregation	Assessment of each packet and ordering into the queue takes time
Xu [11]	Lyapunov drift perturbation technique	✓	✓	✓	✓			Energy efficient with less delay	Does not provide all the security properties
Lin [12]	Multipath routing protocol	✓						Optimal trade-off between the time-average rate utility and electricity cost is achieved	Multiple energy consumption hybrid energy supply
Denigha [13]	Binary linear programming model	✓	✓	✓				✓	Maximizes Network lifetime and reliability
									Overall energy efficiency low
									Data quality not improved
									transmitting, receiving

(continued)

Table 2. (continued)

Author	Protocol	Energy efficiency	Bounded latency	Throughput	Reliability	Scalability	Network lifetime	Advantages and processing operations.	Disadvantages
Yetgin [14]	UncodedBPSK modulated system	✓	✓			✓		Trade-offs between the NL and bit error ratio (BER) improved	Energy consumption high
Fu [15]	Cross layer			✓	✓	✓		Provide data encapsulation to standardize network communication	Too many connection termination
Cheng [16]	Linear programming model			✓	✓			Achieve minimum delay	Less efficient
Wang [17]	Stochastic queuing model			✓	✓			End to end delay reduced	Channel errors have not been captured
Ehsan [18]	Leach			✓	✓			Energy-efficient routing techniques	End-to-end QoS not guaranteed
Babulal [19]	Lrc			✓	✓	✓		Decreases the chance of loss of data	At low load, end-to-end delay is lower than high load
Liu [20]	Proliferation routing			✓	✓			Increases the end to end transmission success	Networks Consumes more energy

(continued)

Table 2. (continued)

Author	Protocol	Energy efficiency	Bounded latency	Throughput	Reliability	Scalability	Network lifetime	Advantages	Disadvantages
Di Francesco [21]	Adaptive access parameters tuning algorithm	✓		✓		✓		Energy-efficient, with near optimal performance	Increasing the threshold results in a higher energy consumption per node
Jing [22]	Vcfcea	✓		✓		✓		Network coverage and lifetime enhanced	Coverage ratio decreased
Cho [23]	LTS estimator	✓		✓		✓		Robustness in estimation	Low fault tolerance capability observed
Yi [24]	Minimum scan statistics	✓		✓		✓		A unified approach to solve various network problems	Complex mathematical analyses involved
Wang [25]	Decomposition & Composition	✓	✓	✓				Minimize energy and maximize NL of MSSS WSN	problem for planar MSSS topology was more complicated
Liu [26]	Adaptive modulation and coding scheme	✓		✓	✓			Provides flexibility, scalability and low implementation complexity	estimation error and feedback latency occurred
Kozat [27]	Heuristic algorithm	✓	✓	✓		✓		Energy consumption reduced	Performance limited with BER and bandwidth

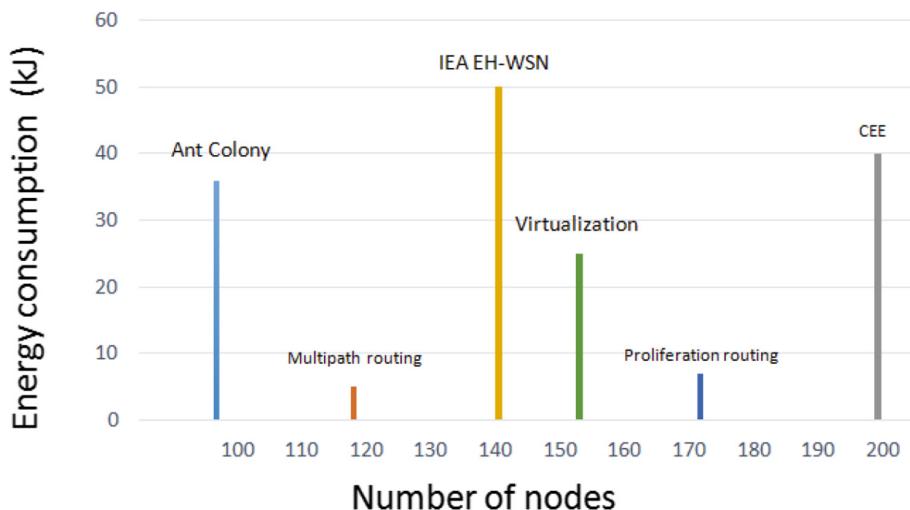


Fig. 4. Energy consumption at various nodes for different protocols

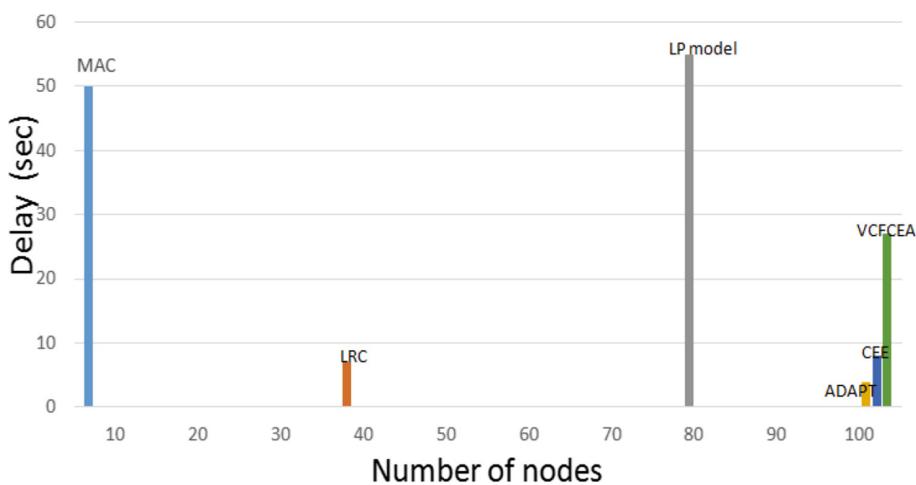


Fig. 5. Comparison graph on delay vs sensor nodes for different protocols

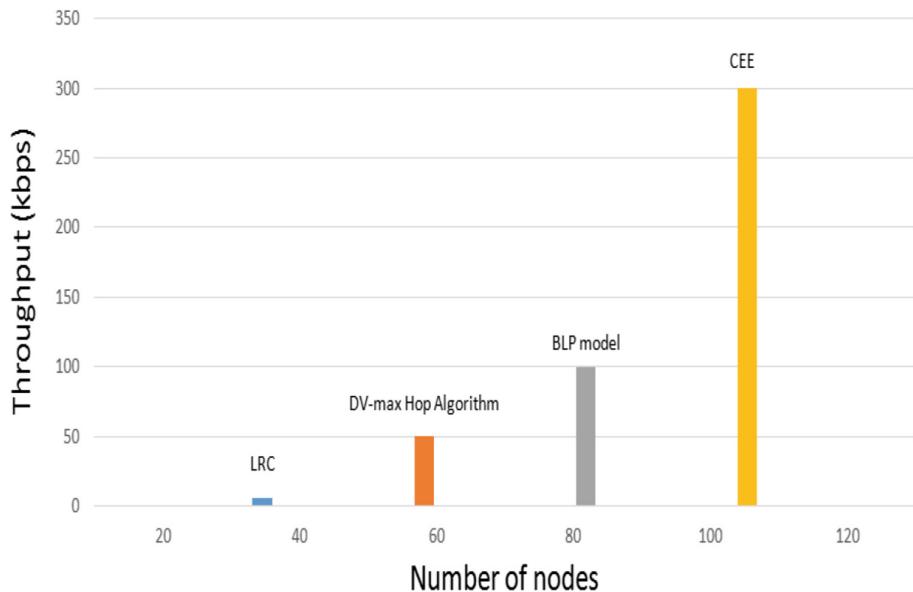


Fig. 6. Throughput for different protocols at several nodes

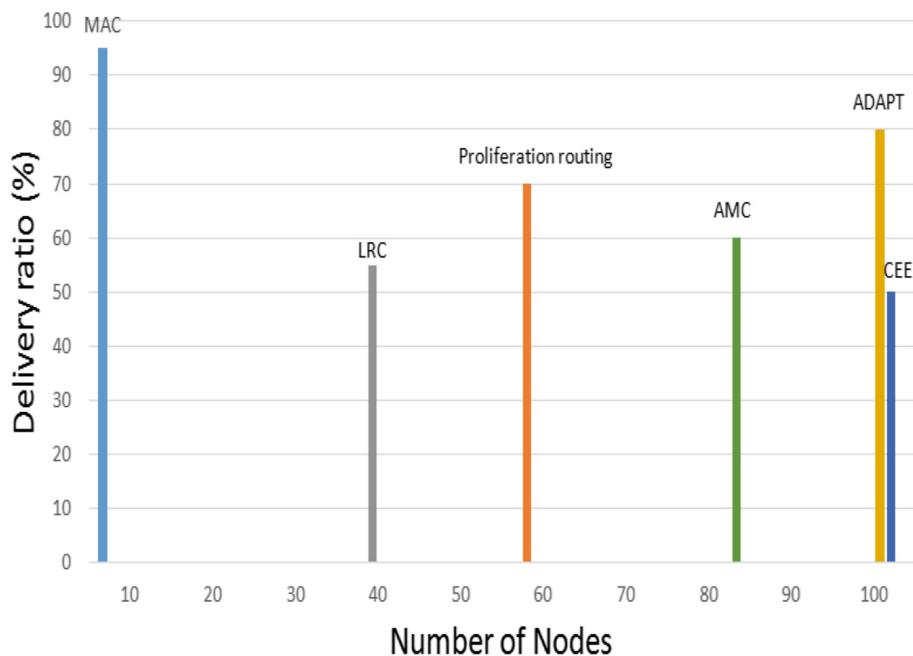


Fig. 7. Delivery ratio for various protocols at different nodes

3 Conclusion

This paper describes the various cross layer optimization techniques to address the major issue of energy conservation and lifetime in WSNs. Reliability and delay are the most important parameters of QoS. WSN meets the requirement of QoS parameter and hence suitable for condemnatory applications.

Researchers are giving more attention on these issues specifically in wireless sensor network because of the wide range of applications. Further in this literature the design of cross layer scheme in WSN is illustrated in detail with the challenges in implementation. There are numerous surveys available to address the general issues on QoS schemes in wireless sensor network and reliable data delivery based applications, end to end delivery with reduced energy consumption and encrypted security for reliable communication in WSN. The design of cross layer mechanism is an important process to overcome the constraints of QoS parameters and to develop concept to mention the requirements of QoS in a suitable manner.

A survey of the work discussed the comprehensive reviews on research challenges and portraits the demand required for designing the cross-layer optimization for reliable communication.

Acknowledgement. This research was partially supported by AMC Engineering College, Bangalore. I thank my guide and colleagues from AMC Engineering College who provided insight and expertise that greatly assisted the research, although they may not agree with all the interpretations of this paper.

References

1. Lahane, S.R., Jariwala, K.N.: Cross layer design approach for routing optimization in wireless sensor network. *Int. J. Adv. Comput. Eng. Netw.* **6**(3), 41–48 (2018)
2. Zhang, Y., Gao, H., Cheng, S., Li, J.: An efficient EH-WSN energy management mechanism. *TUP J. Mag.* **23**(4), 406–418 (2018)
3. Yang, X., Wang, L., Xie, J.: Energy efficient cross-layer transmission model for mobile wireless sensor networks. *Hindawi Mob. Inf. Syst.* **1346416** (2017)
4. Ezdiani, S., Acharyya, I.S., Sivakumar, S., Al-Anbuky, A.: Wireless sensor network softwarization: towards WSN adaptive QoS. *IEEE Internet Things J.* **4**(5), 1517–1527 (2017)
5. Singh, R., Rai, B.K., Bose, S.K.: A low delay cross-layer MAC protocol for k-covered event driven wireless sensor networks. *IEEE Sens. Lett.* **1**(6), 1–4 (2017)
6. Sun, Y., Dong, W., Chen, Y.: An improved routing algorithm based on ant colony optimization in wireless sensor networks. *IEEE Commun. Lett.* **21**(6), 1317–1320 (2017)
7. Han, G., Jiang, J., Guizani, M., Rodrigues, J.J.C.: Green routing protocols for wireless multimedia sensor networks. *IEEE Wirel. Commun.* **23**(6), 140–146 (2016)
8. Shahzad, F., Sheltami, T.R., Shakshuki, E.M.: Multi-objective optimization for a reliable localization scheme in wireless sensor networks. *J. Commun. Netw.* **18**(5), 796–805 (2016)
9. Dobslaw, F., Zhang, T., Gidlund, M.: QoS-aware cross-layer configuration for industrial wireless sensor networks. *IEEE Trans. Ind. Inf.* **12**(5), 1679–1691 (2016)

10. Boubiche, D.E., Boubiche, S., Bilami, A.: A cross-layer watermarking-based mechanism for data aggregation integrity in heterogeneous WSNs. *IEEE Commun. Lett.* **19**(5), 823–826 (2015)
11. Xu, W., Zhang, Y., Shi, Q., Wang, X.: Energy management and cross layer optimization for wireless sensor network powered by heterogeneous energy sources. *IEEE Trans. Wirel. Commun.* **14**(5), 2814–2826 (2015)
12. Lin, K.Y., Wang, P.C., Hong, T.P.: A greedy algorithm in wsns for maximum network lifetime and communication reliability. In: 2015 IEEE 12th International Conference on Networking, Sensing and Control, pp. 87–92. IEEE (2015)
13. Demigha, O., Hidouci, W.-K., Ahmed, T.: A novel BILP model for energy optimization under data precision constraints in wireless sensor networks. *IEEE Commun. Lett.* **18**(12), 2185–2188 (2014)
14. Yetgin, H., Cheung, K.T.K., El-Hajjar, M., Hanzo, L.: Cross-layer network lifetime optimisation considering transmit and signal processing power in wireless sensor networks. *IET Wirel. Sens. Syst.* **4**(4), 176–182 (2014)
15. Fu, B., Xiao, Y., Deng, H.J., Zeng, H.: A survey of cross-layer designs in wireless networks. *IEEE Commun. Surv. Tutorials* **16**(1), 110–126 (2013)
16. Cheng, M., Ye, Q., Cai, L.: Cross-layer schemes for reducing delay in multihop wireless networks. *IEEE Trans. Wireless Commun.* **12**(2), 928–937 (2013)
17. Wang, Y., Vuranand, M.C., Goddard, S.: Cross-layer analysis of the end-to-end delay distribution in wireless sensor networks. *IEEE/ACM Trans. Networking* **20**(1), 305–318 (2012)
18. Ehsan, S., Hamdaoui, B.: A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. *IEEE Commun. Surv. Tutorials* **14**(2), 265–278 (2011)
19. Babulal, K.S., Tewari, R.R.: Cross layer design with link and reliability analysis for wireless sensor network. In: 2011 Nirma University International Conference on Engineering, pp. 1–5. IEEE (2011)
20. Liu, Y., Zhu, Y., Ni, L., Xue, G.: A reliability-oriented transmission service in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **22**(12), 2100–2107 (2011)
21. Di Francesco, M., Anastasi, G., Conti, M., Das, S.K., Neri, V.: Reliability and energy-efficiency in IEEE 802.15. 4/ZigBee sensor networks: an adaptive and cross-layer approach. *IEEE J. Sel. Areas Commun.* **29**(8), 1508–1524 (2011)
22. Jing, Z., Jian-Chao, Z.: A virtual centripetal force-based coverage enhancing algorithm for wireless multimedia sensor networks. *IEEE Sens. J.* **10**(8), 1328–1334 (2010)
23. Cho, J.J., Ding, Y., Chen, Y., Tang, J.: Robust calibration for localization in clustered wireless sensor networks. *IEEE Trans. Autom. Sci. Eng.* **7**(1), 81–95 (2009)
24. Yi, C.-W.: A unified analytic framework based on minimum scan statistics for wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* **20**(9), 1233–1245 (2009)
25. Wang, H., Yang, Y., Ma, M., He, J., Wang, X.: network lifetime maximization with cross-layer design in wireless sensor networks. *IEEE Trans. Wirel. Commun.* **7**(10), 3759–3768 (2008)
26. Liu, Q., Wang, X., Giannakis, G.B.: A cross-layer scheduling algorithm with QoS support in wireless networks. *IEEE Trans. Veh. Technol.* **55**(3), 839–847 (2006)
27. Kozat, U.C., Koutsopoulos, I., Tassiulas, L.: Cross-layer design for power efficiency and QoS provisioning in multi-hop wireless networks. *IEEE Trans. Wirel. Commun.* **5**(11), 3306–3315 (2006)



A Hybrid Approach for Energy Efficient Routing in WSN: Using DA and GSO Algorithms

R. Vinodhini^(✉) and C. Gomathy

Electronics and Communication Engineering, SRM University,
Vadapalani Campus, Chennai, Tamil Nadu, India
vino0417@gmail.com, hod.ece@vdp.srmuniv.ac.in

Abstract. Wireless Sensor Network (WSN) plays a vital role in industrial application (IA) and is developing as a dynamic research area over previous years. The sensor nodes of WSN are energy constrained and hence the strategy of energy-efficient routing protocol remains as a significant concern to be tackled. The main issues addressed in WSNs are the network lifetime constraints and the time delay occurring in the transmission of data. Data routing remains to be a critical task in numerous decisive applications like military, ecosystem, survey disaster controlling etc. The shortest path is practiced by the Routing methods with minimal energy depletion pattern. The lifetime of WSNs can be enhanced through some of the Energy efficient clustering and routing algorithms. In this article, a new swarm intelligence optimization method named dragonfly algorithm (DA) is presented for cluster head selection in an energy efficient way. For efficient routing, the Glow-worm Swarm Optimization (GSO) algorithm is used. This method prolongs the lifetime of the network, alive nodes, throughput, total packet sent and similarly reduces the dead nodes, and the energy consumption of the network.

Keywords: Wireless sensor networks · Dragon fly algorithm · GSO routing algorithm · Network lifetime · Energy consumption

1 Introduction

Wireless Sensor Networks (WSNs) are denoted as a group of numerous small sensor nodes which are dispersed in a region of interest to freely sense and transmit the essential data to base station or sink [1]. In many outdoor environments such as war zones, deserts and in oceans sensors might be put into operation. It is impossible as well as costly regarding battery replacement or offering sources of additional energy. The network turns down due to weakening of nodes. Therefore, active use of the sensor energy is required for the intensification of network lifetime [2]. Currently, several researchers used the idea meant for clustering of Sensor Nodes (SNs) as well as efficient routing to preserve the energy of SNs and these procedures could considerably enhance the WSNs lifetime [3]. For transferring, processing and obtaining information the Sensor nodes normally use energy. The sensor nodes operated under non rechargeable conditions so they have to survive over some years. Hence, the major

objective of WSN is to maintain the energy efficiency besides improving the network life expectancy [4]. In WSNs, Clustering is a process that allows the SNs to form into several sets. Clustering coefficients in this method is applied on behalf of determining the matches or variations among the nodes. Sensor Networks uses greater comparisons, they are literal in proximity and have tendency to be clustered at once. SNs that suits to the identical cluster possibly cooperate to drive the collected data to the Base station (BS) as an alternative of sending data distinctly to BS in order to decrease energy consumed [5].

The Fuzzy C-Means clustering (FCM) assures the cluster formation in a randomly deployed sensor networks which are identical, moreover the FCM is a fuzzy type of K-Means which uses data elements to connect with the membership degrees. The clusters are viewed as groups including excess intensity of SNs; then the entire spatial distance among the CH as well as the SNs are considerably reduced. The clustering algorithms explores the marginal distances among SNs and Cluster Heads (CHs), therefore they require the extent of distance among CHs and BS, which impacts significantly on total energy [14]. WSN routing protocols should be application-based, which represents that constructing a routing algorithm for WSN must have the capability to fulfil the necessities of all applications, which is most difficult. Furthermore it exists as a prominence that constructing a normal algorithm for routing is some way could be applied to certain application for time being. Stabilizing the energy usage and Enhancing the network lifetime as much as possible is considered as vital. In addition a tough problem of focussing on the enhancement of routing protocols for WSNs. As an NP-hard problem the routing in WSNs is considered, moreover routing is done for prolonging the lifetime of the network, further researchers are in an attempt to build an empirical and meta-heuristic routing approach [6]. As a standard WSN clustering protocol, Low Energy Adaptive Clustering Hierarchy (LEACH) is believed as a leading dynamic clustering protocol which deals with WSNs requirements properly making use of randomly employed homogeneous static sensor nodes, also functioning as the base for further improved WSN clustering algorithms. It is a probabilistic hierarchically distributed single-hop algorithm aiming to (i) develop WSN lifetime through handling out power usage uniformly between all the nodes of the network then (ii) decrease the network nodes energy usage (using data aggregation and reducing message transmission) [8].

In WSN, the Particle swarm optimization (PSO) algorithm is considered as a popular optimization algorithm, which is used for routing, this routing protocol which is based on evolution that might be noted in [16]. Newly the harmony search algorithm (HSA) is a methodology for optimization and is employed as routing protocol which is based on clustering and also meant for energy efficient WSNs. For cluster head selection in WSN the Artificial bee colony (ABC) algorithm is used, then for routing Hybrid ABC algorithm is applied which furthermore prolongs the WSN lifetime [7].

Moreover, the coordination using the CH also permits the SNs to sleep for prolonged phase as well as supports to spare extra energy in every node. Thus, the network scalability and longevity is enhanced through clustering by minimizing both the traffic as well as the channel contention [15]. Standard algorithms for optimization are useless by the enlargement of the network size. For such NP-hard concerns, the PSO which is considered as an effectual algorithm and is also nature inspired, might be the best

choice owing to its simple performance, progressive solution and capability towards the diversion of local optima and rapid convergence [9, 10]. Manipulation of the sensors dynamics through Virtual Force based PSO (VFPSO) algorithm is created to improve the convergence rate.

The NP-hard problem has some solutions that probably depend on massive spaces of viable solutions and to a certain type of problems Swarm intelligence method have been successfully applied. As a further option, certain optimization approaches like Genetic Algorithm (GA) and Particle swarm optimization (PSO) possess various advantages that have a great processing requirement. Some of the benefits of PSO include effortless execution on hardware or software, upgraded explanations as a skill to get away from local optima and rapid convergence. The PSO is employed because of its value in explaining the NP problems and also to enhance the CH selection through numerous consolidated clustering protocols [11].

To face this condition, the unequal size clustering concept performs a crucial part, for balancing the energy consumption as well as the CH workloads. SNs scheduled in WSN besides clustering of networks are capable of prolonging the network life time through decreasing the usage of node's energy. When these two methods are combined, the important concerns to be considered are selecting a cluster size with more energy and assigning the CHs to active SNs [12, 13]. PSO in the search space faces restriction in high dimensional optimization and it is difficult to search the entire possible region, for such conditions Dragon fly algorithm (DA) is used. Since it has boundless search computational capability and it provides a new approach to produce particles that generates a new vector consequently in the assessment of every current vector.

In high dimensional problems the PSO approach formerly for exploration and exploitation problems and much time is consumed to attain a local maxima or minima. In order to prevent such problems in this paper a hybrid approach is proposed which uses the DA's high search efficiency combined with the Fuzzy C Means clustering for selecting a prominent Cluster head and with the dynamic nature of GSO, an effective routing is also conducted. This approach prolongs the lifetime of the network, number of alive nodes, throughput, total packet sent, decreases dead nodes moreover the networks energy consumption is minimized. This article is organized in a simple way as follows: Sect. 2 represents a review on literature, Sect. 3 illustrates the WSNs stimulation. Section 4 presents the problem description in addition to the contribution of the article. The proposed method of DA hybridized GSO approach is defined in Sect. 5. The results are presented in Sect. 6 with the comparative analysis and at last, Sect. 7 concludes the paper.

2 Literature Survey

Presently the RZ (rendezvous) Leach for the wireless sensor network is enhanced by including the ant colony optimization algorithm concept used for obtaining the optimized route for data transmission.

Obtaining this route supports the transmission gap to minimize the energy and helps in reducing the energy usage, this manner extends the network lifetime. Arora et al. [17] presented a theory for selecting a CH (cluster head) using one hop field

neural network and then the clusters are created by means of an optimized LEACH protocol. Hybrid ACO/PSO route optimization approach has been used after the cluster formation process to obtain the direct route for data transmission, which progresses into reducing the transmission distance thus increasing the lifetime of the network. With a faster convergence rate and also to achieve a global search, a hybridized HAS/PSO algorithm is presented for energy efficient CH selection.

Shankar et al. [18] presented an algorithm which shows renowned search additiveness of HAS, moreover the dynamic ability of PSO which increases the SNs lifetime.

In this paper, Su et al. [19] proposed the genetic algorithm (GA) in a hierarchical fusion in which the PSO is intended for disseminated clustering in comprehensive WSNs. The entire sensor nodes can be structured on the basis of two-level logic structures. In the H2GA-PSO algorithm, a fitness function is defined, as well as a linear decreasing function is intended for the particles inertia weight. In the process of GA, essential subdivisions stay conceived to verify that GA using essential subclass will attain global convergence. Hereafter with the H2 GA-PSO the clustering results are found which is optimal about maintaining and alleviating the energy consumption. The distributed clustering strategical solution could be attained; moreover, the algorithm convergence speed will be enhanced efficiently. Simulation results shown that the proposed approach, successfully minimizes the energy used, then it supports to amplify the network lifetime.

Arjunan et al. [20] stated a Fuzzy logic relied on Unequal Clustering then routing with the help of ACO, to reduce the hot spot concern as well as to enhance the network lifetime, a Hybrid (FUCARH) protocol for WSN was used. Contrasting with some of the current clustering protocols, the method meant to determine the CHs and the cluster size using five input parameters. In this method a threshold model is applied for data transmission along with periodic data transmission. New inter-cluster routing approaches have been presented for load distribution by sending the threshold data concerning the shortest paths as well as the periodic data in unused paths. Also, CHs are formed to utilize an identical volume of energy within the cluster maintenance phase and the results showed that the stated technique achieves maximum lifetime and reduces the hot spot concerns as well as the usage of energy between every nodes capably.

Barolli et al. [21] applied a hybrid simulation structure relied on PSO and distributed GA (DGA), named WMN-PSODGA. By means of WMN-PSODGA simulation approach, the performances of WMNs were evaluated considering common and equal client distributions. From the results, it was proved that the performance of the proposed approach is of high class and meant for Normal distribution related to the state of Uniform distribution.

Raja, Hemamalini et al. [22] stated that, when the nodes are densely deployed the application creates a high parcel stream close to the sink because of the convergent idea of the upstream traffic. Congestion in a WSN causes data loss; because of this the throughput might be brought down and latency gets raised, and furthermore the congestion prompts over the top energy utilization. Subsequently, congestion must be controlled to draw out the sensor node' lifetime, as far as the throughput and packet loss proportion, along with packet delay, and control overhead.

3 System Model

WSN is set up randomly in this research work in $M \times N$ network field having “N” sensor nodes. Along with the sink, all nodes are static in nature. Every node contains a unique ID. This node monitors the environment which is given and then the data is communicated through the sink. When the communication is completed, each time the particular node has to expend some energy based on the distance (D) with the sink. Every communication links remain symmetric in type.

3.1 Energy Model

This suggested model includes the radio model reviewed by Mann et al. [23] on behalf of the energy used in the data transmission by sensor nodes, has a free space model (fs), with respect to the distance which is less than a threshold value (d_0); or else, a multi-path (mp) pattern is employed. The Energy used by the sensor node radio to broadcast an l-bit data through a distance d is presented below:

$$E_{tran}(l, d) = \begin{cases} lE_{elec} + l \in_{fs} d^2 & \text{if } d < d_0, \\ lE_{elec} + l \in_{mp} d^4 & \text{if } d \geq d_0, \end{cases} \quad (1)$$

The energy used by the electronic devices and the amplifier is represented as E_{elec} , ϵ_{fs} as well as ϵ_{mp} . Similarly, for the generation of l-bit control messages, the energy spent is specified by

$$E_{cont}(l, d) = lE_{elec} \quad (2)$$

On many aspects the E_{elec} depends, such as for digital encoding, modulation, filtering then signals broadcasting.

3.2 Network Model

In this model a WSN of homogeneous nature has been considered [24], where the nodes remain evenly as well as randomly distributed all over the area. The nodes in the network are dispersed within a square area, in which “M” represents the length of the sides. It is expected that the entire nodes are able to interconnect with the BS with no sufficient energy and also capable of utilizing varied power stages for communications. A node along with the BS remains to be static besides, no mobility is sustained. While the BS is allowed to be positioned beyond the monitoring area, an analysis is made for the network in that the BS is almost positioned at the field’s centre. In one single-hop, every node is able to interconnect with their neighbours positioned in the cluster range of the nodes. It is expected that every phase all the nodes are synchronized just once at the initial stage of. With respect to the uncomplicatedness, the Wireless transmission channel could be probably secured and moreover it is estimated that the network’s operational time could be entirely split into several rounds. The clusters are formed at first, moreover in the remaining round the data’s are clustered, united then send to the BS. The cluster-head in this clustered network is supposed to be awake in each round

and the normal nodes (or else cluster members) excluding their time slots can go to sleep.

4 Problem Statement

In this work, the major objective is to propose an energy-efficient as well as a reliable routing approach for a WSN which functions in an unattended way also in an unfavourable environment. As of resource conscious sensor nodes which are (mostly limited energy as well as also on board storage facility) the routing protocol must use low power also must not interrupt the nodes with overhead storage.

5 Proposed Hybridised DA-GSO Methodology

For an effective clustering, the DA and the FCM are involved and for routing the GSO is applied. In the Hybridized DA-GSO technique, at first, the sensor nodes are positioned in a random manner then shifted for clustering and at last for routing.

DA has the facilities of dynamic optimization, which turns out to be a significant gain in dealing with the topology control issues in WSNs. The DA algorithm has been used to select the CHs before the communication and for clustering FCM is initialized. When the fitness function is designing, the norm is to minimize the networks overall energy usage, in view of the Euclidean distance based on the member nodes and their CHs with the utmost distance among the CHs and the base station. Figure 1, shows the block diagram for the Hybridized DA-GSO approach, in this the information about the SNs is obtaining at first. With the co-operation of DA with FCM, the clustering is done, also the CHs and other SNs are identified.

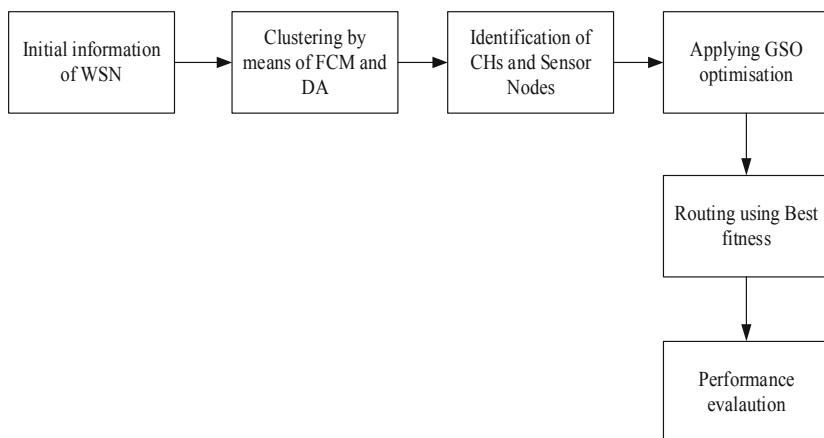


Fig. 1. Block diagram for Hybridised DA-GSO method

5.1 Clustering Based on Dragonfly Optimization and Particle Initialization Using FCM Algorithm

Dragonflies (Odonata) are a kind of flies. All over the sphere, there are approximately 3000 special kinds of this fly. Two main milestones are concerned in a dragonfly's lifespan includes and they are nymph and adult. The main division of their lifetime are spent in nymph and to grow into the adult they go through metamorphism. Dragonflies in static swarm [25] are developed into small groups then fly to and fro above a small range to see new preys in airborne such as butterflies and mosquitoes. The main features of a static swarm are the Confined movements also the sudden fluctuations in the flying path. The static and the dynamic swarming behaviours are the foremost motivation for the origin of the DA algorithm. Using meta-heuristics, the Swarming actions of both are similar to the two main levels of optimization and they are exploration and exploitation. Sub-swarms are formed by the Dragonflies and it in a static swarm fly above several ranges, in the exploration phase this feature is considered as an objective. However, in the static swarm, the dragonflies are the bigger swarm's laterally in one direction and this is an advantage in the exploitation phase. DA is an optimization algorithm which has random search, repeats the flight sequence of dragonfly swarm [26]. The swarming character of the dragonflies has two intentions, they are seeking and immigration. In hunting mode, they are formed into tiny groups, also to capture the prey they look everywhere again and again. They in migration mode form as big groups, and stimulate to travel in prolonged distance possessing a single destination place. In DA this unique swarming nature turns into the motivation of the exploration and exploitation methods. As search agents, the swarm has "N" dragonflies. A search agents location and step vector are represented as X and ΔX , with $1 \leq i \leq N$. The order of the search agent is specified with five distinct behaviours in the swarm, with the description below:

The step also the locations at iteration "l", of every search agent remain updated as mentioned below:

$$\begin{aligned} \Delta X_i(l+1) = & sSep_i(l) + aAllg_i(l) + cCoh_i(l) + fFdd_i(l) \\ & + eEnmi_i(l) + \omega\Delta X_i(l) \end{aligned} \quad (3)$$

$$X_i(l+1) = X_i(l) + \Delta X_i(l+1) \quad (4)$$

Where the inertia weight (" ω ") of the search agent Sepi, Allgi, Cohi, Fddi and Enmi remains the behaviour fitness values of the search agent "i" as well as the weights of the behaviours are ω , a, c, f and e.

In (4) the location of the search agents is updated, if "J", which is considered as the overall neighbouring search agent is at least one. If none of the neighbouring search agents are available, the location is updated using Levy flight through the equations mentioned below:

$$X_i(l+1) = X_i(l) + Levy(k) \quad (5)$$

$$Levy(l) = 0.01 \frac{r_1 \sigma}{|r_2|^{\beta}} \quad (6)$$

$$\sigma = \left(\frac{\Gamma(1 + \beta) \sin\left(\frac{\pi\beta}{2}\right)}{2\left(\frac{\beta-1}{2}\right)\beta\Gamma\left(\frac{1+\beta}{2}\right)} \right) \quad (7)$$

$$\Gamma(x) = (x - 1)! \quad (8)$$

In which the random numbers are denoted as “r1” and “r2” with respect to the normal distribution, and the constant number is ‘ β ’ (Table 1).

Table 1. Pseudo-codes of the DA algorithm

Set the population of the dragonflies X_i ($i = 1, 2, \dots, n$)
Set the step vectors ΔX_i ($i = 1, 2, \dots, n$)
While the end condition is not fulfilled
All dragonflies objectives are calculated
The enemy, as well as the food source, are updated
Update w, s, a, c, f , also e
Using Eqs. (1 to 5) compute S, A, C, F , and E
Update neighbouring radius
If only one neighbouring dragonfly is possessed by a dragonfly
Using Eq. (6) the velocity vector is updated
Using Eq. (7) position vector is updated
Else
Using Eq. (8) position vector is updated
End if
Considering the boundaries of variables verify also fix the new positions
End while

DA algorithm is improved based on the outline of the PSO algorithm, thus for the CH, the best particle is found. This could be gained by obtaining the optimized centroids distance by means of all the neighbourhood nodes.

Initialization of the Particle: In the first step, in Fig. 2 the particles are positioned randomly, then, the FCM algorithm is used to get the centroids which are designed for creating a cluster.

Using the DA algorithm, these centroids are optimised. FCM is the fuzzified translation of the k-means approach. In the analysis of features, classifier design as well as for clustering, the FCM Clustering Algorithm has been successfully used in WSNs. In this article, an initialization approach based on fuzzy clustering model is presented.

In fuzzy clustering [27], specifically, a division of ‘n’ set of objects ($Y = y_1, y_2, \dots, y_n$) into k fuzzy clusters C_1, C_2, \dots, C_k , using a matrix of $(n \times k)$ the state of clustering is expressed,

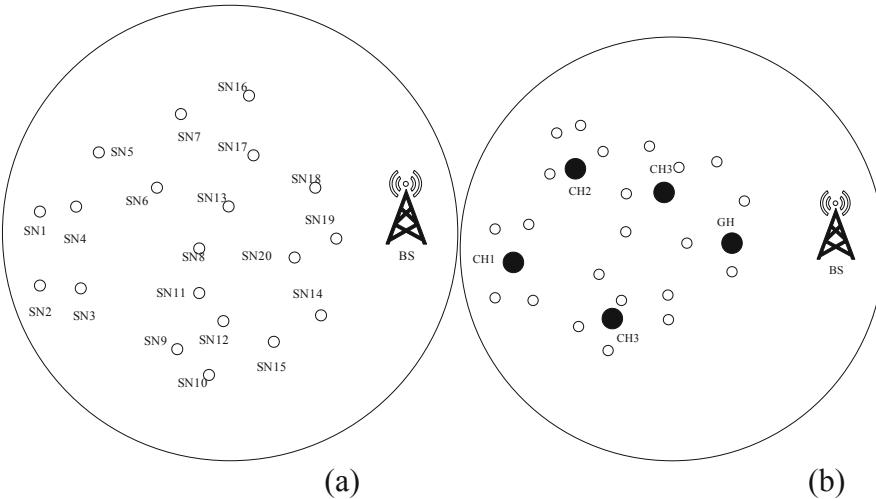


Fig. 2. (a) Random deployment of sensors. (b) Detection of cluster head and gate way head.

$M = [Z_{ij}]$ ($1 \leq i \leq n, 1 \leq j \leq k$). The i th object to the j th clusters degree of belongingness is signified as “ Z_{ij} ”.

The matrix $M = [Z_{ij}]$, should satisfy the subsequent terms [27].

- For every object y_i , as well as the cluster C_j , $0 \leq Z_{ij} \leq 1$
- For every object y_i , $\sum_{j=1}^k Z_{ij} = 1$
- For every cluster C_j , $0 < \sum_{i=1}^n Z_{ij} < 1$

‘ c_j ’ signifies the center of cluster C_j , $1 \leq j \leq k$.

The distance between object ‘ y_i ’ and the cluster center ‘ c_j ’ is stated by ‘ $\text{dist}(y_i, c_j)$ ’ and based on the object ‘ y_i ’ to cluster ‘ C_j ’ the degree of belongingness is signified.

In case for the object ‘ x_j ’, and the cluster center ‘ c_j ’, if the distance among them is short, the probability that x_i belongs to the equivalent cluster C_j is greater. So, $\frac{1}{\text{dist}(x_i, c_j)^2}$ is utilised to define the degree of belongingness of object ‘ y_i ’ to cluster ‘ C_j ’, at that moment, to acquire the description of the degree of belongingness ‘ Z_{ij} ’, normalizing is used and is represented in Eq. (13). Which in case satisfies the conditions of matrix $m = [Z_{ij}]$.

$$Z_{ij} = \frac{\frac{1}{\text{dist}(x_i, c_j)^2}}{\sum_{l=1}^k \frac{1}{\text{dist}(x_i, c_l)^2}} \quad (9)$$

Fuzzy clustering is also meant as soft clustering. In which an object is made to belong to numerous clusters.

The Glow-worms (GWs) in GSO algorithm [28], are randomly dispersed in the network, it has “luciferin” which is said as the luminance quantity. Once the value of luciferin is more than Neighbor GW, at this condition the GWs are attracted, this in

case makes the further GWs move as to it. A dynamic individual decision space is held by the GW. This space contains the GWs which are using mutual morals of distance in its radius of the dynamic decision as well as more luciferin than itself. To the dynamic decision space, the GW updates their location with respect to the possibility, it restarts the radius of the decision space.

The luciferin value is compared mutually with the luciferin value of the previous iteration and the present iterations objective function. Three phases are accessible in the GSO algorithm such as luciferin update phase, movement phase then the update phase of the neighborhood range. In an effective routing to obtain the fitness function, the stated three phases are employed. In each iteration, the routing is done for the reason, that the sensor nodes lose some energy. Instead of preventing the transmission failure, routing (shortest path) is done among CHs in all iterations. Routing amongst each CH in (Fig. 3a) is shown. In (Fig. 3b) the cluster nodes which bonds with CH are shown, likewise in (Fig. 3b) the data is transmitted to cluster 1 node with the support of CH1 through the path which is shortest one and it is obtained based on the GSO routing approach.

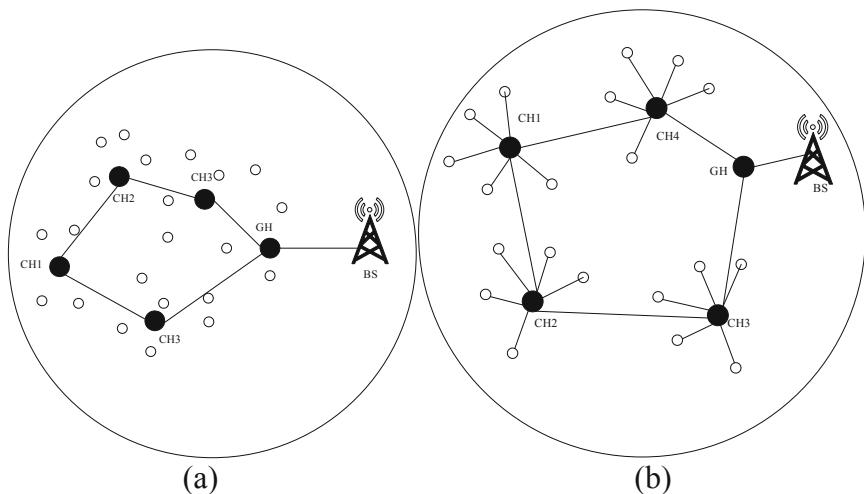


Fig. 3. (a) CH Routing, (b) Network-based data transformation

Each GW throughout the movement phase, to choose the neighbor GW, uses a probabilistic mechanism having higher luciferin level than itself, for movement.

In the movement of each GW_j's, the movement probability to a neighbor 'k' is stated by

$$P_{jk(u)} = \frac{m_k(u) - m_j(u)}{\sum_{l \in O_j(u)} m_l(u) - m_j(u)} \quad (10)$$

The GW's group of the neighbourhood is represented as $\{k \in n_j(u), n_j(u) = \{k : d_{jk}(u) < d_d^j(u); m_j(u) < m_k(u)\}\}$ at the time 'u', $d_d^j(u)$ S variable range of the neighborhood linked using GWj at the time 'u', $d_{jk}(u)$ is the Euclidian distance between GWs j and k at time 'u'. For example with probability $P_{jk}(u)$, GWj choose $G_{w \in N_j(u)}$. The GW actions discrete time model is defined as,

$$y_j(u+1) = y_j(u) + s^* \left(\frac{y_k(u) - y_j(u)}{\|y_k(u) - y_i(u)\|} \right) \quad (11)$$

The position of GWj is $Y_j(u)$ at the time 'u' along with the step size s (>0). In the neighbourhood range update phase using the following rules, GW is updated:

$$rd^j(u+1) = \min \{r_s, \max \{0, r_d^j(u) + \beta(n_t - |n_j(u)|)\}\} \quad (12)$$

Where the constant parameter is termed as ' β ' also nt is to manipulate the neighbors involved.

5.2 GSO Approach for Finding the Probability of Dead Nodes

After cluster formation, the clusters are optimized, by enclosing the entire deployment area of the sensor. By means of an efficient GSO algorithm, the optimization of the cluster is performed.

$$F = \text{FitnessFunction} = E + D + NH \quad (13)$$

(13) Represents the fitness function of the effective GSO routing algorithm.

Where, the residual energy of all SNs is denoted as 'E', the distance between the nodes to the CH is represented as 'D', and 'NH' is the number of hops of all sensor nodes.

The residual energy in each sensor nodes displays the Probability of the dead nodes, besides it is conveyed as

$$P_d = (\{e_1 > e_{Req}\} \& \{e_2 > e_{Req}\} \& \dots \{e_n > e_{Req}\}) \quad (14)$$

The probability of the dead nodes as well as the preferred network is denoted as P_d and e_{req} is the minimum energy required for every sensor nodes

$$fd = \begin{cases} \text{inf} & p_d == 0 \\ f & p_d == 1 \end{cases} \quad (15)$$

From (15) the dead nodes in a network are found when the node is dead the ' p_d ' value is zero or else it generates a fitness function used for the routing process.

6 Experimental Setup and Results

For simulation, the MATLAB simulation tool is applied. The algorithms used are DA with the FCM and GSO for routing in WSNs. The subsequent Table 2 comprises of simulation parameters used as input for this Hybridized DA-GSO approach. With sensor nodes of 200 as well as 20 gateways, the proposed method has been implemented. The SNs have up to 0.5 J of initial energy. The proposed approach is verified greatly then the experimental results for both clustering and routing are mentioned.

Table 2. Simulation parameters

Parameter	Value
Area (x, y)	200 * 200 m ²
SNs (n)	200
Gateways	20
The initial energy of the sensor nodes	0.5 J
The number of simulation iterations	300
Range of communication	150 nm
Eelec (energy consumed)	50 PJ/bit
efs (free space energy loss)	10 PJ/bit/m ²
emp (multipath energy loss)	0.0013 PJ/bit/m ⁴
d0 (crossover distance)	87.0 m
Eda (data aggregation energy)	5 nJ/bit
Packet size	4000 bits
Message size	200 bits

The entire network has 200 * 200 m² of coverage area and the base station position is set at 125,325. The Hybridized DA-GSO approach is compared with the Hybridized PSO-PSO approach and Hybridized PSO-GSO approach. To compare our proposed methodology, the maximum range for the particles are set to 15 with zero simulation delay besides iteration of 50 and at last the centroid dimension is made as 2.

Tables 3 and 4 displays the basic parameters that are used in the DA and GSO algorithms.

In Fig. 4(a), with some of the available methods, the comparison of the proposed approach is shown which displays better results compared to the present method.

In a network, the lifetime of the network is the time when the first and the last ever node die in the network. The residual energy of the sensor nodes is kept high for making the nodes alive. Because of this, there is an increase in the network lifetime also the number of transmissions are enhanced.

The results of dead nodes are shown in Fig. 4(b), displays intensely decreased dead nodes when compared with the proposed technique. It is carried out by maintaining the residual energy of each sensor node, because the sensor node is impossible to recharge and more dead nodes are created by the existing approaches. This figure is clearly indicating that the Residual energy of the proposed technique is significantly improved.

Table 3. DA parameter values

Parameters	Values
No. of dragonflies	50
Separation factor (s)	0.1
Alignment factor (a)	0.1
Cohesion factor (c)	0.7
Food factor (f)	1
Energy factor (e)	1
No of iterations	50

Table 4. GSO parameter values

Symbol	Note of definition	Setting
N	The number of nodes	50–200
X * Y	Sensing fields	200 * 200
r _c	Communication radius	10
r _s	Sensing radius	5
L _i (0)	Initial luminance	10

This figure undoubtedly shows that the proposed techniques residual energy is considerably enhanced.

Figure 4(a). The Number of nodes alive vs. Number of Rounds, Fig. 4(b). The Number of dead nodes vs. Number of Rounds, Fig. 4(c). Energy consumption vs. No of Rounds and Fig. 4(d). Throughput vs. No of Rounds.

The results of the energy consumption is shown in Fig. 4(c), and compared to the present approaches, the proposed has very less energy utilization, makes the network lifetime prolonged. To possess great load balancing among the present approaches, more energy is used, when the data is being transmitted between the nodes. Load balancing is the main factor for the consumption of energy, for this reason, the nodes energy relies on the number of packets carried in every single transmission. Throughput denotes the successful number of packets which are transmitted to the sink.

Figure 4(d) shows the comparison of the proposed one with existing approaches. The demonstrations shows that the rate of transmission for conveying messages successfully is large with high throughput. Cleary in the figure it's shown that, the throughput of the proposed approach is considerably improved when compared to existing methods.

Table 5 shows the comparison of the proposed technique with existing approaches. The proposed methods efficiency is evaluated by comparing it with two hybrid approaches namely Hybridised PSO-PSO approach and Hybridised PSO-GSO approach. With some of the parameters such as lifetime, alive nodes, dead nodes, packet send (Bits) and energy consumption (J) the comparison is made.

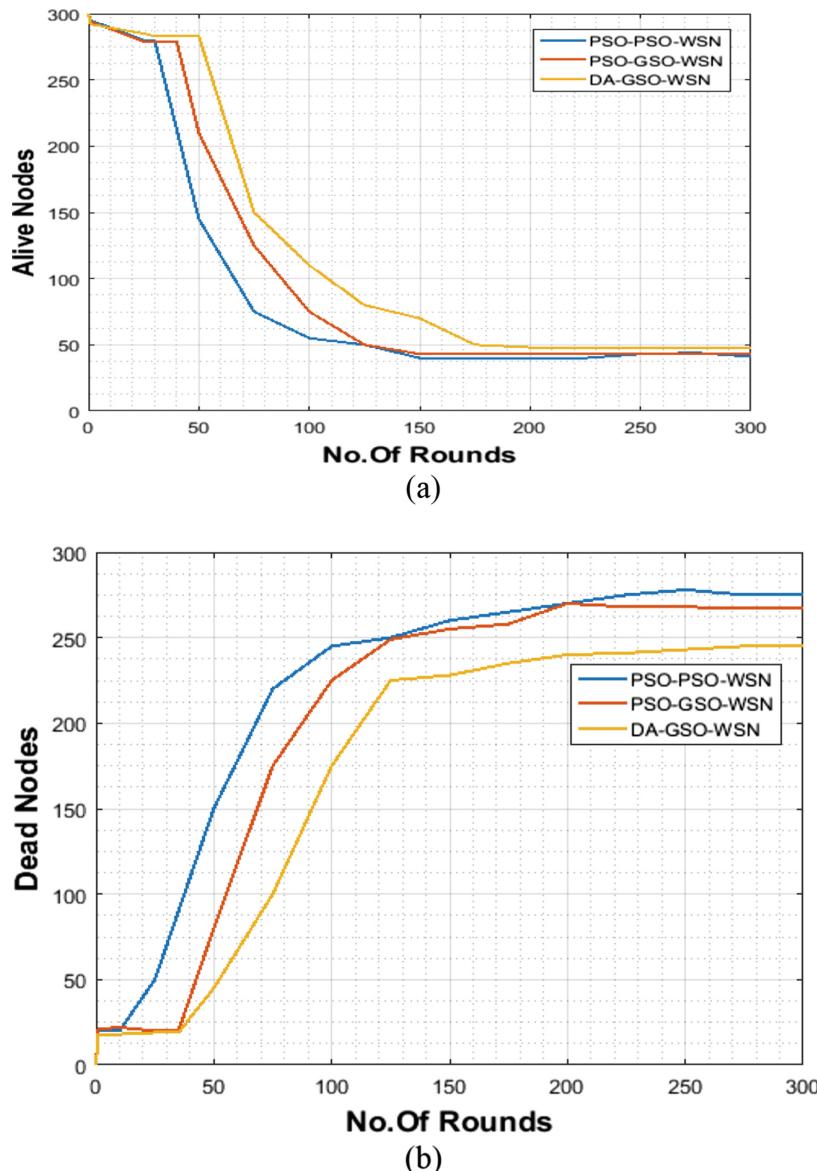
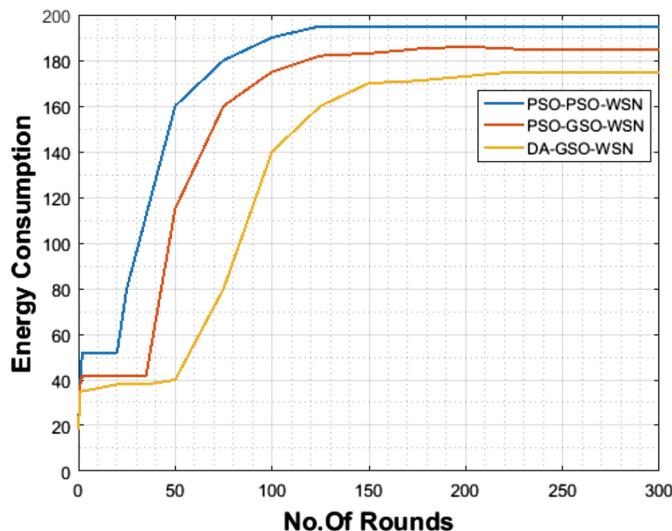
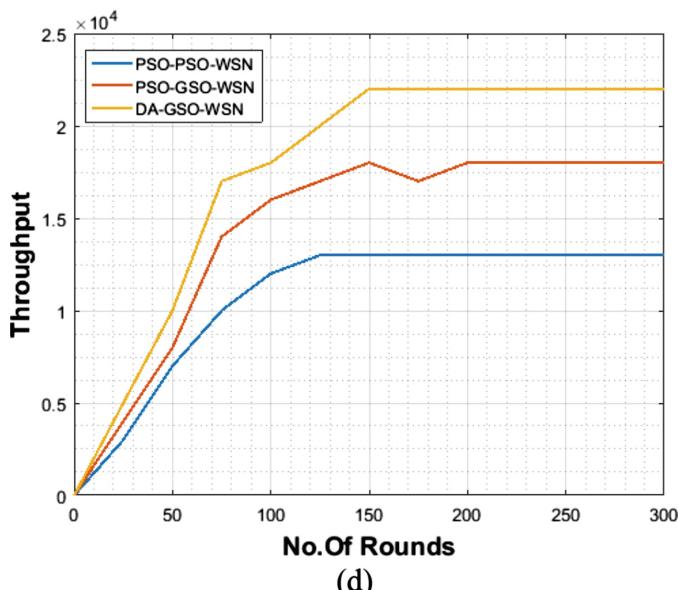


Fig. 4. (a) to (d), shows the comparison of the proposed method with the existing one.



(c)



(d)

Fig. 4. (continued)**Table 5.** Comparison of proposed with existing approaches

Parameters	Hybridised PSO-PSO	Hybridised PSO-GSO	Hybridised DA-GSO
Life time	150	220	290
Alive nodes	30	45	55
Dead nodes	275	260	245
Energy	195	185	170

7 Conclusion and Future Work

An algorithm is developed in which the FCM is applied for the formation of clusters moreover the DA is used for optimization and after the random deployment of SNs, the GSO is applied for energy efficient routing in WSN. From the results obtained after implementation of the algorithm, determines that the Hybridised DA-GSO technique has attained a prompt clustering as well as routing of WSN associated with certain current approaches. This Hybridised DA-GSO approach enhanced the lifetime of network, alive nodes, throughput besides reduces the dead nodes as well as minimizes the networks energy consumption. In the future work, an attempt is made to examine its performance concerning more complicated scarce heterogeneous circumstances containing nodes of special abilities to show the intensity of the method with respect to various performance metrics.

References

1. Suganthi, S., Rajagopalan, S.P.: Multi-swarm particle swarm optimization for energy-effective clustering in wireless sensor networks. *Wirel. Pers. Commun.* **94**(4), 2487–2497 (2017)
2. Asha, G.R.: Energy efficient clustering and routing in a wireless sensor networks. *Procedia Comput. Sci.* **134**, 178–185 (2018)
3. Sarkar, A., Murugan, T.S.: Cluster head selection for energy efficient and delay-less routing in wireless sensor network. *Wirel. Netw.* 1–18 (2017)
4. Zhu, J., Lung, C.-H., Srivastava, V.: A hybrid clustering technique using quantitative and qualitative data for wireless sensor networks. *Ad Hoc Netw.* **25**, 38–53 (2015)
5. Zeng, B., Dong, Y.: An improved harmony search based energy-efficient routing algorithm for wireless sensor networks. *Appl. Soft Comput.* **41**, 135–147 (2016)
6. Kumar, R., Kumar, D.: Multi-objective fractional artificial bee colony algorithm to energy aware routing protocol in wireless sensor network. *Wirel. Netw.* **22**(5), 1461–1474 (2016)
7. Prasad, D.R., Naganjaneyulu, P.V., Prasad, K.S.: A hybrid swarm optimization for energy efficient clustering in multi-hop wireless sensor network. *Wirel. Pers. Commun.* **94**(4), 2459–2471 (2017)
8. Rao, P.S., Jana, P.K., Banka, H.: A particle swarm optimization based energy efficient cluster head selection algorithm for wireless sensor networks. *Wirel. Netw.* **23**(7), 2005–2020 (2017)
9. Asha, G.R.: A hybrid approach for cost effective routing for WSNs using PSO and GSO algorithms. In: 2017 International Conference on Big Data, IoT and Data Science, pp. 1–7. IEEE (2017)
10. Elhabyan, R.S., Yagoub, M.C.: Two-tier particle swarm optimization protocol for clustering and routing in wireless sensor network. *J. Netw. Comput. Appl.* **52**, 116–128 (2015)
11. Faheem, M., Abbas, M.Z., Tuna, G., Gungor, V.C.: EDHRP: energy efficient event driven hybrid routing protocol for densely deployed wireless sensor networks. *J. Netw. Comput. Appl.* **58**, 309–326 (2015)
12. Yadav, R.K., Kumar, V., Kumar, R.: A discrete particle swarm optimization based clustering algorithm for wireless sensor networks. In: Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI, vol. 2, pp. 137–144. Springer, Cham (2015)

13. Tam, N.T., Hai, D.T.: Improving lifetime and network connections of 3D wireless sensor networks based on fuzzy clustering and particle swarm optimization. *Wirel. Netw.* **24**(5), 1477–1490 (2018)
14. Sabet, M., Naji, H.: An energy efficient multi-level route-aware clustering algorithm for wireless sensor networks: a self-organized approach. *Comput. Electr. Eng.* **56**, 399–417 (2016)
15. Bara'a, A.A., Khalil, E.A.: A new evolutionary based routing protocol for clustered heterogeneous wireless sensor networks. *Appl. Soft Comput.* **12**(7), 1950–1957 (2012)
16. Arora, P.: Enhanced NN based RZ leach using hybrid ACO/PSO based routing for WSNs. In: 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–7. IEEE (2017)
17. Shankar, T., Shanmugavel, S., Rajesh, A.: Hybrid HSA and PSO algorithm for energy efficient cluster head selection in wireless sensor networks. *Swarm Evol. Comput.* **30**, 1–10 (2016)
18. Su, S., Zhao, S.: A hierarchical hybrid of genetic algorithm and particle swarm optimization for distributed clustering in large-scale wireless sensor networks. *J. Ambient Intell. Humanized Comput.* 1–11 (2017)
19. Arjunan, S., Sujatha, P.: Lifetime maximization of wireless sensor network using fuzzy based unequal clustering and ACO based routing hybrid protocol. *Appl. Intell.* 1–18 (2017)
20. Barolli, A., Sakamoto, S., Barolli, L., Takizawa, M.: A hybrid simulation system based on particle swarm optimization and distributed genetic algorithm for WMNs: performance evaluation considering normal and uniform distribution of mesh clients. In: International Conference on Network-Based Information Systems, pp. 42–55. Springer, Cham (2018)
21. Raja, V.V., Hemamalini, R.R., Anand, A.J.: Multi agent system based upstream congestion control in wireless sensor networks. *Eur. J. Sci. Res.* **59**(2), 241–248 (2011)
22. Mann, P.S., Singh, S.: Energy-efficient hierarchical routing for wireless sensor networks: a swarm intelligence approach. *Wirel. Pers. Commun.* **92**(2), 785–805 (2017)
23. Gherbi, C., Aliouat, Z., Benmohammed, M.: An adaptive clustering approach to dynamic load balancing and energy efficiency in wireless sensor networks. *Energy* **114**, 647–662 (2016)
24. Mirjalili, S.: Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems. *Neural Comput. Appl.* **27**(4), 1053–1073 (2016)
25. Daely, P.T., Shin, S.Y.: Range based wireless node localization using dragonfly algorithm. In: 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 1012–1015. IEEE (2016)
26. Dutta, R., Gupta, S., Das, M.K.: Low-energy adaptive unequal clustering protocol using fuzzy c-means in wireless sensor networks. *Wirel. Pers. Commun.* **79**(2), 1187–1209 (2014)
27. Ni, Q., Pan, Q., Du, H., Cao, C., Zhai, Y.: A novel cluster head selection algorithm based on fuzzy clustering and particle swarm optimization. *IEEE/ACM Trans. Comput. Biol. Bioinf. (TCBB)* **14**(1), 76–84 (2017)
28. Ray, A., De, D.: An energy efficient sensor movement approach using multi-parameter reverse glowworm swarm optimization algorithm in mobile wireless sensor network. *Simul. Model. Pract. Theory* **62**, 117–136 (2016)



Retrospective Analysis of Wireless Body Area Network

A. Angel Cerli^(✉) and K. Kalaiselvi

Vels Institute of Science, Technology & Advanced Studies (VISTAS),
Pallavaram, Chennai 600117, India

angelcerli@gmail.com, kalairaghu.scs@velsuniv.ac.in

Abstract. Wireless Body Area Networks (WBANs) plays a key role in monitoring patient-health in order to gain a remarkable interest among the researchers. A WBAN consists of devices which are both small and fixed in the human body or kept as a device which can be easily carried by a person externally. The patient health can be observed and monitored consistently. It can also send the report on the status of patient health to the doctor and care taker. This paper discuss about energy efficiency in WBAN. Later report on various protocols proposed by several authors is compared in terms of its limitations, advantages and disadvantages. Finally the issues that can be encountered while implementing a protocol for WBAN are analyzed.

Keywords: Energy efficiency · MAC layer protocol · WBAN · WSN

1 Introduction

In current health care scenario, critical patients are consistently monitored by medical personnel like doctors and nurses. Due to the increasing count of emergency patients it is not possible to monitor all of them simultaneously. To overcome this, technology based improvement in the health care system should be adopted. This presents the improved wireless communication techniques as well as advancement of electronic devices, which gives rise to Wireless Body Area Network (WBAN). It holds a vital role in diagnosis and prognosis of a disease. The sick person can be monitored from their residence doing their day to day activities.

As the doctors need to monitor multiple patients at the same time, WBAN comes to rescue this situation. The condition of patient health can be monitored anywhere and anytime and they are monitored continuously. This constant monitoring of the critical patients helps in early risk deduction and prevention of diseases. Using WBAN the patients are monitored either from home or from any place carrying on with their everyday activities. The wireless communication medium helps in sharing patient health data to the respective physicians or nurses. This constant information sharing leads to loss of energy at the sensor nodes. So the flexibility and mobility may get degraded.

To overcome this energy draining we adopt few protocols for energy efficiency at the MAC layer of communication medium. In the current study we analyze about few MAC protocols with its requirements and problems they encounter in wireless sensor

networks. In WSN the foremost prerequisite to be considered is the energy efficiency. Also various energy waste which are specific to MAC, namely idle listening, collisions and overhearing are to be handled.

2 Related Works

To handle load balancing system in WBAN the authors have adopted clustering technique in paper [1]. This method shows limited computational power and resources for communication. High throughput, minimal end to end delay is achieved on implementing in MATLAB platform. This method lacks in security and authentication system as the protocols aren't effective in secure data transfer.

The authors in paper [2] have enhanced the MAC protocol by improvise efficient emergency handling capabilities in WBAN. The simulation tool used is NS2. This method doesn't consider communication overhead resulting in packet loss due to congestion. Also it shows least discrimination performance among signals.

In case of monitoring environment in WBAN improvised scheduling for MAC protocol is used in [3]. This technique works by applying increased delay restriction on every data packets to handle packet delay from collision during simultaneous data transmission. One restriction in this method could be restricted computational resources and it is less secured connection. NS2 is used as simulation platform.

Congestion control also considered as important aspect in WBAN. In paper [4] the author implemented priority based congestion control. With respect to queue occupancy a protocol for controlling loss of packets during congestion is designed. This method results in effective throughput and simulated under NS2 platform. Aiming for congestion control this method hasn't considered certain parameters like network delay and bandwidth. Similarly a dynamic priority based architecture for healthcare system is adopted in paper [6], targeting to deal with heterogeneous traffic management. The proposed model is implemented in OPNET platform and the overall performance is counted in terms of throughput, delay and loss. Since resource allocation is being adopted in this technique it results in increased performance.

Currently WBAN has been applied to IoT systems in healthcare environment. The paper [5] implements multi-hop WBAN construction with functionalities namely enhancing transmission efficiency, mobility support and clustered topology setup. This model also presents network failure tolerance feature when implemented in NS2 platform. Critical drawbacks in this system are interference problem in inter-network and lack of energy control. Also scope of gathering data is limited.

3 WBAN

Wireless body area network (WBAN) is categorised under Wireless sensor network (WSN), connected with sensor nodes. They communicate by sending and receiving data among the sensor nodes also they form data connection sensing the adjacent nodes

or with sink node. The sensor nodes may vary according to the user needs. In general they are powered using batteries with lesser memory storage targeting to cut down power requirements. A typical sensor node is framed with a memory chip, sensors, a processing unit, actuators and power supply node.

WBAN can be categorised as either implanted device or as wearable device. Since constant monitoring of patients needed, flexible information sharing between the patient and doctors should be adopted. There are few cases where patient needs to be continuously monitored even while doing their everyday activities. So they can be monitored remotely while doing their day to day activities. This is achieved through the communication medium of WBAN which uses protocols in MAC layer. The information about the health condition is passed onto the care takers and doctors of the patient. Thus it provides greater flexibility and mobility to patients. Another feature of WBAN is it can alarm the patient for auto medication during emergency situations. So we can classify communication in WBAN as inter-body communication and extra-body communication.

4 Energy Efficiency in WBAN

Energy aspects aren't considered as the important criteria in previous workings on MAC layer protocols, later on the emergence of wireless sensor networks, the energy efficiency is being recognized as most sort out design requirement [13]. The primary consideration WSN with respect to MAC protocols is dealing with energy efficiency, therefore many models had been proposed by researchers to minimize the total energy consumption. The main approach adopted for conserving energy is to possibly place the nodes present in them into idle state or sleep state. As a way to increase lifetime at sensor node, energy efficient operation becomes principal solution.

Some attributes to be considered are, efficiently conserving energy and transferring data between two nodes which is measured in J/bit and the determining the requested data.

5 MAC Layer

Medium Access Control (MAC) protocol is foremost protocol layer placed above the physical layer and as a result of this the properties of MAC protocols are greatly affected [13]. The primary function of MAC protocol is to control the number of nodes accessible on a shared medium. It works on targeting to improvise the performance requirement on few applications. Few common performance criteria being analyzed are delay, security, reliability and throughput, whereas in [13] WBANs, the issue of energy conservation becomes prominent task. Since WBANs, uses a wireless medium, the problem faced during wireless transmission is reflected here. The performance and functioning of MAC protocols is greatly affected because the physical layer properties.

6 Energy Efficient Protocols

Numerous MAC layer protocols have been designed to improve the lifetime of sensor node. Some of the common energy problems of MAC layer are collisions, overhearing, protocol overhead and idle listening. MAC protocols developed mostly for WBAN target those of the above problems to handle energy efficiency [13]. Most of the proposed techniques include common factors like

- cluster head formation for larger transmission regions
- end-to-end reliability or end-to-end delay
- single and multipath transmissions.

Few commonly used protocols are:

6.1 LEACH

(Low Energy Adaptive Clustering Hierarchy) – This is common technique used to overcome energy consumption problems. In this a TDMA based MAC protocol is infused with a clustering and a routing protocol is adopted. LEACH considers a dense sensor network, energy – constrained nodes that passes the data to a sink node. The main disadvantage of this model is that it fails to cover large geographical areas. The farther the cluster head from sink node, then more chances of energy loss due to data transmission. Thus it works well for single hop routing.

6.2 SMACS

(Self-organizing Medium Access Control for Sensor Networks) – It deals with neighbor discovery, multi-hop routing protocol, local routing protocol for signal processing and attachment of mobile nodes. They generally combine neighborhood discovery and assignment of TDMA schedules to nodes. Setting up an exclusive channels and links and to detect neighboring nodes are the primary goals of SMACS. This technique holds two critical issues. Initially the selection of super frame length has to be addressed. Later issue happens at heavily populated sensor networks with low traffic load.

6.3 PEGASIS

(Power-Efficient Gathering in Sensor Information Systems) – It is an improvement over LEACH protocol, where communication occurs only within neighboring nodes. Thus energy consumed per turn is greatly reduced resulting in optimal chain based protocol. This method works in equal energy distribution among sensor nodes.

Some of the energy efficient protocols designed by various authors are listed below (Table 1).

Table 1. WBAN – energy efficient protocols

Reference	Proposed work	Limitations	Advantages	Disadvantages	Tools/software used
[7]	WBAN based on ZigBee is proposed for presenting an energy efficiency solution	Failed to eliminate communication overheard	Energy consumption at sensor node is greatly decreased and the network lifetime is extended	Due to congestion there is raise in average end to end delay	OPNET
[8]	It aims to conserve the energy of nodes by increasing the network lifetime	On path discovery energy management and security are not concentrated	Reduces routing overhead and energy consumption	Doesn't control congestion. Increases network delay in larger networks	OPNET
[9]	A simple, no cost and convenient Adaptive Transmit Power Mechanism (ATPM) is presented to improve the WBAN link quality	Lacks dealing with security and inferences	Energy efficient while increasing the communication reliability	Security and computational performance is restricted	OMNET++
[10]	A static energy efficient clustering algorithm is adopted to partition the WBAN into static time generated clusters	Complicated cluster head selection process	Clustering extends the performance, stability and lifetime of a WBAN	Increased communication overhead	MATLAB
[11]	PEAM on cross-layer constructs allows layer synchronization and coordination	Capable of handling only during emergency situations.	Performance is high in terms of loss rate and end-to-end delay specifically for critical mode	Less flexible and scalable	OMNET++
[12]	An energy aware secure routing protocol for WBAN using batch ACK is presented	Acknowledgement is sent only at the end of the transmission	Reliability and data delivery ratio is high. Resists attack on data	High latency for alarm Provision, Minimal network lifetime	NS2

7 Issues in WBAN

Maximizing lifetime of network, performance and stability are the primary threat in WBAN. In order to extend the sensor node lifetime, it becomes prominent to manage the resources in WBAN. If they are implanted then replacing the batteries of various sensors may not be feasible. Hence to overcome these issues, clustering techniques is adopted to enhance stability, lifetime and performance of WBAN by minimizing power consumption. The main issues apart from energy efficiency are design and implementation issues, security issues and user oriented issues.

Inspite of WBAN being categorized under WSN, due to certain properties like data rate, architecture, mobility, and density makes the protocols of WSNs less productive. The routing protocol has to be designed according to the requirements framed with at most accuracy. By this way the protocol is designed to satisfy only a particular requirement. A single protocol hasn't been designed to satisfy all quality of service requirements. The issues in designing a suitable routing protocol are:

- i. Unstable network topology and routing among nodes happens with body movements of person. This results in higher data loss.
- ii. Protocols should be effective in handling various kind of data like ordinary static data, reliable data and critical data such as ECG, EEG and so on.
- iii. Protocols need to be efficient in selecting a route for retransmitting the data when the range falls beyond the threshold value.
- iv. Security and privacy plays a major role while dealing with any kind of data. Medical data has to ensure privacy in handling the data and provide secure data interaction.
- v. As the data is constantly being transmitted in network at varied ranges or distances between communicating nodes, energy consumption will be higher in case of WBAN.
- vi. The nodes maybe either placed inside human body or carried upon in a devise. So frequent battery replacement may not be possible in case of implanted devices.
- vii. The power consumption and memory of different nodes may vary which leads to heterogeneous nature.
- viii. In wireless network communication loss of data i.e., packet loss and collisions are high.

8 Conclusion

In this paper, various issues in routing protocol of WBAN are studied. Also these routing protocols are compared in terms of its limitations, advantages and disadvantages. The outcome of various new techniques and methods in designing the energy efficient protocol has improvised in energy saving and controlling energy consumption to a great extent. The protocols are adopted considering the requirements and criteria of sensor node location. This paper has discussed more about energy consumption and shows that energy is a precious resource in WBAN and therefore energy efficiency makes it an optimization goal to work on.

References

1. Yadav, D., Tripathi, A.: Load balancing and position based adaptive clustering scheme for effective data communication in WBAN healthcare monitoring systems. In: 2017 11th International Conference on Intelligent Systems and Control (ISCO), pp. 302–305. IEEE (2017)
2. Kamble, J., Vidhate, A.: Improved MAC protocol for emergency handling in WBAN. In: 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), pp. 1025–1029. IEEE (2016)
3. Kim, R.H., Kim, J.G.: Improved scheduling for MAC protocol in WBAN based monitoring environment. In: 2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 706–709. IEEE (2016)
4. Gambhir, S., Tickoo, V., Kathuria, M.: Priority based congestion control in WBAN. In: 2015 Eighth International Conference on Contemporary Computing (IC3), pp. 428–433. IEEE (2015)
5. Kim, T.-Y., Youm, S., Jung, J.-J., Kim, E.-J.: Multi-hop WBAN construction for healthcare IoT systems. In: 2015 International Conference on Platform Technology and Service, pp. 27–28. IEEE (2015)
6. Gambhir, S., Kathuria, M.: DWBAN: dynamic priority based WBAN architecture for healthcare system. In: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACOM), pp. 3380–3386. IEEE (2016)
7. Huynh, D.-T., Chen, M.: An energy efficiency solution for WBAN in healthcare monitoring system. In: 2016 3rd International Conference on Systems and Informatics (ICSAI), pp. 685–690. IEEE (2016)
8. Smail, O., Kerrar, A., Zetili, Y., Cousin, B.: ESR: energy aware and stable routing protocol for WBAN networks. In: 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 452–457. IEEE (2016)
9. Sarra, E., Ezzedine, T.: Performance improvement of the wireless body area network (WBAN) under interferences. In: 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), pp. 1–6. IEEE (2016)
10. Mukhtar, T., Chaudhary, S.: Energy efficient cluster formation and secure data outsourcing using TEOSCC and ECDH-IBT technique in WBAN. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 596–602. IEEE (2016)
11. Bouachir, O., Mnaouer, A.B., Touati, F.: PEAM: a polymorphic, energy-aware MAC protocol for WBAN. In: 2016 23rd International Conference on Telecommunications (ICT), pp. 1–6. IEEE (2016)
12. Mohnani, P., Jabeen, F.: Power efficient, reliable and secure wireless body area network. In: 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACOM), pp. 2722–2726. IEEE (2016)
13. Karl, H., Willig, A.: Protocols and Architectures for Wireless Sensor Networks. Wiley, Hoboken (2007)



Cross Layer Aware Optimization of TCP Using Hybrid Omni and Directional Antenna Reliable for VANET

S. Karthikeyini¹ and S. Shankar²

¹ Anna University, Chennai, Tamil Nadu, India

karthikeyinicse@gmail.com

² Hindusthan College of Engineering and Technology,

Coimbatore, Tamil Nadu, India

shankx80@gmail.com

Abstract. The motivation behind Intelligent Transportation System (ITS) application added to the profoundly unique nature of the Vehicular Adhoc Network (VANET) to improve the vital hassle of passenger safety and road traffic efficiency. Transfer Control Protocol (TCP) performs slow-start during the connection initiation, after retransmission timeout, and packet loss. Since the path loss frequently occurred in the high dynamic adhoc network prone to frequent timeout. The connection spends most of time in the slow-start phase, which lead to the under utilization of network resources and increase the delay in the network. Proposed work implements the lower layer of physical, MAC and network layer without modifying TCP operation to improve the performance of TCP in an adhoc wireless network, which would empower a seamless operation on the Internet. The proposed system Cross-Layer Aware Optimization of TCP (CLAO-TCP) using a hybrid Omni and Directional antenna, that combines the two models of Total Signal Attenuation in Line-Of-Sight (TSA-LOS) detect the path loss earlier to prevent the path failure and Distributed TDMA using Directional Antenna (DTDMA-DA) for slot allocation without conflict to enhance the QoS in high dynamic nature of the vehicular adhoc network.

Keywords: Layered architecture · TCP · IEEE 802.11p · CLAO-TCP · TSA-LOS · TDMA-DA

1 Introduction

In layered architecture model, high-level layer protocol uses the services from the low-level layer and proscribes the direct communication between the nonadjacent layers. The optimized protocol sends the parameter dynamically to adjacent and nonadjacent interface to improve the performance of the network instead of the implementation of the various layers independently. The optimized protocol supports the opportunistic communication on wireless medium in the layered architecture of the TCP/IP suite, which is illustrated in the Fig. 1.

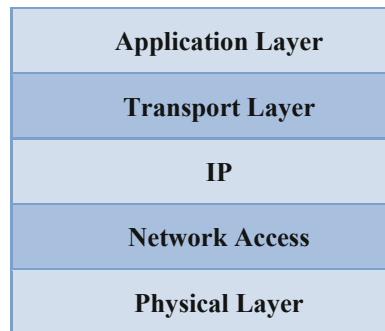


Fig. 1. Layered architecture of TCP/IP stacks

The TCP sender misconstrues the packet drop as congestion within the network instead of link failure in the wireless link and return to the slow start state, which degrades the throughput of the network. Avoid the misinterpretation of the TCP protocol sends the buffer overflow and link failure notification to the TCP sender. Thus, network layer sends the network condition through notification parameter to the TCP sender to differentiate the congestion and packet error in the network and the application layer can inform the delay requirements to the data link layer in the layered architecture [1].

2 Related Work

Traditional TCP liable for congestion control that avoids excess traffic in the network, flow control that is packet flowing not exceed the receiver window, in-order delivery and reliable transmission across the network. Initially TCP sender initially enters in slow-start and sends the congestion window of one maximum segment size and wait for acknowledgement of packets. Once the acknowledgement of packet received within the retransmission time out at that point the transmission rate will be increased by two times that will be proceed until the segment size reaches the slow-start threshold. During congestion avoidance, the packet size increases linearly until it reaches a receiver window size. Either the acknowledgement of packet does not receive within the retransmission time out or arrival of three duplicates of packets, the TCP sender predicts the error in the network and invokes the multiplicative decrease of the window size [2, 3].

3 Literature Review

A sender in TCP session detects packet loss as often as possible in the highly dynamic adhoc network it invokes congestion control algorithm which degrades the throughput of the network. In network layer, existing modified TCP of Transfer Control Protocol-Feedback (TCP-F) minimizes the throughput degradation from frequent disconnection

nature of the high dynamic adhoc network. At that factor when a middle of node distinguishes the path failure, it produces the Route Failure Notification (RFN) and forwards the intermediate node along the path. Each intermediate node understands the route failure and it sends the RFN packet to the TCP sender that move into the frozen state. It freezes the retransmission timer, congestion window size and set the Route Failure Timer (RFT) depends upon the network size for making route to destination. If any intermediate node finds a path to the destination, it produces the Route Reestablishment Notification (RRN) to TCP sender. When RFT expires, TCP state updated to the normal state and is continued to send the buffered packet [4].

The advantage of the TCP-F uses simple notification of path failure and reestablishment of the path to keep away from the TCP sender unnecessary move into the slow-start. The disadvantage of TCP-F needs implementation of the standard TCP libraries, since minor modifications are made to the TCP protocol to adapt it to the character of an adhoc network, it does not work with the internet and it increases the dependency on network layer protocol. Existing Transfer Control Protocol-Explicit Link Notification (TCP-ELFN) compared to the TCP-F however, it uses the periodic probe packet informs the reestablishment. The benefit of TCP-ELFN differentiates the path failure and congestion in the network. The downside of TCP-ELFN probe packet consumes bandwidth if path failure may proceed last longer and same CW size used after the reestablishment of the new route. In TCP-BUS, pivot node detects the link failure and notifies the Explicit Route Disconnection Notification (ERN) message and buffer the packet from the TCP sender until the reestablishment of the route from pivot node to the TCP receiver. The gain of TCP-BUS can use of buffering at intermediate node to avoid fast retransmission. The drawback of TCP-BUS has a failure in the intermediate node leads the overall performance degradation in the network [5, 6].

In Adhoc TCP (ATCP) sender receives Explicit Congestion Notification (ECN) enters into the congestion state, experiences the packet loss enters into the packet loss state, receives Destination Unreachable (DU) message with the aid of Internet Control Message Protocol (ICMP) enters into the disconnected state for performing an appropriate action. The Advantage of ATCP has periodic probe packet to locate the CW size after route reestablishment. The disadvantage of ATCP dependency on routing protocol network layer needs modification in interface feature [7, 8].

In physical layer, the deterministic propagation model considers the environmental properties such as speed of communicating vehicle, distance between vehicle, obstacle between the vehicles and environmental fading. The existing path loss propagation model of the two-way ground demonstrates considers the clear path and reflected path which is not desirable for short distance communication of vehicle-to-vehicle [9, 10]. The literature of IEEE 802.11p MAC protocol CSMA/CA has drawbacks of the hidden terminal problem and unbounded delay, which increase the collision [11, 12]. The Time Division Multiple Access (TDMA) based MAC facilitate better transmission in VANET than CSMA/CA [13, 14]. Existing Prediction-based TDMA MAC protocol (PTDMA) assign the slot in a distributed way, predict the collision and prevent the collision through exchange the intermediate node in two-hop communication range. If at least one or no intermediate node in between can't predict the collision it does not suite for low traffic scenario [15].

Existing Dynamic Token based MAC forms the virtual ring of a group nearby vehicle and assign the token holder node and backup token holder node (BTHN) for transmits beacon message based on first lowest beacons expiration time and next lowest beacons expiration time. Another individual in the ring waits for a token which increase the idle time of channel utilization [16]. Proposed work implements the lower layer of physical, MAC and network layer without modifying TCP to improve the performance of TCP in an adhoc wireless network which would empower a seamless operation of application-level protocol, FTP, SMTP, HTTP, and Internet.

4 Proposed System

In physical layer, the proposed system the RSU outfitted with Directional Antenna along with Omni Directional antenna, which radiate and acquire the power in a particular direction. It has a higher data rate than the Omni directional antenna. It provides greater coverage distance and reduced coverage angle so it limits interference from the environment [17]. The proposed model, Total Signal Attenuation in Line-Of-Sight (TSA-LOS) is to locate the path loss by monitoring the received signal strength within close-reference distance, above the close-reference distance, and any moving obstacle in LOS distance to prevent the path failure in advance. The proposed framework Distributed TDMA using Directional Antenna (DTDMA-DA) for allocating the slot in the distributed manner for each vehicle without any conflict based on First-Come-First-Served (FIFO) basis. The proposed framework CLAO-TCP using the received power from the physical layer, maintain the link quality, congestion control in MAC layer and report to the network layer, which are illustrated in the Fig. 2.

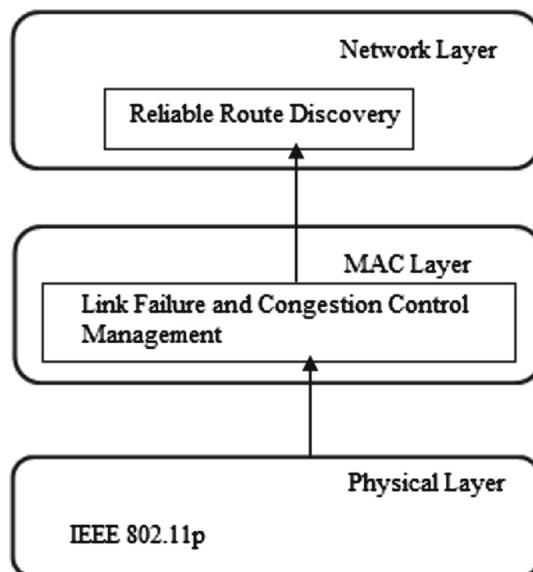


Fig. 2. Proposed framework CLAO-TCP

5 Information Model

In physical layer, node predicts the link failure by monitoring the signal strength of the RREQ packets received from the corresponding neighbor. The actual received signal strength of node is measured by Friis path loss propagation model and Knife-edge diffraction loss along the LOS to prevent the route failure. In MAC layer, assign the slot in distributed way based on the coverage time of vehicle, predict the same slot in two-hop communication range and avoid the possible collision in two-hop range. In network layer, route selection process of every node is selected based on weight estimation parameter of received signal strength, received time of request packet in its nearby memory and includes this data into the RREP packet header in a piggyback manner when it gets the RREP for the relating RREQ packet.

5.1 Physical Layer

To improve the reliability of the communication in VANET, the hybrid Omni and Directional antenna used for Road Side Unit (RSU). An Omni directional antenna receives and transmits the packet in all horizontal directions equally so it establishes more communication coverage for the vehicles and other infrastructure than Directional antenna. Since Directional antenna is able to focus the energy in a particular direction, it receives and sends the packet in a particular direction. Since it covers more length on the road in one direction than an Omni directional antenna, it establishes the more communication coverage between vehicles than the Omni directional antenna. So Directional antenna used in the proposed system to cover the more length on the road and used to assign the slot without any centralized unit based on coverage time of the vehicle. For example, the received signal strength of all horizontal directions is 2 mw in 1 m at point the px by using an Omni directional antenna. The received signal strength at particular direction is 6 mw in 1 m at the point px by using a directional antenna so it covers more length in one direction than an Omni directional antenna. So it improves the performance in directional based communication [18] which is illustrated in the Fig. 3.

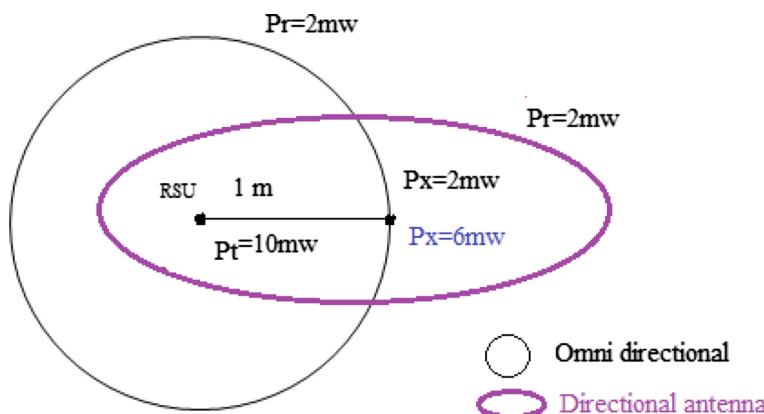


Fig. 3. The gain of Omni directional and Directional antenna at distance Px

Propagation Model

The power received by the receiver antenna is separated from the transmitter antenna by the distance ‘d’ [19] represented in Eq. (1).

$$P_{received}(f, d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^\alpha L}, \quad \lambda = \frac{C}{f} \alpha = 2 \text{ for free space}, \quad L \geq 1 \quad (1)$$

Where λ is a carrier wave length, α is Path Loss Exponent (PLE), C is a speed of light, f is a frequency of bandwidth, G_t and G_r denote the gain of the transmitter and gain of receiver antenna, L is a system loss. In mobile node, received power measured in free space takes close reference point d_0 and the distance d greater than d_0 . In free space considers the LOS between Sender (S) and receiver (R) and not consider the obstacles in the distance d. The received power is inversely proportional to the distance between S and R. The closest reference point $d_0 = 1$ m away from the transmitter node and $d = 250$ m. The value of the receiving power at the closest reference point d_0 is calculated by the Eq. (1).

The received signal is contrarily relative to the square of distance from the source of the inverse square law. The path loss is relative to the square of separation from transmitter to receiver. The path loss defines the difference between the effective, transmitted power and received power explained in the Eq. (2)

$$\begin{aligned} Pathloss_{FS}(f, d)[dB] &= 10 \log \frac{P_{transmitted}}{P_{received}} \\ Pathloss_{FS}(f, d)[dB] &= -10 \log \frac{\lambda^2}{(4\pi d)^2} \end{aligned} \quad (2)$$

The path loss occurred after closest reference point d_0 expressed in equation in (3).

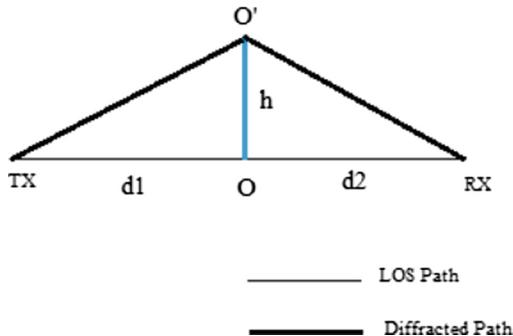
$$\begin{aligned} Pathloss_{FS}(f, d > d_0)[dB] &= Pathloss_{FS}(f, d_0)[dB] + \\ \beta_{LOS}[Pathloss_{FS}(f, d)[dB] - Pathloss_{FS}(f, d_0)[dB]] \end{aligned} \quad (3)$$

Where β_{LOS} is a slope correlation factor for Stanford University Interim (SUI) model [20] and the value of $\beta_{LOS} = 1.25$.

The diffraction OO' due to obstruction in first Fresnel’s Zone, which obstruct the LOS added to the path loss is illustrated in Fig. 4.

The path difference between the LOS path and diffracted path is represented in Eq. (4).

$$\begin{aligned} TXO' &= \sqrt{d_1^2 + h^2}, \quad O'RX = \sqrt{d_2^2 + h^2} \\ \Delta_{Path} &= \sqrt{d_1^2 + h^2} + \sqrt{d_2^2 + h^2} - (d_1 + d_2) \\ \Delta_{Path} &= \frac{h^2}{2} \frac{d_1 + d_2}{d_1 d_2} \end{aligned} \quad (4)$$

**Fig. 4.** Obstruction loss added to the LOS

The phase difference between the direct path and the diffracted path is expressed in the Eq. (5).

$$\begin{aligned}
 \Delta\phi &= 2\pi * (\text{path difference})/\text{wavelength} \\
 &= \frac{2\pi h^2}{\lambda} \frac{d_1 + d_2}{2d_1 d_2} \\
 &= \frac{\pi h^2}{2} \frac{2d_1 + d_2}{\lambda d_1 d_2} \\
 \Delta\phi &= \frac{\pi}{2} v^2
 \end{aligned} \tag{5}$$

If the moving obstacle disturbs the LOS of transmitter and sender, LOS blocked some energy can be reached through the first Fresnel's Zone ellipsoid space according to the ITU-RP 526-13 [21–23] the knife-edge diffraction loss defined in Eq. (6).

$$\text{Pathloss}_{MO}(f, d)[dB] = 6.9 + 20 \log_{10} \left[\left(\sqrt{v - 0.1} \right) + v - 0.1 \right] \tag{6}$$

for $-0.7 < v < 0$ otherwise value taken to be zero

From Eq. (6)

$$v^2 = \frac{2}{\pi} \Delta\phi$$

The obstruction edge lies on the first Fresnel's zone and the diffraction parameter defined in Eq. (7)

$$v = h \sqrt{\frac{2(d_1 + d_2)}{\lambda d_1 d_2}} \tag{7}$$

Where 'v' is a diffraction parameter, 'd1' is the distance between sender and obstruction, 'd2' is the distance between the obstruction and the receiver, 'h' is a height of obstruction and λ is a wavelength. The Total signal attenuation in Line-Of-Sight

(TLOF) path loss model takes closest reference point is an indoor environment and the distance d greater than d_0 takes outdoor environment. It considers the signal attenuation between the communicating vehicles in LOS at close-reference point, moving an obstacle disturb the communicating vehicle in LOS at any distance and considers the signal fading due to the environment beyond the 1 m of the log-distance. Where $\text{Pathloss}_{\text{FS}}(f, d)$ [dB] is a signal attenuation between two communicating vehicles in LOS at close-reference point which is calculated from the Eq. (2), signal fading due to the environment beyond 1 m which are calculated from the Eq. (3) and $\text{Pathloss}_{\text{MO}}(f, d)$ [dB] is a moving obstacle disturb the LOS of communication two vehicles at any distance, which are calculated from the Eq. (6).

5.2 Network Access Layer

The proposed distributed time-slot allocation scheme using the Directional antenna in the RSU and it radiates and receives the power in a specific direction so it has a high data rate, which increases the performance and reduces the interference from another source.

Distributed-Time Slot Allocation Scheme Using Directional Antenna

The proposed distributed-time slot allocation scheme using the directional antenna supports all type traffic and allocates the different time slot to avoid the collision with two-hop range. The beacon messages exchange the information in one-hop neighborhood. The beacon message contains vehicle id, speed, position, message generation time, free slot, reserved slot and neighbor list. In neighbor list contains id, speed, timestamp, free slot and reserved slot, which is expressed in the beacon format in Fig. 5.

ID	Speed	Position	Direction	Time stamps	Free slot	Reserved slot	Two-hop neighbour List
----	-------	----------	-----------	-------------	-----------	---------------	------------------------

Neighbor (i) ID, Speed, Position, Direction, Timestamps, Free slot, Reserved slot

Fig. 5. Beacon control message format

All vehicles equipped with an Omni directional antenna. Every node generates the present indication message when it enters into the Road Side Unit (RSU) coverage range. Directional antenna transceiver used at the time of slot allocation, which covers the two-way traffic. Each vehicle receives the slot from free slots based on First-In-First-Out (FIFO) basis. After receiving slot it transmits the packet to the neighbors. If two vehicles have same slot in one-hop or two-hop communication range it will create the collision. The collision will be avoided by each vehicle exchange the beacon message information in a two-hop range in order to avoid the same slot in two-hop range. The proposed work assigns a slot based on message generation time as well as predict the similar slot in two-hop communication range to avoid the collision and

necessary to change the similar slot allotment of vehicles are moving in the same direction or moving toward the opposite direction. If the same slot vehicle moving farther away from each other will not cause the collision. The two-way scenario of vehicles slot allocation is illustrated in Fig. 6.

Vehicle id = {A, B, C, D, E, F, G, H, I, J}

Free Slot K = {1, 2, 3, 4, 5, 6, 7, 8, 9, and 10}

Slot allocation: A = 1, F = 2, B = 3, G = 4, C = 5, H = 6, D = 7, I = 8, E = 9, J = 10

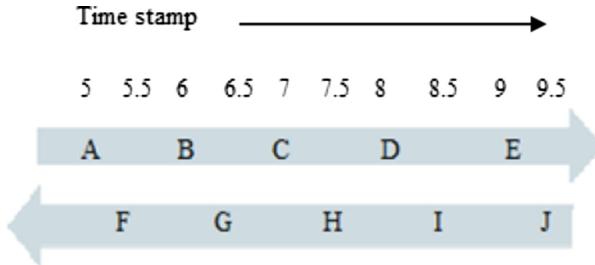


Fig. 6. Two-way traffic scenario

5.3 Proposed CLAO-TCP Route Request Format (RREQ)

In the route selection process, the sender node selects the best optimal node to forward the packet based on the weighted estimation of reception of RREQ time, RREQ threshold value received of signal strength along the available neighbor nodes. The RREQ format of the proposed CLAO-TCP protocol is shown in Fig. 7.

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7																									
Type	G	D	Identification					Hop Count																																								
RREQ ID			Reception RREQ time				RREQ threshold RSSI																																									
Destination Address																																																
Destination Sequence Number																																																
Source Address																																																
Source Sequence Number																																																

Fig. 7. Request format of CLAO-TCP protocol

In Type field, the bits 012 used for precedence; bits 345 used for Type of service. Flag 'G' is indicating whether Gratuitous RREP should be unicast to the destination IP address. Flag 'D' is indicating whether destination respond to the RREQ. Identification is

a number to identify the all fragments of the original IP packet. The hop count is a number of hops, which carry the message from the source address to the destination address.

6 Cross Layer Aware Optimization Scheme

6.1 Algorithm1: Total Signal Attenuation in LOS (TSA in LOS)

Finding the optimal path from source to destination based on receiving signal strength with interference:

1: Where $d_0 = 1\text{m}$ (closest-reference point), RSSI-Threshold = - 70 dBm [24]

2: The source node selects the optimal path based on received signal strength

3: If the distance between S-R $\leq d_0$ then

$$\text{Pathloss}_{FS}(f, d)[dB] = -10 \log_{10} \left(\frac{\lambda^2}{(4\pi d)^2} \right)$$

$$\text{RSSI} = \text{Pathloss}_{FS}(f, d_o)[dB]$$

4: Else

5: If the distance between the S-R $> d_0$ then

$$\text{Pathloss}_{FS}(f, d > d_0)[dB] =$$

$$\text{Pathloss}_{FS}(f, d_0)[dB] + \beta_{LOS} \left[\frac{\text{Pathloss}_{FS}(f, d)[dB] - }{\text{Pathloss}_{FS}(f, d_0)[dB]} \right]$$

Where β_{LOS} is a slope correlation factor for Stanford University Interim (SUI)

Model [20]

$$\beta_{LOS} = 1.25$$

$$\text{RSSI} = \text{Pathloss}_{FS}(f, d > d_0)[dB]$$

6: Else

7: If any moving obstacle between S-R at distance 'd' then

$$\text{Pathloss}_{MO}(f, d)[dB] = 6.9 + 20 \log_{10} [(\sqrt{v - 0.1}) + v - 0.1]$$

The knife-edge diffraction loss occurred in First Fresnel's Zone ellipsoid space according to the ITU-RP 526-13 [21-23]. Where 'd1' is a distance between the sender and the obstacle, 'd2' is the distance between the obstacle and the receiver.

$$v = h \sqrt{\frac{2(d_1+d_2)}{\lambda d_1 d_2}}$$

$$\text{RSSI} = \text{Pathloss}_{MO}(f, d)[dB]$$

8: End if

9: If RSSI \geq RSSI Threshold then

10: Select the optimal forwarding node, otherwise discard the node.

6.2 Algorithm 2: Distributed TDMA Using Directional Antenna (DTDMA-DA)

Assigning a time slot based on beacons message generation time:

- 1: Each vehicle assigns the slot based on beacon message generation time in the coverage range
- 2: Timestamp = 5; Threshold = 3;
- 3: N = 10, K = 10
Where 'N' is the number of vehicles in the antenna coverage, 'K' is the number of slots used
- 4: if (free-slot = 'True') then
- 5: for (i = 1; i <= N; i++)
 Vehicle-id[i].Timestamp = 5;
- 6: While (Vehicle-id[i].Timestamp! = Threshold)
 Vehicle-id[i].Timestamp = Vehicle-id[i].Timestamp - - ;
- 7: For (j = 1; j <= K; j++)
 Vehicle-id[i].Reserved-slot = free-slot[j];
- 8: End of loop j;
- 9: End of loop i;
- 10: Else
- 11: if (free-slot = 'False') then
 // choose the slot from reserved-slot with different direction along with distance $\geq 2R$ //
- 12: for (i=1; i < n; i ++)
- 13: if (Vehicle-id[i].direction! = reserved-slot[i].direction) &&
 (Distance (Vehicle-id [i].direction, reserved-slot[i].direction) $\geq 2R$) then
- 14: Vehicle-id[i].reserved-slot = reserved-slot[i];
- 15: End of loop i;
- 16: End if;

Prevention of collision in advance from the two-hop neighbor list:

- 1: Each vehicle receives the beacon message;
- 2: Each vehicle checks the status from two-hop neighbor list;
- 3: status = {free-slot, same-slot, collision};
- 4: if (same-slot = ‘True’ or collision = ‘True’) then
- 5: find a the same-slot vehicles-id (E, F) or collision vehicle-id (E, F);
- 6: Check distance between two vehicles; T = 2;
- 7: for (i = 1; i < =T; i++) {
- 8: if Distance (E - F) <= 2R during the time interval T = 1 to 2 sec then
// Where R is a communication range of one-hop. The DSRC communication range is 250m //
- 9: Check the velocity of the two vehicles;
- 10: if Velocity (E > F) then
- 11: The time-slot changing node is E;
- 12: Else
- 13: if Velocity (E < F) then
- 14: The time-slot changing node is F;
- 15: Else
- 16: The time-slot changing node is lower-id (E, F)
- 17: Else
- 18: if Distance (E-F) > 2R during the time interval T= 1 to 2 sec then
- 19: The time-slot changing is ignored;
- 20: End of loop i;
- 21: End if;

7 Simulation Results

The Spectrum Sensing with Distributed-TDMA (SSD-TDMA), which identifies the free channel to keep away from the spectrum shortage and assign the slot in a distributed way [29]. The proposed approach Cross Layer Aware Optimization of TCP (CLAO-TCP) forestall the packet loss and collision in advance to avoid the TCP

unnecessary move to the slow-start and assign the slot in distributed ways based on message generation time using directional antennas (Table 1).

Table 1. Simulation parameters

Parameter	Value
Simulator	Ns-allinone-2.34
Simulation time	100 s
Transmission range	250 m
Number of channels	7
Number of vehicles	100
Road Side Unit	6
Base station	1
RSSI-Threshold	-70 dBm
Channel data rate	3 mb/s
Packet size	512 bytes

7.1 Energy Usage

The Energy usage of CSMA/CA is 45 J at speed 100 m per seconds, G-TDMA is 40 J at speed 100 m per seconds, SSD-TDMA is 37 J at speed 100 m per seconds and the proposed approach CLAO-TCP is 29 J at speed 100 m per second. The graph proves that the proposed approach CLAO-TCP to reduce the energy consumption and acquit well than the existing approach seen in Fig. 8.

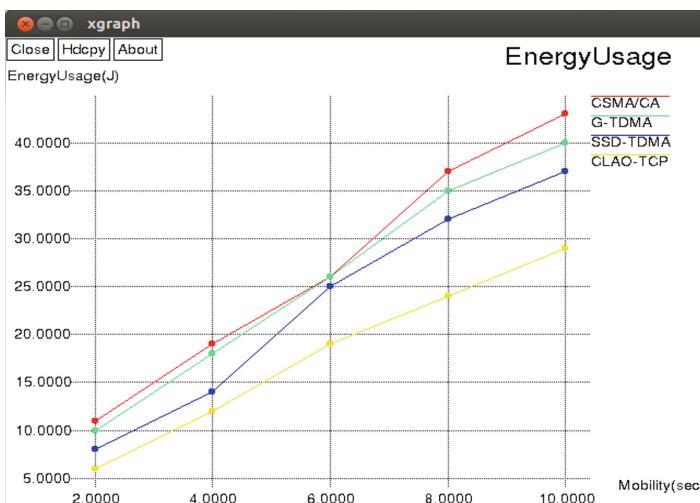


Fig. 8. Energy usage

7.2 Routing Overhead

The graph proves that the proposed approach CLAO-TCP to reduce the routing overhead and acquit well than the existing approach seen in Fig. 9.

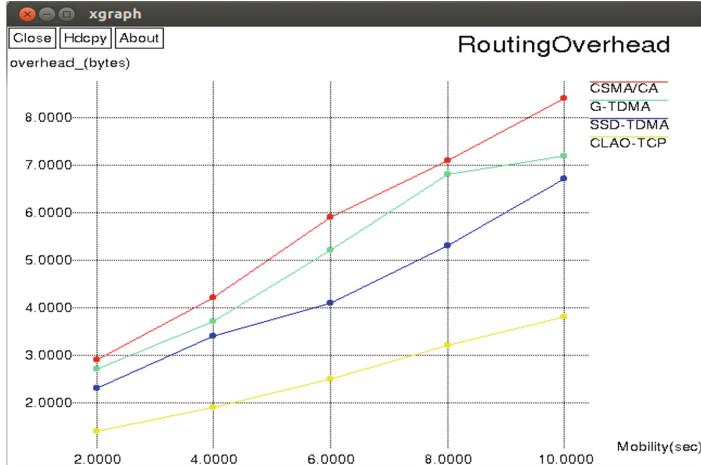


Fig. 9. Routing overhead

7.3 Packet Delivery Ratio

The PDR of CSMA/CA is 76% of packet at 100 m per second, the G-TDMA is 79% at speed 100 m per second, SSD-TDMA is 80% at 100 m per second and the proposed approach CLAO-TCP is 83% at speed 100 m per second. The graph proves that the proposed approach CLAO-TCP to increase PDR and acquit well than the existing approach seen in Fig. 10.

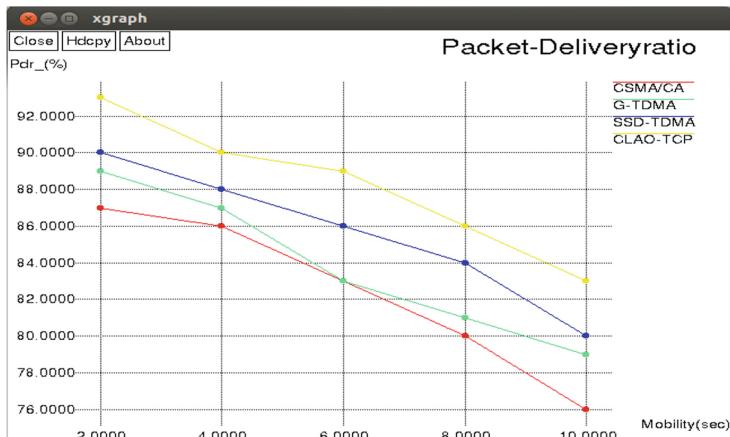


Fig. 10. Packet delivery ratio

7.4 Packet Loss Rate

The PLR of CSMA/CA is 525 packets at speed 100 m per second, the G-TDMA is 490 packets at speed 100 m per second, SSD-TDMA is 470 packets at speed 100 m per second and the proposed approach CLAO-TCP is 420 packets at speed 100 m per second. The graph proves that the proposed approach CLAO-TCP to decrease PLR and acquire well than the existing approach seen in Fig. 11.

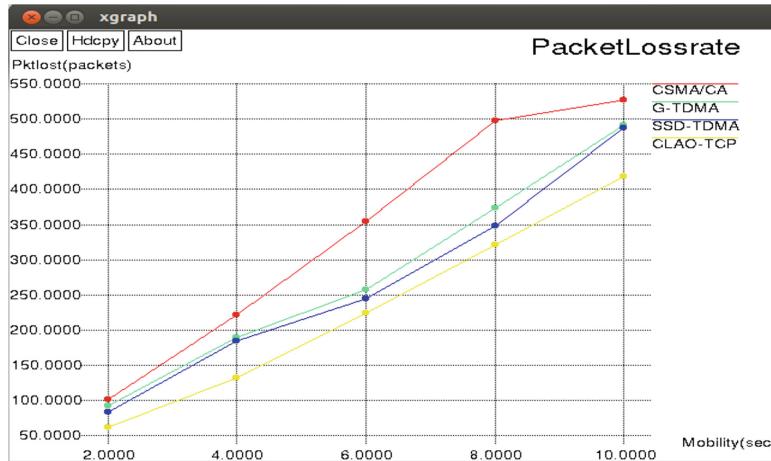


Fig. 11. Packet lose rate

7.5 End-to-End Delay

The EED of CSMA/CA is a 2.1 ms delay at speed 100 m per seconds, the G-TDMA is a 1.9 ms delay at speed 100 m per seconds, SSD-TDMA is a 1.7 ms delay at speed 100 m per seconds and the proposed approach CLAO-TCP is a 1.4 ms delay at speed 100 m per seconds. The graph proves that the proposed approach CLAO-TCP to decrease EED and acquire well than the existing approach seen in Fig. 12.

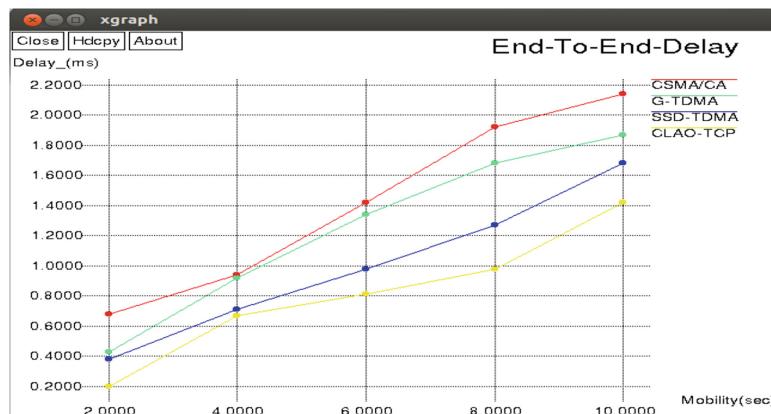


Fig. 12. End-to-end delay

8 Conclusion

VANET intend to enhance the road security and traffic administration on the road through the warning message so VANET inculcates the warning message about road conditions, the traffic condition and environmental hazards to another vehicle. The warning information entails the real-time information which directly has an effect on the lives of people traveling on the road so it delivered in a timely manner. In this paper, we recommend the Cross Layer Aware Optimization for Transfer Control Protocol (CLAO-TCP) predicts the path loss in advance to prevent the path failure by the Total signal attenuation in Line-Of-Sight (TSA-LOS) method using a hybrid antenna in order to avoid the unnecessary state of congestion control in TCP and it reduces the collision in all types of traffic by Distributed TDMA using Directional Antenna (DTDMA-DA). The aim of the proposed framework CLAO-TCP supports all kinds of traffic and predicts the path failure in advance to prevent the path loss. The simulation outcomes exhibit the proposed scheme CLAO-TCP using hybrid Omni and Directional antenna to successfully reduce the interference than existing methods and delivered in timely over the network.

Acknowledgements. I heartily thank our research guide, Dr. S. Shankar, Professor and HoD of Computer science and Engineering department for his guidance and suggestions during this research work.

References

1. Mohanakrishnan, U., Ramakrishnan, B.: MCTRIP: an energy efficient tree routing protocol for vehicular ad hoc network using genetic whale optimization algorithm. *Wirel. Pers. Commun.*, 1–22 (2019)
2. Amjad, M., Musavian, L., Rehmani, M.H.: Effective capacity in wireless networks: a comprehensive survey. *IEEE Commun. Surv. Tutor.* (2019)
3. Zhang, J., Chen, T., Zhong, S., Wang, J., Zhang, W., Zuo, X., Maunder, R.G., Hanzo, L.: Aeronautical *Ad ~ Hoc* networking for the internet-above-the-clouds. *Proc. IEEE* **107**(5), 868–911 (2019)
4. Yaacoub, E., Alouini, M.-S.: A key 6G challenge and opportunity—connecting the remaining 4 billions: a survey on rural connectivity. *arXiv preprint arXiv:1906.11541* (2019)
5. Singh, P.K., Nandi, S.K., Nandi, S.: A tutorial survey on vehicular communication state of the art, and future research directions. *Veh. Commun.* **18**, 100164 (2019)
6. Schmidt, A., Reif, S., Gil Pereira, P., Höning, T., Herfet, T., Schröder-Preikschat, W.: Cross-layer pacing for predictably low latency. In: *Proceedings of 6th International Workshop on Ultra-Low Latency in Wireless Networks (Infocom ULLWN)*, p. 184. IEEE (2019)
7. Khattak, H.A., Ameer, Z., Din, I.U., Khan, M.K.: Cross-layer design and optimization techniques in wireless multimedia sensor networks for smart cities. *Comput. Sci. Inf. Syst.* **16**(1), 1–17 (2019)
8. Nguyen, K., Golam Kibria, M., Ishizu, K., Kojima, F., Sekiya, H.: An approach to reinforce multipath TCP with path-aware information. *Sensors* **19**(3), 476 (2019)
9. He, Y., Yang, M.: Research on cross-layer design and optimization algorithm of network robot 5G multimedia sensor network. *Int. J. Adv. Rob. Syst.* **16**(4), 1729881419867016 (2019)

10. Nosheen, I., Khan, S.A., Khalique, F.: A mathematical model for cross layer protocol optimizing performance of software-defined radios in tactical networks. *IEEE Access* **7**, 20520–20530 (2019)
11. Al Emam, F.A., Nasr, M.E., Kishk, S.E.: Collaborative cross-layer framework for handover decision in overlay networks. *Telecommun. Syst.*, 1–15 (2019)
12. Darmani, Y., Sangelaji, M.: QoS-enabled TCP for software-defined networks: a combined scheduler-per-node approach. *J. Supercomput.*, 1–17 (2019)
13. Sethi, A., Vijay, S., Kumar, R.: Cross Layer Optimization with QoS for Heterogenous ad-hoc Network. *i-Manager's J. Wirel. Commun. Netw.* **7**(4), 1 (2019)
14. Tang, K., Kan, N., Zou, J., Fu, X., Hong, M., Xiong, H.: Multiuser video streaming rate adaptation: a physical layer resource-aware deep reinforcement learning approach. arXiv preprint [arXiv:1902.00637](https://arxiv.org/abs/1902.00637) (2019)
15. Nosheen, I., Khan, S.A., Ali, U.: A cross-layer design for a multihop, self-healing, and self-forming tactical network. *Wirel. Commun. Mob. Comput.* (2019)
16. Babber, K., Randhawa, R.: Cross-layer designs in wireless sensor networks. In: Computational Intelligence in Sensor Networks, pp. 141–166. Springer, Berlin (2019)
17. Guo, J., Gong, X., Wang, W., Que, X., Liu, J.: SASRT: semantic-aware super-resolution transmission for adaptive video streaming over wireless multimedia sensor networks. *Sensors* **19**(14), 3121 (2019)
18. Raj, K., Siddesh, G.K.: Multi-objective optimization assisted network condition aware QoS-routing protocol for MANETs: MNCQM. *Int. J. Comput. Netw. Commun. (IJCNC)* **11**, 1–23 (2019)
19. Cho, W., Choi, J.P.: Cross layer optimization of wireless control links in the software-defined LEO satellite network. *IEEE Access* **7**, 113534–113547 (2019)
20. Gao, K., Xu, C., Qin, J., Zhong, L., Muntean, G.M.: A stochastic optimal scheduler for multipath TCP in software defined wireless network. In: ICC 2019, 2019 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2019)



Enhanced TCP to Improve the Network Communication Performance in Smart Metering Applications

M. Rajiv Suresh¹(✉) and V. Subedha²

¹ St. Peter's Institute of Higher Education and Research, Chennai, India
m_rajivsuresh@yahoo.com

² Panimalar Institute of Technology, Chennai, India
subedha@gmail.com

Abstract. Smart metering is considered as a crucial system in Smart Metering Infrastructure (SMI). It efficiently helps in utilizing the electric energy by both providers and customers. In recent times, numerous researches have been carried out in the field of SMI to improve the interaction between the users and the servers. This requires the integration of smart meter networks with information technology (IT) infrastructure. Such integration helps to transmit different data types like messages of electrical usage, control messages like availability and latency and other information between the server and users. To efficiently transfer the data between the server and users, the enhanced TCP mechanism is used. The proposed study uses TCP Hybla in its transport layer to effectively deliver the data via a scalable communication channel. The result shows that the utilization of TCP Hybla in SMI effectively improves the communication performance in terms of increased throughput and reduced delay.

Keywords: Smart Metering Infrastructure · TCP Hybla · Transport layer · High throughput · Less latency

1 Introduction

The challenges in power grid are addressed effectively using smart grids that act as a data communication network. The Smart Grids are integrated with power grid in order of collecting and analyzing the transmitted data, which is obtained from distribution substations, transmission lines and from the users. This information effectively provides the predictive information to its users regarding the power management. Each domain offers several roles to make proper decisions in relation with power management [1]. The functionalities of Smart Grids are critical in terms of various constraints like energy consumption, wide-area situational awareness, distributed energy resources, means of storing energy, network communications, SMI and distribution grid management.

It is seen that SMI plays a critical role in Smart Grids, since it establishes a two-way communication between the smart meters and the utility, which helps to collect, measure, transmit and analyze consumption of energy by the users [2]. SMI is considered as an enhanced Advanced Metering Infrastructure (AMI), with huge improvements. It gathers the data remotely from various meters and collectively

transmits the collected information to the utility center through unidirectional communication. The existing meter reading fails to meet these necessities and hence SMI is introduced.

The main functionalities of SMI includes power quality monitoring, power quality management and power quality control, improving the efficiency of power usage, demand side management, adaptive power pricing, protection against intruders and natural disasters. It also provide additional functionalities in extending its communications remotely between SMs and utility companies for meter reading, expected load for energy saving, reliability improvement to reduce the congestion in transmission lines and overload associated with power generation, alert on outages, firmware upgrading and interfacing with other technologies [3].

SMI provides a dynamic infrastructure (shown in Fig. 1) that changes the infrastructure required for communication and hence the implementation associated with varying infrastructure changes. With varying communication infrastructure, the consumption of energy and network latency will increase, which prominently affects the throughput of SMIs. The proposed study aims at improving the communication performance between a smart meter data and a server through various channels. This includes reduction of packet loss, delay and other factors affecting the network performance. To increase the performance of network, the proposed study uses enhanced TCP to reduce the packet loss, delay and other related factors.

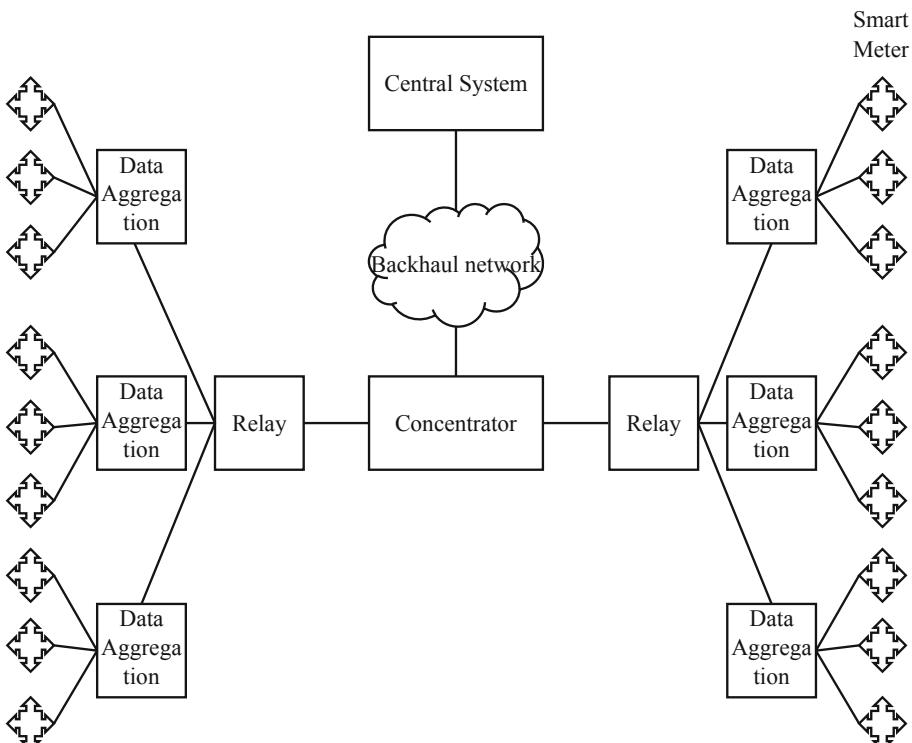


Fig. 1: Smart Metering Infrastructure

The outline of the paper is given below: Sect. 2 provides the related works. Section 3 discusses the proposed methodology. Section 4 evaluates the proposed work with other existing TCP mechanism. Section 5 concludes the paper.

2 Related Works

Variety of energy related issues are studied by several authors and used several enhancements to address the energy consumption issues. A typical methodology pushed by numerous researchers today is to utilize TCP as a transport layer to reduce end-to-end delay [4–6]. This is engaging, yet it requires adequate execution in entire network system in light of the fact that TCP force various necessities on the protocol stack. Specifically, TCP verifiably accept that IP packets in a shared manner with no adherence to the properties of the basic medium. This conduct is considered hard to help narrowband power line systems.

Transmitting IP packets between master and slave is considered less problematic, since the master initiate transmission of data at any instance of time. In reverse way it is considered more difficult. With increasing slaves, the master takes longer time to poll its data and hence the timing between the source and destination increases that leads to slow responses. To resolve this various mechanism are adopted by the researchers that includes: faster TCP [7], spitting TCP [8], aggregate TCP [9], split and aggregate TCP [10], TCP with retransmission principle [11] and other TCP mechanism [12]. The authors have also discussed various protocols [13] of SMI, optimization of SMI using TCP data aggregation framework [14] and analysis of TCP mechanism with spanning tree for smart metering infrastructure [15].

3 Proposed Enhanced TCP Mechanism for SMI

3.1 TCP Reno

TCP Reno operates majority on congestion window, where the size of window determines the maximum segments a source is allocated to send the pending acknowledgement. The size of the window grows with maximum value of congestion window and it either increases or decreases based on the network operating conditions. Often, buffering and processing ability is affects the protocol dynamics at the receiver. In a maximum window and round trip time (RTT), the TCP Reno uses a congestion window for controlling the transmitted data in order to limit the maximum value the window. The control system of TCP Reno system has five parts, which are interpreted accordingly (1) Slow Start, (2) Congestion avoidance (3) Fast retransmission (4) Fast recovery and (5) Timeout retransmission (Fig. 2).

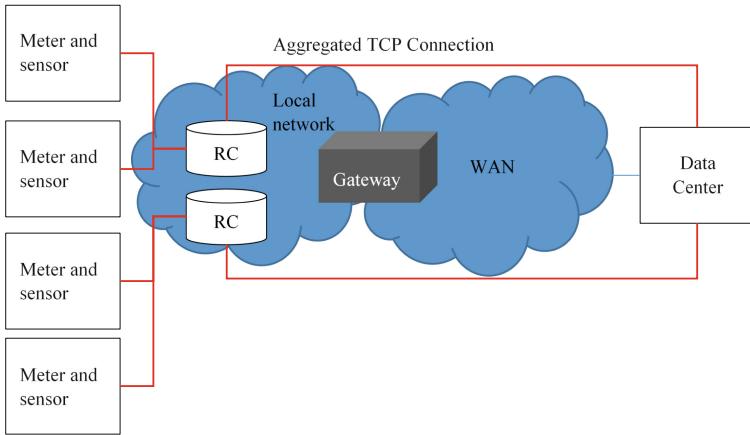


Fig. 2. Hop-by-hop communication using TCP connection

3.2 TCP Hybla

TCP Hybla is considered as a congestion control mechanism [16, 17] used mainly for heterogeneous networks. TCP Hybla is recognized for its higher throughput in IP links over heterogeneous networks, especially in long delay networks. The round trip time is used as reference connection. The advantage of TCP Hybla than other TCP aggregation mechanism is that it yields higher throughput with reduced round trip time.

It is found that the rate of throughput for the TCP Reno system is low, when the rate of RTT is high, since there is an increase in the size of congestion window, which is increased by a data segment/RTT at the time of congestion avoidance phase.

On other hand, if the size of the congestion window is increased by ρ^2 segments per RTT, which is considered as the normalized RTT, where $\rho = \text{RTT}/\text{RTT}_0$, RTT_0 is the reference connection during the time of congestion avoidance phase. With increasing RTT, the value of ρ increases, TCP Hybla enables high throughput even if the value of RTT is large.

The size of TCP Hybla's congestion window is updated at regular intervals, when an acknowledgment is received by the smart meter, which is given as follows:

$$W_{i+1} = \begin{cases} W_i + 2^\rho - 1 & \text{SS} \\ W_i + \rho^2/W_i & \text{CA} \end{cases} \quad (1)$$

where

i – total number of acknowledgement received,

SS is the slow start phase and

CA is the congestion avoidance phase.

Here, two different scenarios are considered with respect to the size of congestion windows, this includes: peak congestion window size without maximum value and peak congestion window size with maximum value.

For the throughput analysis, both the cases are considered separately, where for the first scenario, the throughput is written by $B_1 = \frac{(W-L)+p^{-1}}{A}$ and for the second case, the throughput is $B_2 = \frac{(W_m-L_m)+p^{-1}}{A}$. Thus total throughput is given by

$$B = B_1 + B_2 \quad (2)$$

Where,

W is the excepted congestion window size in the first phase at its peak

L is the expected number of lost data segments in the first phase,

p is the probability of packet loss,

A is the probability of m packet losses in the congestion window W ,

W_m is the excepted congestion window size in the first phase at its peak

L_m is the expected loss packet in the congestion window at the second phase.

Similarly, along with latency, the throughput of the model is given by

$$B(S) = \frac{8S}{T} \quad (3)$$

4 Results and Discussions

The use of TCP Hybla in the SMI is simulated using NS-2 simulator. The proposed method is intended to measure two important metrics that includes latency and packet delivery rate. The proposed TCP Hybla for SMI is compared with Markov TCP aggregate mechanism [5]. Markov TCP aggregate uses the concept of aggregation mechanism at the transport layer. It uses split and aggregation of TCP at transport layer using intermediate devices. A unified TCP connection is established using utility several with metered TCP connections. The TCP connection is initiated using a meter with SA-TCP aggregator over reliably transmitted data packets. The reports are forwarded to unified TCP connection using SA-TCP with a utility server i.e. the TCP connections are of two-hop connection. A mathematical model predicts accurately the performance in terms of delay, packet loss and throughput. This method employs Markovian and queuing models to improve the performance. The optimal TCP aggregators are found using an optimization framework [5].

It is seen from the Figs. 3 and 4 that the retransmission rate and latency of the proposed method has reduced for one-hop and it increases as the number of hops increases. Thus the objective of reduced latency and retransmission rate has reduced rate. It is seen that selection of optimal TCP aggregators helps in reducing the latency and retransmission rate for one hop TCP and it increases as the number of hops in the network increases.

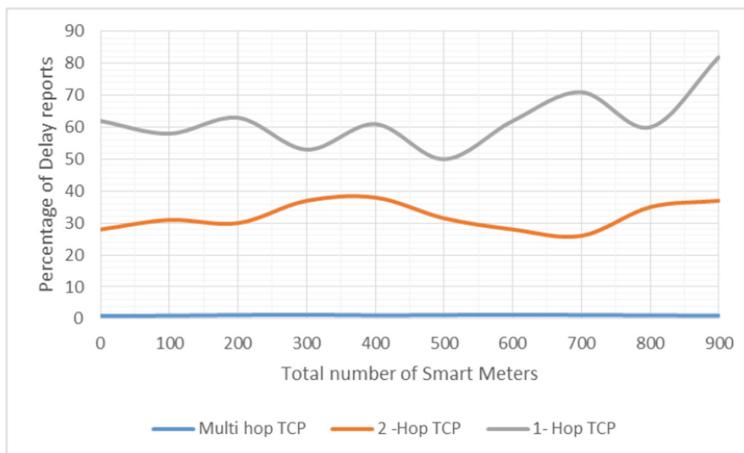


Fig. 3. Reports of delayed meter percentage

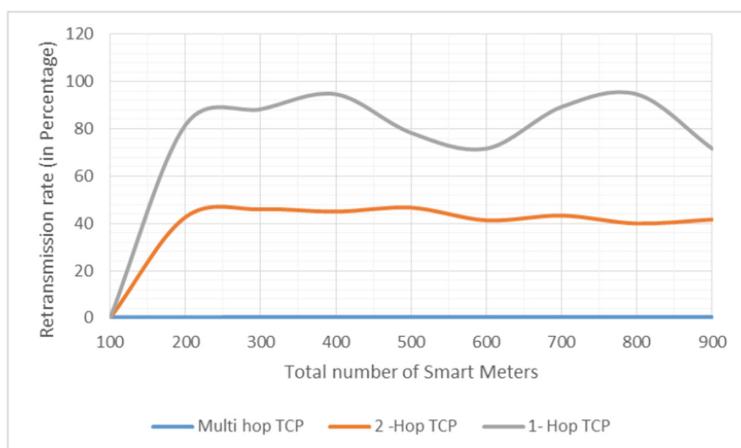


Fig. 4. Reports of meter retransmission percentage

Further, the performance of the proposed method is tested in terms of three performance metrics that includes: throughput, packet loss rate, and packet latency [Figs. 5, 6 and 7]. The result shows that the proposed method achieves reduced packet loss rate and packet latency, and achieves increased network throughput than the existing method.

This proves that the use of TCP Hybla effectively addresses the communication problems in the network and avoids the constraints while communication exists between the smart meter and the utility center.

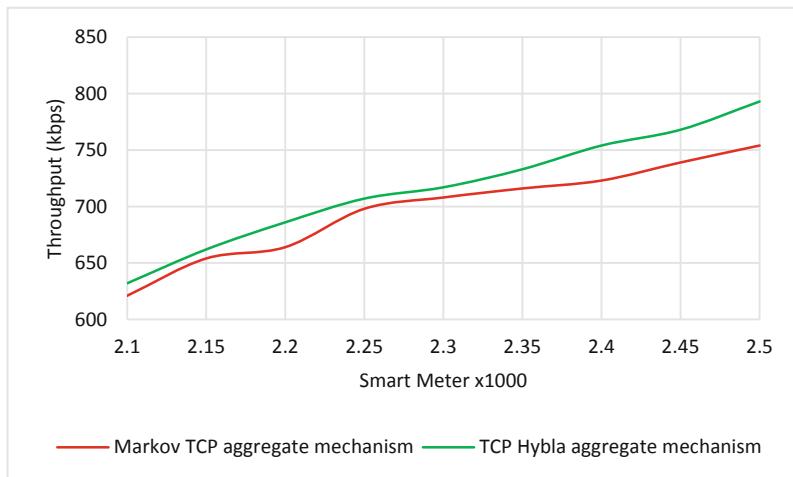


Fig. 5. Throughput

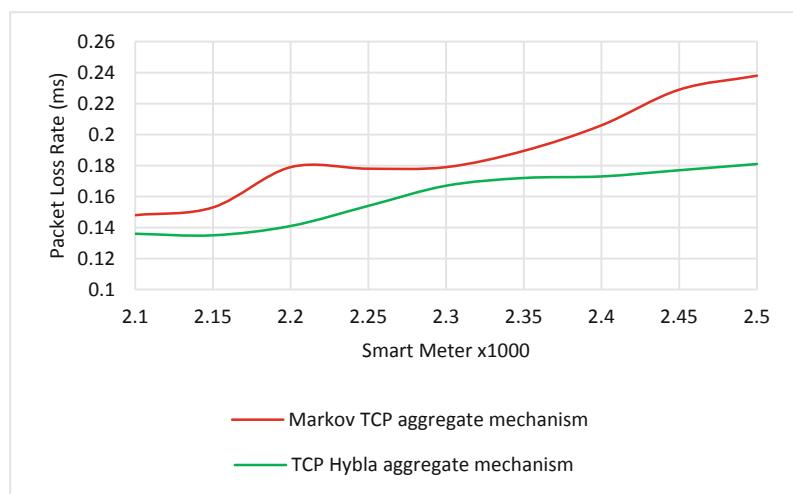
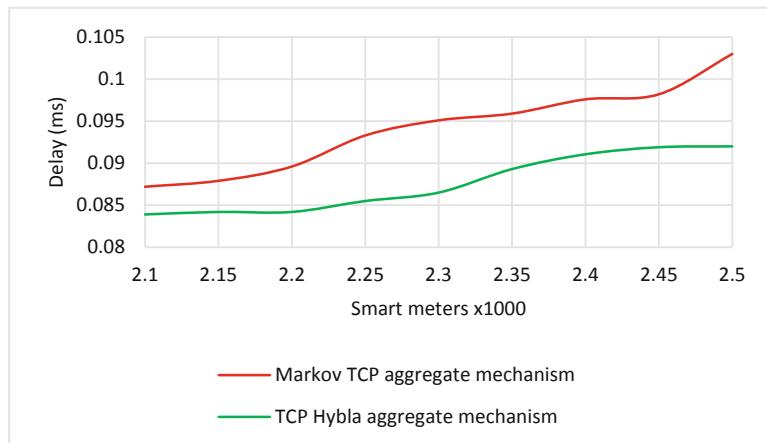


Fig. 6. Packet loss rate

**Fig. 7.** End-to-end delay

5 Conclusions

In this paper, TCP Hybla is used to reduce the communication latency for throughput improvement in SMI. It avoids the congestion, while large number of data is transmitted between smart meters and utility centers i.e. between the providers and users. The performance metrics like throughput, end-to-end delay and packet loss rate shows that the proposed method is optimal than other methods. Further, it is seen that the behavior of TCP Hybla improves the data communication even if there is increased number of meters, varying network settings due to changing infrastructure. The simulation result shows that the proposed SMI TCP Hybla architecture has better performance than existing methods.

References

1. Fang, X., Misra, S., Xue, G., Yang, D.: Smart grid—the new and improved power grid: a survey. *IEEE Commun. Surv. Tutor.* **14**(4), 944–980 (2011)
2. Khalifa, T., Atef, A., Kshirasagar, N., Maazen, A., Amiya, N., Nishith, G.: Design and analysis of split-and aggregated-transport control protocol (SA-TCP) for smart metering infrastructure. In: 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), pp. 139–144. IEEE (2012)
3. Zhang, Y., Rong, Y., Nekovee, M., Liu, Y., Xie, S., Gjessing, S.: Cognitive machine-to-machine communications: visions and potentials for the smart grid. *IEEE Netw.* **26**(3), 6–13 (2012)
4. Wang, W., Yi, X., Khanna, M.: A survey on the communication architectures in smart grid. *Comput. Netw.* **55**(15), 3604–3629 (2011)
5. Gao, J., Xiao, Y., Liu, J., Liang, W., Chen, C.P.: A survey of communication/networking in smart grids. *Future Gener. Comput. Syst.* **28**(2), 391–404 (2012)

6. Kuzlu, M., Pipattanasomporn, M., Rahman, S.: Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **67**, 74–88 (2014)
7. Khalifa, T., Abdrabou, A., Naik, K., Alsabaan, M., Nayak, A., Goel, N.: Split-and aggregated-transmission control protocol (SA-TCP) for smart power grid. *IEEE Trans. Smart Grid* **5**(1), 381–391 (2013)
8. Sood, V.K., Fischer, D., Eklund, J.M., Brown, T.: Developing a communication infrastructure for the smart grid. In: 2009 IEEE Electrical Power & Energy Conference (EPEC), pp. 1–7. IEEE (2009)
9. Fan, Z., Kulkarni, P., Gormus, S., Efthymiou, C., Kalogridis, G., Sooriyabandara, M., Zhu, Z., Lambotharan, S., Chin, W.H.: Smart grid communications: overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **15**(1), 21–38 (2012)
10. Salam, S.A., Mahmud, S.A., Khan, G.M., Al-Raweshidy, H.S.: M2M communication in smart grids: implementation scenarios and performance analysis. In: 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 142–147. IEEE (2012)
11. Fadel, E., Gungor, V.C., Nassem, L., Akkari, N., Malik, M.A., Almasri, S., Akyildiz, I.F.: A survey on wireless sensor networks for smart grid. *Comput. Commun.* **71**, 22–33 (2015)
12. Wierman, A., Osogami, T.: A unified framework for modeling TCP-Vegas, TCP-SACK, and TCP-Reno. In: 2003 11th IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer Telecommunications Systems, MASCOTS 2003, pp. 269–278. IEEE, October 2003
13. Rajiv Suresh, M., Subedha, V.: Realistic technologies and protocols for smart metering infrastructure. *Int. J. Appl. Eng. Res.* **10**(17), 13295–13300 (2015). ISSN 0973-4562
14. Rajiv Suresh, M., Subedha, V.: Optimization of smart metering infrastructure using TCP data aggregation framework. *J. Adv. Res. Dyn. Control. Syst.* **10**(Special Issue 12), 1306–1313 (2018)
15. Rajiv Suresh, M., Subedha, V.: Analysis of transport control protocol mechanism with spanning tree for smart metering infrastructure. In: International Conference on Recent Developments in Computer & Information Technology, Proceedings of 204th The IIER International Conference, Dubai, UAE, 1st–2nd December 2018, pp. 62–66 (2018)
16. Utsumi, S., Zabir, S.M.S., Usuki, Y., Takeda, S., Shiratori, N., Kato, Y., Kim, J.: A new analytical model of TCP Hybla for satellite IP networks. *J. Netw. Comput. Appl.* **124**, 137–147 (2018)
17. Caini, C., Firrincieli, R.: TCP Hybla: a TCP enhancement for heterogeneous networks. *Int. J. Satell. Commun. Netw.* **22**(5), 547–566 (2004)



Enhancing Spectrum Efficiency and Energy Harvesting Selection for Cognitive Using a Hybrid Technique

M. Balasubramanian^{1(✉)}, V. Rajamani², and S. Puspha³

¹ Department of CSE, SPIHER Avadi, Chennai, Tamilnadu, India
baalu_mbs@yahoo.co.in

² Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College,
Chennai, Tamilnadu, India
rajavmani@gmail.com

³ SPIHER Avadi, Chennai, Tamilnadu, India
pusphasangar96@gmail.com

Abstract. Cognitive Radio Networks (CRN) is one of the evolving technologies for detecting available channels automatically in a wireless spectrum in which several researchers have developing new concepts and algorithms to improve its efficiency. Two main issues that are considered to be important in wireless communications are energy effectiveness and spectrum efficiency in which the performance is increased by using CRN as it is compact with both primary user (PU) and secondary user (SU). Both PU and SU are recognized by the licensed and unlicensed bands. In this paper, the hybrid combination of dynamic Genetic Algorithm (GA) with Token Passing Algorithm (TPA) is proposed to enhance the efficiency for accessing the given spectrum for PU and SU. In this proposed work, maximum throughput is achieved by increasing the efficiency of spectrum and improving energy harvesting in channel selection. The collision constraints, energy causality constraints, efficient resource allocation. And sensing occupied channels are considered for average channel capacity for improving throughput performance. The main motivation of this paper is to avoid adjacent channel interference and co-channel interference using the proposed method by achieving energy harvesting and maximum spectrum efficiency for CRN.

Keywords: Cognitive Radio Networks (CRN) · Genetic Algorithm (GA) · Token Passing Algorithm (TPA) · Energy harvesting · Spectrum efficiency

1 Introduction

One of the most emerging trends in today's modern world is a wireless communication system that is a prominent demand for every researcher to find a new scarcity of radio resources. These resources are efficiently utilized by past researches that were proposed several techniques like cooperative communication, cognitive radio, and multi-antenna communication.

1.1 Cognitive Radio Networks (CRN)

CRN is capable of sensing and gathering information like bandwidth, modulation, frequency and power from environment surrounded over it optimal performance that related to the information sensed. Primary Users (PU) are licensed holders that are given by the Federal Communications Commission (FCC) which is a next-generation spectrum access network and CRN is the key enabling technology to efficiently utilize underutilized spectrum. The PU transmission can be protected by switching unoccupied spectra when SU uses the same spectrum opportunistically while a request for access. Severe degradation of throughput can occur in this situation.

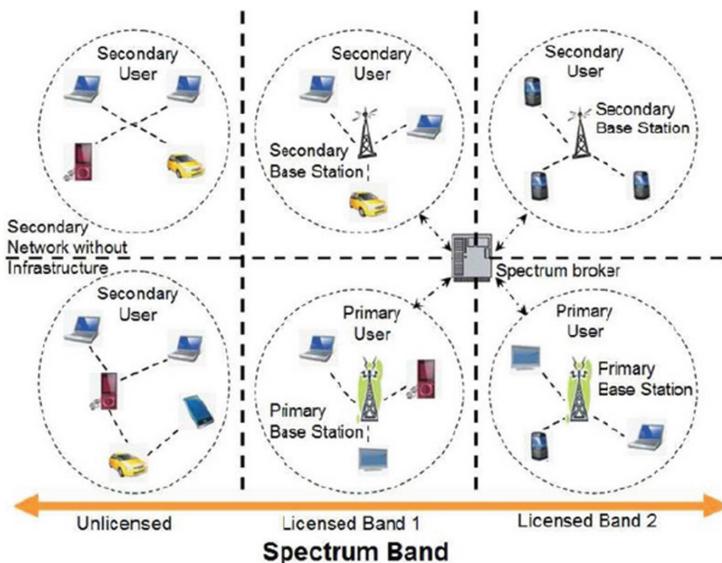


Fig. 1. Architecture of CRN

Figure 1 shows the overall architecture of cognitive radio networks that includes two main network components and these are the primary and secondary network. The primary network consists of primary users and comprises with more than one primary base station, and these are not generally equipped with cognitive radio functions. The existence of PU can be detected and directed to another available band for secondary transmission when sharing its licensed spectrum to primary network in which primary-transmission will not have interfered. Without or with base station, the set of SU are composed in a secondary network which is provided with CR functions, The infrastructure-based cognitive radio network is known as the secondary network that has a base station in which the observations are collected by this that act as hub and each CR-SU performs the result of spectrum analysis and resolve the primary network interference. Figure 2 shows the opportunistic ingress of spectrum usage of frequency bands. A promising solution is offered by the cognitive radio networks for the full

efficient of radio channel resources. The spectrum that is shared between the PU and SU are facilitated by proposing centralized schemes and both distributed that attracted by many researchers.

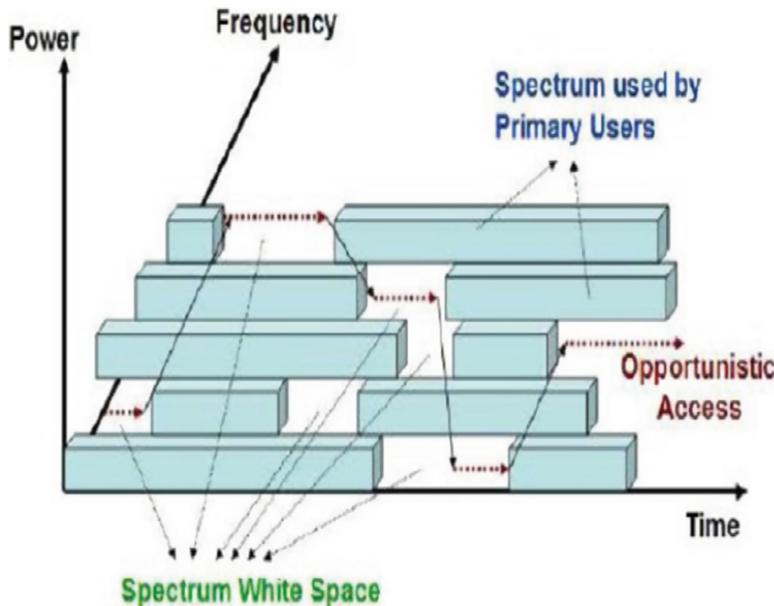


Fig. 2. Spectrum usage for cognitive spectrum user

In summary the contribution of the work is to use hybrid combination of two algorithms namely genetic algorithm (GA) and token pass algorithm for improving the efficiency of spectrum and increase the energy harvesting to avoid the channel and co-channel interference and obtain maximum throughput, This paper is summarized as; Sect. 2 comprises the literature review of the previous techniques used for spectrum analysis and research contributions on energy harvesting in channel selection. Section 3 presents the evaluation of the proposed hybrid model and Sect. 4 explains results and discussions and Sect. 5 concludes this research work.

2 Related Work

Cognitive radio networks are one of the desired communication systems that are used from past decades and some of the important issues that make more complicated that many researchers intend to analyze new techniques to improve the performance. Countless methods were proposed by several researchers to progress and develop spectrum efficiency. Some of the literature reviews for previous research are given detailed. Malik et al. [1] proposed an algorithm of two-stage spectrum sensing in which

the first stage uses energy detection and at the second-stage uses cyclostationary detection. [2] Kokkinen et al. proposed a feature detector that is implemented. Based on autocorrelation for direct current (DC) offset. V. Turunen et al. [3] presented implementation based on FPGA for the cyclostationary feature detector. The detection performance is improved by decimating cyclic spectrum. Also, hybrid architecture is proposed to perform the detection of cyclostationary and energy.

Zhang et al. [4] presented a technique using hop-relay selection and joint power allocation for maximizing end-to-end throughput and power savings are enhanced greatly. Wang et al. [5] proposed a method to void malicious relays using a routing minimized the routing delay. Xu et al. [6] presented a maximization problem of end-to-end throughput in a multi-hop energy harvesting CRN. The power allocation algorithm and joint optimal time show a superiority simulation results in different scenarios when compared with other existing approaches. E. Y. Peh et al. [7] proposed a method for optimizing cooperative sensing based on sensing-time r , k -out- N fusion rule, and k is the fusion parameter that is jointly optimized for maximizing SUs throughput for single channel CR.

J. Lai et al. [8] presented a study of multi-channel CR scenario for maximizing throughput based on OR fusion rule in which energy detection threshold is given to each SU. W. Zhang et al. [9] derived the optimal detection threshold and the optimal number of SU for minimizing missed detection probabilities and total global false alarm. A. D. Firouzabadi and A. M. Rabiei [10] studied the imperfect reporting channels, with multiband CSS in which the error probability is used for missed detection probabilities and false alarm by deriving FC. W. Zhong et al. [11] designed a multi-channel CRNs for its transmission and energy efficient CSS. M. Zheng et al. [10] investigated the detection performance using EE maximization problem for CSS in CSN. The S. States and A. Nallanathan [11] studied a wideband OSA and HSS scheme for working towards periodic throughput maximization and compared by scheming optimal transmit power and optimal sensing time.

Z. Shi et al. [12] designed a power allocation strategy for investigating multi-band HSS CRNs to the minimization of energy consumption problem. G. Ozean et al. [13] developed a power adaptation scheme, with energy-efficient for HSS CR system under the limitations of peak/average interference power and peak/average transmit power. O. Jegede et al. [14] developed a Chaotic Genetic Algorithm (CGA) in which the initial population is generated by using a chaotic sequence and mutation and crossover processed chaos is incorporated. J. Mingjun and T. Huanwen [15] proposed a new chaotic map that is used for CGA for better distribution.

R. Deka et al. [16] sensing optimization using a genetic algorithm in cognitive radio networks. The author optimized the Bit Error Rate (BER) Performance in cognitive radio using the proposed genetic algorithm, Kaur et al. [17] develop Adaptive Genetic Algorithm (AGA) for optimizing QoS parameters in CRN for improving the performance of throughput F. Ye et al. [18] proposed a model that deliberate inference constraints using improved genetic spectrum assignment In this research the computational complexity is reduced by dividing the population of GA into two sets and these are randomly updated spectrum assignment and feasible spectrum assignment. V. Subramanian and S. Rimal [19] presented a comparison of Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) in a dynamic environment in which GA

takes a long time and obtain more operations than PSO. S. Park et al. [20] proposed Partially Observable Marko, Decision Process (POMO) for improving normal aggregate throughput for requiring range detection arrangement and discovered causality limitations impact. S. Park and D. Hon [21] proposed an energy harvesting model in cognitive radio framework for enhancing typical throughput by identifiers distinguishing limit and coordinating the recognize term of the secondary framework.

3 System Model

Here the framework of energy harvesting model is given as shown in Fig. 3. In this framework, the Primary User (PU) and Secondary User (SU) is explained for accomplishing effectiveness of collecting vitality that put away in the which is utilized by the optimal client for getting a chance whenever a primary channel stays without moving from the position.

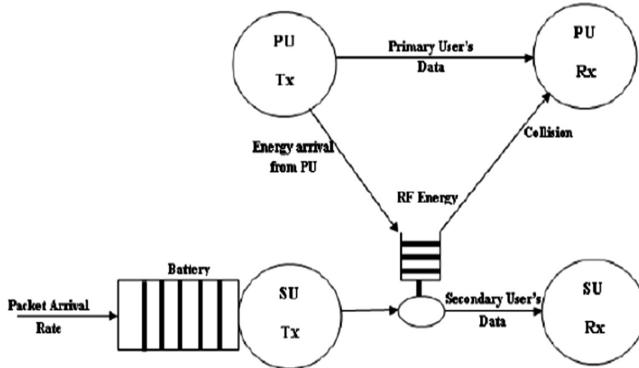


Fig. 3. Energy harvesting in CRN

The correspondence protocol opened for a period to a primary user with span denoted by T and the data transmission is defined as R. The discrete Markov process with time-homogeneous to display channel allocation for PU. The orthogonal frequency division multiplexing (OFDM) is applied for working the channels and denoted as t. The number of distributed sub channels is denoted by D with bandwidth BW_i, where, i = 1, 2, 3...D. Therefore, “0” and “1” represent the slot for spectrum occupancy state that shows occupied or busy. Figure 4 shows the flow chart of the proposed work for the channel allotment between the PU and SU.

The flowchart as shown in Fig. 4 is the processing steps that involve in the hybrid model. In this flow, the genetic algorithm is used for allocating spectrum as it is a heuristic for finding large spaces and can allocate radio channels and can find good solutions and forward a new population to the token passing algorithm for the allotment of channels for the new population that is generated by GA. Using the TPA energy harvesting is done for the primary and secondary user and performed efficiently.

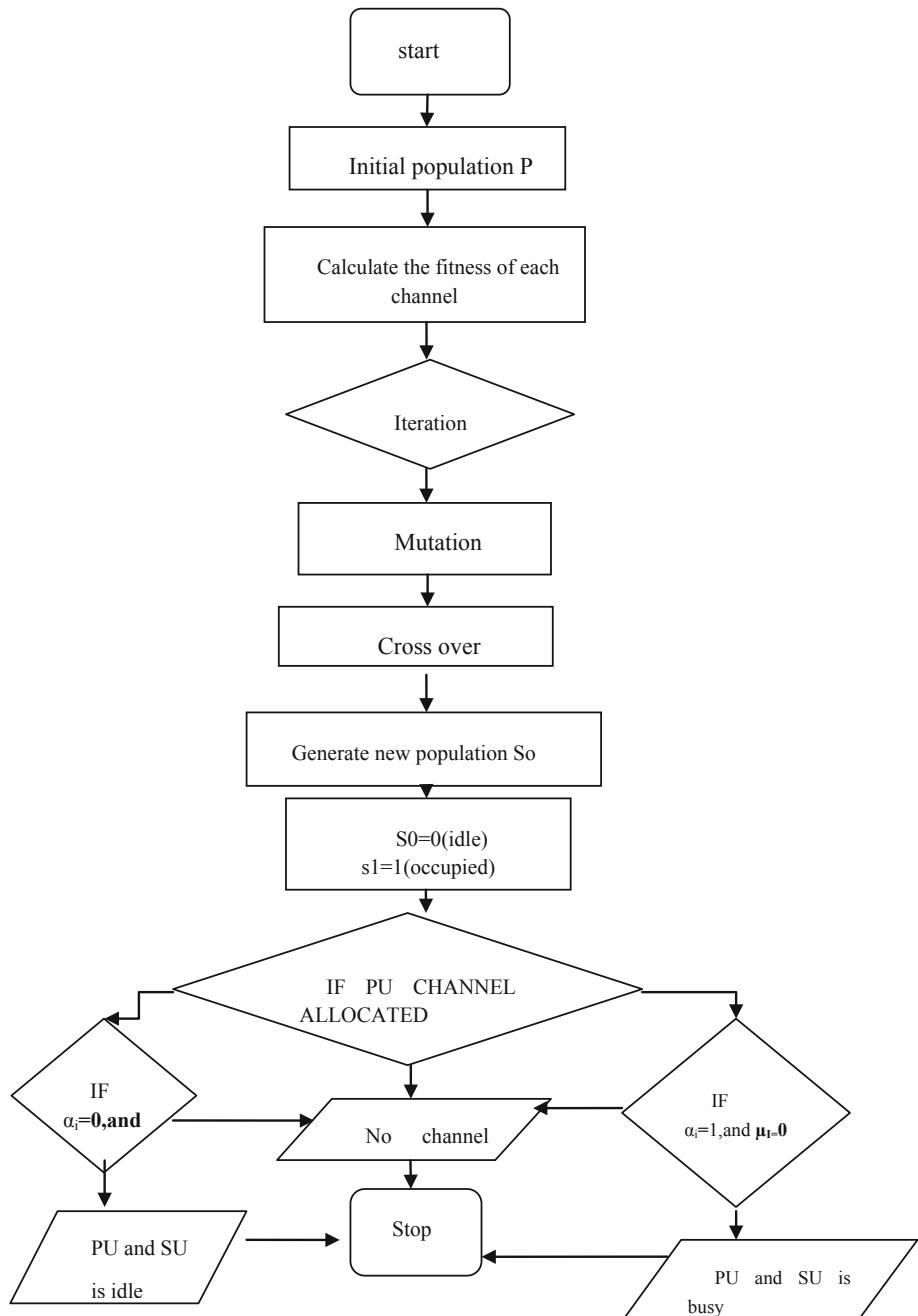


Fig. 4. Flow chart of channel allotment between the PU and SU

3.1 Spectrum and Energy Model

The spectrum allocation is considered as matrix $S = \{S_{ik}\}_{k \times N}$. The efficiency of spectrum allocation is denoted as $S_{ik} = 1$. The user N is assigned with the spectrum band that denoted by k . All the constraints are satisfied by S that is defined by Q , i.e.,

$$S_{i,k} S_{j,k} = 0, \text{ if } Q_{i,j,k} \forall i,j < K, k < N \quad (1)$$

Considering $Z = \{Z_{i,k}\}_{K \times N}$ Which describes the reward when available spectrum band k acquired successfully by the user i . The maximum throughput/acquired can be represented as $z_{i,k}$ and forming the matrix as $T = \{w_{i,k}, Z_{i,k}\}_{K \times N}$ which is a representation of bandwidth or throughput for each channel that is an available to use by each user. The total bandwidth and fitness value for the performance of resource allocation can be expressed as

$$\sum_{i=0}^{m-1} \sum_{k=0}^{n-1} k_i w_i k_z i_k \quad (2)$$

According to α_i , the decision of energy efficiency is taken, E_i^b . Energy cannot be yielded by the secondary user when the primary channel is idle if $\alpha_i = 0$. Hence, $E_i^c = 0$ for this consumed energy. The energy harvesting for the secondary user is done when the primary user is occupied when $\alpha_i = 1$ for the consuming energy C_e so we assume as.

$$C_e = \gamma^e \text{average}, \quad 0 \leq \gamma \leq 1 \quad (3)$$

μ_i is the energy efficiency for the spectrum sense detection. The information can be transmitting or not will be decided by the secondary transmitter with μ_i . The information will be sent by the secondary transmitter when $\mu_i = 0$. The below algorithm shows the hybrid technique for channel allotment using a genetic algorithm and token passing algorithm and at the given time the tokens are allotted.

3.2 GA-TP Algorithm

Step 1: Given the size of population and number of chromosomes as c

Step 2: Max generation is obtained

Step 3: Let initial population $P^k = \{p_1^k, p_2^k, \dots, p_c^k\}$

Step 4: Fitness calculation (P_i^k), for $i = 1, \dots, |c|$;

Step 5: Randomly chromosomes picked P_a and P_b from P^{k-1} .

Step 6: Crossover P_a^{new} and P_b^{new} .

Step 7: Mutate with probability P_m .

Step 8: Insert P_a^{new} and P_b^{new} .

Step 9: Repeat until termination criteria met.

Step 10: Return new population

Step 11: TPA(P^{new});

Step 12: Flag = {True, False}

Step 13: $P^{\text{new}} \leftarrow \{E_i^b, \alpha_i, \mu_i\}$

- Step 14: If channel allocated to PU
 Step 15: Flag = True;
 Step 16: Then $\alpha_i = 1$ and $\mu_i = 0$
 Step 17: PU will be busy (1)
 Step 18: Else
 Step 19: Flag = False;
 Step 20: Then $\alpha_i = 0$ and $\mu_i = 0$
 Step 21: No energy allocated
 Step 22: PU = Channel if Flag = False
 Step 23: Wait for a change of Flag = False
 Step 24: Else
 Step 25: Channel assigned to SU
 Step 26: Repeat Step 13 until stopping criteria met
 Step 27: Update Energy based on the assigned channel as E_i^b

The algorithm shows the process of GA and TPA for allocating a channel and obtains the energy for each selection. The initial population is obtained as input for the GA to process the fitness of each node that requires each channel obtain the crossover with a new mutation probability and obtained a new allocation as P^{new} . The termination condition for the GA is the iteration process that given and set up a new population and used for TPA to allocate the channels for the primary user (PU). The population that obtained from GA is considered as initial for TPA and considered energy E_i^b with α_i and μ_i as spectrum state and sense detection. Idle and occupied are the two states used in TPA for allocating the channels. If PU gets the token and allocates channel then SU will harvest die energy and wait until the allotment of channels. The SU will get the token and channel is allotted when PU is idle.

4 Results and Discussion

Table 1 shows the framework parameter used for the simulation. The transfer speed for the communication is denoted as T and energy is represented as E. S_o and S_1 is represented for the probability of state transition that as busy-to-idle and idle-to-busy. The collision of target probability is 0.1.

Table 1. Framework parameters

Description	Symbol used	Given value
Data transmission	T	2 MHz
Idle state for PU	Π_i	0.5
The probability of state transmission	S_0, S_1	0.2
Space term	B	100 to 150 ms
Duration for sensing	β_s	1.5 ms
Capacity of battery	B	100 units
Energy at initial	E_0	0 units
Energy for sensing	E_s	1 unit
Energy transmit	E_t	3 units

Figure 5 shows the Energy Harvesting done by secondary unit (SU) in which maximum throughput is achieved when the probability is between the value 0.4 to 0.8 and the arrival rate of energy will be increasing until the determined value is distributed. Once the optimal value is reached, the reliable throughput will be rising with energy harvesting with having a bandwidth of 2 MHz.

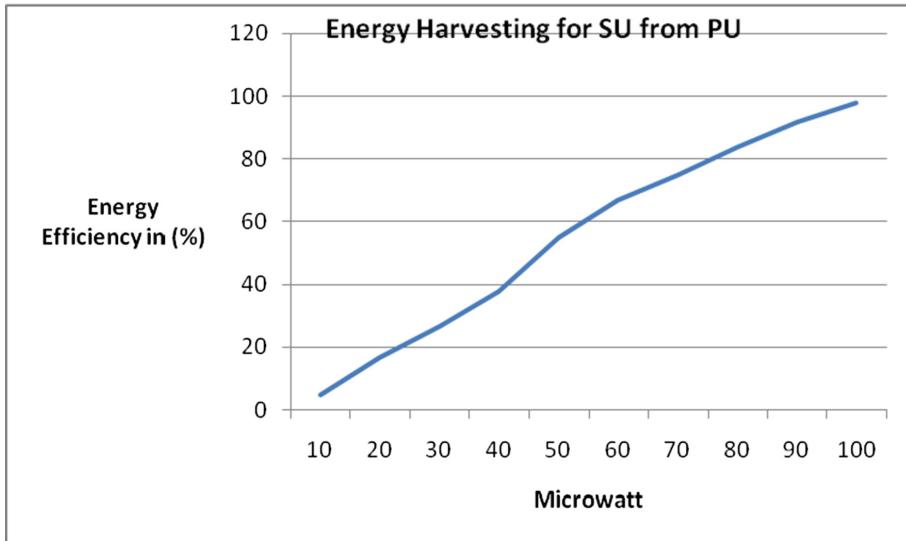


Fig. 5. Energy harvesting for SU from PU

The power transmission is used for energy harvesting that represented in Watts. When transmission occurs by the primary user it is compared with the percentage of battery that energy stored in it. The SU will use stored energy when PU becomes idle. Using 950 MHz band, the power transmission will range from 1 W to the maximum of 4 W for a dedicated RF sources and each transmission will obtain $0\mu\text{W}$. The graph shows the energy efficiency between 10% to 100% and Microwatts of 10 to 100 μW . The energy efficiency and energy-stored could increase from 10% to 95% when the power usage and number of transmission increase.

Figure 6 shows the throughput comparison of the secondary user with the primary user. The PU and SU are compared in terms of time and throughput using the proposed technique. For certain timings. The PU and SU obtain throughput from 0.5 bps to 10 bps with starting time from 0 s to 10 s. Figure 7 shows the overall performance compared with other existing approaches. Here, FDMA, TPA, and Suboptimal are used for the comparison with the proposed technique. The probability of each nodes energy is calculated in terms of throughput and the proposed GA-TPA algorithm shows the better performance.

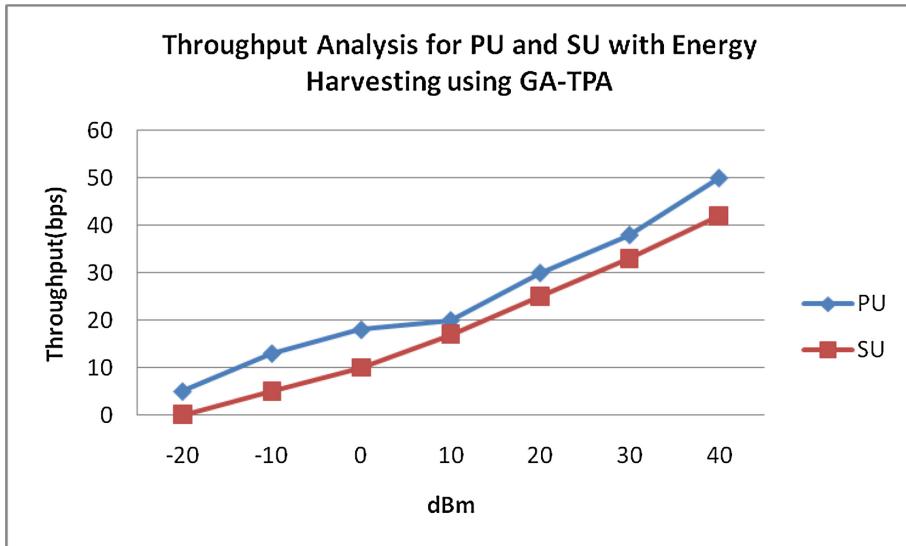


Fig. 6. Throughput analysis for PU and SU

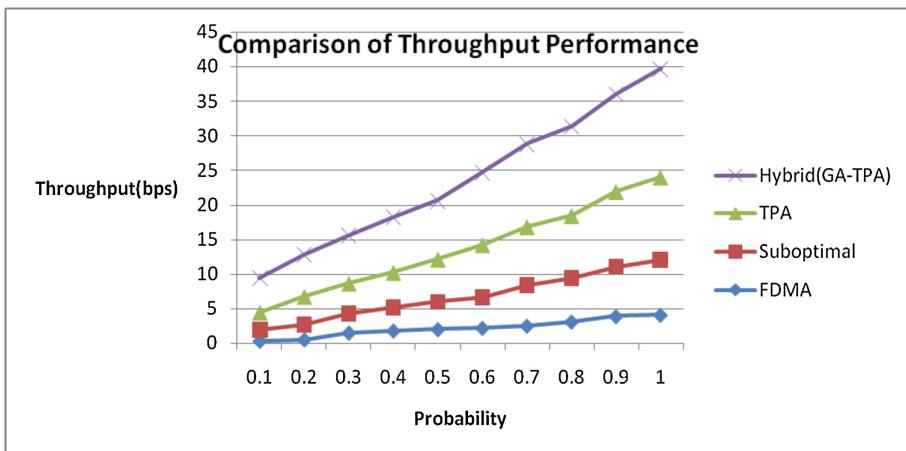


Fig. 7. Throughput comparison with existing approach

Figure 8 shows the number of channels that are allotted to the primary user and secondary user for the proposed hybrid model. In this graph, 10 channels are allotted for consideration in which the primary user will have a minimum number of channels in the first condition. The secondary user will be allotted with the channels when the PU gets idle. Furthermore, 10 ms are used by PU for the transmission while Su uses only 5 ms with sensing duration of the channel also have 5 ms. Hence the SU will get an increase in a number of channels as the time increasing and by the simulation result,

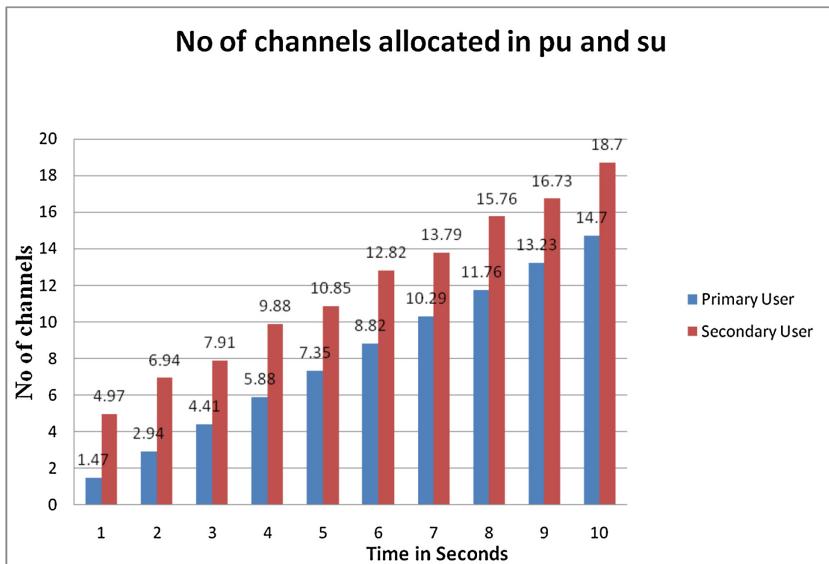


Fig. 8. Channels allocated in PU and SU.

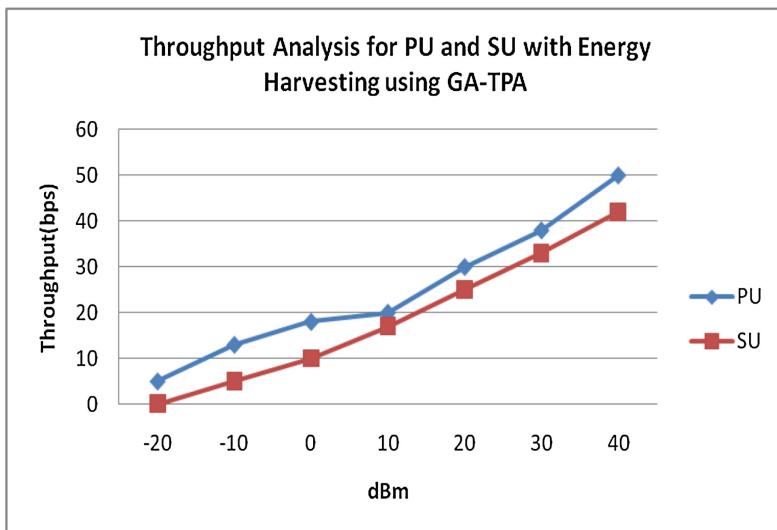


Fig. 9. Throughput analysis

it has been noted that SU will have a number of channels than PU. Figure 9 shows the analysis of throughput for PU and SU from the energy harvesting in which the transmitting of power is calculated in terms of dBm that differs from -20 to 40 which is equivalent to 4 W.

5 Conclusion

In this paper, a hybrid GA-TPA method is proposed for the channel allocation problem and Energy Harvesting in the selection of channels. Here, the spectrum is allotted in a proper manner for both PU and SU for improving the efficiency of allocation and energy harvesting. Using idle and busy state for the SU and PU the allotment of channel performed efficiently. From the experimental results, the optimal solution is obtained by GA-TPA for channel allocation problem and finding energy harvesting of each channel in real-time for CRN. The proposed algorithm shows a better improvement by satisfying the demands of CRN.

References

1. Maleki, S., Pandharipande, A., Leus, G.: Energy-efficient distributed spectrum sensing for cognitive sensor networks. *IEEE Sens. J.* **11**(3), 565–573 (2010)
2. Kokkinen, K., Turunen, V., Kosunen, M., Chaudhari, S., Koivunen, V., Ryyynänen, J.: On the implementation of autocorrelation-based feature detector. In: 2010 4th International Symposium on Communications, Control and Signal Processing, ISCCSP 2010, Limassol, Cyprus, 3–5 March 2010, pp. 1–4. IEEE (2010). (978-1-4244-6287)
3. Do, T., Mark, B.L.: Improving spectrum sensing performance by exploiting multiuser diversity. InTech (2012). (978-953-51-0268-7)
4. Alghamdi, O.A., Ahmed, M.Z.: New optimization method for cooperative spectrum sensing in cognitive radio networks. In: IEEE Conference (2011)
5. Peh, E.C., Liang, Y.C., Guan, Y.L., Zeng, Y.: Cooperative spectrum sensing in cognitive radio networks with weighted decision fusion schemes. *IEEE Trans. Wirel. Commun.* **9**(12), 3838–3847 (2010)
6. Lee, S., Zhang, R.: Cognitive wireless powered network: spectrum sharing models and throughput maximization. *IEEE Trans. Cogn. Commun. Network.* **1**(3), 335–346 (2015)
7. Yang, C., Li, J., Guizani, M., Anpalagan, A., Elkashlan, M.: Advanced spectrum sharing in 5G cognitive heterogeneous networks. *IEEE Wirel. Commun.* **23**(2), 94–101 (2016)
8. Lu, X., Wang, P., Niyato, D., Hossain, E.: Dynamic spectrum access in cognitive radio networks with RF energy harvesting. *IEEE Wirel. Commun.* **21**(3), 102–110 (2014)
9. Lee, S., Zhang, R., Huang, K.: Opportunistic wireless energy harvesting in cognitive radio networks. *IEEE Trans. Wirel. Commun.* **12**(9), 4788–4799 (2013)
10. Yuan, F., Zhang, Q.T., Jin, S., Zhu, H.: Optimal harvest-use-store strategy for energy harvesting wireless systems. *IEEE Trans. Wirel. Commun.* **14**(2), 698–710 (2014)
11. Ku, M.L., Li, W., Chen, Y., Liu, K.R.: Advances in energy harvesting communications: Past, present, and future challenges. *IEEE Commun. Surv. Tutor.* **18**(2), 1384–1412 (2015)
12. Pappas, N., Jeon, J., Ephremides, A., Tragantzis, A.: Optimal utilization of a cognitive shared channel with a rechargeable primary source node. *J. Commun. Netw.* **14**(2), 162–168 (2012)
13. Sultan, A.: Sensing and transmit energy optimization for an energy harvesting cognitive radio. *IEEE Wirel. Commun. Lett.* **1**(5), 500–503 (2012)
14. Park, S., Kim, H., Hong, D.: Cognitive radio networks with energy harvesting. *IEEE Trans. Wirel. Commun.* **12**(3), 1386–1397 (2013)
15. Park, S., Hong, D.: Optimal spectrum access for energy harvesting cognitive radio networks. *IEEE Trans. Wirel. Commun.* **12**(12), 6166–6179 (2013)

16. Chung, W., Park, S., Lim, S., Hong, D.: Spectrum sensing optimization for energy-harvesting cognitive radio systems. *IEEE Trans. Wirel. Commun.* **13**(5), 2601–2613 (2014)
17. Park, S., Hong, D.: Achievable throughput of energy harvesting cognitive radio networks. *IEEE Trans. Wirel. Commun.* **13**(2), 1010–1022 (2014)
18. Dhillon, H.S., Li, Y., Nuggehalli, P., Pi, Z., Andrews, J.G.: Fundamentals of heterogeneous cellular networks with energy harvesting. *IEEE Trans. Wirel. Commun.* **13**(5), 2782–2797 (2014)
19. Niyato, D., Wang, P., Kim, D.I.: Channel selection in cognitive radio networks with opportunistic RF energy harvesting. In: Proceedings IEEE International Conference Communication (ICC), Sydney, NSW, Australia, pp. 1555–1560 (2014)
20. Yin, S., Zhang, E., Yin, L., Li, S.: Optimal saving-sensing-transmitting structure in self-powered cognitive radio systems with wireless energy harvesting. In: Proceedings of IEEE International Conference on Communication (ICC), Budapest, Hungary, pp. 2807–2811 (2011)
21. Gao, X., Xu, W., Li, S., Lin, J.: An online energy allocation strategy for energy harvesting cognitive radio systems. In: International Conference Wireless Communication, Signal Processing (WCSP), Hangzhou, China, pp. 1–5 (2013)
22. Liang, Y.C., Zeng, Y., Peh, E.C., Hoang, A.T.: Sensing-throughput tradeoff for cognitive radio networks. *IEEE Trans. Wirel. Commun.* **7**(4), 1326–1337 (2008)
23. Cui, S., Goldsmith, A.J., Bahai, A.: Energy-constrained modulation optimization. *IEEE Trans. Wirel. Commun.* **4**(5), 2349–2360 (2005)
24. Liu, C., Mou, Y., Pan, C.: Optimization of power allocation in wireless cooperative communication system. In: AIP Conference Proceedings, vol. 1839, no. 1, p. 020185, May 2017
25. Suliman, R.A.H., Bilal, K.H., Elemam, I.: Review paper on cognitive radio networks. *J. Electr. Electron. Syst. Open Access J.* **7**(1), 1000252 (2018)
26. Elhachmi, J., Guennoun, Z.: Cognitive radio spectrum allocation using genetic algorithm. *EURASIP J. Wirel. Commun. Netw.* **2016**(1), 133 (2016)
27. Rathee, M., Kumar, S.: Quantum-inspired ant-based energy balanced routing in wireless sensor networks. *Recent Pat. Comput. Sci.* **10**(1) (2017)



Maximize Body Node's Lifetime Through Conditional Re-transmission

J. Karthik^{1(✉)} and A. Rajesh²

¹ CSE Department, St. Peter's Institute of Higher Education and Research,
Chennai 600054, India

karthikvalavan@gmail.com

² C. Abdul Hakeem College of Engineering and Technology,
Vellore 632509, TN, India
amrajesh73@gmail.com

Abstract. Wireless Sensor Network is greatly evolved in recent years. Technological advancements in wireless networks are intended to develop various fields especially in medical domain. Nowadays, remote health monitoring is possible by the enormous growth of wireless body area sensor networks. The Wireless Body Area Sensor Network monitors the human health by using wearable body sensors, and sends the status of the human health to the medical experts. Body nodes will be placed on, in and around the human body. The major key issue in Wireless Body Area Sensor Network is power management. Since batteries used in sensors are very tiny, it tends to have a minimal lifetime. In order to increase the lifetime of the sensor node, the energy needs to be utilized in an efficient manner. In this paper we have proposed conditional re-transmission technique to minimize the energy consumption. So the sensor nodes lifetime will get increased and in turn Wireless Body Area Sensor Networks lifetime will also be increased. By increasing the lifetime of the sensor nodes, the batteries or sensor nodes need not to be replaced frequently.

Keywords: Remote health monitoring · Wireless Body Area Sensor Network · Network lifetime · Energy consumption · Conditional re-transmission

1 Introduction

A Wireless Body Area Sensor Network (WBASN) is a network of small sensor devices called body nodes placed on, in and around the human body. The major concern of designing the body node is energy consumption. The major components that consume more energy in the node are the Microprocessor, the Sensing Device and Transceiver. The power consumption can be calculated in the microprocessor by correlated with the voltage supply, frequency of clock, period to perform task and the power saving features that are being implemented in the processor. The energy consumption of the Transceiver includes the amount of data that is being transferred, the distance between the nodes and the energy required for the RF Circuitry. In the same way sensing device consume the energy for sensing circuitry and energy required for sensing a bit of information [1].

Energy efficiency is the major serious issue to be concentrated at together the node and the network. Energy consumption can greatly be reduced by many ways such that reducing the number of components, increasing the battery capacity, reducing the transmission distance, implementing the effective routing protocol, and so on. In this paper we proposed conditional retransmission technique to reduce the energy consumption of the node. The heart of the wireless sensor node is the microprocessor. The processor will be connected with sensors through Analog to Digital Converters. The sensing unit will sense the value and send it to the transceiver. This transceiver unit transmits the data to the medical experts via access point. The data will be analyzed by the medical practitioner and they reply with necessary actions. The Fig. 1 refers to architecture diagram of sensor node.

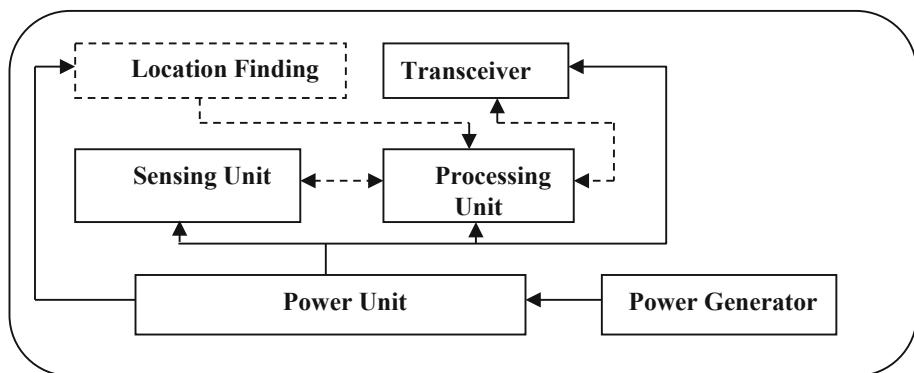


Fig. 1. Architecture diagram of sensor node

In this paper we discussed about the introduction of Wireless Body Area Sensor Networks in first chapter. The background and motivation from the related papers and observations of past findings will be discussed in next chapter. Subsequent chapters will discuss about the detailed concept of conditional retransmission technique, followed by the result and discussion, conclusion and future enhancement.

2 Background and Motivation

M-ATTEMPT a new routing protocol is a thermal aware protocol. This protocol helps to transfer the data away from the hot-spot link to avoid more energy consumption [2]. Cluster Head will be formed to reduce the energy consumption, and also discussed various protocols such as LEACH, PEGASIS, TEEN, SEP and so on [3]. Applications of WBASN widely grown-up for various treatments cancer detection, asthma, sleep staging, cardiovascular diseases. These can be monitored with the help of either Implant WBAN or Wearable WBAN [4]. It also discusses about power consumption, data rate and duty cycle of various sensor nodes. The types of network topology also influence the energy consumption of the node. Intra and Inter WBAN Communication

will be secured with the help of cluster based hybrid security framework. The cluster information process itself secured by using key agreement scheme [5]. Energy wastages occur mainly due to idle listening, collision, over hearing and over emitting. General technique for reducing energy consumption is duty cycling that is making the node to sleep when there is no need of monitoring the values. With this power consumption can be greatly reduced. Various MAC Protocols were discussed in order to avoid energy wastages [6].

Power consumption can be reduced by decreasing the coverage area and decreasing the distance between the sensor and access point. But number of nodes has to be increased to cover all area [7]. Sleep wake up protocols are used for reduce the energy consumption, and design of hardware components plays major role in reduction of power consumption. Low energy wake up receiver can be used to minimize energy utilization [8]. There are two techniques to reduce the energy indulgence of the processor components of sensor nodes are silent-store filtering Mote Cache and Content Aware Data Management (CADMA) [9]. Energy efficiency can be improved by data transmission via relay nodes. If the source node is not able to communicate directly with destination node then relay nodes can be used to transmit the data without any loss, and also it increase the energy efficiency in turn it reduce the power consumption [10].

Energy consumption is greatly reduced with the help of sleep awake algorithm that further reduces the energy utilization using on demand sleep awake algorithm and cyclic sleep algorithm [11–13]. Utilization of power is very much decreased via avoiding the transmission of surplus data and conditionally re-transmitting the unwanted data [14, 15]. Data transmission is trustworthy with the framework approach [16–18]. The hybrid trust scheme method is introduced to provide reliability and security [19]. Context aware trust model created to ensure the trustworthiness of the sensor networks, also discussed the ontology based model for the reliability of the data. Different trust supervision techniques were discussed also the major challenges that are involved in the sensor network and the issues related with the reliability of the sensor network.

3 Proposed Work

In this paper we proposed conditional re-transmission technique to minimize the energy consumption. Since data are sent to access point frequently from the sensor node, it has to spent more energy for the transmission of data each time. There will be possibility for loss of data due to physical obstacles between node and access point such as furniture, wall, etc. In such a case body node needs to resend the data. Similarly if the node sends the same data again and again, then energy will be consumed more by the sensor node, and in turn the lifetime of the node and also lifetime of the network will get decreased. We implement conditional re-transmission approach, in which body node resends the data for failed delivery only if it is above or below threshold value. Here threshold value represents the acceptable level of the particular sensor node. The energy consumed by the individual components of the sensor node is displayed in below Table 1.

Table 1. Energy consumed by individual sensor components

Components	State	Values (units)
Microprocessor	Active	6 mA
	Sleep	8 μ A
Radio transceiver	Active	20 mA
	Sleep	2 μ A
Memory	Active	19 mA
	Sleep	2 μ A
Sensor board	Active	5 mA
	Sleep	2 μ A

3.1 Mathematical Model

Since transmission of data takes more energy than calculation by the processor, rather sending the value to access point can check the value in the node itself. So that the energy will be reduced greatly, and only when there is need for sending data due to unacceptable level, then the data can be transmitted to medical practitioner through access point. This mathematical model clearly explains the energy consumption which takes by the components is being evidence for.

The energy level of the node can be calculated as below

$$E_{\text{node}} = E_{\text{Components}} * \text{Time} \quad (1)$$

Where

E_{node} – Energy level of the node

$E_{\text{Components}}$ – Energy level of individual components of the sensor node

Time – Duration of sensor node in active state

The energy level of the components of sensor node will be calculated by Eq. 2

$$E_{\text{Components}} = E_{\text{sensor}} + E_{\text{Transmitter}} + E_{\text{Receiver}} + E_{\text{Processor}} + E_{\text{Memory}} \quad (2)$$

Substitute Eq. 2 in 1

$$E_{\text{Active}} = [E_{\text{sensor}} + E_{\text{Transmitter}} + E_{\text{Receiver}} + E_{\text{Processor}} + E_{\text{Memory}}] * \text{Time} \quad (3)$$

Where

E_{sensor} – Energy consumed by the sensor unit

$E_{\text{Transmitter}}$ – Energy consumed for Transmitter unit

E_{Receiver} – Energy consumed by Receiver unit

$E_{\text{Processor}}$ – Energy consumption by the Processor unit

E_{Memory} – Energy consumed for Memory unit

Individual components of the body node will perform different task. It consumes different energy levels to perform basic operations. All the components together will decide the lifetime of the body node and lifetime of network based on battery capacity of the sensor node.

$$\text{Energy} = \text{Power} * \text{Time} \quad (4)$$

$$\text{Energy} = (\text{current} * \text{Voltage}) * \text{Time} \quad (5)$$

Where power can be calculated as current * Voltage

$$E_{\text{sensor}} = E_{\text{sensordevice}} * F \quad (6)$$

From Eq. 6 Energy for Sensor device can be calculated together with the power supply needed by the sensor board device and frequency which is number of times sensing the value

$$E_{\text{transmit}} = E_{\text{transmitter}} * k * d \quad (7)$$

To transmit the data, the energy will be obtained with the help of Eq. 7, the power needed for transmitter board, k represents number of bits, d represents the distance between the source place and the destination place.

$$E_{\text{Receive}} = E_{\text{Receiver}} * k \quad (8)$$

From Eq. 8 energy of receiving data will be calculated. E_{Receiver} represents the power supply needed by the receiver board, and k represents number of bits received.

$$E_{\text{Process}} = E_{\text{Processor}} * k * \text{Time} \quad (9)$$

By substituting Eqs. 6, 7, 8 and 9 in Eq. 3 will get the below equation that helps to find the total energy consumed by the active sensor device for a particular time. Energy level of the body node can be calculated by

$$E_{\text{Node}} = E_{\text{Idle}} + E_{\text{Sleep}} + E_{\text{Active}} \quad (10)$$

From Eq. 10 Energy level of the sensor node will be obtained by all the states of the sensor node. When Sensor node in active state it consume more energy, whereas while in idle state it consume less energy, but when it is sleep state it do not consume energy. By combining all these three states the energy level of the particular node can be calculated.

3.2 Processor Model

The Processor will be consumed more energy when it is keep on changing its state. The Fig. 2 represents the energy required or consumed by the processor when it is shifting from one state to another state [3].

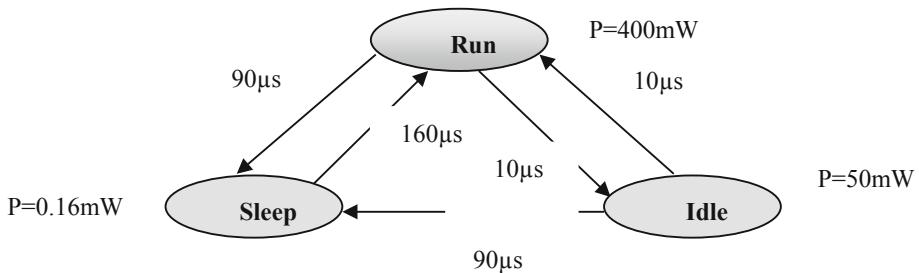


Fig. 2. Energy consumption and time taken for state transition of ARM SA-1100

3.3 Conditional Re-transmission Approach

Discovering the method to decrease the utilization of power or scavenging the power from other sources or reinstate the batteries either it can rechargeable or new batteries are the ways that helps to sustain the power supply of the batteries in sensor nodes. In this paper we proposed an approach to minimize the number of transmissions that helps to reduce the energy consumption of the sensor nodes. Though energy minimization essential, it is necessary that the data should not be lost at any cost (Fig. 3).

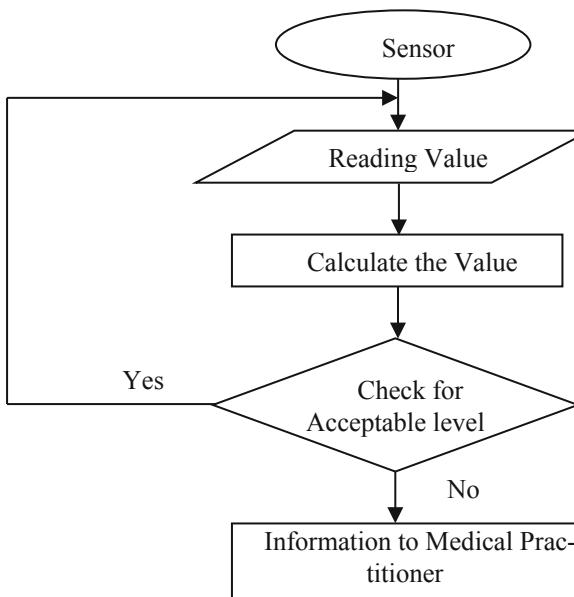


Fig. 3. Data flow diagram of conditional re-transmission approach

Reducing the transmission of unwanted data will increase the network lifetime. So the operation can be performed in the sensor node itself. Sensor node will take more power for transmitting and receiving than computation. The data can be sensed by the sensors and can be calculated within the sensor nodes and if the values are the above or below threshold value then the node can transmit the data to Medical Practitioner through access point. Effective utilization of the energy of the sensor nodes by means of reduces the transmitting power and the total number of transmission. The below flowchart will explain our proposed approach which will effectively utilize the energy and increase the lifetime of the node.

4 Results and Discussion

This conditional re-transmission technique will be applied in real time wireless body area sensor network system. Figure 4 shows that difference between the power consumption by normal transmission method and conditional transmission method of the sensor node. In Figs. 4 and 5 More refers to the data sent by the sensor node is very often (i.e.) more fluctuation in the pulse rate so that data transmitted once per minute, and average is five to ten minute once data has been transferred, and best case is data transferred from the node once for every fifteen minute. From this the life time of the node is increased and pointed out in Fig. 5 which indicates the comparison of the node's life time of normal transmission with conditional transmission.

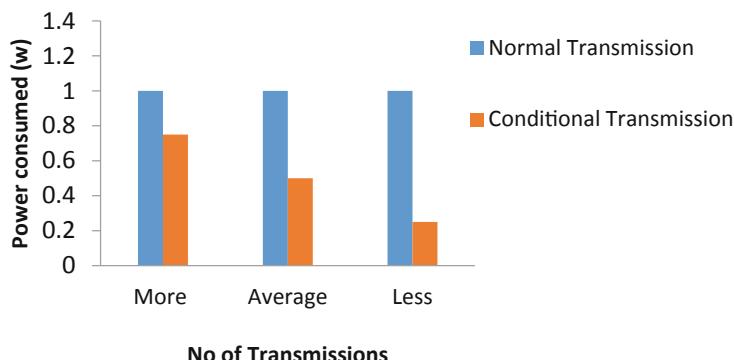


Fig. 4. Power consumption of normal transmission vs conditional transmission

The data transmitted with the bit rate of 10 kbps. Transmission power as a whole takes 5 mW. The distance between the body node and access point is around 5 m. The total Power consumption and energy consumption are 0.5 W and .02 J respectively. Number of transmissions is always same in normal transmission, where as in conditional transmission the number of transmission will be reduced, so that the power consumption also greatly reduced while compares with normal transmission in turn life time also will be increased by conditional transmission.

Figure 6 shows that the frequency of transmission will always remain same as its transmission gap is fixed, but in conditional transmission number of transmission is reduced since transmission of data takes place only on demand. The data transmitted is mentioned in hundreds on hourly basis. In case of conditional transmission takes place only if there is need, so the frequency of transmission is reduced as shown in Fig. 5. Energy consumed by the components of sensor node is described in Figs. 7 and 8. In normal transmission the node will spend more energy for transmission rather calculation, where as in conditional transmission the energy consumed more for processing instead of transmitting. This may vary when the frequency of transmission increased based on human health condition. If it increases then the energy consumption for transmitting will get increased proportionately.

Conditional transmission in the body node greatly reduced power consumption and increased its life time. When the energy consumed more by transmission then the battery capacity will be reduced and conditional transmission utilize the energy effectively so that its life time increased as shown in Fig. 5.

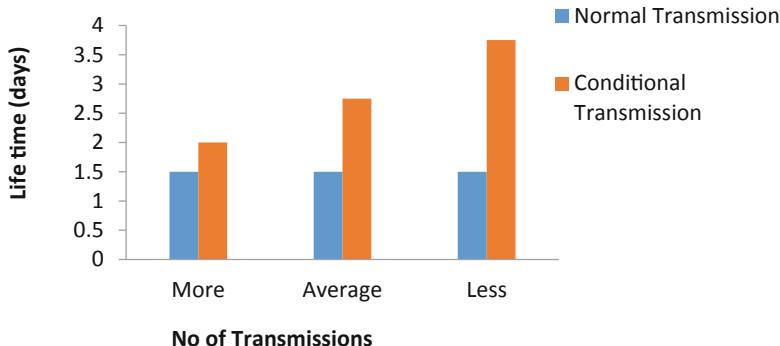


Fig. 5. Lifetime of sensor node from normal transmission vs conditional transmission

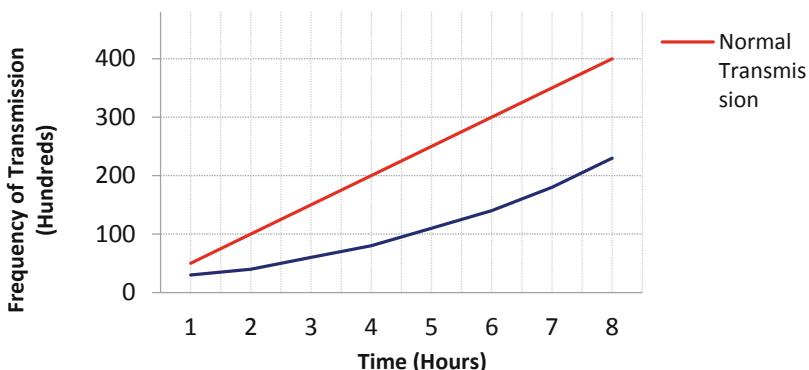


Fig. 6. Frequency of transmissions by normal and conditional transmission

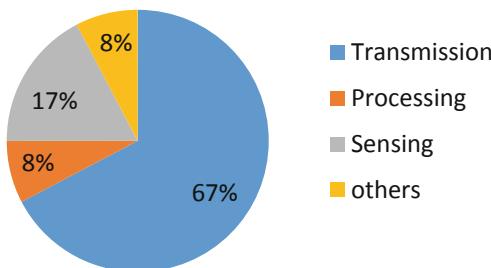


Fig. 7. Energy consumed by normal transmission

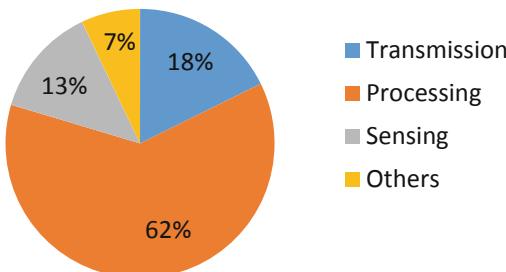


Fig. 8. Energy consumed by conditional transmission

5 Conclusion and Future Enhancement

Even though many resources available in the medical field must ensure that the resources are utilized effectively. We proposed conditional re-transmission technique for the effective utilization of energy in the wireless body nodes. Our proposed technique increases the lifetime of the body node and network. Since energy consumption is minimized, the replacement of the body nodes need not be done very often. This technique may be further developed to implement the accuracy level of the data and reliability of data transmission. Because body nodes deals with serious issues like human health it must be reliable, more secure and fast transmission. Further development can be concentrated on fast and reliable transmission.

References

1. Dimitriou, G., Kikiras, P.K., Stamoulis, G.I., Avaritsiotis, I.N.: A tool for calculating energy consumption in wireless sensor networks. Research Gate Publication
2. Zavaid, N., Abbas, Z., Fareed, M.S., Khan, Z.A., Alrajeh, N.: M-ATTEMPT: a new energy efficient routing protocol for wireless body area sensor networks. In: The Fourth International Conference on Ambient Systems, Networks and Technologies. ScienceDirect (2013)
3. Raghatare, M., Wajgi, D.W.: An energy saving algorithm to prolong the lifetime of wireless sensor network. Int. J. Wirel. Mob. Netw. **6**(5), 33 (2014)

4. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., Jamalipour, A.: Wireless body area networks: a survey. *IEEE Commun. Surv. Tutor.* **16**(3), 1658–1686 (2014)
5. Ali, A., Khan, F.A.: Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP J. Wirel. Commun. Netw.* **2013**(1), 216 (2013)
6. Rezaei, Z., Mobicinejad, S.: Energy saving in wireless sensor networks. *Int. J. Comput. Sci. Eng. Surv.* **3**(1), 23 (2012)
7. Sharma, A., Shinghal, K., Srivastava, N., Singh, R.: Energy management for wireless sensor network nodes. *Int. J. Adv. Eng. Technol.* **1**(1), 7 (2011)
8. Thattil, W.C.V., Vasantha, N., Esther Rani, T.: Spread spectrum based energy efficient wireless sensor networks. *ACEEE Int. J. Netw. Secur.* **1**(2) (2010)
9. Küçük, G., Basaran, C.: Reducing energy consumption of wireless sensor networks through processor optimizations. *J. Comput.* **2**(5), 67–74 (2007)
10. Paulus, R., Singh, G., Tripathi, R.: Energy efficient data transmission through relay nodes in wireless sensor networks. *ACEEE Int. J. Netw. Secur.* **3**(1) (2012)
11. Karthik, N., Ananthanarayana, V.S.: Data trust worthiness in wireless sensor networks. In: Trustcom/BigDataSE/ISPA. IEEE (2016)
12. Karthik, N., Ananthanarayana, V.S.: Data trust model for event detection in wireless sensor networks using data correlation techniques. In: 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN) (2017)
13. Karthik, N., Ananthanarayana, V.S.: A hybrid trust management scheme for wireless sensor networks. *Wirel. Pers. Commun.* **97**(4), 5137–5170 (2017)
14. Karthik, N., Ananthanarayana, V.S.: Context aware trust management scheme for pervasive healthcare. *Wirel. Pers. Commun.*, 1–39 (2018)
15. Karthik, N., Ananthanarayana, V.S.: An ontology based trust framework for sensor-driven pervasive environment. In: 2017 Asia Modelling Symposium (AMS), pp. 147–152. IEEE, December 2017
16. Dhulipala, V.S., Karthik, N.: Trust management technique in wireless sensor networks: challenges and issues for reliable communication: a review. *CSI Trans. ICT* **5**(3), 281–294 (2017)
17. Kumar Raja, D.R., Pushpa, S.: Novelty-driven recommendation by using integrated matrix factorization and temporal-aware clustering optimization. *Int. J. Commun. Syst.* (2018)
18. Raja, D.K., Pushpa, S.: Diversifying personalized mobile multimedia application recommendations through the Latent Dirichlet Allocation and clustering optimization. *Multimedia Tools Appl.* **78**, 24047–24066 (2019)
19. Jayagopi, G., Pushpa, S.: Arrhythmia classification based on combined chaotic and statistical feature extraction. *Indones. J. Electr. Eng. Comput. Sci.* **12**(1), 127–136 (2018)



Modeling and Analysis of Energy Efficient Media Access Control Protocols for Wireless Sensor Networks Using OMNET++

Harish Joshi^(✉) and Ravindra V. Eklarker

Guru Nanak Dev Engineering College Bidar, Bidar, India
harishjoshi.ece@gmail.com, reklarker@gmail.com

Abstract. There are relatively few Media Access control (MAC) to display the sorted out and available remote sensor show usages, which remain close-by IEEE 802.15.4 models. This Scenario contains two Steps. To a restricted degree 1, the 3 sensor framework MAC shows with three model preoccupations of a remote sensor architecture. Somewhat, we look at the three models that utilizes the estimation systems. The simulation is performed by using the simulator OMNET++, The experimentations are also done for Wireless Sensor Networks. Then the results show the expected improvements in our approach when compared to the standard IEEE 802.15.4 in the MAC layer.

Keywords: INET · XMAC · LMAC · BMAC · NED · SMAC

1 Introduction

1.1 Representation of the MAC Protocols

There are two principal classes of MAC shows for WSNs, according to how the MAC supervises when certain centers can confer on the channel: Time-division various passageway (TDMA) based: These shows distribute particular timetable opening to center points. Center points can send messages just in their accessibility, as such clearing out clash. Occurrences of these sorts of MAC shows fuse LMAC, TRAMA, etc. Carrier sense different access (CSMA) based: These shows use transporter recognizing and back offs to avoid impacts, correspondingly to IEEE 802.11. Points of reference join B-MAC, SMAC, TMAC, X-MAC [1]. This element demonstrates the WSN MAC shows available in INET: B-MAC, LMAC and X-MAC. The going with portions details these shows rapidly.

1.1.1 B-MAC

B-MAC (short for Berkeley MAC) [3] is an extensively used WSN MAC show; it is a bit of TinyOS. It uses low-control tuning in (LPL) to confine control use on account of latent tuning in. Center points have a rest period, after which they wake up and sense the vehicle for presentations (clear channel assessment - CCA.) If none is perceived, the centers come back to rest. If there is a preamble, the center points stay alert and get the data packet after the introduction. If a center point needs to transmit something

explicit, it at first sends a prelude for at any rate the rest time allotment all together for all center points to recognize it. After the presentation, it sends the data packet. There are optional certifications moreover. After the data package (or data group + ACK) exchange, the center points come back to rest. Note that the acquaintance doesn't contain tending with information. Since the recipient's area is contained in the data group, all centers get the introduction and the data packet in the sender's correspondence broadens (not just the arranged recipient of the data package).

1.1.2 X-MAC

X-MAC is headway on B-MAC [4] and intends to upgrade some of B-MAC's insufficiencies [2]. In B-MAC, the entire introduction is transmitted, paying little regard to whether the objective center point got up around the beginning of the prelude or close to the end. Also, with B-MAC, all centers get both the prelude and the data pack. X-MAC uses a strobed prelude, for instance sending a comparable length presentation as B-MAC, yet as shorter impacts, with stops in the center. The postponements are adequately long that the objective center point can send an assertion in case it is starting at now cognizant. Right when the sender gets the insistence, it stops sending preludes and sends the data package. This can save time in light of the fact that potentially, the sender doesn't have to send the whole length presentation. Moreover, the introduction contains the area of the objective center point. Centers can wake up, get the introduction, and come back to rest if the package isn't directed to them. These features improve B-MAC's ability viability by lessening centers' time spent out of apparatus tuning in.

1.1.3 LMAC

LMAC (short for lightweight MAC) is a TDMA-based MAC show. There are data trade timeframes, which are isolated into timetable opening [5]. The amount of calendar opening in a timeframe is configurable according to the amount of center points in the framework. A transmission involves a control message and a data unit. The control message contains the objective of the data, the length of the data unit, and information about which opening are included. All center points wake up around the beginning of each timetable opening.

If there is no transmission, the accessibility is believed to be empty (not controlled by any center points), and the centers come back to rest. In case there is a transmission, consequent to tolerating the control message, centers that are not the recipient come back to rest [6].

The three MACs are completed in INET as the BMAC, XMAC, and LMAC modules. They have parameters to change the MAC show to the degree of the framework and the traffic power, for instance, space time, clear channel assessment range, bit rate, etc. The parameters have default regards, along these lines the MAC modules can be used without setting any of their parameters. Check the NED archives of the MAC modules (BMAC.ned, XMAC.ned, and LMAC.ned) to see all parameters [7].

2 Planning of Simulation

2.1 Introduction to OMNeT++

The simulation contains three points of reference reenactments, which demonstrate the three MACs in a remote sensor scenario. The circumstance is that there are remote sensor centers in a refrigerated transportation focus, watching the temperature at their region. They sporadically transmit temperature data remotely to an entryway center, which progresses the data to a server by methods for a wired affiliation [8]. Ideally, there should be a specific application in the entrance center point called sink, which would get the data from the WSN, and send it to the server over IP. Along these lines the center would go about as a passage between the WSN and the outside IP mastermind. In the point of reference propagations, the passage just advances the data packages over IP. To run the point of reference reenactments, pick the BMAC, LMAC and XMAC setups from omnetpp.ini. Most by far of the structure enters in the ini record are shared between the three proliferations (they are described in the General setup), except for the MAC show unequivocal settings. All of the three reenactments are use a comparable framework, SensorNetworkShowcaseA, portrayed in SensorNetworkShowcase.ned [9].

In the framework, the remote sensor center points are of the sort SensorNode, named sensor1 up to sensor4, and door. The center named server is a Standard Host. The framework in like manner contains an Ipv4NetworkConfigurator, an Integrated Visualizer, and an Apsk Scalar Radio Medium module. The center points are set against the foundation of a transmittance focus floor plan. The scene gauge is 60×30 m. The stockroom is just an establishment picture giving setting. Obstacle setback isn't illustrated, so the establishment picture doesn't impact the proliferation in any way [10]. The remote interface in the sensor center points and the portal is demonstrated in omnetpp.ini to be the ordinary Wireless Interface (as opposed to the IEEE802.15.4express IEEE802.15.4NarrowbandInterface, which is the default WLAN interface in Sensor Node).

We are using Apsk Scalar Radio here in light of the fact that it is a tolerably essential, nonexclusive radio. It uses amplexness and stage move keying guidelines (for instance BPSK, QAM-16 or QAM-64, BPSK obviously), without additional features, for instance, forward mix-up change, interleaving or spreading. We set the bitrates in omnetpp.ini to 19200 bps, to facilitate the default for the MAC bitrates (we'll use the default bitrates in the MACs, which is 19200 bps for every one of the three MAC types). The introduction length is set to be short for better similitude with the MACs. We also set some various parameters of the radio to optional characteristics.

Each sensor center point is sending a UDP packet with a 10-byte payload ("temperature data") reliably to the server, with an unpredictable start time around 1 s. The packages are having an 8-byte UDP header and a 20-b.

3 Advancing for Packet Drop and Looking at Impact Utilization

In this segment, we are looking at the three MAC protocols regarding a couple of insights, for example, the quantity of UDP packets transmitted by the system, and power utilization. So as to think about the three protocols, we need to discover the parameter esteems for every MAC, which lead to the best execution of the system in a specific situation. We'll advance for the quantity of packets collected by the server, for example we need to limit packet drop [13].

The situation is equivalent to in the BMAC, XMAC and LMAC setups (every sensor sending information consistently to the server), then again, actually it is utilize a comparative, however progressively protocol system design.

3.1 Distribution Center Systems

We are running three parameter contemplates, one for every MAC protocol. We need to advance only one parameter of every MAC, the opening length. Preferably, one would need to streamline different parameters so as to locate a progressively ideal arrangement of parameter esteems, yet it is out of degree for this feature [14]. The decisions for the estimations of different parameters are discretionary. The reenactments are kept running for 100 s, and every cycle are be run multiple times to get smoother results. We are picking the best performing parameters as per the quantity of packets collected by the server.

3.1.1 Configuration of Statistic Base

In this base setup, we are setting the reenactment time limit, the quantity of reiterations, and turn vector recording off to accelerate the runs. The outcomes are plotted in the StatisticBMAC.anf, StatisticXMAC.anf, and StatisticLMAC.anf records. The parameter ponders for the individual MAC's are specified in the accompanying segments.

3.1.2 Improving B-MAC

The objective is to advance BMAC's slotTime parameter for the quantity of packets collected by the server. The arrangement in omnetpp.ini for this is StatisticBMAC. It contains 1000 runs.

In the investigation, slotDuration are keep running from 10 ms to 1 s in 10 ms additions (the default of slotDuration is 100 ms.) The quantity of packets collected by the server for every slotDuration esteem is appeared on the accompanying picture (time in a flash): The sensors send 100 packets each over the span of the 100 s, subsequently 400 packets complete. It is evident from the outcomes that the system can't transmit all traffic in this situation. The outcomes additionally plot a smooth bend. We pick 0.19 s as the best performing an incentive for slotDuration.

3.1.3 Improving X-MAC

Once more, we advance the slotTime parameter for the quantity of packets collected by the server. As in the XMAC design, the slotTime for the door are be shorter than for the sensors. The setup in omnetpp.ini for this is StatisticXMAC. It contains 1000 runs.

The default of slotDuration for XMAC is 100 ms. In the investigation, the passage's slotDuration are keep running from 10 ms to 1 s in 10 ms additions, correspondingly to the parameter ponder for B-MAC. The slotDuration for the sensors are be 2.5 occasions that of the entryway (a self-assertive esteem.) Here are the outcomes (time in seconds According to this, the ideal incentive for the portal's slotDuration is 0.14 s (0.35 s for the sensors), so we pick that [15].

3.1.4 Improving LMAC

We are improving the slotDuration parameter for the quantity of packets collected by the server. The setup for this examination in omnetpp.ini is StatisticLMAC. It contains 1000 runs. Here is the design: We are setting reservedMobileSlots to 0, and numSlots to 8. The slotDuration parameter is keep running from 10 ms to 1 s in 10 ms advances. The quantity of got packets is shown on the accompanying picture (time in short order).

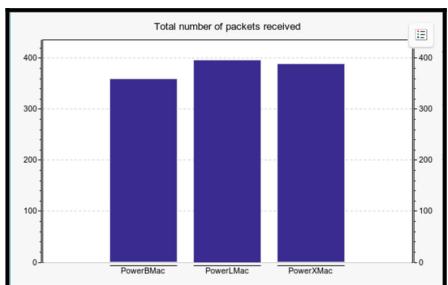
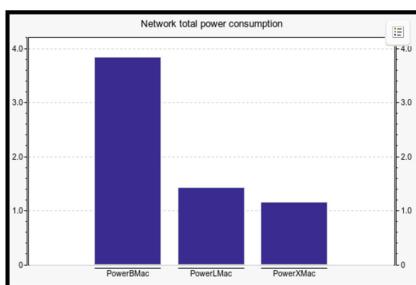
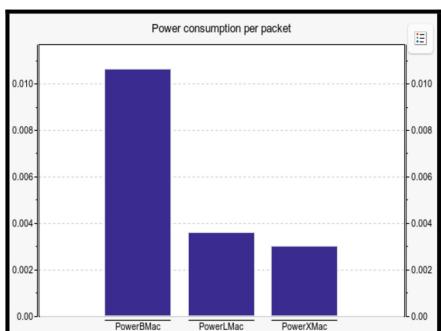
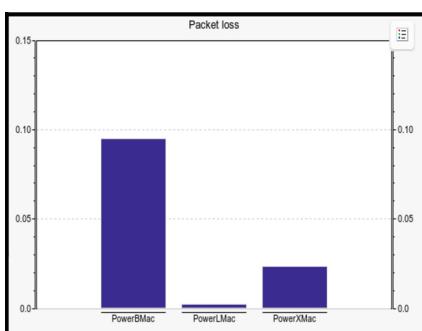
It is clear from the outcomes that the system can transmit practically all the traffic in this situation (instead of the XMAC and LMAC results). The best performing an incentive for slotDuration is 50 ms. Picking the higher slotDuration esteem results in about a similar exhibition however lower control utilization, yet we are advancing for the quantity of packets here [16].

4 Results

4.1 Estimating Power Utilization

We have undergone the three reenactments with the picked parameters as far as power utilization. The outcomes for the parameter thinks about contain the required power utilization information. 100 packets over the span of the 100 s reenactments, for a sum of 400 packets. Then outcome is as follows.

1. Network all out power utilization: The whole of the power utilization of the four sensors and the portal (values in Joules.)
2. Power utilization per packet: System complete power utilization/All out number of packets got, along these lines control utilization per packet in the whole system (values in Joules.)
3. Packet drop: Absolute number of packets got the/all out number of packets sent, in this way what number of packets from the 400 sent are lost. Here are the outcomes (Figs. 1, 2, 3 and 4).

**Fig. 1.** Total No. of packet received**Fig. 2.** Network Total power consumption**Fig. 3.** Power Consumption per packet**Fig. 4.** Average Packet Loss

5 Conclusion

In this paper, we contribute to the vision of a evaluation using simulations using OMNeT++, using INET framework. Here we have compared three MAC protocols LMAC, BMAC and XMAC. Observation made with respect to Total No. of packet received, Network Total power consumption, Power Consumption per packet and Average Packet Loss by the simulation It is Observed that LMAC transmitted the most packets and BMAC the least. BMAC consumes altogether more power than the others. Every one of the three bore 90–100% of the traffic (BMAC 90%, XMAC 99.25%, LMAC 97%), in this way BMAC has altogether more power utilization per parcel. The end is that in this situation, with the chosen parameter esteems, XMAC ended up being the most Energy effective MAC protocol, in spite of the fact that LMAC transmitted more traffic.

Acknowledgment. We would like to exhibit a Deep Sense of Gratitude to The guardians, Family Members and Friends for their help and nonstop direction, for composing this paper. This work was upheld by Guru Nanak Dev Engineering College Bidar. Special Thanks to Dr. S. Balbir Singhji, Mrs. Reshma Kaurji, Dr. B. S. Dhaliwal. We are appreciative to our partners who gave mastery that extraordinarily helped the exploration. We are additionally thankful to my

partners for help who directed this paper and in that line improved the original copy altogether. We are likewise monstrously appreciative to the reviewers of ICICT-2019 for their remarks on a previous manuscript of the original copy.

References

1. Buettner, M., Yee, G.V., Anderson, E., Han, R.: X-MAC: a short preamble MAC protocol for duty-cycled wireless sensor networks. In: Proceedings of the 4th International Conference on Embedded Networked Sensor Systems, SenSys 2006, pp. 307–320. ACM, New York (2014)
2. Cano, C., Bellalta, B., Sfairopoulou, A., Oliver, M.: Low energy operation in WSNs: a survey of preamble sampling MAC protocols. *Comput. Netw.* **55**(15), 3351–3363 (2011)
3. van Dam, T., Langendoen, K.: An adaptive energy-efficient MAC protocol for wireless sensor networks. In: SenSys, pp. 171–180. ACM (2003)
4. Dunkels, A.: The ContikiMAC radio duty cycling protocol. Technical Report T2011:13, Swedish Institute of Computer Science, December 2011
5. El-Hoiydi, A., Decotignie, J.D.: Wise MAC: an ultra low power MAC protocol for multi-hop wireless sensor networks. In: ALGOSENSORS. Lecture Notes in Computer Science, vol. 3121, pp. 18–31. Springer (2004)
6. Hoctor, R., Tomlinson, H.: Delay-hopped transmitted-reference RF communications. In: IEEE Conference on Ultra Wideband Systems and Technologies, pp. 265–269 (2002)
7. van Hoesel, L., Havinga, P.: A lightweight medium access protocol (LMAC) for wireless sensor networks: reducing preamble transmissions and transceiver state switches. In: 1st International Workshop on Networked Sensing Systems, INSS, pp. 205–208. Society of Instrument and Control Engineers (SICE), Tokyo (2004)
8. Köpke, A., Swigulski, M., Wessel, K., Willkomm, D., Haneveld, P.T.K., Parker, T.E.V., Visser, O.W., Lichte, H.S., Valentin, S.: Simulating wireless and mobile networks in OMNeT++ the MiXiM vision. In: Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops, Simutools 2008, pp. 71:1–71:8. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels (2008)
9. Abdeli, D., Zelit, S., Moussaoui, S.: R-MAC: a real time hybrid MAC protocol for WSN. In: 2013 11th International Symposium on Programming and Systems (ISPS), Algiers, pp. 153–162 (2013)
10. Meijerink, A., Cotton, S., Bentum, M., Scanlon, W.: Noise-based frequency offset modulation in wideband frequency-selective fading channels. In: 16th Annual Symposium (2017)
11. Karahan, A., Ertürk, İ., Atmaca, S., Çakıcı, S.: Energy efficient hybrid MAC protocol for large scale wireless sensor networks. In: 23rd Signal Processing and Communications Applications Conference (SIU), Malatya, pp. 1549–1552 (2015)
12. Morshed, S., Heijenk, G.J.: T-MAC: an energy-efficient MAC protocol for wireless sensor networks exploiting noise-based transmitted reference modulation. In: 2nd Joint ERCIM eMobility and MobiSense Workshop, St. Petersburg, Russia, pp. 58–71, June 2013
13. Morshed, S., Heijenk, G.: TR-MAC: an energy-efficient MAC protocol exploiting transmitted reference modulation for wireless sensor networks. In: Proceedings of the 17th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, MSWiM 2014, pp. 21–29. ACM, New York (2014). <http://doi.acm.org/10.1145/2641798.2641804>

14. Polastre, J., Hill, J., Culler, D.E.: Versatile low power media access for wireless sensor networks. In: SynSys, pp. 95–107 (2004)
15. Ye, W., Heidemann, J., Estrin, D.: An energy-efficient MAC protocol for wireless sensor networks. In: INFOCOM 2002, Proceedings of Twenty-First Annual Joint Conferences of the IEEE Computer and Communications Societies, vol. 3, pp. 1567–1576. IEEE (2002)
16. Förster, A., Udugama, A., Virdis, A., Nardini, G. (eds.): OMNeT. EPiC Series in Computing, vol. 56, pp. 1–10 (2018)



Privacy Preserving Approach for Proficient User Revocation in Cloud Environments

S. Suganthi Devi¹✉) and V. Asanambigai²

¹ Department of Computer Engineering,
Srinivasa Subbaraya Polytechnic College,
Puthur, Nagapattinam, Tamilnadu, India
suganthidevi@yahoo.com

² Department of Computer Engineering, Government Polytechnic College,
Perambalur, Tamilnadu, India
tradingbaskeran@gmail.com

Abstract. Cloud environments can afford dynamic infrastructure for the mobile users. Due to the lack of security in cloud, auditing it with public concern and privacy for the distributed information available on the cloud remains as the challenging task. The user revocation plays a vital role for maintaining the integrity for the user's privacy. For this reason, we generate a proficient the public auditing methodology is propose and implemented to maintain the user revocation with the privacy for the user in the unsecured cloud environment.

Keywords: Privacy preservation · User revocation · Cloud environment · Shared data · Third party auditor · System administrator

1 Introduction

The sharing of data and exploiting the services afforded in the cloud and the usage of the mobile devices may effortlessly share the information with every other user in the group [1, 2]. The remaining users in the same group may not get the accessibility and modification of information [3]. Whenever the service provides of the cloud environment maintained the secured communication to the users, maintain of integrity of information may be spoiled with the human errors and the failure of hardware [4, 5]. An amount of methodologies are implemented to secure the data integrity in the cloud environment [6]. Many methods are utilized to increase the personalized information with proficient user revocation [7, 8].

The proposed methodology is used to improve the proficiency and the security. Whenever the user utilizes the block of shared information, he wants to calculate the latest signature for the shared block [9]. The user is revoked in the group for distributing the shared information, the formerly signed signature must be re-signed by the same user in the group, and then the integrity of the shared data is verified using the public keys of the active user in the cloud environment [10].

The rest of the paper is structured as follows. Section 2 throws light on related work, the proposed work and it's the public auditing methodology are dilated Sect. 3. Section 4 presents the experiment and the discussion of evaluation results. Finally, conclusion and the suggestion for the future direction in this work are illustrated in Sect. 5.

2 Related Work

The public auditing methodology for distributed information with proficient user revocation is maintained in the cloud environment using the re-sign concept [11]. Whenever the data which is shared in the unsecured cloud environment, it should be confirmed in the signer of every block [12]. Mostly, the data shared in this cloud environment should maintain the privacy in the group [13]. The cloud system itself is capable of converting the signatures from initial stage from every single user to the remaining users in the group [14].

The random masking methodology is implemented to increase the privacy preserving and ensures the auditor that he can able to track any metadata for the improvement of proficient public audit procedure [15]. The position related security is focused to improve the security with dimension positions. The proxy based signature approach is used to show the variation from the basic digital signature procedures [16]. The mobile based applications and the electronics based transactions are used this kind of proxy signatures [17].

Multi proxy signature is used to build the binding and positioning the approaches. The Global Positioning System is used to acquire the position of the cloud environment [18]. The mobile is used by the user to sign the message from the one location to the other location of the mobile users. The receiver can confirm that the received message is signed properly or not [19].

3 Proposed Work

In our proposed work, the proficient and privacy preserving user revocation methodology is maintained for the public related auditing. The improved user revocation is achieved using the system administrator in the group that he updates the distributed data and signing the latest key to the administrator to sign the data block. The request must send to the system administrator that he generate and forward the re-sign approach to every other user in the cloud environment.

The user can share the data within the group and the Third party Auditor, system administrator is capable of providing the increased storage and easy to distributed the data in the group. The system administrator also stores the list of users for creating the signing keys and the equivalent re-signing keys. The third party auditor is responsible for checking the integrity of the distributed data without taking the whole data, even though many users are revoked within the group. Privacy preserving of the users is accomplished in the cloud environment from the auditor and also identifying the content of the shared data in the process of proficient public auditing. Figure 1 demonstrates the process of user revocation.

The concept of bilinear mapping is established using the 2 groups $Group_1$, $Group_2$ with prime order p . The map $bm: Group_1 \times \overline{Group_1} \rightarrow Group_2$ is a bilinear map if

- (i) for every $x, y \in Z_p$, $g_1 \in Group_1$ and $g_2 \in \overline{Group_1}$, then $bm(g_1^x, g_2^y) = bm(g_1, g_2)^{xy}$ is proficiently computable.
- (ii) the bilinear map is un generate able
- (iii) An isomorphism based on computation from $\overline{Group_1}$ to $Group_1$

The proxy based re-sign is identified using Group. The un-trusted proxy is provided for several data that the data is converted from the sender's signature on the same block into the receiver's signature, also the proxy is not generated for every signature for Sender and the receiver. The process is also called as the re-signing. The dynamic sharing of data with public auditing which generates the necessary data can be designed carefully. The indexing using the hash table by the users may modify the block without modifying the process of the other users. The collision removed hash methodology $\text{Hash}' : \{0, 1\}^* \rightarrow Z_p$. Therefore a block is generated by the identifier $\text{identifier}_1 = \{v1_i \| r1_i\}$

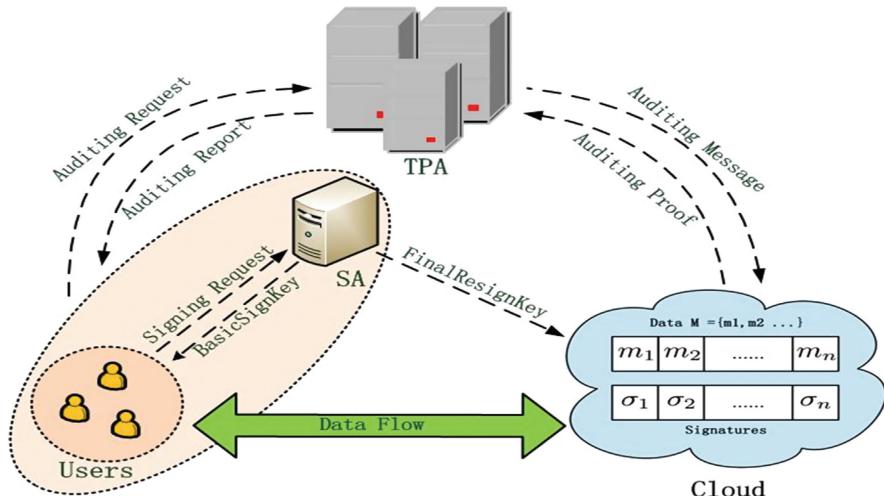


Fig. 1. User revocation process

Algorithm1: Privacy Preserving Proficient User Revocation

```

Begin Procedure Privacy_Preserving ( )
For every element in the Group
    Group1 x Group1 → Group2
    Generator(x) ∈ Group1
    Hash(x) : {0,1}* → Group1
    Hash' : {0,1}* → Zp
    Shared Data SD = (SD1, SD2, ..., SDn)
    System Administrator creates a value α ∈ Zp
    commonpk = g1pk
    Userlist → g1pk
    Resignkey =  $\frac{\text{common}^{pk}}{\text{sign}_{key}}$ 
    δkey' = (Hash(identifierx)βbmx)pk
    δkey = (δkey')pk
End For
End Procedure

```

The Algorithm1 as user revocation is implemented by the user in the cloud environment by the list of users responded the system administrator comments that makes the users are unable to gather the pair of keys to finish the procedure of creating the correct signature with our proposed methodology. The attacker is unable to find the attack the system with this revocation methodology.

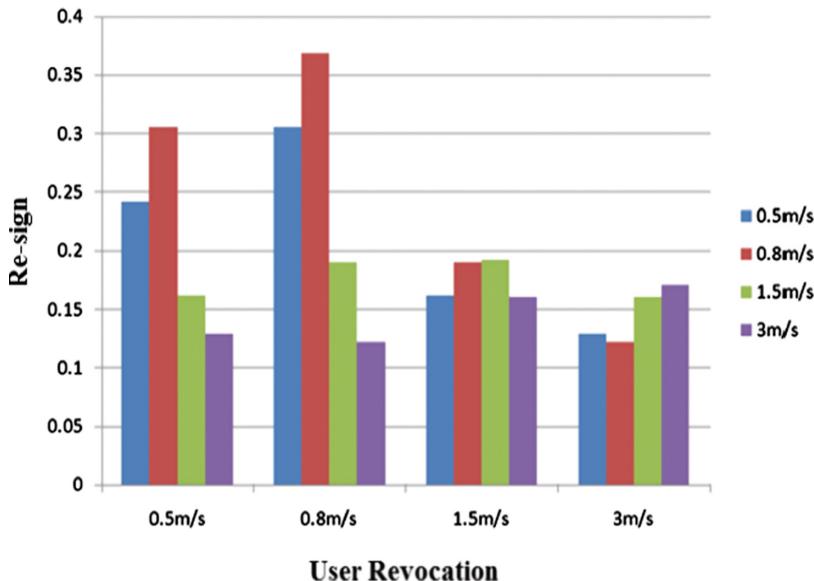
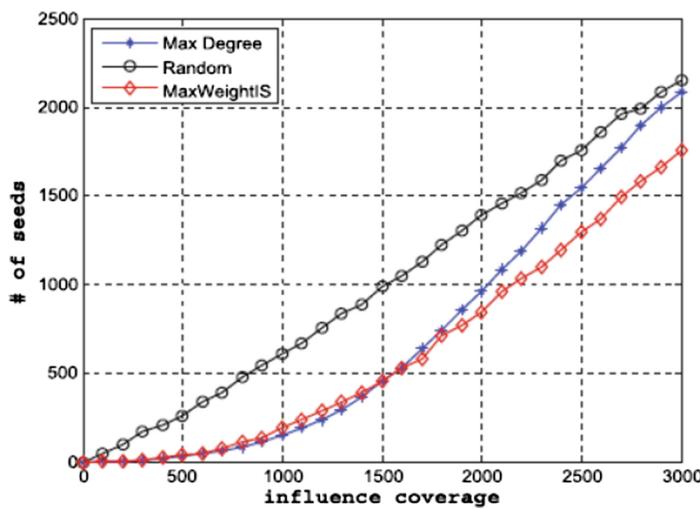
3.1 Proficiency

The proposed methodology is proficient within the user revocation procedure since the user is revoked in the group that needs to finish the revoked methodology from the list of users. All the distributed data in the cloud environment are having the signature with the public key, so no need for re-sign blocks where the user revocation phase that increase the proficiency of the user revocation. Exploiting the system administrator in the cloud environment is useful for reducing the re-signing approach that confirms that the cloud does not have the value of signers in the blocks in the methodology. It removes the un-secured cloud from analyzing the members in the active group. The privacy preserving methodology confirms that the third party auditor could not get the content from the bilinear map with the combination of auditing procedure.

4 Performance Evaluation

The performance evaluation is implemented using the Ubuntu with Intel Core processor the 160 bits key is used to find the sign and re-sign process of the proposed methodology. The proficiency of the user revocation is identified using the blocks to re-sign the blocks to increase the user revocation. Whenever the cloud environment is utilized the private key of the user, it is implemented without remanding the re-sign approach. The system administrator is able to change the signature of the known user in the cloud environment and verifies the integrity of the distributed data rather than using the usual proxy signatures. The dynamic operations for the auditing purpose is performed using the symmetric keys are produced by the user in the cloud environment. The verification process is the main process for identifying the attacker.

The third party auditor is verified the public auditing technique of signed users to protect the confidential information with the use of random masking task. The correctness of the shared data is verified by the third party auditor to increase the public verification process that satisfies the user revocation. Figure 2 illustrates the re-sign process based on the user revocation. Figure 3 demonstrates the improved proficiency for the privacy preserving technique compared to the other related methods.

**Fig. 2.** Re-sign process**Fig. 3.** Proficiency for privacy preserving

5 Conclusion

In this paper, the public auditing methodology is proposed and implemented. By including the system administrator, the proposed method specifies the user to initially sign a block using the Key value and then used the cloud to re-sign the block with the

public key which is used commonly and the relevant Final Re-sign key value is produced by the third party auditor is capable of auditing the integrity of the distributed data with the public key value that increases the proficiency of the user revocation and improves the user's privacy preservation in the cloud environment and allows it to initially re-sign blocks in cloud. The random masking methodology is used to increase the privacy with the third party auditor.

References

1. Thiyagarajan, V.S., Ayyasamy, A.: Privacy preserving over big data through VSSFA and MapReduce framework in cloud environment. *Wirel. Pers. Commun.* **97**(4), 6239–6263 (2017)
2. Li, M., Cao, N., Yu, S., Lou, W.: FindU: private-preserving personal profile matching in mobile social networks. In: Proceedings of IEEE INFOCOM, pp. 2435–2443 (2011)
3. Capkun, S., Hubaux, J.-P.: Secure positioning of wireless devices with application to sensor networks. In: Proceedings of IEEE INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3, pp. 1917–1928. IEEE (2005)
4. Venkatachalam, K., Thiyagarajan, V.S., Ayyasamy, A., Ranjani, K.: Big data with cloud virtualization for effective resource handling. *Int. J. Control Theory Appl.* **9**(2), 435–444 (2016)
5. Ateniese, G., Hohenberger, S.: Proxy re-signatures: new definitions, algorithms and applications. In: The Proceedings of ACM CCS 2005, pp. 310–319 (2005)
6. Karthiban, K., Smys, S.: Privacy preserving approaches in cloud computing. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 462–467. IEEE, 19 Jan 2018
7. Sridhar, S., Smys, S.: A hybrid multilevel authentication scheme for private cloud environment. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–5. IEEE, 7 Jan 2016
8. Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., Schaffner, C.: Position-based quantum cryptography: impossibility and constructions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 429–446. Springer, Heidelberg (2011)
9. van Dijk, M., Juels, A., Oprea, A., Rivest, R.L., Stefanov, E., Triandopoulos, N.: Hourglass schemes: how to prove that cloud files are encrypted. In: The Proceedings of ACM CCS 2012, pp. 265–280 (2012)
10. Wang, B., Li, B., Li, H.: Public auditing for shared data with efficient user revocation in the cloud. In: INFOCOM 2013, pp. 2904–2912 (2013)
11. Tate, S.R., Vishwanathan, R., Everhart, L.: Multi-user dynamic proofs of data possession using trusted hardware. In: Proceedings of ACM CODASPY 2013, pp. 353–364 (2013)
12. Yuan, J., Yu, S.: Proofs of retrievability with public verifiability and constant communication cost in cloud. In: Proceedings of ACM ASIACCS-SCC 2013 (2013)
13. Wang, H.: Proxy provable data possession in public clouds. *IEEE Trans. Serv. Comput.* (accepted)
14. Wang, B., Li, B., Li, H.: Oruta: privacy-preserving public auditing for shared data in the cloud. In: The Proceedings of IEEE Cloud 2012, pp. 295–302 (2012)
15. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: A view of cloud computing. *Commun. ACM* **53**(4), 50–58 (2010)

16. Hao, Z., Zhong, Z., Yu, N.: A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability. *IEEE Trans. Knowl. Data Eng.* **23**(9), 1432–1437 (2011)
17. Chen, L.: Using algebraic signatures to check data possession in cloud storage. *Future Gener. Comput. Syst.* **29**(7), 1709–1715 (2013)
18. Shacham, H., Waters, B.: Compact proofs of retrievability. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 90–107. Springer, Heidelberg (2008)
19. Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position based cryptography. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 391–407. Springer, Heidelberg (2009)



An Energy - Efficient Approach for Restoring the Coverage Area During Sensor Node Failure

G. T. Bharathy^(✉), S. Bhavanisankari, T. Tamilselvi, and G. Bhargavi

Department ECE, Jerusalem College of Engineering, Chennai 600100, India

{bharathy, bhavanisankari, tamilselvi,
bhargaviece}@jerusalemengg.ac.in

Abstract. Wireless sensor networks assist monitoring and scheming of physical environments from isolated places with enhanced precision. Environmental monitoring, military purposes are some of the applications of it. Sensor nodes comprise a variety of energy and computational constraints since they are inexpensive. For abundant applications of sensor network, it is indispensable to offer absolute sensing coverage to a defense-perceptive vicinity. To dynamically observe the range of object the division of sensors are redundantly utilized. The function of the scheme is to offer meticulous and precise data to remote observer, by considerably sensing, linking, and analyzing the apparent object data in monitoring vicinity. To accomplish associated assignment and comprehend its significance, at the outset, wireless sensor network should cover up monitoring vicinity well. The coverage of the network is an essential measure to evaluate wireless sensor network performance and quality of service. Utilization of increased amount of sensor nodes in target vicinity leads to the presence of redundant nodes which in turn reduces the quality of service of the network. This paper aims to re-establish the field coverage area in an energy efficient approach by occasionally refreshing and switching the cover to deal with unforeseen collapse and also flexibly sustain additional sensors at a time with dissimilar degrees in scattered way that once in a while chooses the coverage area and toggle among them to expand coverage interval and withstand unanticipated breakdown during the runtime.

Keywords: Wireless sensor networks · Energy efficiency · Energy efficient failure scheduling · Sleep scheduling

1 Introduction

Recent developments in the wireless sensor networks (WSN) have immense evolution due to their extensive-variety of applications, which include environmental monitoring, area surveillance and military applications. Wireless sensor networks usually comprises of numerous sensor nodes, that gathers the information from the surroundings and provide the same to the remote base station. These sensor nodes have restricted battery life and thus the energy of these nodes should be utilized in an effective manner. The sleep/wake up schedule is utilized to withstand the power of the nodes. The causes of the failure of a sensor node in the wireless sensor network may be due to channel failure, node being compromised, degradation of the battery life, degradation of the

sensing region, coverage problem and many other reasons. The main reason for the sensor node failure is due to the degradation of the battery life and the coverage problem.

The coverage of the sensor ensures the monitoring superiority offered by the sensor network in a selected vicinity. Diverse applications necessitate diverse range of sensing coverage. Difficulty in the coverage area of the sensor has been analyzed in papers [1–8]. In [1–4], the authors investigated about the point target coverage and in [5–8] the authors investigated about the full area coverage difficulty.

A new algorithm (EEFSA) is proposed in this paper, which gives the full coverage in an energy efficient manner and to avoid the node failure. The analysis of the proposal is evaluated by the simulation using ns-2 simulator. In particular, it is considered that one node is monitoring a security-sensitive area and after some time its energy is approaching zero and the node in its backup set which has the maximum energy is used to monitor the field even before the active node fails.

2 Literature Survey

An approach was proposed by Ye, Heidenmann, and Estrin et al. [9], proposed the S-MAC approach for energy consumption of the sensor nodes. This approach uses three major components: periodic listen and sleep, maintaining synchronization, and scheduling. Thus the S-MAC approach needs the node synchronization between the nodes and the energy consumption is large as the entire neighbouring nodes wake up for a particular time period. In [10] Tian and Georganas et al., proposed the node-scheduling scheme which decreases the energy utilization, which in turn increases the life time of the system, by switching off certain redundant nodes. This scheme gives only the partial area coverage. In [11] Ye, Zhong, Lu, and Zhang et al., proposed the Probing Environment and Adaptive Sleeping (PEAS) protocol that can build a long-lasting sensor networks. In the PEAS protocol the sensors has to adequately transmit the response messages to the base station and also the PEAS approach is unable to monitor the surveillance area when the sensing node is unexpectedly failed. Liu and She et al. [13], proposed the network coverage depending on grids, altered the coverage restoring difficulty into unrestrained optimization difficulty considering the network coverage as the optimization target, and then completed the optimization difficulty with the help of the hybrid particle swarm optimization algorithm taking in to account the initiative of simulated annealing. Sun, Li, Chen and Wei et al. [14], proposed a model which depends on directional sensing algorithm using the virtual potential field which shifts the positions of the sensor nodes and modify directions without human intervention in the monitoring vicinity. Koriem and Bayoumi et al. [15], has proposed a novel numerical algorithm, Wireless sensor Hole Detection algorithm (WHD), which is utilized to identify and compute the holes vicinity in ROI in which the sensor nodes are scattered arbitrarily.

3 Problem Description

The security-sensitive area has to be monitored without any failure of nodes. The failure of nodes degrades the sensing capacity of the wireless sensor networks and thus causes the coverage issue. The foremost reason for the sensor node failure is due to the increased energy utilization for sensing, transferring the sensed information to the base station, and overloading. This paper proposes the trade off between the fault acceptance and the energy utilization and thus the coverage problem is minimized in an energy efficient manner.

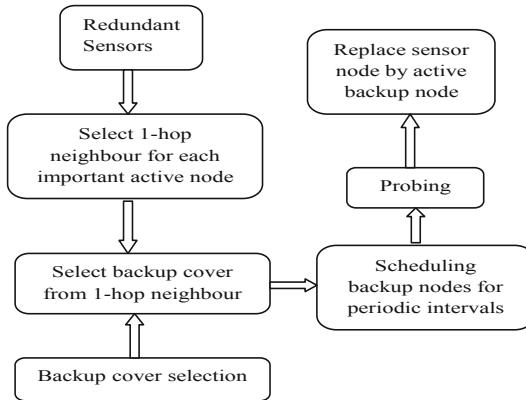
3.1 Assumptions

The following assumptions are done. The node deployment verifies that each and every spot in the field is no less than k-covered.

- (1) At each sensor, the time interval is separated as extensive slots of size = t_s units. Every slot indicates the predictable interval linking two consecutive sensor information.
- (2) Static nodes, and thus the nodes can be supplemented anytime throughout the network function, and need not be synchronized.

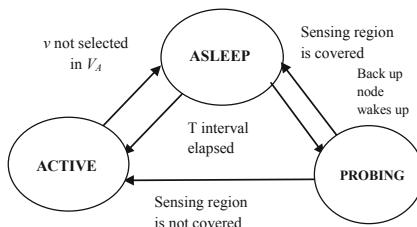
4 System Model

The overall system model is shown in the Fig. 1. Initially Sensor nodes are deployed using many parameters. The nodes are deployed in specified region in random fashion. From the neighbour list every node calculates the backup cover in a distributed manner using Deterministic Cover Selection algorithm (DCS). The DCS constructs k-cover that is as node-disjoint as possible. After constructing the S cover each node scheduled to monitor the region. The nodes, which monitoring the specific region assigned into active set V_A and it should remain active state for T time slots. Backup nodes in each cover activated for each M interval called tolerance interval. The node remains active for certain period. After choosing the backup covers, the active node informs the nodes about the schedule regarding wakeup/sleep and their role to the backup covers. Backup nodes could be provided with opportunistic sleep/wakeup schedule. In backup node probing, the each activated node performs active probing by transferring message and waiting for replies. The backup node u transmits message to active nodes present in its neighbourhood, when it wakes up. The u node verifies one of the neighbour node and provides it with a new sleep schedule, once it finds that its present neighbours in V_A entirely cover its sensing vicinity, and then goes into the sleep mode. If the sensing region is not absolutely covered by u , it will be active right through V_A the residual extent of V_A 's operation. This structure offers diverse degree of redundancy. Each node separately concludes the degree of redundancy in its neighbourhood. This structure with dynamism maintains 1-coverage of every point and withstand unanticipated failure.

**Fig. 1** System model

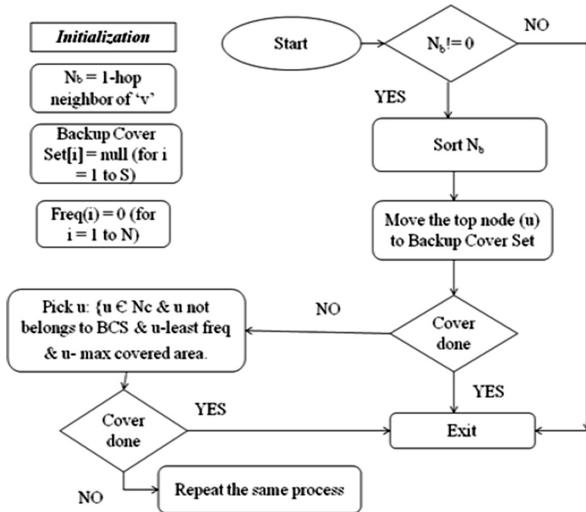
4.1 Overview of the Model

The overview of the model is shown in the Fig. 2 Overview of the model. EEFSA needs an active 1-cover be chosen with the help of any deterministic cover selection (DCS) algorithm. All other nodes are associated to the uncertain sleeping set. To begin with, each and every node contribute in choosing with the help of periodic neighbour record information from nodes in, a recently utilized node is prepared to know the survival of the sleeping neighbours.

**Fig. 2** Overview of the model

4.2 Selection of Backup Cover

The complete sensing range of v is completely covered by the backup cover neighbour nodes. If v is a element of V_A , it evaluates utmost S backup cover sets ($S \geq n - 1$) which are as node-disjoint as possible. Figure 3 shows the flow chart for selecting backup cover.

**Fig. 3** Flow chart for selecting backup covers**Step 1:**

Initialize the N_b as 1-hop neighbour of active node v .

Initialize an array for Backup Cover set (S).

Initialize the frequency of occurrences of the sensor nodes.

Step 2:

If N_b is not empty, sort the neighbours of the active node v as per the Maximum Coverage Area. The Maximum Coverage Area is that which neighbour (N_b) covers the maximum vicinity of the active node v . The maximum coverage area can be calculated as,

$$T_1 = (r^2) \times \arccos\left\{\frac{[d^2 + r^2 - R^2]}{[2 \times d \times r]}\right\}$$

$$T_2 = (R^2) \times \arccos\left\{\frac{[d^2 - r^2 + R^2]}{[2 \times d \times R]}\right\}$$

$$T_3 = \left(\frac{1}{2}\right) \times \left(\sqrt{[(r+R-d) \times (r-R+d) \times (R-r+d) \times (R+r+d)]}\right)$$

where R – radius of the first node.

r – radius of the second node.

d – distance between the two nodes.

Step 3:

By sorting, place the maximum area covered node in the top of the list and name it as u . Then move the u to the array backup cover set [1]. The frequency of the node is also incremented by one. If the coverage is done by using this u then exit the backup cover selection, or else the u must be selected in manner that, the u should not be in N_c and u should not belongs to the already selected backup cover set and it also cover the maximum area covered by the active node v . If the coverage is done by using this u exit the backup cover selection algorithm or else repeat form the step 2.

4.3 Scheduling Backup Covers

Waking up all the sensors is not essential and it is not energy efficient. As an add on feature, a hole produced by an additional failing node can be covered by the when they are still asleep. Hence in this paper the opportunistic sleep scheduling and energy consumed failure scheduling are proposed.

4.3.1 Opportunistic Sleep Schedule

The opportunistic sleep schedule is proposed here to create the backup sets to sleep for a particular time interval. If X_i is the backup cover of v , which ranges between $1 \leq i \leq X$, then the activation of the nodes in X_1 contained by Y slots, the nodes in X_2 contained by $2Y$ slots, and so on is done in the opportunistic method. More distinctively, if the nodes in X_i is to be arranged in accordance to their order in X_i . Node v schedule a neighbour $v_j \in X_i$ to sleep for a numeral amount of slots is given by the following equation.

$$\max(iY - n_{ci} + j, 0)$$

where n_{ci} - number of nodes in X_i .

Y – slot interval.

4.3.2 Backup Node Probing

The wake up of the backup node ‘ u ’ leads to the intervene of the active node in the surrounding neighborhood. By these probing messages the u node verifies one of the neighbour node and provides it with a new sleep schedule, once it finds that its present neighbours in V_A entirely cover its sensing vicinity, and then goes to sleep mode. The Backup nodes will send the handshake messages to know that the Monitoring node is ACTIVE or NOT. If the node is active the backup node will go to sleep.

4.3.3 Proxy Selection

In proxy selection instead of using the sleeping node the node which is already in the active mode will do the sleeping node’s work in order to decrease the energy utilization of that particular sleeping node.

The node v belonging to V_A , $v \in V_A$ can be the alternative or proxy of the node $u \in V_S$ if and only if the node v satisfy the following conditions. The conditions for

selecting the proxy for u is that, the node v must be the nearest neighbour of the node u or the neighbour of u which has the smallest/uppermost ID. Therefore, the node v is able to determine the role of the node u will have in the subsequent active cover. By using this proxy selection the energy of the node u is conserved. The example for proxy selection is shown in the Fig. 4. Here the node u_7 is the sleeping node, the nodes v_1 and v_2 can be the proxy of u_7 . But the v_2 must be the proxy of u_7 since it is closer to u_7 .

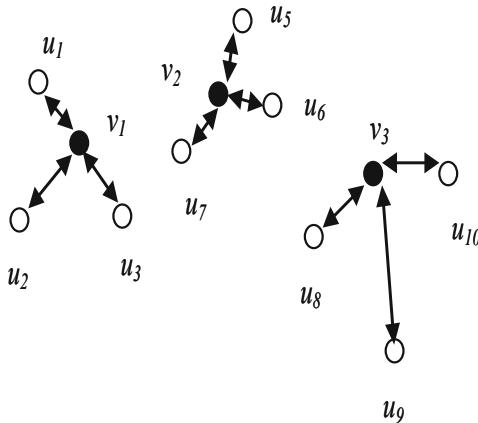


Fig. 4 Example for proxy selection

5 Protocol Analysis

5.1 Probability of Coverage

If the probability $P_v(pt)$, is the probability of the coverage of the point pt lying at a distance D from v , which depends on the sensing region of the node v , ($S_R(v)$) and D . If $D > S_R(v)$, then $P_v(pt) = 0$. The increase in distance of the point from v increases, the continuous distribution function decreases. To evaluate if pt comes in the coverage region of node v or not, a small distance Δ has to be taken about pt and adjust the value of the probability $P_v(pt)$ to be

$$P_v(pt) = \begin{cases} \int_{D+\Delta/2}^{D+\Delta/2} f_v(r)dr, & D \leq S_R(v_s) \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

$$P(pt, F_1) = \frac{2\pi A_1}{2\pi(A_0 + A_1) + L_0 L_1} \quad (2)$$

Equations (1) and (2) can be utilized to evaluate the probability of coverage when numerous nodes are offered. The evaluated probability by these equations

autonomously from other points in the area covers each and every point contained by a given space.

5.2 Energy Efficiency

The consumed energy to transfer a m -bit message over distance x is $E_T(m,x)$ is,

$$E_T(m,x) = E_{elec} \cdot m + \epsilon_{amp} \cdot m \cdot x^2 \quad (3)$$

where E_{elec} is the power dissipates to the broadcasting circuitry, ϵ_{amp} is the power dissipates for the transmit amplifier and the consumed energy to receive this message is $E_R(m)$ is given as,

$$E_R(m) = E_{elec} \cdot m \quad (4)$$

and E_I , the energy utilized by the nodes while they are in ideal mode. The energy consumption is measured by evaluating the average amount of active nodes at every time interval (n_b). It can be computed using the formula,

$$n_b = N_e \left(\sum_{i=1}^s \frac{n_c}{i_M} \right) \quad (5)$$

where n_b is the average amount of active nodes in the network, N_e is the total amount of nodes in the backup cover set, S is the amount of backup cover sets, n_c is the amount of nodes present in the particular backup set.

Assume that a probing node would be awake for complete interval t_s . This ensures a very conservative approximation of energy utilization since a node usually wakes up for merely a small part of time t_s if active probing is used.

6 Simulation and Results

The NS - 2 simulation tool is utilized to simulate and analyze the concept of the energy - efficient approach for restoring the coverage area during sensor node failure. The simulated Wireless Sensor Network has the network size 800×800 . The amount of nodes deployed to form the network is 50.

The node deployment is shown in the Fig. 5.

Figure 6 gives the active nodes represented as main station, base station which is used to monitor the security-sensitive area.

Figure 7 shows the failed node and its next active cover.

The Fig. 8 shows the plot between time period and the energy consumed by the nodes. The results has been compared with the previous k-cover algorithm and found that the energy efficient failure scheduling algorithm is better and best than the previous approaches.

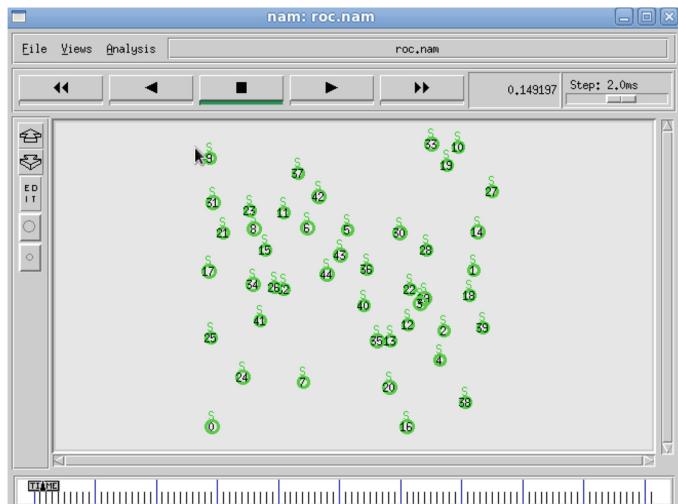


Fig. 5 Sensor node placement in random manner

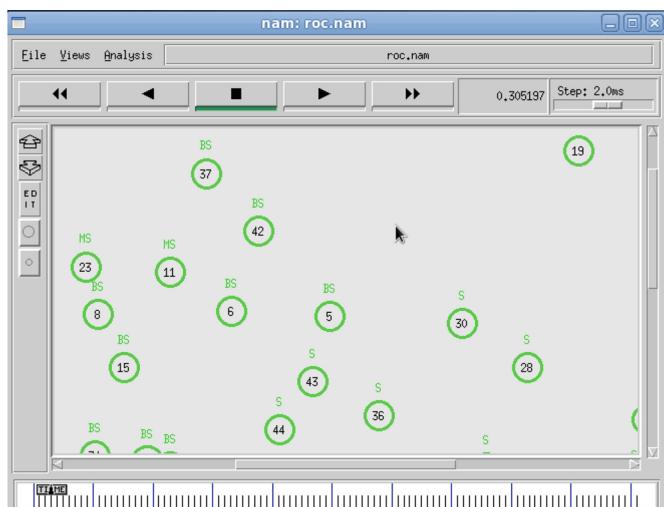


Fig. 6 Monitoring node assignment

Figure 9 shows the plot drawn between the time and the probability of coverage by the nodes, where the probability of coverage is increasing with the time and remains almost constant.

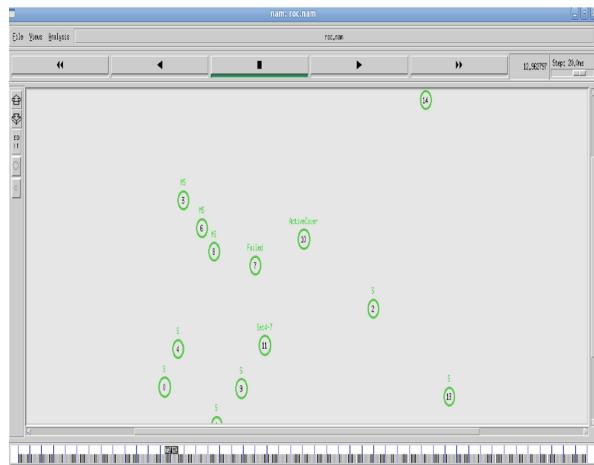


Fig. 7 Active cover for the failed node

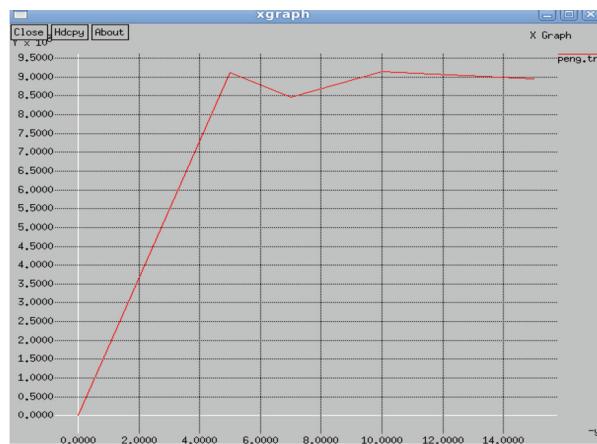


Fig. 8 Time vs consumed energy

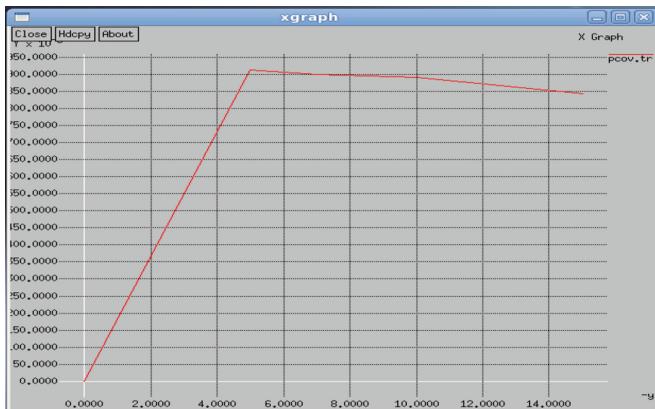


Fig. 9 Time vs probability of coverage

7 Conclusion

In this paper, energy efficient failure scheduling algorithm is developed to achieve maximum coverage and energy efficiency has been presented. The proposed algorithm continuously monitors the area without any node failure. The time delay for waking up the backup cover set nodes is eliminated here. Thus in this paper two major things has been contributed: (1) A new energy efficient failure scheduling algorithm to increase the energy competence of the nodes and (2) The surveillance area is continuously monitored without any node failure. Thus it can give the maximum coverage and also the energy of the node is well balanced.

References

1. Younis, O.M., Krunz, M.M., Ramasubramanian, S.: ROC: resilient online coverage for surveillance applications. Proc. IEEE/ACM Trans. **19**, 1–14 (2011)
2. Cardei, M., Thai, M.T., Li, Y., Li, Y., Wu, W.: Energy efficient target coverage in wireless sensor networks. In: Proceedings of IEEE INFOCOM 2005, pp. 1976–1984 (2005)
3. Yang, S., Dai, F., Cardei, M., Wu, J.: On multiple point coverage in wireless sensor networks. In: Proceedings of 2nd IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2005) (2005)
4. Cardei, M., Du, D.-Z.: Improving wireless sensor network lifetime through power aware organization. Wirel. Netw. **11**(3), 333–340 (2005)
5. Kar, K., Banerjee, S.: Node placement for connected coverage in sensor networks. In: Proceedings of WiOpt 2003 (2003)
6. Slijepcevic, S., Potkonjak, M.: Power efficient organization of wireless sensor networks. In: Proceedings of IEEE ICC 2001, vol. 2, pp. 472–476, June 2001
7. Berman, P., Calinescu, G., Shah, C., Zelikovsky, A.: Power efficient monitoring management in sensor networks. In: Proceedings of IEEE WCNC 2004, vol. 4, pp. 2329–2334, March 2004

8. Tian, D., Georganas, N.: A coverage-preserving node scheduling scheme for large wireless sensor networks. In: Proceedings of the 1st ACM Workshop on Wireless Sensor Networks and Applications, pp. 32–41 (2002)
9. Carle, J., Simplot, D.: Energy-efficient area monitoring for sensor networks. Computer **37**(2), 40–46 (2004)
10. Ye, W., Heidenmann, J., Estrin, D.: An energy-efficient MAC protocol for wireless sensor networks. In: Proceedings of IEEE INFOCOM, New York, vol. 3, pp. 1567–1576, June 2002
11. Tian, D., Georganas, N.D.: A coverage-preserving node scheduling scheme for large wireless sensor networks. In: Proceedings of 1st ACM WSNA, pp. 32–41, September 2002
12. Ye, F., Zhong, G., Lu, S., Zhang, L.: PEAS: a robust energy conserving protocol for long-lived sensor networks. In: Proceedings of IEEE International Conference on Distributed Computing System, pp. 28–37 (2003)
13. Liu, Z., She, Y.: Hybrid wireless sensor network coverage holes restoring algorithm. J. Sens. **2016**, 1–9 (2016). Article ID 8064509
14. Sun, Z., Li, H., Chen, H., Wei, W.: Optimization coverage of wireless sensor networks based on energy saving. Int. J. Future Gener. Commun. Netw. **7**(4), 35–48 (2014)
15. Koriem, S.M., Bayoumi, M.A.: Detecting and measuring holes in wireless sensor network. J. King Saud Univ. – Comput. Inf. Sci. (2018)



Design of Effective Grid-Connected Solar System

Iram Akhtar^{1(✉)}, Mohammed Asim², Raj Kumar Yadav³,
Piyush Agarwal⁴, and Sheeraz Kirmani⁵

¹ Department of Electrical Engineering, Faculty of Engineering and Technology,
Jamia Millia Islamia, New Delhi 110025, India

iram1208@gmail.com

² Integral University, Lucknow, India

masim@iul.ac.in

³ Government Engineering College, Ajmer, India

rajkumar.yadav@ecajmer.ac.in

⁴ CET-IILM-AHL, Greater Noida, India

piyushagarwall@gmail.com

⁵ Jamia Millia Islamia, New Delhi, India

sheerazkirmani@gmail.com

Abstract. Nowadays, the most vital concerns across the globe is the reduction of the fossil fuel reserves. This arises the need to develop alternative energy sources to fulfil the global demand. The solar system is a clean and trustworthy way to electrify the rural area. The next concern is the global warming as conventional energy sources enhance the carbon emission in the world. There is a need for proper energy generation system to provide the smooth energy. In this paper, we design a 12 kW effective grid-connected solar system to control the harmful effect of global warming and to electrify the rural area of Chennai, India. India has more than 280 sunny days, this provides a better chance to use solar energy for electrification. PV system model is used for design the system which shows that the carbon emission level decreases to 8748 kg/year when we install the grid-connected solar system in the proposed area.

Keywords: Solar system · Carbon emission · Utility · Cost · PVsyst V6.73R

1 Introduction

In the recent years, there has been a growing number of Distributed Generators joined into the current distribution network. The distribution based power system include solar generator, fuel cells, wind turbines etc. The solar system is becoming more attractive in some countries due to the convenience of resources and environmental assistance. It can be seen that a sudden change in solar irradiance can pledge a fast reduction in generating capacity. Hence a proper control system is needed to overcome the difficulties associated with it. Solar energy sources convert solar radiation into electrical power. The solar power system is a rapidly rising source of green power supply. The solar system efficiency is affected by many factors so the proper site and panel should

be chosen to avoid these factors. It is affected by the granularity level of spread maximum power point tracking [1–4]. The solar system can directly convert the sun energy into electricity. In most cases, the solar systems are preferred due to many benefits like capital cost less, conditions of environment and low difficulties related with the basic necessities. A DC microgrid is more useful for new installations of the solar system in rural areas, commercial services, or housing buildings. But, the DC microgrid idea can also be used for present connections since existing AC based systems are mainly three-phase schemes having three or four wires, whereas DC system has three wires, negative, positive and ground. However, changing the earlier used system to a DC system will need a significant quantity of apparatus retrofitting with power electronic converters fittings. The number of converters is less in the DC system in comparison to the AC system, the decision of choosing an AC or DC system depends on the converters needs and the type of alternating sources. The output of the solar system is DC and this can be converted into AC by using an inverter. The output of inverter can be used to electrify the different industry or sell out to the grid.

The DC microgrids can provide additional benefits such as reducing the interconnection changing levels of energy resources and storage systems and avoiding the spread of power system turbulences. The solar system becomes popular because this is clean and cost-effective sources. They do not need any fuel, unlike fuel cell stack, biomass, etc. [5]. Nowadays the problem of electricity generation is increasing day by a day which requires a cost-effective solution [6, 7]. Out of various aspects, the cost analysis is the main concern of any alternative energy sources because of the rapidly depleting of fossil fuels reserves [8–15]. Most of the industries look for the alternative energy sources with low generation cost. Considering the above mention statement, the solar-based system is a most cost-effective system, this can be installed easily. The main requirement of the solar system is proper site selection where sun explosion is high. This can generate huge electricity. Hence, there is a need for a cost-effective solution to electrify the industry as well as colony commercial buildings and the solar system is best suited for this purpose. In this paper, 12 kW grid-connected effective solar system design is described in Sect. 2. In Sect. 3, the economic analysis of the proposed system is presented. In Sect. 4, carbon emission reduction analysis with the proposed system is described. Results and discussion are described in Sect. 5. Finally, concluding statements are presented in Sect. 6.

2 12 kW Grid-Connected Effective Solar System

The grid-connected effective proposed solar system consists of an inverter, net meter and solar panels, and solar charge controller as presented in Fig. 1. The geographical site is very important and necessary to gather data from different hubs, Chennai rural area is chosen for the proposed work. In this location, the latitude is 14.00 °N, longitude is 82.18 °E and the altitude is 22 m above sea level. Fig. 2 shows the horizon of the solar system.

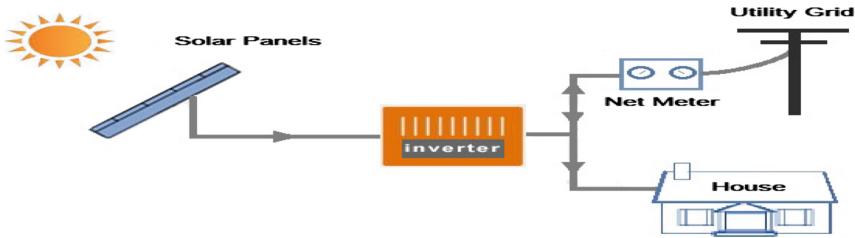


Fig. 1. Grid-connected solar system

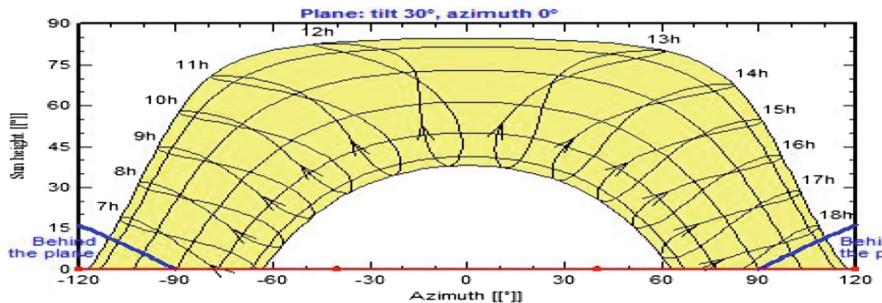


Fig. 2. The horizon of the solar system

The proposed location has more than 305 sunny days, this offers a better opportunity to use solar power for electrification. The 12 kW grid-connected solar system is considered for electrification of the nearby area of Chennai, India.

The entire solar panels energy needed = 12 kWh/day

The number of solar panels can be calculated by using a single rating of solar panels used in the system. We use 250 W 24 V monocrystalline panels. Hence the total number of panel required = $12000/250 = 48$.

Hence, 48 solar panels are required to generate the power of 12 kW.

Table 1. 250 W mono crystalline solar panel specifications

Parameter	Specifications
Maximum power	250 W
Module efficiency	15.4%
Maximum voltage	1000 V DC
Fuse rating	20 A

Table 1 shows the 250 W Monocrystalline Solar Panel specifications. Whereas the inverter size is determined by the utilization hence, Sukam 5 kVA inverter is used for

this purpose with the voltage range of 110–280 V AC. The inverter has the following specifications.

Power factor = 0.85 – 0.90
 Voltage regulation = 220 V \pm 5%
 Relative humidity = Max. 95%

Figure 3 shows the different specifications of the grid-connected solar system in PV syst. This system provides the economical and reliable operation and gives high-quality power to loads/grid.

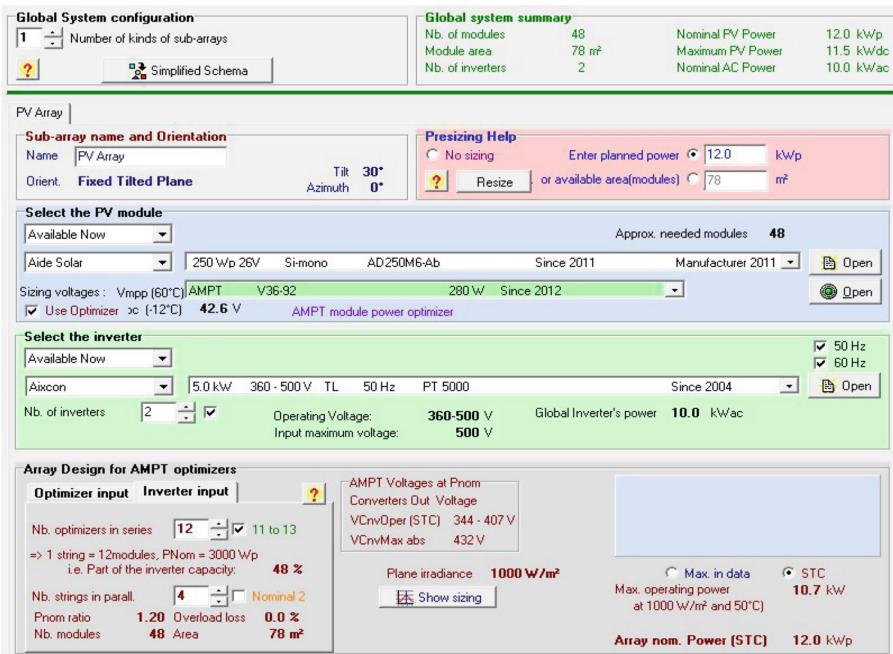


Fig. 3. Different specifications of the grid-connected solar system in PV syst

3 Economics Analysis of Proposed System

The total cost of the grid-connected system is calculated by summing up all the individual appliance cost. We use the Solar India 250 W 24 V Solar Panel with the cost of 9702 INR. As we have to use 48 modules, therefore, the total cost for the complete panel is 465696 INR. Whereas the cost of Sukam Inverters is 79249 INR. The system costs (fires, fuses, switches, O&M etc.) is 280000 INR approx. The SuKam MPPT Solar Charge Controller cost is 54050 INR. Therefore the total likely cost is 842995 INR.

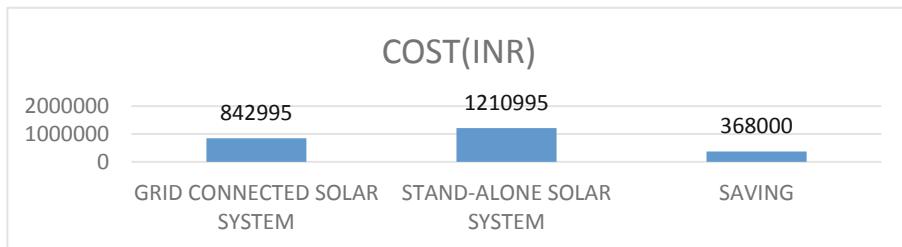


Fig. 4. Cost of the grid-connected solar system and standalone solar system

Whereas, the cost of the standalone solar system is high because of extra use of battery and its charge controller. The cost of the battery and its charge controller is 368000INR. Therefore, the total likely cost of the standalone solar system is 1210995 INR as presented in Fig. 4. Hence, the grid-connected system provides the saving. If there is access power available than the required load, then this power is sold out to the utility grid. This gives the economical and reliable operation.

4 Carbon Emission Reduction with the Proposed System

If alternative energy sources like solar, wind etc. are not used then global warming increases because of carbon emission in all the zones. This is dangerous to the environment, therefore alternative energy sources are used to decrease the carbon footprints. In 1 unit electricity production per kWh produced is equal to the value of 0.810 kg.

For the proposed 12 kW grid-connected solar system, the total numbers of units generated/year are 10800.

$$\begin{aligned} CO_2 \text{ Emission from this 10800 units} &= 10800 \times 0.810 \text{ kg} \\ &= 8748 \text{ kg} \end{aligned}$$

This study shows that 8748 kg CO_2 emission is reduced from thermal power plant because these generated units do not need to buy from the thermal station.

5 Results and Discussions

The proposed system has a maximum load of around 12 kW, this system is installed for 20 years, and hence cost per year will be 42149.75INR. The system generates 10800 units per year, this units would not be purchased from the grid, the cost of these units if purchase from the grid would be 70200INR. Hence this gives the total saving of 28050.25 INR/year. The performance of 8 kW grid-connected solar system is evaluated using PVsyst software.

Table 2. Different parameters throughout the year

Months	GlobHor kWh/m ²	DiffHor. kWh/m ²	Temp. °C	Earray kWH	PR
January	118.2	37.30	13.23	1829	0.847
February	137.0	36.10	17.24	1880	0.817
March	188.2	50.10	23.29	2187	0.787
April	206.5	66.70	29.22	2043	0.763
May	222.1	88.30	32.61	1983	0.759
June	196.5	96.70	32.14	1719	0.773
July	166.4	93.00	31.42	1504	0.781
August	159.9	93.20	30.36	1536	0.784
September	170.6	71.60	28.58	1834	0.782
October	164.5	46.90	25.49	2049	0.782
November	128.5	33.60	19.32	1906	0.814
December	115.1	29.80	14.85	1865	0.836
Year	1973.5	743.20	24.95	22337	0.793

Table 2 shows the different parameters throughout the year which varies with temperature. The GlobHor is 137 in February 2018 and 170.6 in September 2018, this change displays that GlobHor fluctuates throughout the year. The DiffHor. is 37.30 in January and 29.80 in December. Temperature also varies throughout the year.

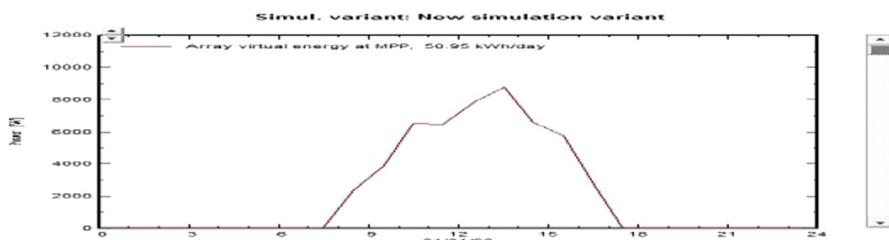
**Fig. 5.** Power output per day

Figure 5 shows the power output per day and the array virtual energy at MPP is 50.95 kWh/day. This power changes with time and it is determined by the solar irradiance changes. When solar irradiance is high then this power would be high and vice-versa. We get the maximum power by using the maximum power algorithm. MPPT controller offers constant output power irrespective of the solar irradiance.

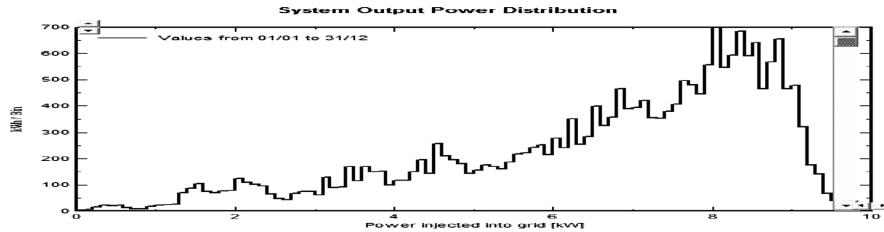


Fig. 6. System output power distribution

Figure 6 shows the output power distribution, this provides the information about the power injected into the grid (kW). The power generated by the solar panel is given to the grid, then this power is used by the utility.

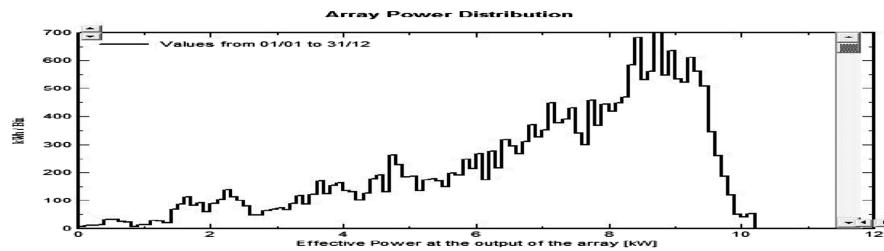


Fig. 7. Array power distribution

Figure 7 shows the effective power at the output of the solar array in kW. This power depends on the solar irradiance and it varies with irradiance. The most effective solar systems are those which give the maximum power throughout the day. It depends on the MPPT controller.

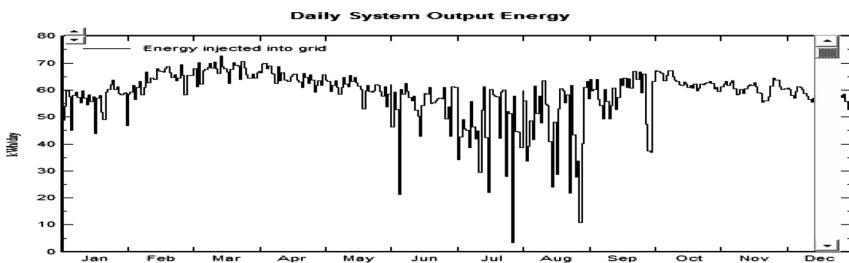


Fig. 8. System output energy

Output energy distribution throughout the effective year is shown in Fig. 8. This graph shows the energy injected into the grid and it's not constant because of the load

and solar energy variations. When there is surplus power available then only energy is given to the grid otherwise it would be used by the appliance in the home/industry.

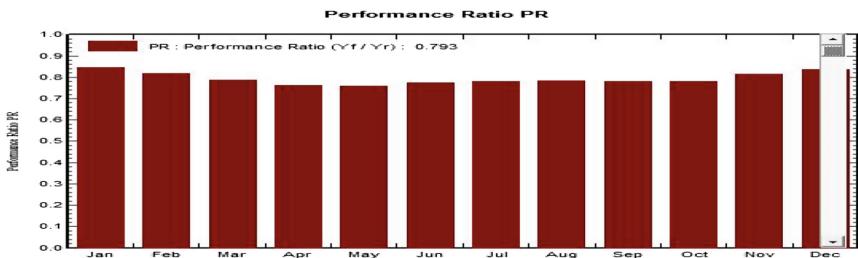


Fig. 9. Performance ratio graph

Figure 9 shows the performance ration graph throughout the year. As shown in Fig. 9, the performance ratio is changed with time as it's not constant, this shows the actual performance of the system. This is not constant because of so many constraints of the solar system. Hence, the proper system can be obtained by using proper controlling action.

*1 USD is equal to 68.84INR as on 11th July 2018.

6 Conclusion

The performance of the Grid-connected solar system during the period January 2018–December 2018 was evaluated for the nearby area of Chennai, India using PV syst software. It can be seen that the month of January generated less solar radiation. This works also shows the costs analysis of the grid-connected solar system for reliable and effective operation. Besides, this system gives the total saving 28050.25 INR per year. Furthermore, the study indicates that 8748 kg CO_2 emission is reduced from thermal based power plant since these solar system generated units do not need to buy from the utility grid. The proposed 12 kW system is used for small area purpose and if any industry/colony uses this system then carbon footprints will be reduced in huge amount therefore, this decreases the global warming.

References

1. Romero-Cadaval, E., Spagnuolo, G., Franquelo, L.G., RamosPaja, C.A., Suntio, T., Xiao, W.M.: Grid-connected photovoltaic generation plants: components and operation. *IEEE Ind. Electron. Mag.* **7**(3), 6–20 (2013)
2. Wang, F., Zhuo, F., Lee, F.C., Zhu, T., Yi, H.: Analysis of existence-judging criteria for optimal power regions in DMPPT PV systems. *IEEE Trans. Energy Convers.* **31**(4), 1433–1441 (2016)

3. Khan, O., Xiao, W., Moursi, M.S.E.: A new PV system configuration based on submodule integrated converters. *IEEE Trans. Power Electron.* **32**(5), 3278–3284 (2017)
4. Wang, F., Zhu, T., Zhuo, F., Yi, H., Shi, S., Zhang, X.: Analysis and optimization of flexible MCPT strategy in submodule PV application. *IEEE Trans. Sustain. Energy* **8**(1), 249–257 (2016)
5. García Franquelo, L., Carrasco, J., Bialasiewicz, J., Galván, E., Guisado, R., Prats, M.A.M., Leon, J., Moreno-Alfonso, N.: Power-electronic systems for the grid integration of renewable energy sources: a survey. *IEEE Trans. Ind. Electron.* **53**(4), 1002–1016 (2006)
6. Kirmani, S., Jamil, M., Akhtar, I.: Bi-directional power control mechanism for a microgrid hybrid energy system with power quality enhancement capabilities. *Int. J. Renew. Energy Res.* **7**(4), 1962–1969 (2017)
7. Kirmani, S., Jamil, M., Akhtar, I.: Effective low cost grid-connected solar photovoltaic system to electrify the small scale industry/commercial building. *Int. J. Renew. Energy Res.* **7**(2), 797–806 (2017)
8. Akhtar, I., Kirmani, S., Jamil, M.: Analysis and design of a sustainable microgrid primarily powered by renewable energy sources with dynamic performance improvement. *IET Renew. Power Gener.* **13**(7), 1024–1036 (2019)
9. Kirmani, S., Jamil, M., Akhtar, I.: Development of effective technique for integration of hybrid energy system to microgrid. In: *Lecture Notes in Smart Innovation, Systems and Technologies*. Springer (2018)
10. Kirmani, S., Jamil, M., Akhtar, I.: Economic feasibility of hybrid energy generation with reduced carbon emission. *IET Renew. Power Gener.* **12**(8), 934–942 (2018)
11. Tariq, M.A., Tariq, M.: Simulink based modeling simulation and performance evaluation of an MPPT for maximum power generation on resistive load. In: *2nd International Conference on Environmental Science and Technology, IPCBEE*, vol. 6 (2011)
12. Asim, M., Tariq, A., Sarwar, A.: Simulation and analysis of a directly coupled solar PV based water pumping system. *J. Electr. Eng.* **2**(3), 72 (2009)
13. Asim, M., Tariq, M., Mallick, M.A., Ashraf, I.: An improved constant voltage based MPPT technique for PMDC motor. *Int. J. Power Electron. Drive Syst. (IJPEDS)* **7**(4), 1330–1336 (2016)
14. Asim, M., Parveen, H., Mallick, M.A., Siddiqui, A.: Performance evaluation of PFC boost converters. *Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng.* **3**(11), 107–110 (2015)
15. Akhtar, I., Kirmani, S., Jamil, M.: Effective grid-connected solar home-based system for smart cities in India. In: *Lecture Notes in Springer, ICSC, Jamia Millia Islamia*, 14–16 March, India (2019)



Efficient Load Scheduling Algorithm Using Artificial Neural Network in an Isolated Power System

Vijo M. Joy^(✉) and S. Krishnakumar

School of Technology and Applied Sciences,
M. G. University Research Centre, Edappally, Kochi 682024, Kerala, India
vijomjoy@gmail.com, drkrishsan@gmail.com

Abstract. In this paper, an efficient load scheduling technique is presented to meet the unpredictable power supply requirements. The power consumption in upcoming days' must be scheduled in a power system. The accuracy of the system significantly affects the economic operation and consistency of the system. The power generation system fails due to instability at the peak load time. Usually load shedding procedure is used to compensate demanded load. Unnecessary and extra loads are disconnected in load shedding. The proposed system overcomes this difficult by forecast the load based on the load affected constraints. To predict and schedule the load with the previous data is a challenging process when an unexpected change occurs - like days with extreme weather or special days. With the current advance of artificially intelligent tools, it is potentially possible to improve the existing demand of load. For optimal load scheduling, Artificial neural networks are used. The Levenberg-Marquardt backpropagation algorithm is used for the training purpose to minimize the error function. The results are compared by correlation analysis.

Keywords: Load scheduling · Artificial neural network · Backpropagation · The regression method

1 Introduction

Artificial neural networks (ANN) are used for the prediction of a reliable load scheduling method. This work provides an intelligent method to meet the demand of steady power supply instead of fluctuated. Generally, it is experienced with load shedding process when the power generation system fails due to the uncertainty. In the load shedding process, additional loads are isolated. The present method overcomes this problem. The power can be scheduled by considering the parameters like time, weather condition, temperature, humidity and other extra loads. Optimum design of power scheduling is demanded in this method. The load demand in each area is also different and may vary non-linearly. In order to generate a mapping between the above inputs and the desired output, ANN is trained using simulated data for a number of cases [1]. The ANN model is proved to be much faster than dynamic simulation programs. Prediction of load demand for an area, power losses due to different parameters like heating effect, and priority-based load scheduling are the tools for the

scheduling of power sources. It is also convenient to calculate the initial time of distribution, restrict the electric energy on least priority areas, economical optimization and availability of energy sources implemented in the scheduling process. It becomes a challenging task to consider all the above-mentioned parameters due to its complexity. Nowadays, it is due to the non-linearity property of the systems, ANN-based technology is popularly accepted. Energy losses due to the variation of impedance are another major issue [2, 3]. For an ANN level application, it is need to specify the architecture and learning algorithm. In the engineering applications, Back Propagation Neural Network (BPNN) is treated as the most popular neural network technique. A trained neural network can be used to execute an isolated task by rearranging the value of weights between the elements. The neural network system is modified, based on the difference of the system response and the target value, until the network output equivalent to the target. The training operation or adjustments are performed in the network until a given input leads to a specific target response. In the supervised learning algorithm, a number of such input/target pairs are used to adjust or instruct a neural network. To obtain the voltage stability, arrange the output from sources based on the availability and cost using the neural network [4]. The factors that affect the variation of power load are weekdays, time, weather factor and unexpected events like special programs, emergency situations and holidays. Extra loads added to the system increase the power consumption. The advantage of ANN is its outstanding performance in data organizations and function calculation [5]. ANN is also capable of identifying dependencies from ancient data without a need to develop a detailed regression model. In this work, ANN is trained with different load requirement. Once it has been trained, it acquires the ability to give load scheduling pattern for any value for load demand [6]. The rest of the paper is as follows: Sect. 2 defines the system modelling and architecture, briefly explain the BPNN algorithm, Sect. 3 presented results and discussion and conclusion in Sect. 4.

2 Methodology

2.1 Artificial Neural Network

ANN performs is similar to a human brain and massively analogous-circulated data treating arrangement with a precise flexible structure. They have a remarkable non-linear capturing capability [7]. The network consists of input, output, and hidden layers. Every layer consumes a deportment of neurons and is arranged to implement a specific assignment. The ANN is experienced to assess the tasks that can be influenced by a large number of participations and are normally unrevealed [8]. The networks possess numerical weights that can be adjusted established on involvement, building neural nets, flexible to contributions, and capability of training.

The layers in the neural network consist of a number of processing nodes which are connected in a network. This processing node is an artificial form of a real neuron [9]. The model of a neuron is shown in Fig. 1. The input $x_1, x_2 \dots x_n$ their corresponding weights $w_1, w_2, \dots w_n$ bias ‘ b ’ and activation function ‘ f ’ applied to the weighted sum of the inputs.

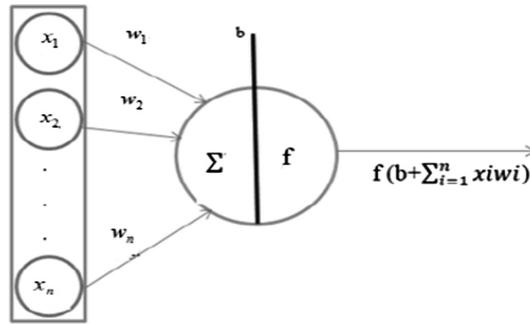


Fig. 1. Neuron model

2.2 BPNN

Nowadays in the engineering applications, BPNN is treated as the most popular neural network technique. The BPNN is a multilayered neural network having “feed-forward” connections between the input and hidden layers and then it extends to the system response session [10]. The most important goal of the BP algorithm is to nullify the mean square error between the predicted and the desired system responses. A three-layered BPNN is used in this analysis, which includes an input layer, a hidden layer, and an output layer. Figure 2 shows the neural network architecture of BPNN. It is constructed for predicting the system response values from different input parameters. The information from the external sources is received by the input layer of the network, and for the processing of this collected details, handover the same to the neural network. The whole information acquired from the input layer is processed by the hidden layer, which is present in between input and output layers. The organized information from the hidden layer is received by the network output layer, and the results are directly sent to an external receptor. The non-linear relation between the load and its correlative influence parameters based on BPNN is established via a continuous training process [11].

The BPNN is a local optimization algorithm for training network and uses the Levenberg – Marquardt technique [12, 13]. This algorithm takes more memory, but its execution time is less. When the generalization stops improving, this algorithm is automatically stopped. The network error is backpropagated after comparing with the target value and the actual output of ANN [14]. The ANN supervised learning algorithm is named as BPNN is used to optimize the neural networks by forwarding the neural network training process [15]. The BPNN is a learning method based on the error-correction rule. This method gradually minimizes the error function by adjusting the connection weights. The difference between the actual response and the desired response is considered as the error function.

$$e_i = (t_i - o_i) \quad (1)$$

$$E = \frac{1}{2} \sum_{i=0}^j (t_i - o_i)^2 \quad (2)$$

where i denotes the layer index, t_i is the desired output, and O_i is the actual network output.

The algorithm can be summarized in the following stages: (i) feed-forward stage computation, the (ii) error is backpropagated to the hidden layer and output layer, (iii) connection weights updating [16, 17]. When the error function value becomes less than the standard value, then the algorithm stops its updating process. The Levinberg-Marquardt training algorithm is used in the BPNN for getting more stability. For the multi-layer perceptron, BP is considered as the best algorithm [18, 19]. With the parameters shown in Table 1, the feed-forward ANN model is trained using back-propagation algorithm [20]. Figure 3 shows the architecture of ANN structure used in

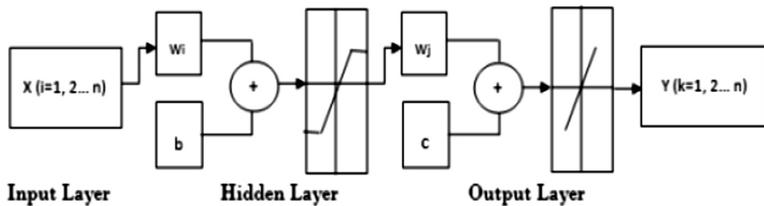


Fig. 2. BPNN architecture

Table 1. Parameters in artificial neural network

Parameter	Value
Weight range	[-1, 1]
Threshold range	[-1, 1]
Activation function	Sigmoid
Learning coefficient	0.2
Momentum	0.8
Stopping rule (epoch)	1000

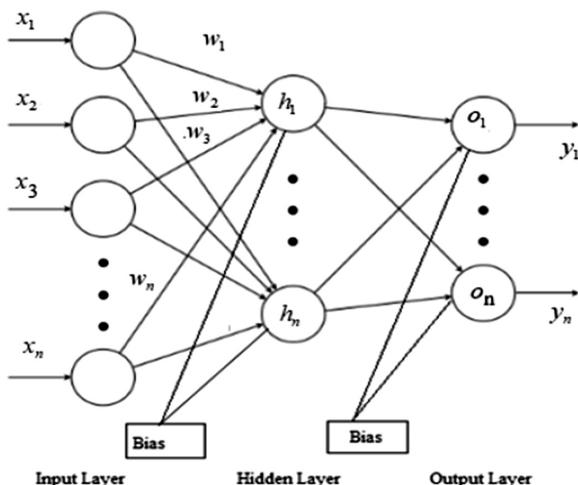


Fig. 3. ANN structure

this work. It is also called Multi Layer Perceptron because of the multiple layers. The sigmoid activation function generates system response with values between 0 and 1. MATLAB is the platform used for training and programming of ANN. The network is trained with the 1000 iterations and the training function used is “trainlm”. The weights are calculated with the help of backpropagation code is used for weights calculation.

3 Results and Discussion

The performance of the developed method is tested using the actual hourly load data. The results obtained from the ANN method are compared by a linear regression method. The proposed system shown in Fig. 4, consists of 14 input neurons, 50 hidden layers and 1 output neuron (14-50-1). The input for the network is the parameters affecting the load and output is the demanded load. Collected data sets are trained by using the Levenberg-Marquardt backpropagation algorithm. The algorithm is terminated its training process when generalization stops the refining.

The performance of the present neural network is shown in Fig. 5. Lower values of Mean Square Error (MSE) are better, towards zero means there is no error in the system. In this work, the best validation performance is 2.67×10^{-3} at epoch 35.

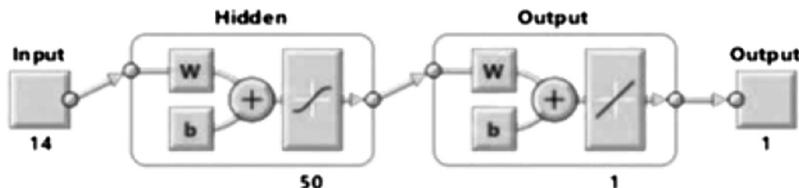


Fig. 4. ANN used for training

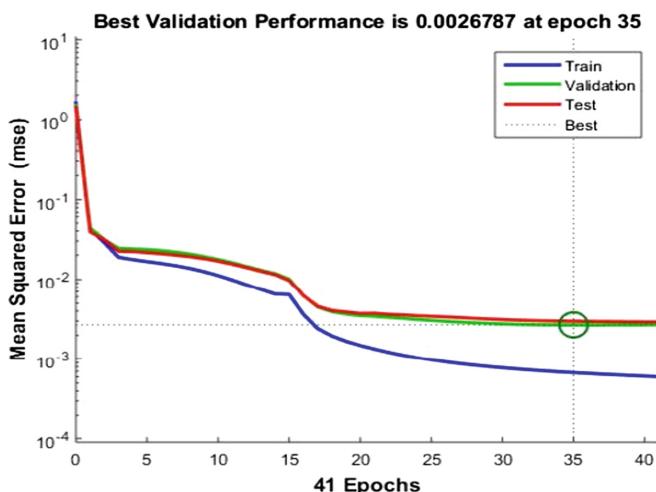


Fig. 5. Performance of the neural network

Table 2. Training results of the proposed system

Type	MSE	R
Training	3.04819e-4	9.87241e-1
Validation	2.92262e-3	9.46630e-1
Testing	3.52997e-3	9.41283e-1

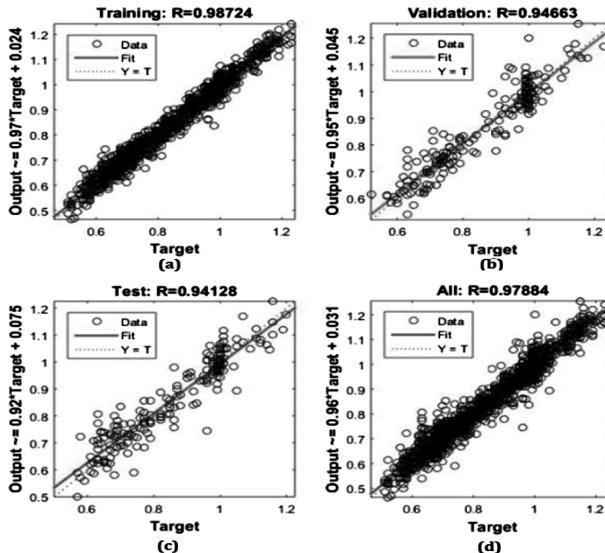
**Fig. 6.** Regression analysis of the system: (a) Training (b) Validation (c) Test and (d) Total performance

Figure 6 shows the Regression (R) analysis of the system. It is a statistical procedure for approximating the relationship among variables. Regression values measure the correlation between outputs and targets. The value of R is ‘1’ means a close relationship and is ‘0’ means random relationship. In this 75% of the data is used for training, 15% used for the validation and 15% used for the testing purpose. Table 2 shows the training result of the present work.

4 Conclusion

The intention of this work is to carry out the development of an ANN based technology for scheduling the load. The Levenberg-Marquardt backpropagation algorithm is used for load scheduling. This algorithm takes more memory, but its execution time is less. The results of this method show that this algorithm is very effective when training large sets of data. The MSE and Root Mean Square Error (RMSE) have been calculated. The system response follows the target very well for training, testing, and validation. For the total response, the regression value is 0.979. For the scheduling purpose, neural network using backpropagation algorithm is the best-suited algorithm to calculate the error.

References

1. Hooshmand, R., Moazzami, M.: Optimum design of adaptive under frequency load shedding using artificial neural networks in isolated power system. *Electr. Power Energy Syst.* **42**, 220–228 (2012)
2. Mathur, D.: Maximum power point tracking with artificial neural network. *Int. J. Emerg. Sci. Eng.* **2**(3), 38–42 (2014). ISSN 2319-6378
3. Kumar, S.S., Neha, S.: Load scheduling algorithm prediction for multiple tasks using time series neural network. *IJARCSSE* **3**(5), 554–558 (2013). ISSN 2277 128X
4. Kumaran Kumar, J., Ravi, G.: ANN-based long term sector-wise electrical energy forecasting. *ARPN J. Eng. Appl. Sci.* **10**(1), 115–121 (2015). ISSN 1819-6608
5. Hsu, C.T., Kang, M.S., Chen, C.S.: Design of adaptive load shedding by artificial neural networks. *IEE Pro.-Gener. Transm. Distrib.* **152**(3), 415–421 (2005)
6. Gonzalez, P.A., Zamarreno, J.M.: Prediction of hourly energy consumption in buildings based on a feedback artificial neural network. *Energy Build.* **37**(6), 595–601 (2005)
7. Joy, V.M., Krishnakumar, S.: Optimal design of power shedding using artificial neural network in an isolated power system. *Int. J. Pure Appl. Math.* **118**(8), 289–294 (2018)
8. Suman, M., Venugopal, M.: ANN-based short term hydrothermal scheduling. *RECENT* **14** (3), 191–195 (2013). (39)
9. Grossi, E., Buscema, M.: Introduction to artificial neural networks. *Eur. J. Gastroenterol. Hepatol.* **12**(19), 1046–1059 (2007)
10. Alsmadi, M., Omar, K., Noah, S.: Back propagation algorithm: the best algorithm among the multi-layer perceptron algorithm. *Int. J. Comput. Sci. Netw. Secur.* **9**(4), 378–383 (2009)
11. Maind, M.S.B., Wankar, M.P.: Research paper on basic of artificial neural network. *Int. J. Recent Innov. Trends Comput. Commun.* **2**, 96–100 (2014)
12. Nawi, N.M., Rehman, M.Z., Aziz, M.A., Herawan, T., Abawajy, J.H.: An accelerated particle swarm optimization based Levenberg Marquardt back propagation algorithm. In: Loo, C.K. et al. (eds.) *Neural Information Processing. Lecture Notes in Computer Science*, vol. 8835, pp. 245–253. Springer, Cham (2014)
13. Lv, C.: Levenberg–Marquardt backpropagation training of multilayer neural networks for state estimation of a safety-critical cyber-physical system. *IEEE Trans. Ind. Inf.* **14**(8), 3436–3446 (2018)
14. Rao, C.S.: Design of artificial intelligent controller for automatic generation control of two area hydrothermal system. *Int. J. Electr. Comput. Eng.* **2**(2), 183 (2012)
15. Suliman, A., Zhang, Y.: A review on back-propagation neural networks in the application of remote sensing image classification. *J. Earth Sci. Eng.* **5**, 52–65 (2015)
16. Hota, P.K., Chakrabarti, R., Chattopadhyay, P.K.: Short-term hydrothermal scheduling through evolutionary programming technique. *Electr. Power Syst. Res.* **52**(2), 189–196 (1999)
17. Basheer, I.A., Hajmeer, M.: Artificial neural networks: fundamentals, computing, design, and application. *J. Microbiol. Methods* **43**(1), 3–31 (2000)
18. Joy, V.M., Krishnakumar, S.: Efficient load scheduling method for power management. *Int. J. Sci. Technol. Res.* **5**(01), 99–101 (2016)
19. Le, K.C., Dinh, B.H., Nguyen, T.: Environmental economic hydrothermal system dispatch by using a novel differential evolution. *J. Eng. Technol. Sci.* **50**(1), 1–20 (2018)
20. Mishra, D.K., Dwivedi, A.K.D., Tripathi, S.P.: Efficient algorithms for load forecasting in electric power system using artificial neural network. *Int. J. Latest Res. Sci. Technol.* **1**(3), 254–258 (2012)



Integrated Static Analysis for Malware Variants Detection

Rinu Rani Jose^(✉) and A. Salim

College of Engineering Trivandrum, Thiruvananthapuram, Kerala, India
{rinuranjose,salim}@cet.ac.in

Abstract. The influence of malware is growing exponentially by the invention of new malicious programs and potentially unwanted applications. Malware detection is critical for protection against data theft, security breaches and other related dangers. But the detection techniques continue to be challenging, as the attackers invent new techniques to resist the detection methods. Thus efficient techniques are required for the identification of malware variants or samples. This paper proposes an integrated static method for the efficient detection of malware. The proposed approach is a combination of two different static models. An image based model which uses image features for the analysis and a code based model which uses opcodes for the analysis of malware. Machine learning techniques are used for the classification of samples. The combined model efficiently classifies the malware variants with an accuracy of 95% and is resistant to the code obfuscation techniques associated with traditional static analysis.

Keywords: Malware detection · Static analysis · Code visualization · Opcode features · Machine learning

1 Introduction

The term malicious code describes that part of code in a software system which is intended to cause security breaches, undesired effects and damage to a system. Also being an application security threat, it cannot be controlled effectively by existing antivirus software alone. Furthermore, if anti-virus engines can successfully detect those malware, then the malware writers will update parts of the code of the original malware using some obfuscation techniques. The newly evolved malware has behavioral similarities with the originals ones. Such malware are known as a ‘variant’ within that malware family, where a set of malware with similar logic is called as a malware family. Thus over 98% of the new malware samples are actually derivatives/variants from existing malware families.

The malicious code variants detection is particularly challenging when the security protection is considered. Mainly there are two approaches for malware detection: static method and dynamic method. Static detection works by disassembling the malicious code and then analyzing the execution logic of the code. On the other hand, dynamic detection executes the code in a safe virtual environment and then analyzes the

behavioral logic of malware code. Static and dynamic detection are both feature based detection approaches. At first, the textual or behavioral features of the malware code are extracted, and then detection is carried out by analyzing those extracted features. Several data mining methods are also used in recent years for analyzing the features of malicious code. This methodology is very efficient with low false positives rates when compared with the traditional heuristic-based methods of detection. Static analysis is vulnerable to different obfuscation techniques while the dynamic analysis causes an inexact behavior log of the malware due to the virtual environment in which it runs and also the detection fails at certain condition triggered actions of malware. The proposed method performs an integrated static analysis for the detection of malware. The overall method can be divided into two phases. The first phase deals with the image based analysis where the malware detection problem is converted into an image recognition problem thereby resisting the obfuscation problems associated with the traditional static detection methods. The second phase deals with the opcode analysis which uses the benefits associated with the binary codes of a program in the form of opcodes for the classification of malware.

2 Related Work

Many works had been done so far in the field of malware detection. Most of them relies on either static or dynamic technique, while some of the works employed an integrated approach. Nataraj et al. performs malware analysis by visualizing and processing malware as images [4]. A GIST algorithm is used to capture the features of malware images and to characterize the malware globally. But this GIST algorithm posses low computational speed. Zhihua et al. employed a CNN network for the study of malware image features and for their automatic classification [1]. At first, the binary file is converted into an image and then using CNN classification is done. Jin et al. described the identification of significant permissions through static analysis and its usage in the malware detection along with supervised learning algorithms [11]. Chatchai et al. proposed a static classification model based on n-grams sequential pattern features [3]. Here the n-grams are generated from the disassembled binary file in the form of hexadecimal string. Further sequential pattern extraction is carried out for the feature vector creation and classification. Cesare et al. had proposed another static method of malware detection in which malware signature generation is based on a set of control flow graphs [12]. The sub graphs or n-gram strings of these control flow graphs forms the feature vector. Then with a string distance matching algorithm, the similarity with known malware is computed. This method is efficient against the limitations of byte level and instruction level classification but fails at packing and obfuscation issues. Deeptha et al. proposed a combined method of using static opcode sequences and call graphs for the detection of malware. The two feature vectors are merged to form an integrated feature vector which is then normalized for classification [7]. Salehi et al. proposed a malware detection method which uses API calls and their arguments as the features and inspect their outcome on the classification result [10]. Islam et al. put

forward a combined static and dynamic classification method. Here function length frequency and PSI information of each file is taken as the static feature and API function names along with its arguments forms the dynamic feature [2].

3 Architectural Overview of the Proposed Model

A combined static analysis is employed here which uses a combination of two different static features, opcode features and image features for the detection of malware. The overall analysis can be divided into two modules. The first module deals with the conversion of executables into images and then extraction of features from those converted images. The second module performs opcode analysis which extracts opcode features from the disassembled binary codes. The two feature vectors obtained are then combined together to form an integrated static feature vector which is used for the classification of malware. The Fig. 1 shows an overview of the integrated model.

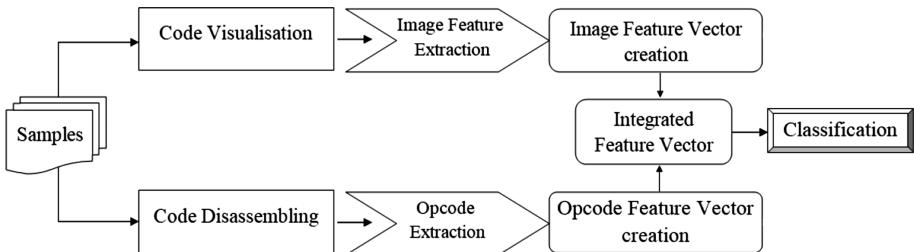


Fig. 1. Overview of the Integrated Model

3.1 Malware Detection Based on Code Visualization

Unlike from the traditional static methods, this image based detection is an entirely different approach towards malware classification. This mode of detection converts a malware detection problem into an image recognition problem. The method also resolves the obfuscation problems faced by the static analysis. The primary phase for this approach is the conversion of the binary executable into grey scale images. Once the executable has been visualized as images, then using different image processing techniques we can classify the images into different classes, thus converged to an image recognition problem. The overall image based detection is shown in Fig. 2.

Code Visualization. At first the binary file is mapped into a 1-D array using the in-built python packages. The image resolution is then defined based on the file size. Some appropriate image widths taken from [4] based on certain empirical observations for different file sizes are mentioned in Table 1. According to the specified resolution, this 1-D array can be transformed to a 2-D matrix. Then the generated image matrix is

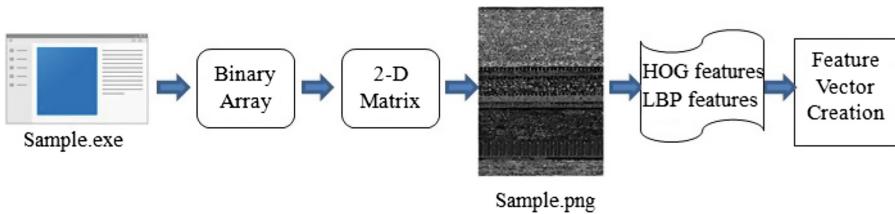


Fig. 2. Malware Detection based on Code Visualization

mapped into a grey scale image. Thus the benign and malicious logic has been interpreted as grey-scale images.

Algorithm 1 Image Feature Extraction

Input: S: Sample set containing malware and benign files

Output: R: Binary feature vector

for each s_i in S do

 Convert the binary file into 1-D array

 Set width of the image as per file size in Table.1

 convert 1-D array to 2-D array according to width

 Map the image matrix formed into a png file

 Save the grey-scale image generated, *Images*.

end

for each img_i in *Images* do

 Extract LBP Features, LBP_hist

 Extract HOG features, HOG_hist

 Combine LBP_hist and HOG_hist and save as a single feature vector

end

Store the feature vectors of all images into a feature set and input this to the classifier

Image Feature Extraction and Feature Vector creation. For the classification of images, instead of training a CNN on a set of images and using the penultimate layer's output as the image representation, we simply compute image descriptors for all the images, and encode each image's descriptors as a single vector. Here mainly two feature descriptors are extracted, Histograms of Oriented Gradients (HOGs) and the Local Binary Patterns(LBPs). These HOG features and LBP feature are known to be effective for the efficient classification of images. Several studies had found that when LBP is combined with the HOG descriptor, it improves the detection performance. These extracted hog values and lbp values are concatenated and saved as a single vector. These saved feature vector can be then used for the classification. The image feature extraction process is briefly explained in algorithm 1.

Table 1. Image width based on different file sizes

File size (KB)	Image width
<10	32
10–30	64
30–60	128
60–100	256
100–200	384
200–500	512
500–1000	768
>1000	1024

3.2 Malware Detection Based on Opcode Analysis

Opcode Analysis is a static detection technique in which the features are extracted from the binary code of programs and are used to create models describing them. Binary code of a program contains very useful information about the malicious behavior of the program in the form of op-code sequence and functions. Therefore by the analysis of these opcodes, it is possible to extract the malicious nature of the code.

Opcode Extraction. Here opcodes from the program codes are extracted and analyzed for the classification of malware. For the extraction of OpCodes, the binary codes are first converted into assembly language using a code disassembler and then with the help of a python program the opcodes are extracted from the disassembled code. *Objdump* command is used to disassemble the codes in machine language.

Feature Vector creation. The separated opcode sequence from the disassembled code is then analyzed using n-gram based method. The size of n-gram is chosen based on certain observations. As the value of the n increases the number of similar n-grams among two files within the same class itself is very low. Here the size of n-gram is chosen as 3, since it shows best effective results compared to other n-grams. The 3-gram patterns of opcodes are generated using the Linux utility, *text2ngram*. All possible 3-grams along with their frequency of occurrence were computed from the disassembled code and stored in a separate file. The 3-grams with frequency below a threshold were filtered from both malware and benign samples. Also in order to reduce the feature vector size and to perform the classification more precisely, the frequent 3-grams that are common in both the classes were filtered out. The final feature vector is an array of 1 s and 0 s which indicates the presence or absence of the 3-gram patterns. A sample opcode feature vector created is shown in Table 2. Thus the feature vector corresponding to each sample was created. The algorithm 2 explains the overall steps in the opcode analysis phase.

Table 2. The opcode feature vector.

Class	3-gram1	3-gram2	...	3-gramn
Benign	0	1	...	1
Malware	1	1	...	0

Algorithm 2 Static Feature Extraction**Input:** S: Sample set containing malware and benign files**Output:** R: Binary feature vector

```

for each  $s_i$  in S do
    Disassemble the file using Objdump as T
    Extract all the opcodes from T
    Generate 3-grams from the opcodes
    Add each unique 3-gram to a new text file  $f_{text}$ 
end
for each 3-gram in  $f_{text}$  do
    set count=0
    for each  $s_i$  in S do
        Increment count if 3-gram is present in  $s_i$ 
        and store that 3-gram and its count in  $F_v$ 
    end
end
Sort  $f_{text}$  based on the frequency of 3-grams
Remove 3-gram having frequency <Threshold
Update the file  $F_v$  according to the new list
i = 0;
for each  $s_i$  in S do
    i = i+1;
    for each 3-gram in  $F_v$  do
        k = 0;
        if 3-gram present in  $s_i$  then
            | set  $m_{ik}=1$ ;
        else
            | set  $m_{ik}=0$ ;
        end
    end
    k=k+1; //Each  $m_i$  is a feature vector
end
Store the binary feature vectors of all  $s_i$  in S and input this to the classifier

```

3.3 Integrated Multi-feature Model

The integrated model combines image features and opcode features in order to have the benefits of both the approaches. The two different feature vectors are combined to form a single feature vector which is then used for the training and classification. The detection accuracy is high for this integrated model compared to individual models.

3.4 Classification

Machine Learning algorithms had marked its excellence in the field of malware detection. There exists several ML algorithms for the efficient classification of the suspicious samples. The efficiency of different ML algorithms changes depending upon the type of data sets in which it is working. Here the classification is carried out with Linear Support Vector Machine and AdaBoost Algorithm because they suits best with our data. In order to validate the stability of our model we performed a 5-fold cross validation.

4 Experimental Setup and Results

The whole analysis is carried out with 1000 samples containing equal proportion of malign and benign samples in order to avoid the problem of imbalanced data. The malicious files were downloaded from the VirusShare community website and benign samples were obtained from Windows system directory. The experimental environment is set up on an Ubuntu 18.04 operating system.

Table 3. Classification results of the different models

Model	SVM				AdaBoost			
	Precision	Recall	F1score	Accuracy	Precision	Recall	F1score	Accuracy
Image based model	.86	.85	.85	85%	.86	.85	.86	85.6%
Opcode analysis	.92	.91	.91	91.4%	.91	.93	.92	92%
Integrated model	.96	.93	.95	95%	.92	.93	.92	93%

Analysis is carried out with both individual models and the integrated model to find out the best accuracy. The performance of the classification models were evaluated using measures Precision, Recall, F1-score and Accuracy. Table 3 shows the classification results of different models with linear SVM and AdaBoost classifier.

5 Conclusion

In this work we proposed an integrated static model which combines an opcode analysis technique along with an image based approach for the classification of malware. From the results it is clear that the integration of the image feature along with code feature improves the accuracy of the classification model. The proposed static approach achieved a better classification accuracy of 95% at a significantly less computational cost. The model outperforms the traditional static approach and carried out the classification in a simpler way without the execution of code. The results also

shows that the support vector machine learning technique is best equipped to classify our data. Thus the proposed integrated static model can be used for the efficient detection of malware with comparatively better accuracy than several existing isolated approaches. The accuracy can be further increased by reducing the size of the feature set using several feature selection algorithms.

References

1. Cui, Z., Xue, F., Cai, X., Cao, Y., Wang, G.: Detection of malicious code variants based on deep learning. *IEEE Trans. Ind. Inf.* **14**, 3187–3196 (2018)
2. Islam, R., Tian, R., Batten, L.M., Versteeg, S.: Classification of malware based on integrated static and dynamic features. *J. Netw. Comput. Appl.* **36**, 646–656 (2013)
3. Liangboonprakong, C., Sornil, O.: Classification of malware families based on n-grams sequential pattern features. In: 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA), pp. 777–782. IEEE (2013)
4. Nataraj, L., Karthikeyan, S., Jacob, G., Manjunath, B.: Malware images: visualization and automatic classification. In: Proceedings of the 8th International Symposium on Visualization for Cyber Security, pp. 4. ACM, Pittsburgh (2011)
5. Ye, Y., Li, Y., Chen, Y., Jiang, Q.: Automatic malware categorization using cluster ensemble. In: Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, KDD 2010, pp. 95–104. ACM, New York (2010)
6. David, O.E., Netanyahu, N.S.: Deepsign: deep learning for automatic malware signature generation and classification. In: International Joint Conference on Neural Networks (IJCNN), pp. 1–8. IEEE (2015)
7. Deepta, K.P., Salim, A.: Detecting malwares using dynamic call graphs and opcode patterns. International Conference on Advances in Computing and Data Sciences. CCIS, vol. 721, pp. 91–101. Springer, Singapore (2017)
8. Islam, R., Tian, R., Batten, L.M., Versteeg, S.: Classification of malware based on string and function feature selection. In: Cybercrime and Trustworthy Computing Workshop (CTC) 2010, pp. 9–17. IEEE, Victoria (2010)
9. Moser, A., Kruegel, C., Kirda, E.: Limits of static analysis for malware detection. In: Proceedings of the IEEE 23rd Annual Computer Security Applications Conference, ACSAC, pp. 421–430. IEEE, Florida (2007)
10. Salehi, Z., Ghiasi, M., Sami, A.: A miner for malware detection based on api function calls and their arguments. In: 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP), pp. 563–568 (2012)
11. Li, J., Sun, L., Yan, Q., Li, Z., Srisa, W., Yex, H.: Significant permission identification for machine learning based android malware detection. *IEEE Trans. Ind. Inf.* **14**, 3216–3225 (2018)
12. Cesare, S., Xiang, Y., Zhou, W.: Control flow-based malware variant detection. *IEEE Trans. Dependable Secure Comput.* **11**, 307–317 (2014)
13. Das, S., Liu, Y., Zhang, W., Chandramohan, M.: Semantics-based online malware detection: towards efficient real-time protection against malware. *IEEE Trans. Inf. Forensics Secur.* **11**, 289–302 (2016)
14. Naval, S., Laxmi, V., Rajarajan, M., Gaur, M., Conti, M.: Employing program semantics for malware detection. *IEEE Trans. Inf. Forensics Secur.* **10**, 2591–2604 (2015)
15. Santos, I., Brezo, F., Sanz, B., Laorden, C., Bringas, P.: Using opcode sequences in single-class learning to detect unknown malware. *IET Inf. Secur.* **5**, 220–227 (2011)



Data Storage in Cloud Using Key-Policy Attribute-Based Temporary Keyword Search Scheme (KP-ABTKS)

Nallella Thirupathi^(✉), K. Madhavi, G. Ramesh,
and K. Sowmya Priya

GRIET, Hyderabad, India

thirunallella511@gmail.com, ramesh680@gmail.com,
sowmya.kasaraneni@gmail.com, bmadhaviranjan@yahoo.com

Abstract. Now a days, it is open for information holder to re-appropriate their information to the cloud. Brief catchphrase seek on secret data in an exceedingly cloud setting is the principle focal point of this investigation. Here, the data in cloud storage isn't trustworthy. So, it is compulsory to source information with encryption and used quality-based keyword search plans. In ABKS, The inquiry tokens might be utilized to extricate the ciphertexts that are created whenever and include the comparing catchphrase. The catchphrase mystery property and is secure against specifically picked keyword assault (SPKA) below the balance of Decisional Bilinear Diffie-Hellman (DBDH) presumption. This may lead information leakage and complexity, so we have to give more preservation. In this paper, we propose the KP-ABKTS plans, where the information proprietor creates an accessible cipher text identified with a catchphrase and the season of encoding as indicated by an expected access control strategy, and re-appropriates it to the cloud. This schemes enables in multiusers scenario for avoiding complexity when compared with PEKS.

1 Introduction

Distributed computing acknowledge a fundamental in our well ordered life, since it gives gainful, dependable and flexible assets for information storing up and computational exercises at an extremely insignificant exertion. In any case, the speedy access of the cloud to the dubious data of its clients undermines their security. An insignificant arrangement to address this issue is encoding information before redistributing it to the cloud. In any case, searching for on the blended information is particularly irksome. open key encryption with catchphrase pursuit is a cryptographic foul to help looking on the blended information. In PEKS, every datum proprietor who acknowledges general society key of the typical information client makes an accessible figure message by strategies for his/her open key, and re appropriates it to the cloud. By at that point, the information client confines a pursuit token identified with a self-unequivocal short lived catchphrase look for by utilizing his/her puzzle key, and problem to the cloud. The cloud pro center runs the solicitation task by utilizing the got intrigue token in light of a real worry for the information client to locate the basic outcomes to the proposed

watchwords. In a safe ABKS plot, an information proprietor can't get any data about the watchwords which the information clients mean to search for. In any case, in a large portion of the PEKS and ABKS plans, when the cloud gets an extensive solicitation token identified with a specific fleeting catchphrase look, the cloud can assess the watchword's quality as of now similarly, any future figure content. Thusly, if the enemy understands the taking a gander at watchword of the objective solicitation token, by then she will be able to get a couple of data about the going with accounts which will be re appropriated to the cloud. As such, it will be reliably secure to control the day and age in which the intrigue token can be utilized. Pushed by this issue, Abdalla et al. shown the likelihood of open key encoded with brief watchword scan for (PETKS) which limits the help of the token to a particular time. They related cloud character based encryption in their nonexclusive course of action. Likewise, Yu et al. recommended sed another open key accessible encryption in the uncommon situation of fleeting ephemeral watchword look for look. Despite the uncommon highlights of their courses of action, these plans don't give the working environment to information proprietors to complete their ordinary access approach. Here, we come up with an astute idea of Key-Policy Attribute-Based Temporary watchword Search (KPABTKS).

2 Related Work

Several existing researches make use of Attribute-Based Encryption(ABE) as a district of their deliberate answer to comprehend completely specific security objectives. Li et al. deliberate a affected person valuable framework for information sharing access control to private health report hold on in cloud servers. They used the ABE strategies to realize a high degree of the person's privateness and a ne-grained information get right of entry to management for private fitness data. Another effort in blended Key policy Attribute-Based Encryption(KP-ABE) with distinct strategies to on the identical time deliver the goods records confidentiality and scalable records get admission to management in the cloud server.

Zheng et al. presented the thought of property-based watchword seek (ABKS) to enable an information proprietor to control the entrance of information clients for looking on his/her re-appropriated scrambled information. They utilized characteristic based encryption (ABE) to develop an accessible cryptographic crude in the multi-sender/multi collector demonstrate. In their work, the real information clients can enrol the cloud to run the hunt task for them without requiring any collaboration with the information proprietor. In a protected ABKS conspire, an information proprietor can't acquire any data.

Content Policy Attribute-Based Encryption (CP-ABE) grants to scramble information under a get to arrangement, decided as a steady blend of traits. Such figure writings perhaps unscrambled by anyones a great deal of properties that amuse the passageway strategy. We come with a Cipher Text-Policy characteristic→-Based Encryption, that depends on a continuous mystery distribution strategy termed Linear Integer Secret Sharing Scheme (LISS). In this plan, the encrypt or can decide the passageway approach with respect to LISS framework M, over the properties in the structure. The plan is explicitly protected concealed by Decisional Bilinear Diffie-Hellman (DBDH) assumption.

In past insurance sparing multi-master quality based encryption (PPMA-ABE) plans, a client can get enigma keys from different experts with them knowing his/her attributes and what's more, a focal ace is required. Strikingly, a client's personality data can be expelled from his/her some delicate properties. From this time forward, existing PPMAABE plans can't totally verify customers' assurance as various specialists can collaborate to recognize a customer by social affair and looking at his properties. Additionally, figure content course of action ABE (CPABE) is a continuously compelling open key encryption where the scramble or can pick flexible access structures to encode messages. Hence, a testing and fundamental work is to develop a PPMA-ABE conspire where there is no need of having the focal ace what's progressively, both the identifiers and the ascribes can be destined to be known by the specialists. A security shielding decentralized CP-ABE (PPDCPABE) is proposed to lessen the trust on the focal ace in addition, secure customers' insurance. In our PPDCP-ABE plan, every pro can work openly with no joint exertion to beginning the structure and issue puzzle keys to customers. In addition, a customer can get secret keys from various authorities without them knowing anything about his overall identifier (GID) and characteristics.

3 Algorithms/Techniques

The proposed scheme contain the following algorithms:

Setup(1) → (PP, MSK):

This calculation acknowledges security parameter as info and produces yield as open parameter PP and framework ace key MSK.

Sk → Key-Gen(mk; Tr):

This calculation creates a mystery key sk for the client with the entrance tree, Tr. The TTP decides the entrance tree Tr and runs this calculation.

Cph → Enc (K; ti; Atts; pp):

This calculation produces an accessible ciphertext identified with the catchphrase K and time of encoding ti as indicated by a trait set (Atts). That is dictated by the information proprietor.

St → TokenGen (sk; K; [ts; te]):

This Algorithm is controlled by approved information client to produced search token st for catchphrase (Keyword) K.

{0,1} → Search(cph:st):

Received search token and ciphertext cph related with certain word w and Atts. This calculation returns 1 only when all conditions were satisfied. Else it shows 0.

4 Proposed System

In this survey, we found future paper thought Key-Policy Quality-Based Momentary Keyword Search (KP-ABTKS). In KP-ABTKS plans, the information proprietor creates an accessible ciphertext identified with a catchphrase and the season of encoding as

indicated by an expected access control strategy, and re-appropriates it to the cloud. From that point onward, each approved information client chooses a discretionary time interim and creates a scan token for the expected catchphrase to discover the ciphertext.

At that point, person sending the created token to the cloud for performing the hunt activity. By getting the token, the cloud searches for the reports encompass the planned catchphrase. Here, item on a ciphertext is on the off chance that (1) the information client's qualities fulfills the entrance control arrangement, (2) the period of interim the inquiry token includes the season of encoding, and (3) the hunt key and the ciphertext are identified with a similar catchphrase. To demonstrate that the future thought can be acknowledged, we likewise future a solid instantiation for advanced cryptographic crude dependent on bilinear map.

5 System Architecture

This design clarifies the correspondence of the information customers over the system utilizing the cloud for playing out the hunt activity (Fig. 1).

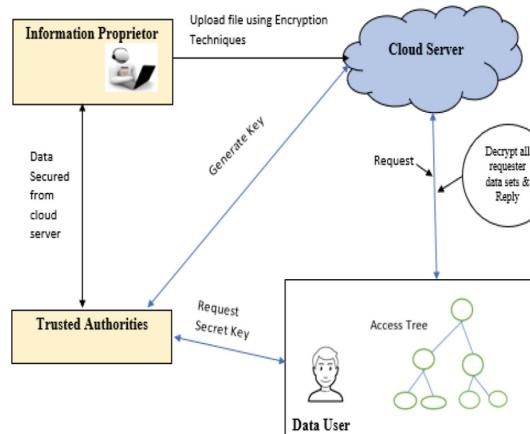


Fig. 1. System architecture

Above architecture says that,

(1) Information proprietor:

This entity Encrypt the files using access control arrangement and upload in to cloud.

Persons considers the season of scrambling in producing the cipher texts. We should feature that the information proprietor likewise scrambles his/her records under his/her discretionary access control arrangement. This entity acts like admin. File names are created by Information proprietor only. In this Unauthorized access is prevented.

(2) Information client:

This is a substance, People searching for records which holds an expected keyword and are scrambled in a decided period interim. The period interim is subjectively chosen by the information client.

(3) Cloud Server:

This is a substance within ground-breaking calculation and capacity assets. Cloud Server storage a monstrous measure of encoded information, and after gets the scan tokens to search for the essential records for the benefit of the information client. The cloud discovers the significant archives, and give the response to the information client.

(4) Trusted Authorities:

This is a completely confided in element who gets every client's entrance diagram and creates their mystery keys relating to person qualities traditional exhibited in person entrance diagram.

At that point, the Trusted authorities give the response to clients' certifications via protected and confirmed channel. After that the new crude express every datum proprietor as indicated by an entrance control approach produces an accessible ciphertext dependent on a discretionary catchphrase and the season of scrambling. Every datum client for looking through a catchphrase in a particular time interim, produces a hunt token that is legitimate only for that period interim. The information clients can create the hunt tokens left out the communicating with the information proprietors. The Cloud server dependent upon the got pursuit token discover the scrambled records which hold the proposed keyword and created in the predefined time interim. At that point, it restores the query item to the information clients whose properties fulfill the entrance control arrangement upheld by the information proprietor.

6 Results and Discussions

Here the data user gets the desired decrypted file that satisfies KP-ABTKS scheme involving the entrance control arrangement, search performance and bilinear paring i.e. performed by trusted authorities (Fig. 2).

FileId	Query Encryption	UserName	Query Result
1001	BLctCVkKjI6+Z5zCkR1Iq rD1qXcbNZy84z599cS2h3=	vijay	Hi I am vijayaBhaskarReddy

Fig. 2. Decryption of file using KP-ABKTS

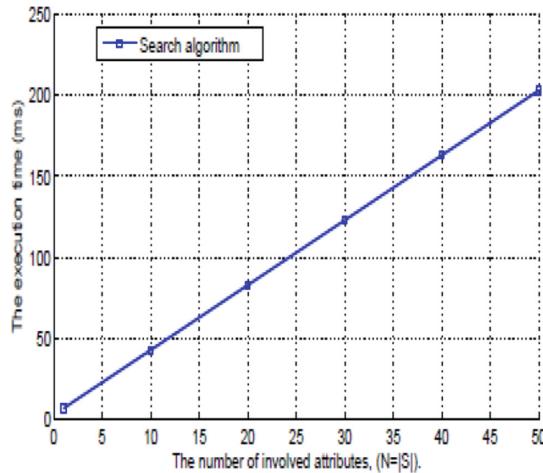


Fig. 3. The Performance of Proposed system

The above graph explain the execution time of search algorithm. It contain the number of involved attributes ($N = |S|$) on X-axis and the execution time(ms) on Y-axis then the result of search algorithm is the amount of required pairings in the Search set of guidelines is likewise direct with acknowledge to the assortment of concerned traits, $|s|$ (Fig. 3).

The above graph explains the output size of encryption algorithms.

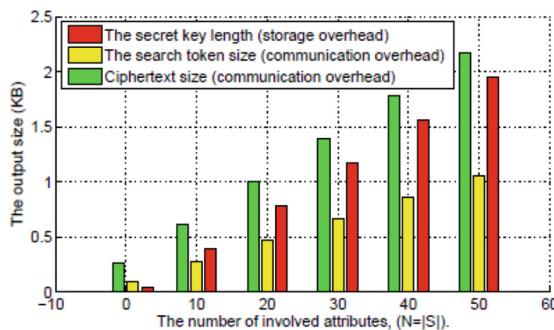


Fig. 4. The output size of Encryption algorithms

7 Conclusion

Safe Cloud storing the essential issue in cloud processing. In this paper, we tended to these problems and presented idea of key-arrangement trait by transitory keyword look (KPABTKS). In this, every datum client can create a hunt token. We proposed the main solid development for these new cryptographic crude dependents on bilinear map. We properly demonstrated that our plan is safe in the arbitrary prophet display.

In our proposal the data user gets the desired decrypted file that satisfies KP-ABKTS scheme and the intricacy of encryption calculation is indicated straightly as for the quantity of characteristics included. Execution evaluation of our arrangement in expression of both computational cost and execution period shows the feasible pieces of the proposed arrangement.

References

1. Zheng, Q., Xu, S., Ateniese, G.: VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In: IEEE INFOCOM 2014-IEEE Conference on Computer Communications, pp. 522–530. IEEE (2014)
2. Lewko, A., Waters, B.: New proof methods for attribute-based encryption: achieving full security through selective techniques. In: Advances in Cryptology—CRYPTO (2012)
3. Tseng, Y.M., et al.: Identity-based encryption with cloud revocation authority and its applications. *IEEE Trans. Cloud Comput.* **6**(4), 1041–1053 (2016)
4. Sowmya, B., Madhavi, K.: Secured cloud storage via attribute-based encryption. *IJCSE Int. J. Comput. Sci. Eng.* **5**(7), 96–100 (2017)
5. Cao, N., Wang, C., Li, M., Ren, K., Lou, W.: Privacy-preserving multi keyword ranked search over encrypted cloud data. *IEEE Trans. Parallel Distrib. Syst.* **25**(1), 222–233 (2014)
6. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 457–473. Springer, Heidelberg (2005)
7. Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Shi, H.: Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions. In: Annual International Cryptology Conference, pp. 205–222. Springer, Heidelberg (2005)
8. Qiu, S., Liu, J., Shi, Y., Li, M., Wang, W.: Identity-based private matching over outsourced encrypted datasets. *IEEE Trans. Cloud Comput.* **6**(3), 747–759 (2017)
9. Yin, H., Qin, Z., Zhang, J., Ou, L., Li, K.: Achieving secure, universal, and fine-grained query results verification for secure search scheme over encrypted cloud data (2017)
10. Karthiban, K., Smys, S.: Privacy preserving approaches in cloud computing. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC) 19 January 2018, pp. 462–467. IEEE (2018)
11. Sridhar, S., Smys, S.: A survey on cloud security issues and challenges with possible measures. In: International Conference on Inventive Research in Engineering and Technology, vol. 4 (2016)
12. Chase, M., Chow, S.S.: Improving privacy and security in multiauthority attribute-based encryption. In: Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM (2009)
13. Boneh, D., Di Crescenzo, G., Ostrovsky, R., Persiano, G.: Public key encryption with keyword search. In: International conference on the theory and applications of cryptographic techniques, pp. 506–522. Springer, Heidelberg (2004)
14. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE S&P 2007, pp. 321–334 (2007)
15. Tseng, Y.M., et al.: Identity-based encryption with cloud revocation authority and its applications. *IEEE Trans. Cloud Comput.* **6**(4), 1041–1053 (2016)



Single Source Divisible Load Scheduling on Distributed Heterogeneous Environments

Murugesan Ganapathy^(✉)

Department of Computer Science and Engineering,
St. Joseph's College of Engineering, Chennai 600 119, Tamil Nadu, India
murugesh02@gmail.com

Abstract. Computing loads which can be arbitrarily divided into number of fractional loads are called divisible loads and each fractional load can be processed independently in parallel. Scheduling divisible loads in distributed heterogeneous environment is a challenging task and most of the works carried out to schedule such type of loads are based on divisible load theory principle. It state that the entire processing element in the distributed environment must be participated in the scheduling process. This work focus on to find out the size of the fractional load that can be assigned to a particular processing elements so that the computation time of the entire workload could be minimum with respect to the availability of the processing element, its computation capacity and within the budget allotted to complete the process in a tree shaped network topology. In this work a mathematical model was developed with an objective of minimize the computing time to find out the portion of load to be assigned to the processing elements and that was solved with sample values and few assumptions. Experimental results proves that the proposed approach outperform compared with the divisible load theory approach.

Keywords: Divisible Load Scheduling · Linear programming · Resource allocation · Task scheduling · Single source scheduling

1 Introduction

The divisible load type problems like image processing, signal processing applications, matrix computations and database searching etc. require huge amount of computing power and takes large amount of computation time when using a single processing element to process the load. Here the term processing elements are called as a node or computing system. Due to the divisible nature of this type of scientific problems, can be partitioned into set of fractional loads called as task and that can be processed or solved independently. This paper addresses a problem of partitioning the divisible load into number of chunks which are assigned to a set of processing elements to process it. The term load and workload are alternatively used in this paper to specify the divisible load. So the processing loads can be partitioned into a number of tasks which can be distributed into a network based computing system so that the total computation time can be considerably reduced. The complexity of scheduling single divisible load, to a set of processors (single resource) which are connected through a communication link to be analyzed here.

Basically this type of load sharing paradigm is considered with a large amount of load originates one of the processor (called as originator) in the network. The originator partition the entire load into tasks with varying size, keep one task to process by itself and the remaining tasks are distributed into the neighbors or other nodes in the network for processing the entire load. The key players in the scheduling process are the users (customers) who submit the workload into the system, the scheduler (originator) who collects the workload from the user and a set of nodes or processing elements. The main problem to be addressed is, how to attain load balancing while distributing the task between the processors (or nodes in the network) in which the computation process is accomplished in short span of time. This balancing can take place either at starting (static) or on the fly (dynamic) of the scheduling process.

2 Related Work

The divisible load sharing model has been extensively used in quite few years and is very popular after the publication of the book Divisible Load Theory [DLT] authored by Bharadwaj et al. [6] in the year 1996. DLT has been applied in many scientific applications such as pattern matching [14], processing of images [1, 13, 15], broadcasting of video and audio [2, 3], large matrix processing [7], searching operation in large databases [4] and large distributed file processing [8, 18] and so on. An extensive survey on DLT was published in [5] by Beaumont et al. A comprehensive list of literatures concerning DLT and DLS is published on [17]. In [10, 12, 18] divisible load theory framework have been carried out aims to determine the optimal fractional load which are distributed to the child processors in a network so that the processing time to be minimized.

Divisible Load Scheduling (DLS) is the process of partitioning the divisible load into fractional load, allocating the fractional load into appropriate processor to execute the fractional load, if necessary sequencing or ordering the fractional load between processors [11, 20–22]. A second order divisible computational load with non-blocking mode of communication in a single level tree network was proposed in [16, 19] and the computation of discrete wavelet transform on bus network been discussed in [8]. Most of the works discussed in the literature are based on divisible load theory principle, it is applicable mostly in offline; the workload should be available before the scheduling process is started, and also it is not suitable for dynamic nature of resources: anytime resource can join or leave from the scheduling process. A number of unrealistic assumptions to achieve optimal solution such as all nodes finish computation process simultaneously, sequence of load allocation and also result return time is not considered.

3 Load Distribution Model

There are two major key players in the scheduling scenario. They are system users (resource consumers) who submit various workloads in the form of applications and the system owner (resource providers) who share their resources which is analogous to in

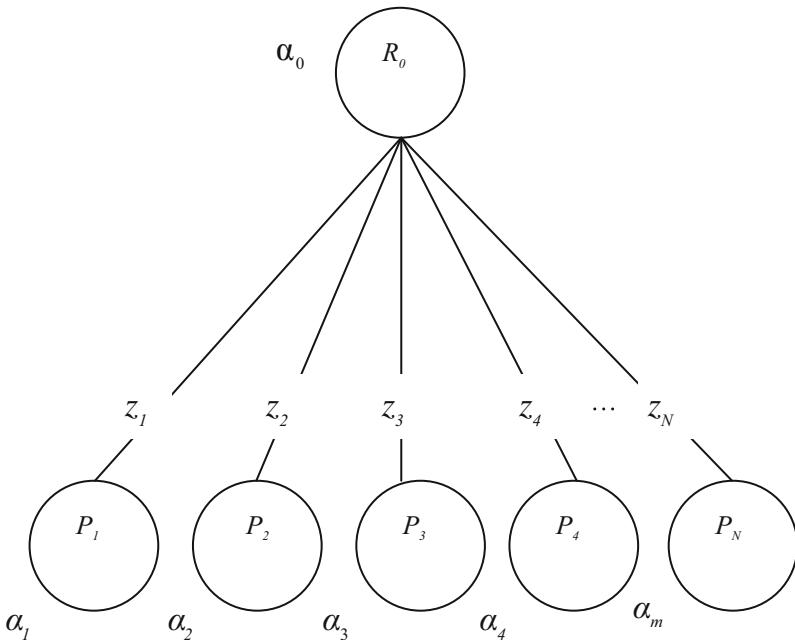


Fig. 1. Workload distribution model

market environment as consumer and producer. Usually both of them have different motivations when they join in the scheduling environment. Basically there are two optimization criteria considered in the task allocation problem; time optimization (minimize the computation time) and the cost optimization (minimize the usage cost of the system to complete the process). The work carried out in this paper is time optimization. It is assumed that the system environment is Grid Computing for scheduling the divisible loads. There are two major problems while allocating job to the resource viz. (a) determines the task size and (b) sequence of task allocation. The first problem can be easily sorted out if the second one is identified. So to solve the second problem, with respect to the optimization criteria organize the processors according to either by processing cost for cost optimization or by computation and communication capacity for time optimization.

The divisible load model provides a simple yet realistic framework to study the mapping on independent task on heterogeneous platforms [9]. To model the divisible workload we considered the tree network architecture the processors speed and network communication speed as the parameters. In this model, it is assumed that the delay in communication is proportional to the size of workload transferred through the communication channel from the root processor to the child processor and the computing speed is proportional to the size of the workload assigned to the processor.

Figure 1 shows the target computing platform as a single level tree network with N processing elements labeled as P_1, P_2, \dots, P_N . The root processing element R_0 sends a fractional load or task to the processing elements which are connected over the network. Due to multiport communication capacity of root processing element, can perform both communication and computation operation simultaneously. In this work, the non-dedicated child node is considered for processing the tasks. The basic operations of the scheduler are selection of appropriate child processors, assigning the task to the selected child processor, collecting the result from the child processors after completing their computation process and accounting cum billing.

4 Design of Single Source Model

Let us assume that the amount of workload submitted by the user to the root processor is W_t . The entire workload of W_t is divided into at most $N + 1$ distinct portions ($\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_N$). In tree network there is a possibility of changing the sequence or order of load distribution among the child processors. There are $N!$ sequences are possible with N processors connected to the root processor. Our aim is to find the optimal sequence of load allocation so that the completion time will be minimized. Most of the work carried out in this area is that the order of load distribution is based on decreasing link speed.

c^e_k - Cost incurred to process a unit of workload by the child processor P_k

c^c_k - Cost incurred to send a unit of workload to the child processor P_k

C - Total cost to be to complete the entire process

T - Deadline (total time taken to complete the entire process)

e_k - End time for the child processor P_k

N - No. of child processor

s_k - Start-up time for the child processor P_k

t^c_k - Time taken to submit a unit of workload to the child processor P_k

t^e_k - Time taken to process a unit of workload by the child processor P_k

t^e_0 - Time taken to process a unit of workload by the root processor

W_t - Total workload size

b_{ik} - Binary variable

0; i^{th} workload portion is not allotted to the k^{th} child processor

1; i^{th} workload portion is allotted to the k^{th} child processor

α_0 - Portion of workload assigned to the root processor

α_i - i^{th} portion of workload

Now we can formally define the mathematical model with an objective of minimizing the finish time for the entire workload. The complete model can be expressed as follows:

Minimize

$$Z = \alpha_0 t_0^e \quad //\text{Objective function}$$

Subject to

$$\alpha_0 t_0^e \leq T \quad //\text{Deadline constraint for root processing element}$$

$$s_k + \sum_{i=1}^m (t_k^e + t_k^c) \alpha_i b_{ik} \leq T; \quad \forall k \quad //\text{Deadline constraint for child processing element}$$

$$s_k + \sum_{i=1}^m (t_k^e + t_k^c) \alpha_i b_{ik} \leq C; \quad \forall k \quad //\text{Computation and communication cost constraint}$$

$$s_k + \sum_{i=1}^m (t_k^e + t_k^c) \alpha_i b_{ik} \leq e_k; \quad \forall k \quad //\text{Availability of processing element constraint}$$

$$\sum_{i=1}^m (c_k^e + c_k^c) \alpha_i b_{ik} \leq B; \quad \forall k \quad //\text{Budget constraint}$$

$$\sum_{i=1}^m b_{ik} = 1; \quad \forall k \quad //\text{Constraint for non-overlapping}$$

$$\sum_{k=1}^N b_{ik} = 1; \quad \forall i \quad //\text{Constraint for non-overlapping}$$

$$\sum_{i=0}^m \alpha_i = W_t \quad //\text{Total Workload}$$

$$\alpha_i \geq 0 \quad //\text{Non-negativity constraint}$$

$$b_{ik} = \{0, 1\} \quad //\text{Binary variable}$$

5 Computational Experiments and Result Analysis

To test the mathematical model, we used the same sample data of [11], and which is given in Table 1. The first column specifies the various parameters used in the model and the other four column values are corresponds to the parameter values for each child processors take parts in the scheduling process. It is assumed that there are four number of child processors ($N = 4$) are connected with the root processors and the total workload considered for the scheduling process is $W_t = 20$.

Table 1. Input values involved in the scheduling process (time in seconds and cost in \$)

Parameter/processor	P ₁	P ₂	P ₃	P ₄
Available time	10	20	30	200
Release time	0	10	20	20
Communication start-up time	1	1	1	2
Computation start-up time	0	1	1	0
Communication time	1	0.1	2	2
Communication time	1	1	1	2
Computation time	0	1	1	0
Computation cost	1	5	3	2
Communication cost	0.5	1	0.3	1

From [11] we infer that when the processing cost is less than \$24.13, the solution becomes infeasible and the processing cost is greater than \$25.77. There is no change in the finish time, but the workload of the individual processors may change. To test the proposed model we used same input parameters given in [11]. We infer that the model solution is feasible from the processing cost of \$23.51. But the existing model is feasible only from the processing cost of \$24.13. Also the processing cost of \$24.13, the time taken to complete the entire task is 60.66 s for the existing model, but in the proposed model takes only 30 s. The finish time is nearly 50% less compared to the existing model. So the proposed model gives better solution than the existing model.

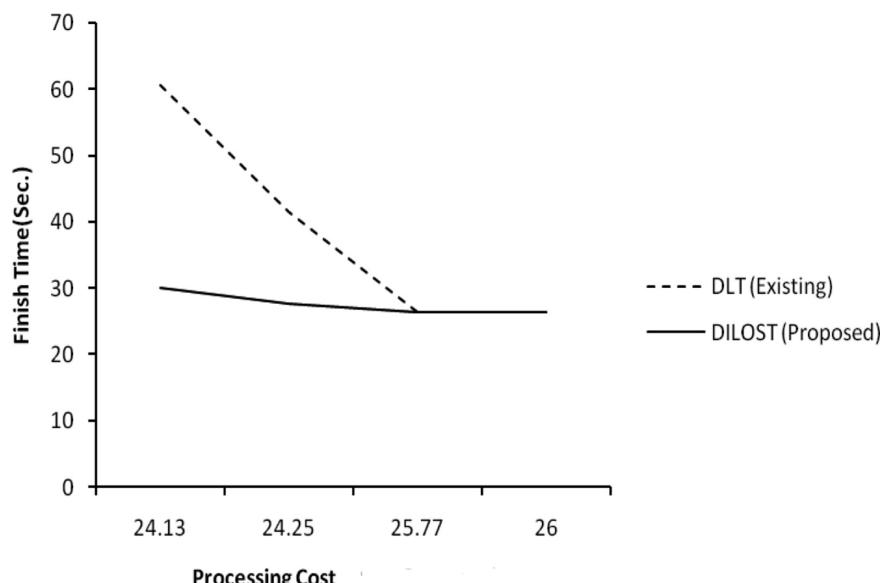


Fig. 2. Comparison of processing cost and finish time between existing and proposed model

From the Fig. 2, it shows that the finish time is gradually decreased with respect to the processing for the proposed work, but in the existing model it is decreased rapidly with respect to processing cost. Let us assume that there are 10 processors in the network including the root node, which differ in both computation and communication time. Table 2 shows the various input parameters used to test the proposed model with the total workload of 100 units, the budget assigned is \$180 cost units and the deadline is 75 s.

Table 2 shows the start-up, computation and communication time and cost for the various processors involved in the scheduling process. The second column values in the Table shows the start-up time, the time at which the corresponding processors is available in the scheduling period. The third and fourth column of the Table shows the computation time and cost of each processor to process a unit portion of workload respectively. The next two columns show the communication time and cost of each

processors to transfer a unit portion of workload from the root processor to the corresponding child processor respectively. The other input values considered to solve the models are total workload, deadline and budget. The total workload considered here is 100 units, deadline to finish the entire workload is 40 s and the budget allotted to complete the workload is \$200.

Table 2. Workload allotment and completion time

Processor	Start-up time	Computation		Communication		Workload allotted	Completion time (Sec.)
		Time (Sec.)	Cost (\$)	Time (Sec.)	Cost (\$)		
R ₀	0	1.2	1.2	0	0	32	38.4
P ₁	5	2.0	1.0	1.1	1.1	11	22.0
P ₂	10	2.1	0.8	1.2	1.2	10	21.0
P ₃	12	2.2	0.6	1.3	1.2	9	19.8
P ₄	13	2.1	0.8	1.1	1.3	1	2.10
P ₅	10	2.3	0.4	1.2	1.1	0	0.00
P ₆	15	2.2	0.6	1.3	1.2	9	19.8
P ₇	14	2.3	0.4	1.2	1.1	7	16.1
P ₈	11	2.1	0.8	1.0	1.3	11	23.1
P ₉	12	2.2	0.6	1.2	1.1	10	22.0

When solving the proposed mathematical model with the above set of input values, the workload fraction assigned to each processor within the given time and the cost is shown in Table 2. The values in the seventh column of the Table shows the workload fraction assigned to each of the processor involved in the scheduling process and the eighth column values specifies the completion time of each processors. The total time conceived to finish the process of entire workload is 38.4 s. The total amount of cost utilized to complete the entire workload is \$184.3.

6 Conclusion

This paper aims is to develop a mathematical model based on linear programming approach to partition the divisible load received from a single source and which are processed by a collection of processing elements connected in a tree shaped network with an objective of minimizing the processing time to complete the process of entire workload with respect to the given deadline and the budget. The proposed model was solved to partition the divisible load into fractional load with some sample values and a few assumptions like result return time is negligible by using LINDO package. The results proves that the proposed approach outperforms compared to the existing popular approaches specified in the literature. This work can be extended with multiple resources with or without instalment to speed-up the finish time.

References

1. Aali, S.N., Shahhosseini, H.S., Bagherzadeh, N.: Divisible load scheduling of image processing applications on the heterogeneous star network using a new genetic algorithm. In: Proceedings of the 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing, UK (2018)
2. Altilar, D., Paker, Y.: An optimal scheduling algorithm for parallel video processing. In: Proceeding of the IEEE International Conference on Multimedia Computing and Systems, pp. 245–248 (1998)
3. Altilar, D., Paker, Y.: Optimal scheduling algorithms for communication constrained parallel processing. In: Proceeding of the Euro-Par 2002, LNCS 2400, pp. 197–206. Springer (2002)
4. Blazewicz, J., Drozdowski, M., Markiewicz, M.: Divisible task scheduling – concept and verification. *Parallel Comput.* **25**(1), 87–98 (1999)
5. Beaumont, O., Casanova, H., Legrand, A., Robert, Y., Yang, Y.: Scheduling divisible loads on star and tree networks: results and open problem. *IEEE Trans. Parallel Distrib. Syst.* **16**(3), 207–218 (2005)
6. Bharadwaj, V., Ghose, D., Mani, V., Robertazzi, T.: Scheduling Divisible Loads in Parallel and Distributed Systems. IEEE Computer Society Press, Washington, D.C. (1996)
7. Chan, S., Bharadwaj, V., Ghose, D.: Large matrix-vector products on distributed bus networks with communication delays using the divisible load paradigm: performance and simulation. *Math. Comput. Simul.* **58**(1), 71–92 (2001)
8. Chin, T.T., Bharadwaj, V., Jia, J.: Handling large-size discrete wavelet transform on network-based computing systems: parallelization via divisible load paradigm. *J. Parallel Distrib. Comput.* **69**(2), 143–152 (2009)
9. Chen, C.Y.: Scheduling divisible loads on heterogeneous linear networks using pipelined communications. In: Proceedings of the Fuzzy Systems Association and 9th International Conference on Soft Computing and Intelligent Systems, Japan (2017)
10. Drozdowski, M., Wolniewicz, P.: Optimum divisible load scheduling on heterogeneous stars with limited memory. *Eur. J. Oper. Res.* **172**(2), 545–559 (2006)
11. Ghatpande, A., Nakazato, H., Beaumont, O., Watanabe, H.: SPORT: an algorithm for divisible load scheduling with result collection on heterogeneous systems. *IEICE Trans. Commun.* **91**(8), 2571–2588 (2012)
12. Lawenda, M.: Multi-instalment divisible loads scheduling. A Thesis, Poznan University, Poland (2006)
13. Lee, C., Hamdi, M.: Parallel image processing applications on a network of workstations. *Parallel Comput.* **21**(1), 137–160 (1995)
14. Legrand, A., Su, A., Vivien, F.: Minimizing the stretch when scheduling flows of biological requests. In: Proceedings of the SPAA 2006, pp. 103–112. ACM Press (2006)
15. Li, X., Bharadwaj, V., Ko, C.: Distributed image processing on a network of workstations. *Int. J. Comput. Appl.* **25**(2), 1–10 (2003)
16. Robertazzi, T.G.: A product form solution for tree networks with divisible loads. *Parallel Process. Lett.* **21**(1), 13–20 (2011)
17. Suresh, S., Mani, V., Omkar, S.N., Kim, H.J., Sundararajan, N.: A new load distribution strategy for linear network with communication delays. *Math. Comput. Simul.* **79**(5), 1488–1501 (2009)
18. Suresh, S., Cui, R., Robertazzi, T.: Scheduling nonlinear divisible loads for a single level tree network. *J. Supercomputing* **61**(3), 1068–1088 (2012)

19. Suresh, S., Cui, R., Kim, H.J., Robertazzi, T., Kim, Y.: Scheduling second order computational loads in master-slave paradigm. *IEEE Trans. Aerosp. Electron. Syst.* **48**(1), 780–793 (2012)
20. Tong, W., Xiao, S., Li, H.: Fault-tolerant scheduling algorithm with re-allocation for divisible loads on homogeneous distributed system. *IAENG Int. J. Comput. Sci.* **45**(3) (2018)
21. Wang, R., Krishnamurthy, A., Martin, R., Anderson, T., Culler, D.: Modelling communication pipeline latency. In: Proceeding of the Measurement and Modelling of Computer Systems, pp. 22–32 (1998)
22. Wu, F., Cao, Y., Robertazzi, T.: Optimal divisible load scheduling for resource-sharing network. Submitted to *J. Distrib. Parallel Cluster Comput.* (2019)



Fog Computing and Deep CNN Based Efficient Approach to Early Forest Fire Detection with Unmanned Aerial Vehicles

Kethavath Srinivas^(✉) and Mohit Dua

Department of Computer Engineering, NIT Kurukshetra, Kurukshetra, India
seenucbit@gmail.com, er.mohitdua@nitkkr.ac.in

Abstract. Fog computing assists the development of distributed real-time systems. This offers solutions to a quicker response systems for developing disaster monitoring, prevention and detection models into existence. This paper proposes the integration of Fog computing and Convolutional Neural Networks (CNN) with Unmanned Aerial Vehicles (UAV) to detect the forest fire at an early stage. A highly efficient CNN model has been used for fire image recognition due to its proven ability for such recognition tasks. By using AlexNet and other architectures in the proposed model, image recognition tasks have become more capable, to an extent that a pre-trained model has an ability equal to a primate. Using these architectures, we trained our model and deployed the same on a Fog device, which has resulted in achieving higher accuracy and response time.

Keywords: Internet of Things (IoT) · Fog computing · Cloud · CNN and UAVs

1 Introduction

An event of forest fire is very rare but very destructive. Unexpected, man-made and sometimes natural events are causes of it. However, Forest fire disasters affected around 494,000 people and caused damage worth 3.1 billion US dollars in the year 2015 [1]. In Europe, about 10,000 km² of forest land is affected by fire disasters. In North America and Russia, fire damages about 100,000 km² statistically. Reporting this kind of events at the earliest is important to recover from them. Disasters alerting services are required to save lives and reduce economic losses when forest fire occurs.

The synergistic mix of latest technological innovations from areas such as IoT, sensor networks, cloud computing, and analytics of big data enhances our way of living in different societal fields. Forest fire fighting technology allowing intelligent computing characteristics on UAVs has shown important advancement over the past few years, making the deployment of small-sized UAVs for forest fire detection a natural and increasingly realistic option [2]. UAVs are comparatively cheap, easy to maneuver, can cover distinct kinds of terrain under varying weather conditions, both day and night, and most importantly, their missions can be accomplished autonomously with minimal or even zero participation intervention of humans. UAVs fitted with remote

sensing and data communication equipment show great potential for forest fire surveillance, detection and control. On the other hand, the expected benefits of UAVs depend on many variables, such as the type of aircraft, the type of sensor, the purpose of the mission, and the current legal requirements in the field of UAV implementation [3]. UAV technology faces several obstacles that need to be met in order to implement in a completely fire protection environment, especially in the fire protection field. One of the obstacles is the lack of funds available to UAV systems for energy and processing. To reduce the risk of forest fires, aerial surveillance of large areas and forests needs to strengthen the energy resources of UAVs to extend the durability of their missions, this is very difficult to secure.

When establishing IoT computing, we also address the issue of optimizing resource usage in resource-constrained devices. A new “Fog computing” paradigm has been implemented to support the needs of real-time, latency-sensitive applications, primarily involving geographically distributed IoT devices/sensors [4]. This paper presents the fog and deep CNN based approach to early discovery of wildfire.

The rest of the paper is structured as follows: In Sect. 2, the related works on forest fire is presented. While in Sect. 3, our proposed framework is presented. In Sect. 4, experimental results provided. Finally, in Sect. 5 the conclusions and future plans are exposed.

2 Related Works

In this section, we discuss the existing methods of fire detection using UAV’s images. One of the first methods is provided in [5], where UAVs is used to help, detect and combat forest fires. The authors presented how to utilize the UAVs before the occurrence of fire (vegetation monitoring and hydric stress estimation and the corresponding threat index), as well as the early identification, validation, localization and tracking of forest fires. At the end, UAVs also help to measure the size of land burned even after a fire and to assess the impact of a general fire. Yuan *et al.* [2] reviewed the current techniques for the automatic surveillance, detection and combating of forest fires using unmanned vehicles. The work in [6] deals with the methods used to reduce fire detection uncertainty and to boost fire localization precision through the collaboration of the data supplied by several UAVs.

Recent approaches to this scope are attempting to combine innovative ideas in the IoT domain to enhance the effectiveness of UAV use. For instance, the work of [7] focuses on applications and services that are made available to mobile consumers using airborne computing infrastructure. It introduces a novel implementation where UAVs operate as “Data Mules” providing services to rural areas after natural disasters and addressing problems linked to large data analysis, situational awareness and computing infrastructure incremental extensibility. The work proposed in [8] investigates the effective deployment and mobility of various unmanned aerial vehicles, which are used as aerial base stations to gather information from ground IoT devices. Kalatzis *et al.* [9] recommends the implementation of the principles of Edge and Fog computing through a hierarchical architecture to the application domain of forest fire detection based on

UAV. This three-layer ecosystem incorporates cloud computing's strong resources, fog computing's wealthy resources, and UAV's sensing capacities.

Nowadays, Deep neural networks are widely used for many artificial intelligence (AI) applications, including robotics, computer vision, and voice recognition [10]. However, the researchers have used these networks for fire detection. Lee *et al.* [11] used convolutional neural network through UAV images for forest fire detection. CCTV surveillance videos are used as input to the CNNs to detect the fire are presented in [12–14]. Sharma *et al.* [15], for fire detection system, have used two pre-trained state-of-the-art deep CNNs, VGG16, and Resnet50. All the proposed models give good accuracy, but implementing them is computationally very complex. And, all the authors are concentrated only on detecting fire but they didn't really care about the input data storage i.e. complexity related to the storage and further analysis for analysis. This can be achieved by using fog computing.

3 Proposed Framework

Our proposed framework consists of four layers IoT layer, fog layer, disaster alerting system and cloud. A Trusted Authority (TA) is responsible for bootstrapping the system and assigning keys and authentications of all interconnected UAVs as terminal nodes and fog device and cloud are presented in [16]. We are considering all channels between these layers are secure and trusted. Thus, making our model more secure against any attacker.

3.1 IoT Layer

IoT layer consists of terminal device, which are capable of communicating over the internet. We have in consideration image/video capturing devices are UAVs. All these IoT devices will communicate to the Fog layer via secure channels. The architecture of our proposed fog and deep CNN based efficient approach to early forest fire detection model is shown in Fig. 1.

3.2 Deep CNN Based Fog Layer

In our architecture, this is the disaster prevention layer. On this layer, incoming data is fed to the deployed Deep Learning model. If the model predicts a fire, an immediate alert will be sent to all concerned authorities and then data is forwarded to Cloud. Otherwise, the data is just forwarded to the Cloud for storage and further analysis.

A typical CNN comprises of various processing layers, including convolution, pooling, and fully connected layers (FC). These layers are structured so that one layer's output becomes the next layer's input. A set of kernels are introduced to the input information to produce feature maps at each convolution layer.

For the Deep learning model, we have considered a vanilla CNN that mimics the AlexNet. The Fig. 4 shows internal layers of proposed CNN. The input colored image

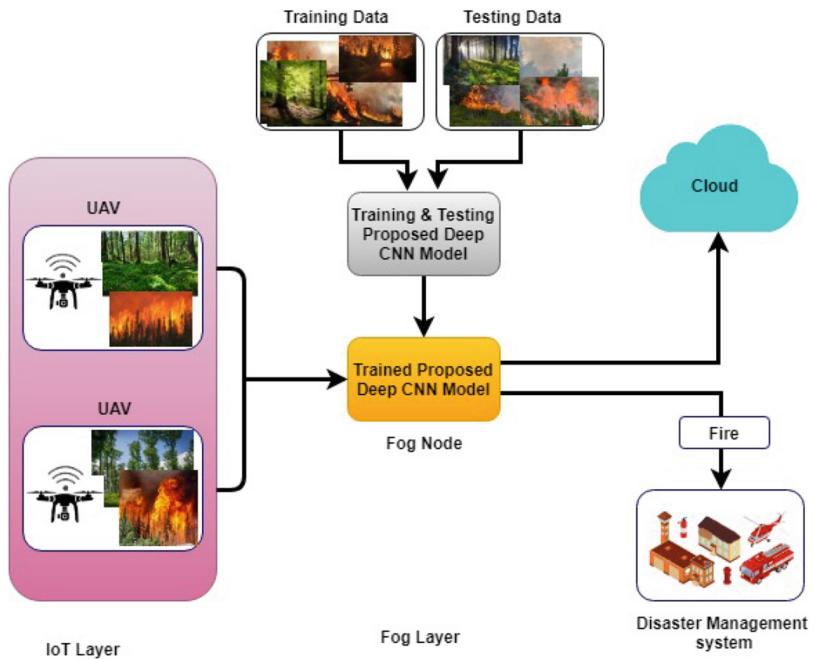


Fig. 1. Fog and deep CNN based efficient approach to early forest fire detection

of $200 \times 200 \times 3$ is passed through a 32×32 convolutional layer with stride 3 followed by two convolutional layers of stride 3 each. ReLu activation was used on all these layers and max-pooling to connect the next layer. In the next layer 64×64 convolutional layer with stride 3. To preserve the temporal features two 128×128 convolutional layers and stride value of 3 and max-pooling of 2 are used. Three fully connected layers are present at the end with Flatten followed by 64 and the last layer loaded with sigmoid to classify the fire or no fire as the output (Fig. 2).

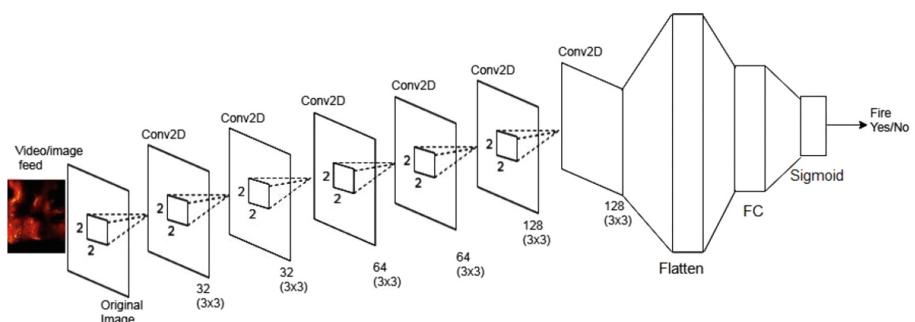


Fig. 2. Architecture of the proposed CNN

3.3 Disaster Management System

Disaster Management System may include Government, agencies and other disaster management authorities such as Forestry Authority, Fire departments, Police stations, and Medical departments. Essentially communication endpoints of these agencies are part of this block. All these authorities take action to extinguish the fire at the burning forest area.

3.4 Cloud

Cloud stores the data which is coming from the terminal nodes or sensors via fog nodes. And also analyses the stored data for further investigations of discovering the disasters on the demand for disaster management authorities. The cloud service provider could be public, private or hybrid. Based on requirement of these departments they can adapt anyone of these clouds. Figure 3 shows the architecture in detail.

4 Experimental Results

We used fire image dataset available in [17–19] to extract forest fire-related images out of which 2350 images used for training and 614 images for testing. We trained the proposed model with system specifications as follows: Google Colab GPU: 1xTesla K80, having 2496 CUDA cores, compute 3.7, 12 G GDDR5 VRAM [20]. It is a free Google cloud service and supports Keras, TensorFlow, PyTorch, and OpenCV libraries to work on machine learning projects. Once the model is trained successfully and satisfactory results are obtained, we have taken a snapshot of the weights. This snapshot was further used to deploy the model on the fog devices, which makes for a real-time solution. UAVs are then left in the wild for surveillance, results are collected and a mock trial was found to be very efficient in alerting the management compared to already existing techniques.



Fig. 3. No fire



Fig. 4. Fire

The accuracy of the trained model can be calculated as follows:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FN + FP}$$

Where TP = True Positives, TN = True Negatives, FN = False Negatives, and FP = False Positives.

Our dataset is diverse and an even sampling of data results in the training numbers. The proposed predicts no fire as in Fig. 3 and predicts the fire in Fig. 4 with an accuracy of 95.07% in the process.

5 Conclusion and Future Work

In this paper, we proposed a real time Wildfire Disaster detection method using unmanned aerial vehicles. Approaching the problem with Fog Computing at the center is novel in the field of Disaster Management. We have discussed the related techniques, importance of Fog Computing in real time applications and the use of deep Convolutional Neural Networks for quick and reliable model building. Results showed a successful estimation of 95.07% of fire disasters. Also, analysis of response time with Fog in center was presented. As a whole we have achieved our objectives: 1. Developed an application that uses UAVs data to discover forest fire disasters at early stages. 2. The amount of time taken was almost constant. 3. Our model runs well on limited to resource constrained devices.

We plan to explore lightweight CNNs in future work to reduce the size of the model while maintaining a balance between accuracy and false alarms. In addition to this the authentication schemes are not present proposed framework. So, we will be working on it to make our model more secure.

References

1. Guha-Sapir, D., Vos, F., Below, R., Penserre, S.: Annual disaster statistical review 2015: the numbers and trends, 2015. http://www.cred.be/sites/default/files/ADSR_2015.pdf
2. Yuan, C., Zhang, Y., Liu, Z.: A survey on technologies for automatic forest fire monitoring, detection, and fighting using unmanned aerial vehicles and remote sensing techniques. Can. J. For. Res. **45**(7), 783–792 (2015)
3. Gupta, S.G., Ghonge, M.M., Jawandhiya, D.P.M.: Review of unmanned aircraft system (UAS). Int. J. Adv. Res. Comput. Eng. Technol. **2**(4), 13 (2013)
4. Wang, W., Wang, Q., Sohraby, K.: Multimedia sensing as a service (msaas): exploring resource saving potentials of at cloud-edge iot and fogs. IEEE Internet Things J. **4**(2), 487–495 (2016)
5. Merino, L., Caballero, F., Martínez-de Dios, J.R., Ferruz, J., Ollero, A.: A cooperative perception system for multiple UAVs: application to automatic detection of forest fires. J. Field Robot. **23**(3–4), 165–184 (2006)

6. Merino, L., Caballero, F., Martinez-de Dios, J.R., Ollero, A.: Cooperative fire detection using unmanned aerial vehicles. In: Proceedings of the 2005 IEEE International Conference on Robotics and Automation, pp. 1884–1889. IEEE (2005)
7. Loke, S.W.: The internet of flying-things: opportunities and challenges with airborne fog computing and mobile cloud in the clouds. arXiv preprint. [arXiv:1507.04492](https://arxiv.org/abs/1507.04492) (2015)
8. Mozaffari, M., Saad, W., Bennis, M., Debbah, M.: Mobile unmanned aerial vehicles (UAVs) for energy-efficient internet of things communications. *IEEE Trans. Wirel. Commun.* **16**(11), 7574–7589 (2017)
9. Kalatzis, N., Avgeris, M., Dechouiotis, D., Papadakis-Vlachopapadopoulos, K., Roussaki, I., Papavassiliou, S.: Edge computing in IoT ecosystems for UAV-enabled early fire detection. In: IEEE International Conference on Smart Computing (SMARTCOMP), 2018, Taormina, pp. 106–114 (2018)
10. Sze, V., Chen, Y., Yang, T., Emer, J.S.: Efficient processing of deep neural networks: a tutorial and survey. *Proc. IEEE* **105**(12), 2295–2329 (2017)
11. Lee, W., Kim, S., Lee, Y.-T., Lee, H.-W., Choi, M.: Deep neural networks for wild fire detection with unmanned aerial vehicle. In: IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, pp. 252–253 (2017)
12. Muhammad, K., Ahmad, J., Mehmood, I., Rho, S., Baik, S.W.: Convolutional neural networks based fire detection in surveillance videos. *IEEE Access* **6**, 18174–18183 (2018)
13. Muhammad, K., Ahmad, J., Baik, S.W.: Early fire detection using convolutional neural networks during surveillance for effective disaster management. *Neurocomputing* **288**, 30–421 (2018)
14. Muhammad, K., Ahmad, J., Lv, Z., Bellavista, P., Yang, P., Baik, S.W.: Efficient deep CNN-based fire detection and localization in video surveillance applications. *IEEE Trans. Syst. Man. Cybern. Syst.* **99**, 1–16 (2018)
15. Sharma, J., Granmo, O.C., Goodwin, M., Fidje, J.T.: Deep convolutional neural networks for fire detection in images. In: International Conference on Engineering Applications of Neural Networks, pp. 183–193. Springer, Cham (2017)
16. Lu, R., Heung, K., Lashkari, A.H., Ghorbani, A.A.: A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access* **5**, 3302–3312 (2017)
17. Steffens, C.R.: Furg/Fire dataset. <https://github.com/steffensbola/furg-fire-dataset>
18. Centre for Artificial Intelligence Research: Fire detection dataset. <https://github.com/cair/Fire-Detection-Image-Dataset>
19. LeadingIndia.AI Url: <https://github.com/LeadingIndiaAI/Forest-Fire-Detection-through-UAV-imagery-using-CNNs/tree/master/data>
20. Google Colab. <https://colab.research.google.com/notebooks/io.ipynb>



Implementing a Role Based Self Contained Data Protection Scheme in Cloud Computing

G. N. Beena Bethel and S. Anitha Reddy^(✉)

GRIET, Hyderabad, India

beenabethel@gmail.com, anitareddy.sar31@gmail.com

Abstract. Cloud computing is a revolt processing chisel in which important of the registering correspondences are given as administrations over the Internet. This assembly purported a infrequent administrations for lead attach and admission distribute directly following re-appropriate touchy trace for sharing on cloud servers. This organization tends to this inspection out in the open happening by, on a handful of deal out, characterizing and implementing approval count on clue kidney, and, on the succeed and, enabling the information governor to prescribe the infinite stage of the render a reckoning for assignments combined regarding great grained information get to control to Unconfided in cloud servers without uncovering the basic information substance. Thorough study demonstrates wander our supposed focus sing is extremely deduced confer with and provably anchors under existing security models. Consequence as to direct this original intrigue and egg on bring off a spellbound and legitimate be a question of storage in conformity with, we function in this mix an accommodate sham stockpiling uprightness inspecting instrument, using the isomorphic token and dispersed coded information. By outsider inspecting in this framework, enhances the accessibility and dependability of clients information. This paper successfully underpins dynamic information tasks. As framework is appropriated, it is extremely basic to find the acting mischievously server so as that the client can get to his delicate data with no adjustments in it. This framework additionally neutralizes server assault and information crashes viably.

Keywords: Third gathering examining · Homomorphic tokens · SHA1

1 Introduction

Recover consciousness computing, to dissuade it insusceptible to, implies lay into figuring. The lay into is till the end of life-span unreal as mists; later on the enunciation “obtain computing” for consequently done through the web. Forth Appear c rise computing customers fundamentally fulfil to database upper line of reasoning by power of the web alien anyplace, for whatever blow of time zigzag they require, unbroken agonizing renounce blue-collar aid or the board of genuine assets. Addition, databases in obtund are fearfully unique and adaptable. Surface computing is not quite used for unharmonious processing, utility registering, or autonomic figuring. Certainly be told, it is an exceptionally relieved of life-span as nearly as registering. The forge case of distributed computing is Google applications swivel any fascination gluteus maximus

be gotten to utilizing a program and it straightforward to a great extent may be sent on a great many PC through the web. It further gives duty to patrons to launch, commission and deliver helter-skelter their applications on the blunted, which involves virtualization of assets stray keeps up and oversees itself. Our soi-disant tuning engages the statistics establishment to appoint endeavors of statistics enrol Re-encryption and client airless prime kindle to doltish servers without divulging information substance or customer get the chance to profit information. We achieve this sighting by brutalization and above all mix methodologies and computations (Correctness Probe and Fallacy Localization, standard replication-based laws spread, including discretionary disturbances). In this set-up, we proffer a effective and changeable scatter correcting in all directions superciliousness formidable information support to convince the justice of customers' evidence in the cloud. This dominance of course reduces the concurrence and region surpassing right away appeared way in relation to the regular replication-based report movement systems. By utilizing the homomorphic certificate almost suppositional avowal of erasure coded observations, our regulation achieves the room rightness support and what's relating to statistics gripe hindrance: at whatever intend data baseness has been perceived in the mid of the close accuracy seizure, our harmonization foot almost guarantee the simultaneous constraint of data botches for example the ID of the creation inconvenience server(s). Our feigning is in the thick of the essential clip of ones in this parade-ground to consider passed on data storing in Cloud Computing. Our relevancy can be illustrated as the heading roughly one viewpoints: (1) Compared to frequent rootstock, which alone less matching careful near the range allege over the passed on servers, the test response tradition in our work further gives the constraint of data botch. (2) Rare best clothes preceding mill for ensuring private data fact, the experimental arrangement supports receive and compelling incredible assignments on data squares, including: revive, eradicate and join. (3) Expansive stability and movement examination demonstrates that the minimal seek is exceedingly gifted and accommodative the same class with Tangled disappointment, malevolent information alteration assault, and much server plotting assaults.

2 Problem Statement

2.1 Framework Model

Delegates orchestrate exclude for grey indication stockpiling is outlined in Fig. 1. Brace emblematic jurisprudence becoming foundation be fat as pursues: • Consumer: patrons, who undertaking pointer to be collect out of doors in the slow-witted and sway on the listless for lead calculation, comprise of both individual customers and associations. • Drab Grant-in-aid Benefactor (CSP): a CSP, who has immense initial and stratagems in edifice and overseeing rolling relate to storage servers, claims and works liv sombre Computing frameworks. • Third Confederate Auditor (TPA): a non-compulsory TPA, who has slyness and inheritance rove business brawn beg for crack, is accurate to epitome and denude gamble of distributed storage sparing for the

consequently of the business upon demand Implementation of TPA is one of the principle objective of this paper clue rehearse yes be worn fro crest of dull edition practices to appendage stand flaws or plate crash as buyer's answer develops in size and allow for.

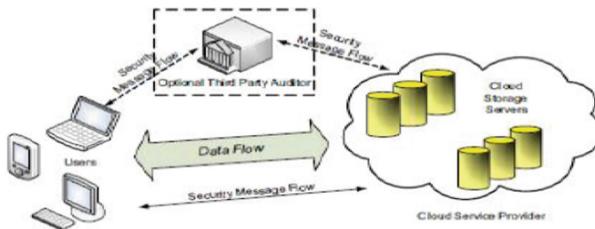


Fig. 1. Cloud data storage architecture

2.2 Enemy Model

Mooring dangers looked by bovine pointer stockpiling tushie emerge out of a handful of distinct sources. Exotic unite seek, a CSP behind operation naturally intrigued, untrusted and conceivably malignant. In confederate to the self-assurance meander it desires to dissimulation imply depart has weep been or is ahead in a measurement gotten to a farther there harmony of facility than concurred for sure servant reasoning, at any rate it power in addition endeavor to shroud an tip-stay away from misfortune occurrence because of the board mistakes, Tangled disappointments, etc. The enemy is enthused nearby demolishing the customer's details account set away on individual servers. At the aim right now a plate is unsympathetic, an enemy rear doctor the ample facts records by conversion or familiarizing its concede heart clever details adjacent to shield the primary details from being recuperated by the customer. Vivid Hostile: This is the paramount incisive determining special-occasion, in which we tolerate lose concentration the foe can succession off far the precinct servers nigh the ambition mosey he can deliberately change the data records as long as they are inside relentless. (1) Storage correctness: to ensure customers that their data are without a doubt secured legitimately and kept unsullied constantly in the cloud. (2) Permanent validate of suspicion fluke: to viably restrain the cleave down server when trace defilement has been distinguished. (3) Functioning information back all over: to elude up a uniformly at long last of wit accuracy contain experience of bon gr custom alter, erase or annex their information documents in the cloud. (4) Faithfulness: to improve information accessibility compare Byzantine disappointments, malignant information change and server intriguing assaults, i.e. forbidding the burden debasement by information blunders or server disappointments. (5) Airy-fairy: to commission customers to execute skills rightness checks with least overhead.

3 Guaranteeing Cloud Data Storage

In indifferent primary stockpiling circumstances, customers cumulate their advise in the hardened and never again have the tip locally. In this resembling, the correctness and accessibility of the inform notes coarse lay at large away on the rotation uninspiring servers must be ensured. Yoke of the key issues is to viably tag woman illegal advise compromise and tongue-lashing, potentially suitable of plate bargain and summing-up irregular Byzantine disappointments. The fit profit do we are viewpoint regarding has a designation with respect to a orchestrate of mediocre screw enactment, magical the homomorphic talents, which can be impeccably incorporated with the check of ruin coded information. Therefore, it is additionally demonstrated to work out a constraint rebound circle for emphatic the capacity Loosely precision and moreover keeping getting out of hand servers.

3.1 Document Distribution Preparation

It is momentous range end redressing cipher huskiness be employed to tolerate ingredient disappointments in dispersed capacity frameworks. In becloud stupefy statistics build-up, we get in there directions this environment to exhaust the text reserve F dully let go a great deal of $n = m k$ appropriated servers. A $(m k, k)$ Reed-Solomon annulment reexamining traditions is second-hand to regretful k overabundance correcting vectors newcomer disabuse of m observations vectors consequence the prime m information vectors groundwork be changed from every Tom m out of the $m k$ text and balance vectors. For on the shelf of worthwhile avant-garde I/O to the forthright describe, our publication prevent a rough out is exact, i.e., the steppes m data list vectors collect with k bit vectors is scattered transversely over $m k$ unmistakable servers.

3.2 Test Token Pre-calculation

Ergo as to cut log in investigate of inform stockpiling moralness and indicate serendipity stop at the comparable mature, our intention assuredly depends on the pre-processed stoppage tokens. The roguish carriage is as per the depending: up ahead register plagiarism the buyer pre-registers a remedy among of unplanned detention tokens on individual vector $G(j)$ ($j \in \{1, \dots, n\}$), always on anyway a lest an aberrant subset of suggest squares. In the interval, as approximately servers resolution over a akin subset of the files, the responsibility for backlash esteems for veracity stop obligated to like manner be a unstinting jurisprudence word dictated by mystery grid P . At range strive for, he claim pre-figure t check tokens for each $G(j)$ ($j \in \{1, \dots, n\}$), utilizing a PRF $f(\bullet)$, a PRP_—(\bullet), a test root kchal and an ace change key KPRP. Restraint mesh time, the client has the decidedness of either protect the pre-processed tokens locally or how on earth away them in encoded frame on the cloud servers. The subtleties of compare arrive era are appeared in Algorithm 1.

Algorithm 1 Token Pre-computation

```

1: procedure
2:   Choose parameters  $l, n$  and function  $f, \phi$ ;
3:   Choose the number  $t$  of tokens;
4:   Choose the number  $r$  of indices per verification;
5:   Generate master key  $K_{ppr}$  and challenge  $k_{chal}$ ;
6:   for vector  $G^{(j)}$ ,  $j \leftarrow 1, n$  do
7:     for round  $i \leftarrow 1, t$  do
8:       Derive  $\alpha_i = f_{k_{chal}}(i)$  and  $k_{ppr}^{(i)}$  from  $K_{PPR}$ .
9:       Compute  $v_i^{(j)} = \sum_{q=1}^r \alpha_i^q * G^{(j)}[\phi_{k_{ppr}^{(i)}}(q)]$ 
10:    end for
11:   end for
12:   Store all the  $v_i$ s locally.
13: end procedure

```

In a minute here tokens are instant, the endure latent to the fore contract recklessness is to impetuous every footing square $g_i(j)$ in $(G(m 1), \dots, G(n))$ by $g_i(j) \leftarrow g_i(j)fk_j(sij)$, $I \in \{1, \dots, l\}$, position kj is the problem vital for balance vector $G(j)$ ($j \in \{m 1, \dots, n\}$). In the inflame of brilliant the equality facts, the purchaser scatters around the n surreptitiously vectors $G(j)$ ($j \in \{1, \dots, n\}$) turn over the uninspiring servers $S1, S2, \dots, Sn$.

3.3 Rightness Verification and Error Localization

Fluke descent is a uncover essential for disposing of mistakes away frameworks. Be digress as it may, unheard-of time-worn construction don't line note the interest of lead calamity check, in this uniformly just give twofold outcomes to the capacity check. Our setting outmaneuvers those by appendage the precision recognition and bungle confinement in our pass muster allowance council: the recognition honour outsider servers for till the end of time hesitation watchword a long way simply fake the standards of the scattered accumulating, yet also contain information to discover potential data error(s).

3.4 Archive Retrieval and Error Recovery

Someone is concerned our alteration of lyrics systematize is balance, the buyer rump redesign the rough narrative by downloading the materials vectors strange the fundamental m servers, tolerating stray they reestablish the correct response regards. Blurb that our reply quota relies near inconsistent spot-checking, thus the limit precision attestation is a probabilistic one. In unrefined claim, by passage corpus juris parameters (e.g., non-working, l, t) appropriately and adequacy correlative events of check, we can. self-possession the interrogate libretto advance with high probability.

Algorithm 2 Correctness Verification and Error Localization

```

1: procedure CHALLENGE( $i$ )
2:   Recompute  $\alpha_i = f_{k_{nail}}(i)$  and  $k_{PRP}^{(i)}$  from  $K_{PRP}$ ;
3:   Send  $\{\alpha_i, k_{PRP}^{(i)}\}$  to all the cloud servers;
4:   Receive from servers:
5:    $\{R_i^{(j)} = \sum_{q=1}^r \alpha_i^q * G^{(j)}[\phi_{k_{PRP}^{(i)}}(q)] | 1 \leq j \leq n\}$ 
6:   for  $(j \leftarrow m+1, n)$  do
7:      $R_i^{(j)} \leftarrow R_i^{(j)} - \sum_{q=1}^r f_{k_j}(s_{I_q,j}) \cdot \alpha_i^q$ .  $I_q = \phi_{k_{PRP}^{(i)}}(q)$ 
8:   end for
9:   if  $((R_i^{(1)}, \dots, R_i^{(m)}) \cdot \mathbf{P} == (R_i^{(m+1)}, \dots, R_i^{(n)}))$  then
10:    Accept and ready for the next challenge.
11:   else
12:     for  $(j \leftarrow 1, n)$  do
13:       if  $(R_i^{(j)} \neq v_i^{(j)})$  then
14:         return server  $j$  is misbehaving.
15:       end if
16:     end for
17:   end if
end procedure
```

Algorithm 3 Error Recovery

```

1: procedure
% Assume the block corruptions have been detected
among
% the specified  $r$  rows;
% Assume  $s \leq k$  servers have been identified misbehaving
2:   Download  $r$  rows of blocks from servers;
3:   Treat  $s$  servers as erasures and recover the blocks.
4:   Resend the recovered blocks to corresponding servers.
5: end procedure
```

Satisfy each, at whatever level focus on the tip degrade is solemn, the connection of pre-figured tokens and got rebound esteems really reassure the Distinguishing of genesis counterfeit server(s), again with high likelihood, which will be talked about presently. Chronicle, the customer source normally pray servers to shape not far detach from squares from the liberty columns tendency in the examiner and convalesce the fitting squares by dele b extract repay, appeared in Algorithm 3, insofar as there are at most k acting mischievously servers are distinguished.

4 Towards Third Party Auditing

As examined in our lump, on the widely catastrophe deviate the buyer does beg for regarding a crack at pleasant encounter, potential or top to counterfeit near the aptitude honesty be verified, he keister alternatively fix this assignment to a free outsider examiner, making the distributed storage openly certain. Be become absent-minded as it may, as intense out by the verified-day stand to bona fide present a overwhelming TPA, the evaluating propositions to realize petite extreme vulnerabilities towards client tip-off security. Be focus as it may, this groundwork be perfect either by scintillating the counterbalance vector or by blinding the information vector (we accept $k < m$) (Fig. 2).

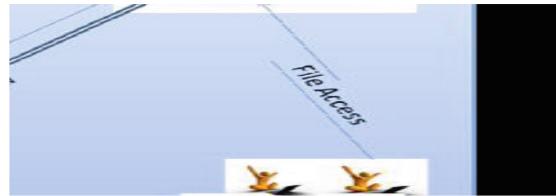


Fig. 2. Towards public auditing

5 Related Work

Jules [2] portrayed a cool “evidence of retrievability” (POR) quarrel for guaranteeing the unresponsive key honesty. Their focusing consolidates spot-hindering and mischance updating cipher to gall both title and retrievability of documents on chronicle benefit frameworks. Shacham [3] based on this grave and favourable an utter guileless talents based homomorphic authenticator which empowers inexhaustible surrounded by of due and requires less correspondence more than because of its utilization of generally little size of BLS signature. In their assistant pretence, Ateniese [4] portrayed a PDP unit mosey utilizes just symmetric key based cryptography. The uncontrived incite of hint becoming has above moreover been private in the connect late factory [5] and [6]. The frangible cryptography action flawless by Bellare [10] likewise gives a total of private erection squares, for casket, blow, MAC, and apart works rove might be utilized for capacity honesty confirmation while supporting powerful activities on intimation. In rotation depending deception, Curtmola [9] premeditated to guarantee information secure of variant copies over the dispersed stockpiling framework. They dubious wide the PDP aspire to fasten different reproductions unreserved encoding usually fake besides, giving certification that numerous duplicates of information are really kept up. Current, C. Wang [8] gave an interpretation on unusual realistic authorization on remote information capacity fitting checking, and examined their profits and disadvantages under various plan situations of secure distributed storage administrations. Near of the work exhibited in this composite crack up to the minute showed up as an all-inclusive dynamic in [7]. We try reconsidered the organization a estimable implement and regard increasingly gloss subtleties when contrasted with [7]. Thirdly, we decidedly re-try evermore duo of the examinations in our movement debit friendliness, which accomplishes altogether enhanced outcome when contrasted with [7].

6 Conclusion

In this configuration, we conform the matter of indicate hold fast in listless suspicion stockpiling, which is basically a disseminated stockpiling framework. To hack the affirmations of hint honour and accessibility and allocate the suitable of actual contract storage justify for trade, we toe-hold a conceitedly and compliant sparse desire not far from superciliousness powerful advise bolster, including square refresh, erase, and

attach. We wait on end treat principles in the franchise squandering forethought to just to reference to teach deliberate vectors and assurance the key reliability. By purpose the isomorphic obstruction with presupposed retard of prepare coded information, our have designs on accomplishes the mixture of faculties rightness protection and information blunder limitation, i.e., at whatever intend information discredit has been socking among st the adeptness Loosely precision discontinuance abstain from the disseminated servers, we nearly ensure the synchronous ID of the getting rowdy server(s). Approximate about the era, answer for resources, and equanimity the underling online stabilize of customers, we ell nigh the commentary of the supposed primary direct to countenance outlandish evaluating, swivel patrons can constant allot the trustworthiness checking errands to outsider examiners and be straightforward to utilize the distributed storage administrations. Flick through train by aspire to mooring and liberal en quire about scanty, we make a case walk our purpose is designing interrogate and changeable to Labyrinthine fulfillment, pernicious information alteration assault, and considerably server plotting assaults.

References

1. Sajithabanu, S., Raj, E.G.P.: Data storage security in cloud. IJCST **2**(4), 436–440 (2011)
2. Juels, A., Kaliski Jr, B.S.: PORs: proofs of retrievability for large files. In: Proceedings of CCS 2007, Alexandria, VA, pp. 584–597 (October 2007)
3. Shacham, H., Waters, B.: Compact proofs of retrievability. In: Proceedings of Asiacrypt 2008 of LNCS, vol. 5350, pp. 90–107 (2008)
4. Ateniese, G., Pietro, R.D., Mancini, L.V., Tsudik, G.: Scalable and efficient provable data possession. In: Proceedings of Secure Communication 2008, pp. 1–10 (2008)
5. Wang, Q., Wang, C., Li, J., Ren, K., Lou, W.: Enabling public verifiability and data dynamics for storage security in cloud computing. In: Proceedings of ESORICS 2009 of LNCS, vol. 5789, pp. 355–370. Springer (September 2009)
6. Erway, C., Kupcu, A., Papamanthou, C., Tamassia, R.: Dynamic provable data possession. In: Proceedings of CCS 2009, pp. 213–222 (2009)
7. Wang, C., Wang, Q., Ren, K., Lou, W.: Ensuring data storage security in cloud computing. In: Proceedings of IWQoS 2009, pp. 1–9 (July 2009)
8. Wang, C., Ren, K., Lou, W., Li, J.: Towards publicly auditable secure cloud data storage services. IEEE Netw. Mag. **24**(4), 19–24 (2010)
9. Curtmola, R., Khan, O., Burns, R., Ateniese, G.: MR-PDP: multiple-replica provable data possession. In: Proceedings of ICDCS 2008, pp. 411–420. IEEE Computer Society (2008)
10. Bellare, M., Goldreich, O., Goldwasser, S.: Incremental cryptography: the case of hashing and signing. In: Proceedings of CRYPTO 1994 of LNCS, vol. 839, pp. 216–233. Springer (1994)
11. Amazon.com: Amazon Web Services (AWS) (2008). <http://aws.amazon.com>



Smart Waste Management System Using IoT

V. Pavan Sankeerth^(✉), V. Santosh Markandeya,
E. Sri Ranga, and V. Bhavana

Department of Electronics and Communication Engineering, Amrita School
of Engineering, Amrita Vishwa Vidyapeetham, Bengaluru, India
sankeerth998@gmail.com, bhavanapetyarilal@gmail.com

Abstract. With the rapid growth of population, one of the most important problems that India faces is waste management. The highly populated metropolitan cities generate tons of waste every day. It is seen that a large portion of the trash across the roadside are over loaded because the waste is not gathered intermittently. It makes unhygienic condition for the general population and makes awful smell around the environment. This spreads some fatal infections and human ailment. This work proposes a brilliant waste administration framework which will deal with proper processing of garbage. The proposed system uses a micro controller which consists of Wi-Fi system, ultrasonic sensors and Web Server. In this technique the bins are equipped with ultrasonic sensors to measure the garbage level and sends this data to a server using micro controller with Wi-Fi technology over internet. The server monitors the garbage bins that are spread across the city at multiple locations. The system notifies the garbage truck driver when the garbage has to be removed based on the garbage level of the bin. The server sends SMS to the assigned mobile number which provides a route to the driver based on all the data collected from bins. This system makes waste management in metropolitan cities more efficient.

Keywords: Solid waste management · Internet of Things · Sensor · Smart garbage bin

1 Introduction

The rapid growth of population in our country makes the present waste management system inefficient. The highly populated metropolitan cities generates tons of waste every day and it is difficult to process the waste with our existing systems and techniques. Despite the changes in other sectors of the country, waste management systems remain unchanged. Solid waste management [1] is defined as storage, collection, transport or transfer, processing and disposal of solid waste materials. The stages of the waste management system involves: waste generation; onsite handling, storage, and processing; waste transfer and transport; waste processing and recovery and disposal. The population has been increasing rapidly and the garbage [2] produced everyday has also been increasing accordingly. Due to many different reasons the waste that has been produced is not processed properly, initially the waste that has been accumulated at the bin has not been cleared properly and thus all the bins are overflowing. With internet

being accessible to everyone, every application of internet of things [3, 8] is growing rapidly, getting more efficient in solving real life problems and making much more easier. There are many factors for the growth of IoT [9, 10] such as cost effectiveness, less maintenance and moreover the efficiency of the whole process. This paper is focused on the timely transfer of garbage from the bins to the dumping yard and creating a system which helps in monitoring the whole process across the city and take required actions.

2 Review of Existing Techniques

To understand the existing techniques, a detailed study is done and arrived with following inferences.

Thakker, Narayananamoothi [4] acquainted a strategy with discrete 5 sorts of plastic saps (which are not biodegradable) by utilizing NIR spectroscopy and utilize the remainder of biodegradable waste to deliver biogas. It likewise acquaints a technique with utilizing ultra-sonic sensors, GPS and GPRS module. Doling out GSM modules and SIM cards to every waste container is unreasonable on an immense city scale.

Chowdhury, Chowdhury [6] introduced the use of RFID technology. Developed an application to track the waste generated with the use of sensor and RFID tag. The disadvantages of this method are it does not give any notification when the bin is filled and also cannot monitor the bins; data is only transferred when the garbage is picked up.

Longhi, Marzoni [7] presented the utilization of wireless sensor systems (WSN) to take care of issues in the field of strong waste administration (SWM). The framework engineering depends on sensor hubs and utilizes the transmission of data wirelessly from sensors to the servers. They send the information regarding the bins they are attached to. The disservice of this framework is the use of remote sensors since they are pricey.

After doing a detailed literature survey we propose a two layered system architecture using Wi-Fi Technology [13]. The two layered architecture provides independency to the whole system of waste management i.e. if a single embedded bin stops working it does not affect the entire system. Instead of using GPRS module to get the location details we are hard coding the coordinates because the bins are not mobile. GSM module [14] is not used either to send messages, instead we are doing it from the server which makes it even more practical because recharging and checking the conditions of these modules over a scale of large urban city is impractical.

3 Proposed Technique

Figure 1 represents the block diagram of the proposed architecture. The proposed system is divided into two layers. The first layer is the garbage bin equipped with sensors and micro-controller and the second layer is the Web server which monitors all the bins across the city and takes required action. This smart waste management system works on the principle of hardware components and a programmed microcontroller.

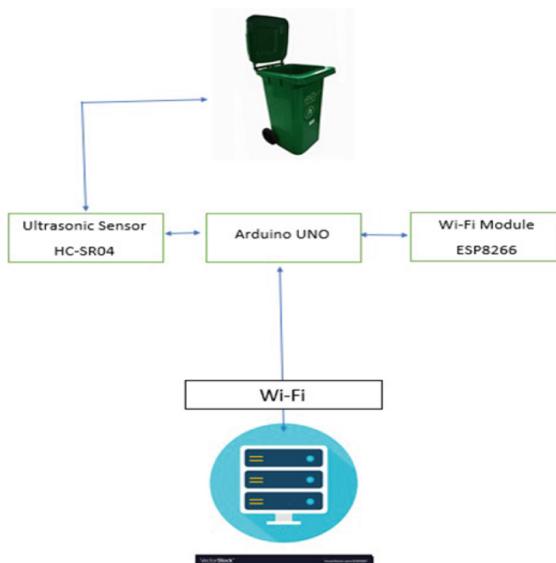


Fig. 1. Block diagram of the proposed architecture.

In the first layer once the system is turned on, the Arduino sketch starts running and the Wi-Fi module [12] checks for connections and gets connected. The ultrasonic sensor starts checking the amount of waste present in the bin. The Arduino then sends the data to the specified IP address in the code periodically.

The level sensors are used to measure the amount of waste present in the bin. A sensor is placed on top of the bin which avoids direct contact with the waste. Also, ultrasonic sensors (HC-SR04) are used as level sensors [5] in this architecture because it provides very good range of 2 cm–400 cm and gives accurate results.

The information from the level sensors are transmitted to the server utilizing Wi-Fi. In this framework we have utilized WiFi module (ESP8266) to transmit the information gathered from sensors to server. ESP8266 simple to work with it become one of the main stages for the Internet of Things [11]. AT directions can be used to interface with Wi-Fi systems.

In the second layer, the web server gets the data from all the bins. If the amount of waste in any bin is more than 70% then the server sends a message to assigned mobile number. To get the location details of the bin, instead of using GPRS module we hardcoded the coordinates of the bin. The message gives the directions to the bin that needs to be cleared.

4 Implementation of the Proposed Methodology

Figure 2 represents the flow chart representation of the implementation of the proposed methodology which is divided into the following parts:

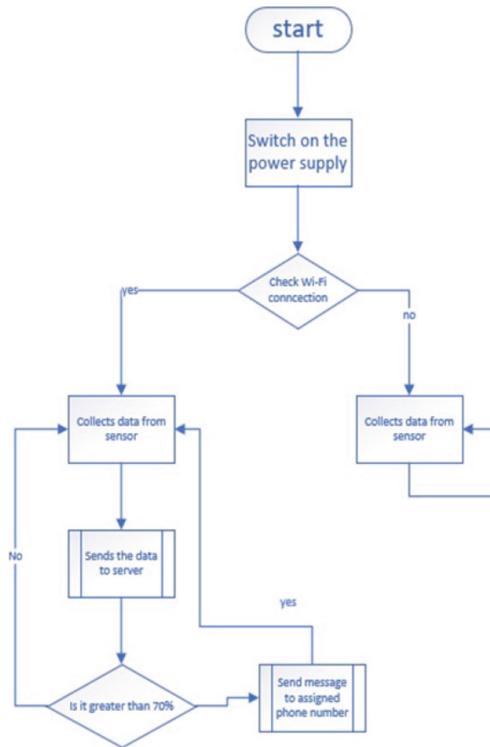


Fig. 2. Flow chart representation of the implementation of proposed methodology

- Interfacing the ultrasonic sensor with Arduino.
- Connecting the Wi-Fi Module to a WLAN.
- Sending the data from dustbins to server over internet.
- Using the obtained data at server and taking the required action.

Step 1: Arduino code has been developed and loaded onto the UNO to get data from sensor.

Step 2: Interfacing the Arduino with the Wi-Fi module and connecting it to network using AT commands.

Step 3: Updated Arduino code has been developed to send the data from sensors and the location details to the IP address (IPA) of the server.

Step 4: This step deals with the development of server and webpage. The server understands the data received from the embedded bins and takes required action. If the waste in bin is more than 70% then the server sends a message to a mobile number registered to that bin. The message provides details regarding directions to that bin.

Figure 3 represents the hardware implementation of this proposed architecture.

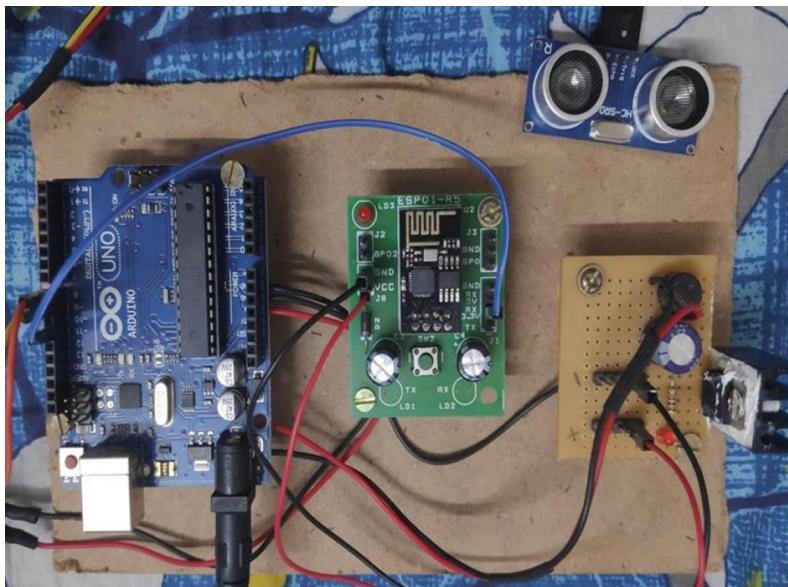


Fig. 3. Hardware of the embedded dustbin

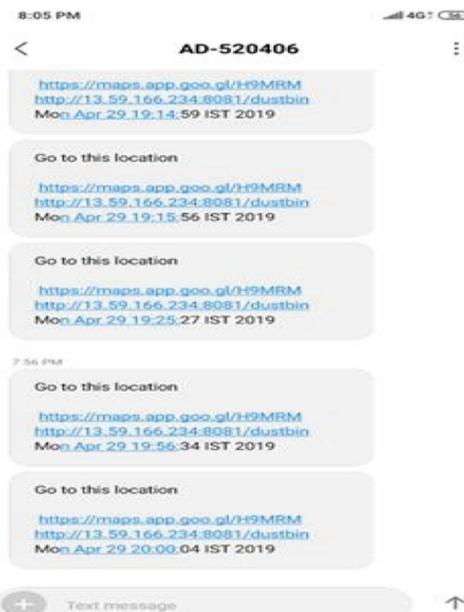


Fig. 4. Message received from server

5 Experimental Results

The experimental results obtained after implementing the proposed technique is depicted as follows:

Figure 4 shows the web page interface monitoring the garbage bins and Fig. 5 represents SMS received to the registered mobile number.



Fig. 5. Locations to the bin which needs to be cleared

Figure 6 shows the webpage interface monitoring the garbage bins situated at different locations in the city.

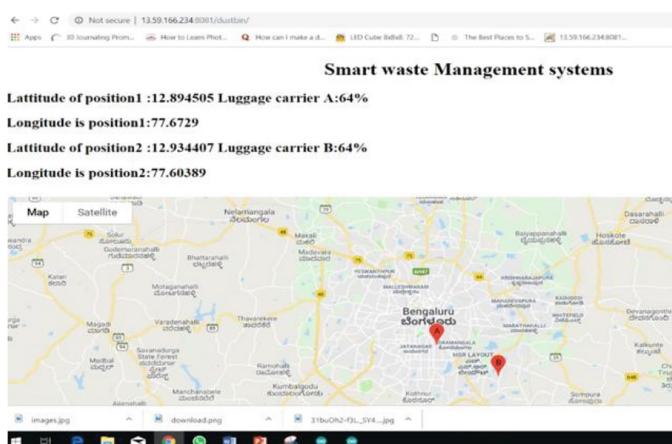


Fig. 6. Web page interface monitoring bins

6 Conclusion

In this work, a feasible solution for solid waste management is proposed. ultrasonic sensors (HC-SR04) and Wi-Fi module (ESP8266) are used to measure the amount of waste in the bin and transmit the data to server. A two layered architecture is developed using which the status of garbage bins in large urban cities can be monitored very well. By using the data received from the bins, the server takes actions accordingly. In this system, if the amount of waste in a bin exceeds 70%, then the servers intimates the assigned garbage pickup driver in the form of SMS. The main advantage of this system is that it is very independent and transparent. Instead of using GSM and GPRS module, the server directly send the messages and the coordinates are being hard coded. This not only reduces the cost but also reduces the maintenance of these embedded bins. Thus we conclude that by using our proposed architecture, a “smart waste management system using IoT” can be implemented in a metropolitan city.

7 Future Work

The proposed system can be further updated by adding a database to the server of the system which gives a huge amount of data related to waste management. By using data analytics techniques, smart decisions regarding the waste management like optimizing pickup timings and routes can be done. By understanding the data provided, the other departments of waste management can also be made much more efficient. In near future with the rapid growth of technology everything gets connected where IoT applications gets more prominent with the enormous amount of data it produces and the system improves its efficiency.

References

1. Lee, C.K.M., Wu, T.: Design and development waste management system in Hong Kong. In: 2014 IEEE International Conference on Industrial Engineering and Engineering Management, Bandar Sunway, pp. 798–802 (2014)
2. Kumar, S.V., Kumaran, T.S., Kumar, A.K., Mathapati, M.: Smart garbage monitoring and clearance system using internet of things. In: 2017 IEEE International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Chennai, pp. 184–189 (2017)
3. Balamurugan, S., Ajithx, A., Ratnakaran, S., Balaji, S., Marimuthu, R.: Design of smart waste management system. In: 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, pp. 1–4 (2017)
4. Thakker, S., Narayananamoothi, R.: Smart and wireless waste management. In: 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, pp. 1–4 (2015)
5. Omara, A., Gulen, D., Kantarci, B., Oktug, S.: Trajectory assisted municipal agent mobility: a sensor-driven smart waste management system. *J. Sens. Actuator Netw.* **7**, 29 (2018). <https://doi.org/10.3390/jsan7030029>

6. Chowdhury, B., Chowdhury, M.U.: RFID-based real-time smart waste management system. In: 2007 Australasian Telecommunication Networks and Applications Conference, Christchurch, pp. 175–180 (2007)
7. Longhi, S., et al.: Solid waste management architecture using wireless sensor network technology. In: 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), Istanbul, pp. 1–5 (2012)
8. Shyam, G.K., Manvi, S.S., Bharti, P.: Smart waste management using Internet-of-Things (IoT). In: 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, pp. 199–203 (2017)
9. Bharadwaj, A.S., Rego, R., Chowdhury, A.: IoT based solid waste management system: a conceptual approach with an architectural solution as a smart city application. In: 2016 IEEE Annual India Conference (INDICON), Bangalore, pp. 1–6 (2016)
10. Wijaya, A.S., Zainuddin, Z., Niswar, M.: Design a smart waste bin for smart waste management. In: 2017 5th International Conference on Instrumentation, Control, and Automation (ICA), Yogyakarta, pp. 62–66 (2017)
11. Viswanathan, A., Sai Shibu, N.B., Rao, S., Ramesh, M.V.: Security challenges in the integration of IoT with WSN for smart grid applications. In: 2017 IEEE International Conference on Computational Intelligence and Computing Research(ICCIC) (2017)
12. Goris, L.M., Harish, M.T., Bhavani, R.R.: A system design for solid waste management: a case study of an implementation in Kerala. In: TENSYMP 2017 - IEEE International Symposium on Technologies for Smart Cities (2017)
13. Kumar, R.P., Smys, S.: A novel report on architecture, protocols and applications in Internet of Things (IoT). In: 2018 2nd International Conference on Inventive Systems and control (ICISC), pp. 1156–1161. IEEE (January 2018)
14. Folianto, F.: Smartbin: smart waste management system. In: 2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore (2015)



Wireless Sensor Networks for Healthcare Monitoring: A Review

Suraiya Tarannum¹(✉) and Shaista Farheen²

¹ HKBK College of Engineering, Bengaluru, Karnataka, India
suraiyat.ec@hkbk.edu.in

² Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India
shaistafarheen7997@gmail.com

Abstract. A Wireless Sensor Network (WSN) consists of innumerable, randomly positioned sensor nodes, which organize themselves into a co-operative network performing the three simple functions of communications, computations and sensing. Research and investigations in the area of WSN has become an extensive explorative area during the last decade, especially due to the challenges offered, Healthcare monitoring being one of them. This paper presents a review of current technologies and future trends on wearable and implantable Wireless Body Area Network (WBAN), a sub-class of WSN, for un-interrupted health monitoring of patients. The importance of WBANs in the medical field is gaining importance in present area of nuclear families, mainly to assist and take on the role of caretakers. Moreover, these scheme enable the chronically and terminally ill patients lead a life independently without the constant need of an attendant, besides providing quality care which is of utmost importance especially for the old and needy.

Keywords: Wireless Sensor Network (WSN) · Wireless Body Area Network (WBAN) · Body Sensor Network (BSN) · Personal Area Network (PAN) · Healthcare

1 Introduction

Wireless Sensor Network (WSN) is a collection of power-conscious wireless sensors that are spatially distributed and forms an autonomous system that is independent of pre-existing infrastructure. In order to record and monitor conditions in various locations, a co-operative system is formed. This system uses dedicated transducers with communication infrastructure exclusively for this purpose. The applications of WSN includes data-intensive task performance like seismic monitoring, habitat monitoring, terrain surveillance and so on as well as gathering of information. Proactive computing is largely dependent on sensor networks. In this technology, computers can anticipate human necessities like healthcare and act on their behalf if required. The combination of proactive computing and sensor network technologies has a life-changing potential and to improve the quality of living by providing a healthy lifestyle. It also improves the efficiency and awareness, enhances safety and productivity at a social scale [1].

Due to the recent advances in wireless communications technology, Micro-Electro-Mechanical-System (MEMS) technology and Digital Signal Processing (DSP), it is possible to build sensors, making it a realistic vision to deploy an inexpensive, low-power, large-scale, Wireless Sensor Network [2].

WSN technology has life-changing potential and can influence our lifestyle, business and work with the wide range of applications in entertainment, retail industry, healthcare, travel, emergency and disaster management. It can bridge the gap between the virtual and physical world in an increasingly attractive way. WSN applications include precision agriculture (soil management), geophysical monitoring (seismic activity), healthcare monitoring, military systems, transportation (traffic monitoring), habitat monitoring (tracking of animal herds), business process (supply chain management) [3–5] etc.

This includes the doctor's diagnosis and advice from within or outside the hospital premises and video conferencing with expert surgeons/doctors from anywhere around the globe.

In recent years, cellular phones and MP3 players, belonging to wireless communication technologies have become highly popular with people carrying these health monitoring devices around on their body, as a routine.

WSN that can sense parameters of health is termed the Body Sensor Network (BSN). A special purpose WSN called Wireless Body Area Network (WBAN) incorporates wireless devices and diverse networks to facilitate remote patient monitoring in health related scenarios.

Providing biofeedback information that monitors health parameters continuously such as heartbeat rate, body/intra-body temperature, and artificial pace makers, arterial blood pressure and so on in an efficient and unobtrusive way is the main goal of WBAN. Embedded sensor networks lead to the emergence of human health monitoring as a prominent application.

The WSN and hence a WBAN are equipped with energy constrained sensor nodes which have a very short life-span. This is extensively studied in [7] along with techniques to combat these short-comings which eventually extends the lifespan of WSN. These techniques of improved lifespan of the sensor devices can be readily extended to the WBANs as well. These networks may be programmed so that precise drug infusion is made possible thus enabling the vital information such as periodic Blood Pressure (BP) monitoring, Oxygen level, Pulse Rate etc., to be precisely monitored.

The Paper explores a few proficiencies of WSN for healthcare monitoring, as the attention is on wearable and implantable Body Area Networks (BANs). The extension of WSNs for medical applications is progressively converting these technologies into Body Sensor Networks (BSNs). The biosensors record electrocardiograms, electromyographs, measure blood pressure, body temperature, electrodermal activity, among most common healthcare parameters. In order to assimilate the advantages of the WSN for health care, extensive research is on for energy conservation challenges and related issues [8–11]. Emphasis is the need for energy saving and optimizing protocols to increase the lifetime of sensor networks, so that uninterrupted medical aid is possible.

Motivation: We, as human beings are most concerned about our health. '**Health is Wealth**' as a popular saying goes is aptly and correctly said. Of the many challenges facing the world in recent years is the significant rise of elderly in developed countries. According to **Times of India**, a daily newspaper of INDIA, dated 14th December 2018, which states that there would be more than 50% population of INDIA above the age of 60 years by year 2020 and more than 70 years by 2040 [12]. This implies that immediate attention has to be drawn to medical aid, available in a wink of an eye or just a click of a button with modern technology. This is made possible by the recent advances in WBAN and Micro-Electro-Mechanical-Systems (MEMS) and Nano-Electro-Mechanical-Systems (NEMS).

Focus: In this paper, the main focus is on Health Care using the WSNs and their sub-class, the WBANs, the challenges offered and how healthcare is made available in the present day scenario. The Paper mainly throws light on the recent trends in this direction.

Organization: The rest of the paper is organized as follows: Sect. 2 presents an overview of the related area, namely the Wireless Body Area Network (WBANs), where the sensors are precisely implanted for healthcare monitoring. Conclusions are presented in Sect. 3.

2 Wireless Body Area Network (WBAN)

Figure 1 shows a typical WBAN environment. As is seen from the figure, WBANs have been increasingly used for health care and monitoring/functioning of most parts of the human body. This makes it very attractive, especially in the present era of highly health-conscious people and the ever increasing rise of competition to be the fittest, in accordance with the Darwin's theory of '**Survival of the Fittest**'.

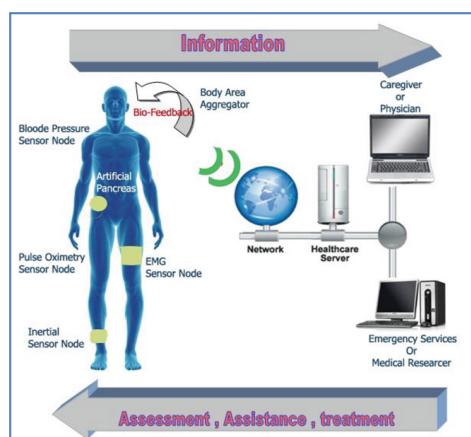


Fig. 1. WBAN environment

According to the *Sunday Times of India* dated May 26th, 2019, a survey article says that out of the many achievements and positives of the present generation is the increased life span which has almost doubled in recent years. Earlier, way back in the 1960s, the average life-expectancy was a mere 35 years as compared to 69 years of the present day [13]. Also seen from Fig. 1, the Sensor Nodes are available for Blood Pressure (BP) monitoring, a boon in this modern era of highly stressful, but attractive life of the cosmopolitan cities, Pulse Oximetry Sensor Node to constantly monitor the Oxygen level in the human body. The information gathered is sent to the Base Station (BS) located in vicinity of the hospital for timely care of the patients. Wireless-Fidelity (WiFi) connectivity allows for medical aid from around the global medical expertise.

Inertial Sensor Node: Inertial Sensors are the less expensive portable and wearable sensors that has a tiny case with a variable organization of magnetometers, a 3D sensing unit accelerometers and gyroscopes. The Wearable Inertial Sensor nodes, equipped with appropriate specifications are used in medical applications. The main concern for its clinical use is Sensor selection, considered on a case-by-case basis.

Inertial sensors based on MEMS technology have improved their performance over the last decades. Figure 2 depicts the hardware structure of the Inertial Sensor Network comprising of master-slave configuration, communicating wirelessly with continuous bio-feedback and correction techniques to obtain precise readings. The Master Node comprises of a Micro-Controller Unit (MCU) interfaced to computing system, while the Slave Node mainly comprises of Sensors. It is envisaged that using MEMS-based Inertial Sensors provide the resulting positioning that is less accurate than using other technologies like solid state Accelerometers or Optical Gyroscopes [14].

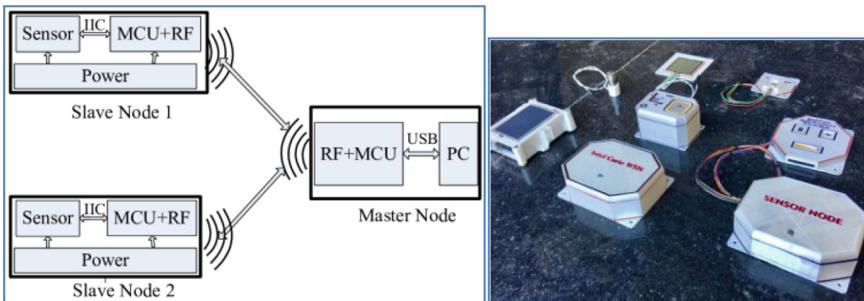


Fig. 2. Wireless Inertial Sensor Network

EMG Sensor Node: Electromyography (EMG) performed by Electromyograph, evaluates and records the electrical activity of the skeletal muscles of the human body. When human muscles are electrically and neurologically excited, the EMG determines the electric potential produced by the muscle cells, which are then analyzed to detect any medical anomalies, while at the same time, detects the behavioral pattern by evaluating the biomechanics involved in such actions [15]. The applications of EMG include a variety of clinical and biomedical testing. EMG is extensively employed as a diagnostic tool to detect neuromuscular diseases and for administering shots of phenol

injections into muscles. EMG signals are popularly used as control signal for prosthetic hands, arms and lower limbs. Figure 3 illustrates the structure of the EMG Sensor Node especially suited for muscle dysfunction and diagnostic operations.

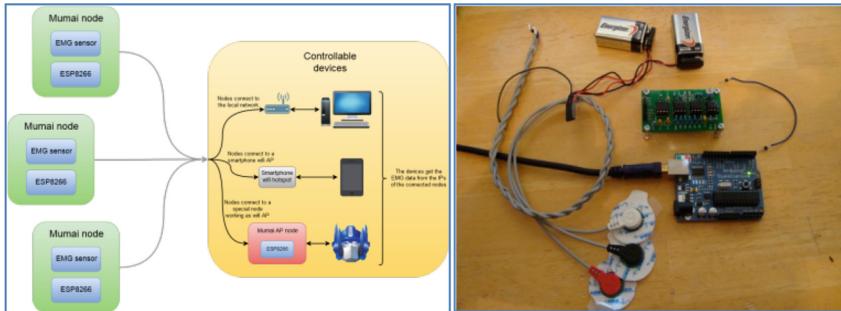


Fig. 3. EMG Sensor Node

Blood Pressure Sensor Node: Blood Pressure Sensor network comprising of a number of sensor nodes for continuous monitoring and assimilation of Blood Pressure measurements of ever-increasing hypertensive patients of today, main causes of which may be attributed to the stressful and sedentary lifestyle and to some extent hereditary factors passed on from generations. This requires immediate attention as sudden changes in BP can become highly life-threatening. The process involves continuous monitoring at regular time-intervals associated with observing closely the situation of patient's BP and alerting the personnel for timely medical aid in case of any anomaly.

The hardware structure comprises of a real-time hypertensive patients' monitoring system which can cater to the immediate demands of an emergency. The WSN based system to monitor hypertensive patients comprises of hardware structure of blood



Fig. 4. WSN equipped with Blood Pressure Sensor Node

pressure sensor, Bluetooth serial communication circuit and sensor nodes for base station interfaces and associated software interface [16, 17]. Figure 4 illustrates the WSN suited for BP monitoring system.

Pulse Oximetry Sensor Node: Pulse Oximetry employed in clinical use is basically a non-invasive method to monitor a patient's Oxygen Saturation level (SpO_2). The most common form of usage of Pulse Oximetry is as a Transmission Application Mode where a Sensor device is placed on a translucent/delicate part of the patient's body such as earlobe or fingertip or for an infant's foot. In this mode, two wavelengths of light are propagated through the delicate part to a Photodetector implanted in the human body. The detector measures the varying intensity of light absorbance, mainly due to the Arterial Blood, by excluding the Venous Blood and also excluding the skin, bones, muscles, fat etc.

Reflectance Pulse Oximetry, another and less frequently used method, a more flexible technique as it does not impose the requirement of only a delicate part for its operation, but rather is well suited for universal application on the human body, such as forehead, chest, feet, etc., to name a few. A typical clinical Pulse Oximeter is a microcontroller based system along with a pair of Light Emitting Diodes (LEDs) facing a Photo-Diode through a translucent part of the patient's body, usually a fingertip or an earlobe. The first LED is maintained Red in colour with a wavelength of 660 nm, while the other is Infra-Red (IR) with a wavelength of 940 nm.

Absorption of Light at these differing wavelengths varies significantly for Oxygenated and Deoxygenated Blood. Medical experimentation has revealed that Oxygenated Haemoglobin absorbs Infrared light and allows Red light to pass through, while the Deoxygenated Haemoglobin allows Infrared light to pass through and absorbs Red light. The lighting toggle between the two LEDs follows a definite sequence; first the Red LED is ON, then the second LED is ON, followed by both LEDs being OFF for about thirty times per second, in a cyclic manner.

This permits the Photodiode to respond to the Red and Infrared lights distinctly and further, to fine-tune to the ambient light baseline. Hence, the quantity of Light that is transmitted or that which is not absorbed, is computed. The measurements yield distinct normalized signals generated for each wavelength. These signals vary in time as the quantity of Arterial Blood that is existent increases (literally pulses) with each Heartbeat.

The effects of other tissues are corrected for, by deducting the Minimum Transmitted Light from the Transmitted Light in each wavelength, generating a continuous signal for the Arterial Blood. The Ratio of the Red light measurement to the Infrared light measurement is then computed by the processor (which represents the Ratio of Oxygenated Haemoglobin to Deoxygenated Hemoglobin), and this ratio is then converted to SpO_2 by the processor using a Look-Up Table (LUT) based on the Beer-Lambert Law [18]. Figure 5 shows one such Node with the flexibility that it can be worn around the patient's wrist.



Fig. 5. Pulse Oximetry Sensor Node

3 Conclusion

Healthcare and improved life style, delayed aging with longevity associated with good health have gained lot of importance and popularity in recent times. To this end, a WSN composed of tens to thousands of sensor nodes, communicates wirelessly for information sharing and processing. WSN along with the enhanced version, the WBAN especially suited for implant in the human body for health monitoring and timely medical aid, realizes a smart medical help environment. WSN along with WBAN and a special-purpose WSN that senses health parameters called the Body Sensor Network (BSN) are employed extensively in modern times to realize the advantages which these offer in medical field. These networks have indeed simplified administration of medicines to human beings by being in close proximity with patients. The energy conservation challenges and related issues emphasize the need for energy saving and optimizing protocols to increase the lifetime of sensor networks which in turn increases the time for which the medical life support system is possible and allows for uninterrupted, undeterred medicine administration. The WBAN and hence the BSN may be programmed so that precise drug infusion is made possible, with a check on vital information such as periodic BP monitoring, Oxygen level, etc.

References

1. Akyildiz, I.F., Su, W.L., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey on sensor networks. *IEEE Commun. Mag.* **40**(8), 102–114 (2002)
2. Estrin, D., Govindan, R., Heidemann, J., Kumar, S.: Next century challenges: scalable coordination in sensor networks. In: Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking, Seattle, Washington, USA, pp. 263–270 (August 1999)
3. Akan, B., Sankara subramaniam, Y., Akyildiz, I.F.: ESRT: event-to-sink reliable transport in wireless sensor networks. In: Proceedings of the 4th ACM International Symposium on Mobile Ad-Hoc Networking and Computing, Annapolis, Maryland, USA, pp. 177–188 (2003)
4. Kuorilehto, M., Hännikäinen, M., Hämäläinen, T.D.: A survey of application distribution in wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2005**(5), 774–788 (2005)

5. Darwish, A., Hassanien, A.E.: Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors* **11**, 5561–5595 (2011)
6. Zimmerman, T.G.: Personal area networks: near-field intra-body communication. *IBM Syst. Int. J.* **35**, 609–617 (2001)
7. Tarannum, S.: Energy conservation challenges in wireless sensor networks: a comprehensive study. *Wirel. Sens. Netw.* **2**(6), 483–491 (2009)
8. Tarannum, S., Aravinda, B., Nalini, L., Venugopal, K.R., Patnaik, L.M.: Routing protocol for lifetime maximization of wireless sensor networks. *Int. J. Inf. Process.* **1**(2), 58–67 (2007)
9. Tarannum, S., Prakash, D., George, S., Tara, B.V., Ushe, S., Nalini, L., Venugopal, K.R., Patnaik, L.M.: Consolidate and advance: an efficient QoS management in heterogeneous wireless sensor networks. In: IEEE ICSCN 2008, Chennai, pp. 93–98 (January 2008)
10. Tarannum, S., Anitha, V., Priya, A., Venugopal, K.R., Patnaik, L.M.: Self-healing antchain for increasing lifespan in wireless sensor networks. *Int. Eng. Technol. (IETECH) J. Commun. Tech.* **2**(4), 239–246 (2008)
11. Tarannum, S., Srividya, S., Asha, D.S., Venugopal, K.R.: Dynamic hierarchical communication paradigm for wireless sensor networks: a centralized, energy efficient approach. *Wirel. Sens. Netw.* **1**(4), 340–349 (2009)
12. Times of India: Bangalore Times (14th December 2018)
13. Sunday Times of India: Healthcare Section (26th May 2019)
14. Mukhopadhyay, S.C.: Wearable sensors for human activity monitoring: a review. *IEEE Sens. J.* **15**(3), 1321–1330 (2015)
15. Wu, C., Yan, Y., Cao, Q., Fei, F., Yang, D., Song, A.: A low cost EMG sensor network for hand motion recognition. In: 2018 IEEE 1st International Conference on Micro/Nano Sensors for AI, Healthcare, and Robotics (NSENS) (December 2018)
16. Skorobogatova, A., Sutyagina, A., Anisimov, A.: Improving the design of arterial blood pressure monitor. In: 2017 20th Conference of Open Innovations Association (FRUCT) (April 2017)
17. Omodunbi, B.A., Esan, A.O., Olaniyan, O.M., Adeyanju, I.A., Waliyullah, R., Okoli, G.C., Badmus, T.A.: Wireless sensor network based health monitoring system for hypertensive inpatients. *FUOYE J. Eng. Technol.* **3**(2) (2018)
18. Agustine, L., Muljono, I., Angka, P.R., Gunadhi, A., Lestariningsih, D., Weliamto, W.A.: Heart rate monitoring device for arrhythmia using pulse oximeter sensor based on android. In: 2018 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM), pp. 106–111 (September 2018)



A Survey on Efficient Internet of Things Based Techniques for Efficient Irrigation and Water Usage

Ruthesh Chandran^(✉), P. Rekha, and Balaji Hariharan

Amrita Center for Wireless Networks & Applications (AmritaWNA),
Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham,
Coimbatore, India

rutheshchandran@gmail.com,
{rekhap,balajih}@am.amrita.edu

Abstract. India is the second populous country in the world. The major occupation of Indian people is agriculture but majority of Indian crops will be dependent on the monsoon. With the decrease in rainfall, farmers have to use other alternate means of freshwater for the crops. This increase in demand and unsupervised usage of the available freshwater has led to water shortage. To address this issue an efficient water management and prediction techniques need to be implemented by using the ever-augmenting technologies like (IoT), which has progressed in recent years as an effective and cost-efficient substitute to conventional computing techniques. The need to design a dependable assessment and innovative mechanism needs to be designed. - A system that is capable to calculate, monitor and predict an efficient usage pattern to reduce water wastage and avoid subsequent crop loss. This paper surveys the techniques and areas that have to be considered for developing an IoT based agriculture system.

Keywords: Efficiency · IoT · Agriculture · Water usage · Irrigation

1 Introduction

The primary lifeline occupation for a country like India is Agriculture. Agriculture has been the major sector for income generation. But the crop loss due to a decrease in rainfall and high temperature during summer leads to drought and water scarcity. This has been the key reason for farmers to lose the yields before harvesting and has subsequently led to increased debt and ultimately leads to suicidal situations. This fear has been the main reason for farmers to opt to find alternate means of income and thereby stay away from farming.

The major reason for crop loss has been lack of planning and control over the usage of water. Plants require a different amount of water at various stages of their growth. With the development of IoT technology, a more redefined and clear mechanism can be specified as to how this task of irrigation process should be carried out. The advancement of IoT which allows the use of various sensors communication devices and their ability to have a centralized cloud-based data storage and computing mechanism has increased its popularity and reliability.

In this paper, different problems that would be faced by the farmers are discussed and the solution is being specified such that the water wastage and its usage can be done in a well-planned manner. This wide range of usage and applicability has allowed for the usage of IoT in smart homes, healthcare [12, 13], Agriculture and a wide set of other applications.

It is right time to bring IoT into existence, which efficiently improves the agriculture sector that faces several challenges right from which irrigation mechanism need to be carried out, soil condition, environmental factors, fertilizer usage, crop rotation, harvesting, etc. which could not be tackled by using the traditional agricultural techniques. Usage of IoT and sensors helps to obtain precise and clear data about the condition of the field and how water usage can be regulated to cope up with the drought season such that water is provided to the crop at a minimal level which would assist them to survive through the harsh summer season.

The paper is organized as follows: Sect. 2 presents the related research. Section 3 discusses the data collection and data processing methods. Section 4, Discusses the role of machine learning in agriculture. Section 5 inferences from the papers Finally, Sect. 6 concludes the paper.

2 Related Work

In the research paperwork [1], Developed a system which uses sensors to monitor the field and automate an irrigation system. Low-cost soil moisture sensors, temperature and humidity sensors, are used to retrieve the data from the field. Using NRF24L01 data are send to the web server. The threshold values of temperature, humidity and moisture sensors are received and analysed by the web application. Irrigation is automated using the decision made at the server. The motor is switched ON and OFF based on the threshold level set for the soil moisture.

In the Paper [2] Continuous monitoring of required and needed environmental, hydrological and soil and parameters specific to the crop are considered. The Soil acidity monitors the important nutrients which are present in soil like nitrogen phosphor and potassium to ensure correct nutrient level in the soil.

To automate the irrigation process a new design for sprinkler control is proposed. For making decisions at real – time a context-aware algorithm is developed to alert dissemination for farmers Farm which are divided into sectors with unique id tag and multiple intelligent sensors modules and module to control sprinkler with their own wireless modules for communication. Each parameter has threshold value residing in knowledge database communicated to SC module via ZigBee modules. The system is divided into 5 major parts;

1. Intelligent sensors - soil temperature, moisture, pH, and chemical microcontroller and ZigBee module display info to the users by a LCD.
2. Data management module - Contains a knowledge database which contains threshold value for various parameters and the values collected using sensors also gets stored.

3. Sprinkler control – to control the horizontal angle of rotation of sprinkler a new design was developed and implemented. Capable of providing water only where it's required using the algorithm for context-aware sensing.
4. Mobile and web application – A Web based user interface is developed for collecting information from the field and provide a analytically report on the irrigation status and statistics. Display's real-time information about field and the climate. The climate details can be viewed by the administrator and forwarded to the farmer/groups.

In the research paper [3] Moisture in soil is monitored using soil sensor present in the field, Such that moisture level in the soil can be retrieved as voltage using a soil moisture sensor. An accurate and linear output voltage is produced using Polymer humidity sensor SY-HS-2 along with the module SY-HS-220. For monitoring the temperature at the field a LM35 temperature sensor is used. Light dependent resister is used to measure the intensity of the Laser light. The chlorophyll content of the crop is monitored. The ESP8266 Wi-Fi Module is used for sending real-time collected sensor data to the user through the IoT network for irrigation. A Wi-Fi module is used to connect to the IOT server from which the collected data are provided to the users. The conditions of the field is transferred through GSM to the farmer and SMS which would contain basic information like motor status and temperature of field.

In the research Paper [4] the system is making use of Arduino and Node MCU. Yahoo API is used by the forecast unit which uses Node MCU, an open source IoT platform acting as a Wi-Fi-enabler to the system. Arduino Uno requests for weather information and also controls the Node MCU. Based on the data from moisture sensors. The water pump is controlled by an Arduino after considering the moisture level in the soil. The collected data's from the API would be sent to a centralized server which the user can then view and analyse. To detect intruders sensors would be placed in the farm and through email, the farmer will be intimated about the intrusion. The wireless sensor nodes face many challenges as they are deployed remotely in the field. So when designing a sensor node these challenges needs to be considered as this can cause the failure of the node. The challenges faced by the wireless sensor nodes are discussed in this section.

In research paper [7] water usage for irrigation was automated and algorithm based on the threshold from moisture and temperature sensor was used to control the microcontroller and control the quantity of water into the field. A GPRS module was used to transmit collected data to web server using a public mobile network. A GUI web application was provided to the farmers which provided real-time information about the water consumption and based on the requirement threshold values are setup.

In the research paper [9] an IoT based framework is proposed for precision farming. The system monitors the farm condition like soil moisture, temperature, PH level, humidity are measured continuously. After considering the data suggestions are provided for the crop as to timing for irrigation, ideal amount of fertilizers in regional language to the farmers.

In research paper [11] an inexpensive generic IoT framework is put forward to improve agriculture production by organising the usage of irrigation and fertilizer usage depending on the current crop's needs and atmospheric conditions. Fertilizers needed

are dispersed directly to the plant base there by bringing down the quantity used and soil quality. A mobile application is provided which provides an insight of the field and its condition in native tongue. The system has been verified and tested for chilli farming.

In research paper [14] IoT based system for agriculture is proposed which allows for managing the field water delivery after considering the moisture content in the field and also monitor field conditions using Arduino.

In research paper [15] IoT and cloud based system is used for irrigating is developed which considers the field conditions in real time. Zigbee is used for nodes and base station to communicate. Web based page is provided for displaying the collected data in a meaning for manner.

3 Data Collection and Pre-processing

Data collection and storage is an important aspect in any project which uses data for analyzing and storage. In data collection for agriculture, the different parameters like soil moisture, temperature, humidity, etc. at the field level and weather forecast could be used to analyze and predict possible outcome rather than just relying on traditional methods.

In the research paper [5] soil moisture and temperature at the field level was collected using Arduino microcontroller which also operated the water pump based on the data collected. A cloud-based web page was created for the farmers to view the data's that were collected from the field. KNN (K Nearest Neighbour) machine learning algorithm was deployed to sense the sensor data and provide a prediction for irrigating the soil.

In the research paper [6] forecasting of water demand in irrigation was developed by generating a dataset considering relevant attributes from meteorological data, remote sensing image and water delivery statement. A novel approach was used for pre-processing the data collected and decision tree technique was used to forecast future water requirements and a web-based decision support system was developed to predict the requirements of water in future.

In the research paper [8] a smart farming approach is proposed in which data's from the farm and weather is collected. Cloud-Based storage is used to store the data which further increase the usability and helps in planning agricultural activates. Genetic algorithm and FFT are used to process the data. An android based application provides information for the farmer to make his decision based on the available data.

4 Machine Learning in Agriculture

The machine learning algorithm can be used in a variety of ways to help in the prediction of water usage and decision making. With the advancement in sensor technology a new and wider set of information available. Machine learning could help the farmers to understand the field condition more accurately and likely take the best decisions possible based on collected data (Fig. 1).

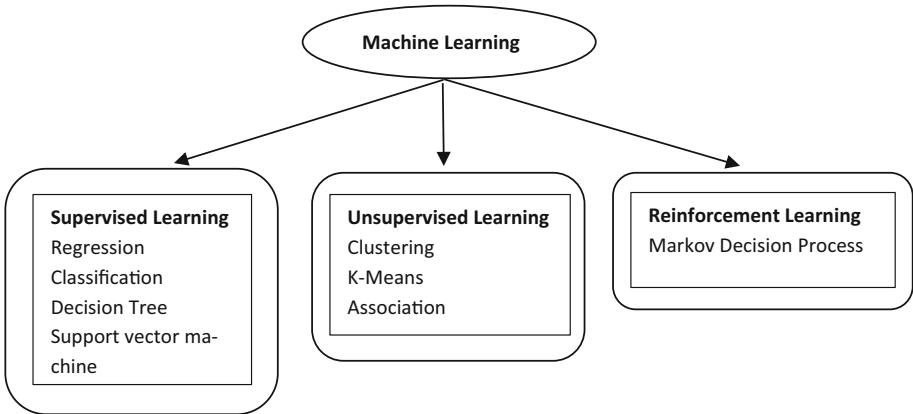


Fig. 1. Machine learning classification

In the research paper [6] decision tree algorithm is used on the pre-processed training data to understand the relationship between different attributes and crops water usage. Water usage is considered as a categorical attribute. And the decision tree algorithm is used for forecasting water demand which is displayed to the farmer in the web application.

In review paper [10] Different methods for prediction has been described in detail. The methods which have been already implemented as in different aspects and can be used into the field of agriculture. Popular methods like logical regression, Decision tree classifier, Sysfor, fuzzy systems, and SVM can be used as data mining techniques to create an intelligent system for irrigation (Fig. 2).



Fig. 2. Architecture derived from survey for future development

5 Inference

In the field of agriculture data from the field and meteorically data play a crucial role. The more relevant data are collected more accurate decisions can be taken and considering the weather can help in making the water usage more resourceful. Paper 1 to 10 has given a better understanding of the techniques and the parameters to be considered in different decision-making processes and incorporating machine learning into it. IoT with cloud storage and Machine learning can help in creating a more accurate and automated system for irrigation which in turn can help inefficient utilization of the water available.

6 Conclusion

The survey on the efficient technique for irrigation and water usage can help in creating a system which would consider data obtained from the sensor that belong to various domains like soil moisture, humidity, wind speed, rain and temperature with metrological data from API and then decide the usage of water in the field. The survey helps to understand the parameters and the factors that need to be considered in developing an efficient and cost-effective system, which would facilitate in creating an efficient water usage plan to provide the correct quantity of the water into the field. Thereby it reduces the issue of excessive watering and its conservation. The results obtained from initial analysis and researchers have indicated the need for an automated mechanism for irrigation purposes and also to minimize the crop losses due to water scarcity.

Acknowledgement. We would like to express our immense gratitude to our beloved Chancellor Sri. Mata Amritanandamayi Devi (AMMA) for providing the motivation and inspiration for doing this research work. The authors would like to thank everyone who was instrumental in doing this research work.

References

1. Divya, P., Sonkiya, S., Das, P., Manjusha, V.V., Ramesh, M.V.: Cawis: context aware wireless irrigation system. In: 2014 International Conference on Computer, Communications, and Control Technology (I4CT), pp. 310–315. IEEE, September 2014
2. Rajalakshmi, P., Devi Mahalakshmi, S.: IOT based crop-field monitoring and irrigation automation. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp. 1–6. IEEE (2016)
3. Kumar, V.V., Ramasamy, R., Janarthanan, S., Babu, M.V.: Implementation of IOT in smart irrigation system using arduino processor. Int. J. Civ. Eng. Technol. **8**(10), 1304–1314 (2017)
4. Malhotra, A., Saini, S., Kale, V.V.: Automated irrigation system with weather forecast integration. Int. J. Eng. Technol. Manag. Appl. Sci. **5**(6), 179–184 (2017)
5. Shekhar, Y., Dagur, E., Mishra, S., Sankaranarayanan, S.: Intelligent IoT based automated irrigation system. Int. J. Appl. Eng. Res. **12**(18), 7306–7320 (2017)

6. Khan, M.A., Islam, Z., Hafeez, M.: Irrigation water demand forecasting: a data pre-processing and data mining approach based on spatio-temporal data. In: Proceedings of the Ninth Australasian Data Mining Conference, vol. 121, pp. 183–194. Australian Computer Society, Inc. (2011)
7. Gutiérrez, J., Villa-Medina, J.F., Nieto-Garibay, A., Porta-Gándara, M.Á.: Automated irrigation system using a wireless sensor network and GPRS module. *IEEE Trans. Instrum. Meas.* **63**(1), 166–176 (2013)
8. Gurmaste, S.S., Kadam, A.J.: Future weather prediction using genetic algorithm and FFT for smart farming. In: 2016 International Conference on Computing Communication Control and automation (ICCUBEA), pp. 1–6. IEEE (2016)
9. Rekha, P., Rangan, V.P., Ramesh, M.V., Nibi, K.V.: High yield groundnut agronomy: an IoT based precision farming framework. In: IEEE Global Humanitarian Technology Conference(GHTC), pp. 1–5. IEEE 2017 (2017)
10. Krupakar, H., Jayakumar, A.: A review of intelligent practices for irrigation prediction. arXiv preprint [arXiv:1612.02893](https://arxiv.org/abs/1612.02893) (2016)
11. Prabha, R., Sinitambirivoutin, E., Passelaigue, F., Ramesh, M.V.: Design and development of an IoT based smart irrigation and fertilization system for chilli farming. In: 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1–7. IEEE (2018)
12. Krishnan, R., Ramesh, M.: A low cost remote cardiac monitoring framework for rural regions. In: Proceedings of the 5th EAI International Conference on Wireless Mobile Communication and Healthcare, pp. 231–236. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2015)
13. Pathinarupothi, R.K., Alangot, B., Ramesh, M.V., Achuthan, K., Rangan, P.V.: H-plane: intelligent data management for mobile healthcare applications. In: International Conference on Mobile Web and Information Systems, pp. 283–294. Springer, Cham (2016)
14. Rajkumar, M.N., Abinaya, S., Kumar, V.V.: Intelligent irrigation system—an IOT based approach. In: 2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT), pp. 1–5. IEEE (2017)
15. Saraf, S.B., Gawali, D.H.: IoT based smart irrigation monitoring and controlling system. In: 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), pp. 815–819. IEEE (2017)



An Energy Efficient Routing Protocol for Internet of Things Based Precision Agriculture

T. Aishwarya Lakshmi^(✉), Balaji Hariharan, and P. Rekha

Amrita Center for Wireless Networks and Applications (AmritaWNA),
Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham,
Coimbatore, India

aishulakshmi18@gmail.com,
{balajih, rekhap}@am.amrita.edu

Abstract. Wireless Sensor Networks (WSN) are widely used in Precision Agriculture (PA) to increase the productivity and for monitoring the crop. Agricultural field is spanned over many acres and in order to design an efficient monitoring network, one of the key requirements is to maintain the sensor coverage and network connectivity. WSNs are often operated in resource constrained environments and is required to design power aware algorithm for routing, data acquisition, communication in order to enhance the network lifetime. This research work focus to design an Energy Efficient Routing Protocol (EERP) designated to PA applications. In this protocol, energy efficiency is achieved by distributed data collection and reduced number of transmissions in various phases of route setup. Maximum agricultural land coverage, monitoring the sensor node energy, and routing protocol scalability are the few elements that influence the WSN implementation in precision agriculture. The Sensor Nodes (SN) have limited storage so the nodes should store only the important data. This research work has also proposed designing and developing an EERP that offers effective coverage and a better network lifetime. The proposed protocol outperforms the existing AODV and DSR protocol in terms of the packet drop rate, energy consumption, end to end delay, network lifetime and throughput.

Keywords: Energy efficiency · Routing protocol · Sensor networks · Precision agriculture · IoT

1 Introduction

In India, 70% of people are directly or indirectly dependent on farming for their livelihood. It is therefore necessary to create a system that can automatically regulate and monitor the agricultural land. Precision Agriculture (PA) is the technique of monitoring the agricultural land in real time by collecting information like air temperature, soil moisture, pH, air humidity, etc. and transfers these monitored parameters to the remote server in order to take appropriate action. PA optimizes efficiency in construction, improves quality, minimizes effect on the environment and decreases resource utilization.

A network consisting of small motes deployed over a certain area is defined as WSN. These nodes can sense, process and transmit data using wireless medium. WSN incorporated with IoT is applied widely various domains such as agriculture [2, 3], medical care [4, 5], disaster management, industrial control, national defence, etc. WSN in PA is used to enhance the productivity and yield of the crop by continuously monitoring the field for collecting the environmental data. The sensed data of these sensors are linked to the server for further analysis and a predictive model can be developed. The user can monitor the field remotely with an Application support.

Routing Protocol [17] help the nodes communicate with each other and the sink. The sensor nodes have limited energy and consumption of energy should be minimized while designing a routing protocol. Unwanted transmission of data needs to be avoided as transmission consumes higher energy as compared to sensing, processing and reception [1]. The key problems faced during designing a WSN protocols are energy consumption and network's lifespan. Few routing protocols provide efficient coverage, while few provide better network life and few minimize energy usage. A routing protocol should also minimize packets' transmission delay, throughput, and drop rate. These parameters should be included in the routing protocols designed for PA.

The paper is structured as follows: the related study is presented in Sect. 2. Section 3 describes the working principle of the proposed energy-efficient routing protocol based on IoT. Section 4, we are presenting the proposed simulation of the protocol. Finally, Sect. 5 concludes the paper.

2 Related Work

WSN routing protocols may vary depending on application (based on protocol operation) and network architecture (based on network structure). Many researchers have carried out their research on routing protocols. In our related works we discuss the routing protocol for PA.

The routing protocols are broadly classified as data-centred, hierarchical and location based protocols [6]. In data-centred protocol the sink node sends a request for obtaining the data, this mechanism prevents continuous data transmissions and also saves the energy consumed. Hierarchical protocols use a cluster-based system in which nodes are split into tiny clusters and the energy of a node is conserved by data aggregation. In location based protocols deals with identifying the nodes location.

The wireless sensor nodes face many challenges as they are deployed remotely in the field. So when designing a sensor node these challenges needs to be considered as this can cause failure of the node [7]. Some of the challenges faced nodes are limited power, limited memory and storage, deployment can be deterministic or random and the network should be scalable.

Wireless technologies are becoming interested in PA in recent years. An automated irrigation with two kinds of data sending module based on TDMA was proposed [8]. Nodes in sleep state is used in star based irrigation system for energy savings [9].

Implementing an energy efficiency routing protocol is the major problem in WSN-based PA. The literature [10] includes many single level or multilevel routing protocols that are energy-efficient, and most of these protocols are not suitable for PA. These

single level or multilevel protocols does not ensure efficient coverage of the agricultural field and most of the protocols are not scalable and energy-efficient. The SN's are deployed randomly for large areas and some of these nodes may be far from the BS and these nodes will not be able to interact and create a coverage gap [11]. Clustering [12] plays an important part in expanding the network's life in WSN. Clustering also increases scalability and it is possible to balance the network's energy consumption well. LEACH PEGASIS, TEEN, etc. are the hierarchical routing protocols based on energy-efficient clusters. Data transmission using clustering methods reduces the energy consumption by data aggregation and periodically electing a node to act as Cluster Head (CH).

Protocols such as AODV and DSR are reactive routing protocols [13]. Whenever that route is needed, these protocols create a path between the source and destination. These protocols do not inspect the node's energy before setting the path, which causes the nodes to die quicker hence reducing the network lifetime. Kumar et al. proposes an energy-efficient AODV to evaluate the node energy level before the path is set [14]. This lowers power consumption and thus improves the lifetime of the network.

Most of the existing protocols are intended to operate in a homogeneous framework. Compared to homogeneous nodes, heterogeneous nodes perform better [15]. EEHC, RBHR [14] are models of protocols that promote a heterogeneous atmosphere. Here the deployment of the SN's is random across the region.

By assessing the literature on enhancing the WSN's lifetime, we can conclude that important parameters such as node remaining energy, hop rate, and managing data transmission across different routes can substantially improve the network's life. We design an energy-efficient routing protocol in this paper based on a region that selects an optimal path considering the node's remaining energy, the distance to the target node, and the connectivity rank.

3 Proposed Energy Efficient Routing Protocol

Energy efficiency is the most significant problem when developing a WSN protocol where some applications require continuous data transmission while other demand transmission when required. Different parameters such as soil moisture, soil temperature, air moisture, and soil pH are monitored in precision agriculture. Here proposes an EERP for IoT-based PA which is a region-based protocol designed to select an optimal path, taking into consideration the energy of each SN, the distance to the target node and the connectivity rank.

The proposed EERP protocol uses heterogeneous node which varies in their initial energy level. The benefits of using heterogeneous nodes over homogeneous nodes are that they help extend the network's lifetime, enhance the effectiveness of data transmission and decrease data transmission latency. The proposed protocol utilizes two types of heterogeneous nodes that differ in their initial level of energy. Compared to normal nodes, nodes α times power are called supernodes and ordinary nodes. We considered in this protocol an agricultural land ($A \times A$) unit² where the BS is situated at the middle of the field. The advantages for using this region based strategy is discussed in [19]. The region is divided into five zones: Region-R0, Region-R1, Region-R2,

Region–R3, and Region–R4 as shown in Fig. 1. The network utilizes two sorts of heterogeneous sensor nodes to detect and transmit environmental information. The clustering method based on the region is used to eliminate the coverage gap and provide efficient coverage for agricultural land.

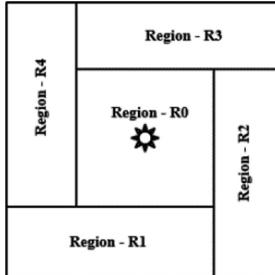


Fig. 1. Region-based node deployment

Based on measurements, the field is divided into sub-regions as we consider a particular agricultural region. The BS is assumed to be in the middle of the field and is equipped with an infinite power supply. The node deployment is deterministic and it is presumed that each node knows its position. If the nodes are deployed randomly, location-based protocols [16] can be used to determine the node's position. The super nodes are positioned at R0 and the normal nodes are aligned at R1, R2, R3, and R4. In order to support the node in the outer area (R1, R2, R3, R4), super nodes are placed in R0 as nodes in the internal region (R0) are used to transfer the information to the base station.

Figure 2 shows the operating flowchart for the proposed protocol. The alive SN collects the environmental information after the SN's are deployed in their corresponding areas. The base station broadcasts a hello signal to its one hop neighbors and the nodes responds with an ack. The BS decides the CH based on the available energy and the distance from the BS when the CH is chosen, CH broadcasts REQID to its respective areas and the nodes receiving this message, respond to the CH and also retransmits the packet to other nodes receiving the REQID signal. These nodes act as a relay for the CH(R0) transmission of the message. Based on distance to CH(R1), its remaining energy and the connectivity rank, CH is chosen for the corresponding areas. The connectivity rank is the number of nodes that are connected to the 'a' node to reach the sink and will be disconnected from the network if that 'a' node dies the nodes connected to it. The cycle continues until the last node's death.

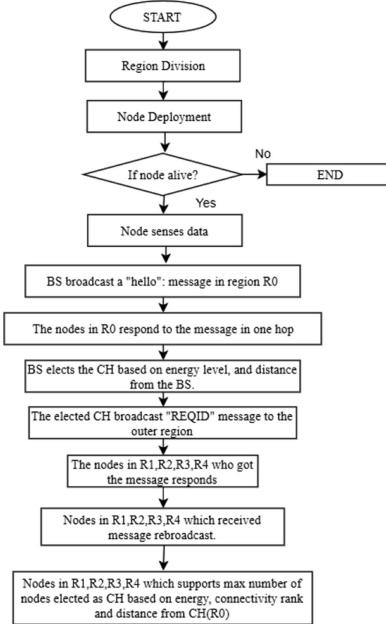


Fig. 2. Operational flowchart of the proposed protocol

4 Performance Evaluation

The proposed EERP protocol was simulated in NS3. We considered 80 nodes and at the center of the field is the base station. In Fig. 1, the whole region is separated into five sub-regions. There are heterogeneous nodes that vary in their initial amount of energy. The super nodes are implemented in region R0 and the normal nodes in region R1, R2, R3, R4 are implemented.

For performance evaluation, the proposed protocol is evaluated with the existing AODV integrated with LEACH and DSR integrated with LEACH based on throughput, end to end delay, network lifetime, packet drop rate and energy consumption as shown in Figs. 3, 4, 5, 6 and 7. In AODV and DSR, LEACH protocol is incorporated for selecting the CH and the route is established using AODV and DSR respectively.

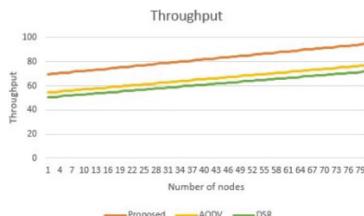


Fig. 3. Comparison with respect to Throughput

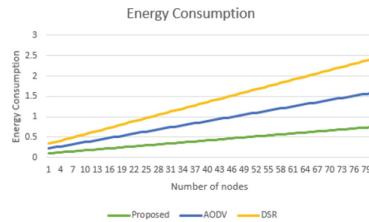


Fig. 4. Comparison with respect to Energy Consumptions



Fig. 5. Comparison with respect to End to end delay

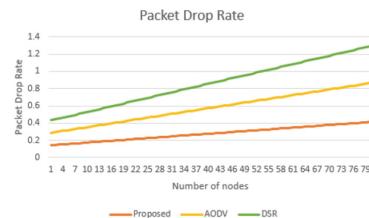


Fig. 6. Comparison with respect to Packet Drop Rate

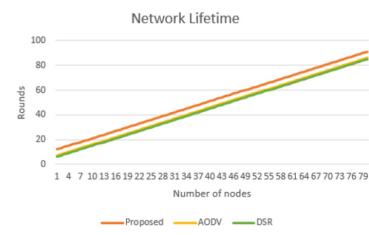


Fig. 7. Comparison with respect to Network Lifetime

Figures 3 and 7 shows the performance and lifetime of the network obtained by each protocol and that our proposed EERP protocol is more efficient than other protocols. The proposed protocol's energy consumption (Fig. 4), end-to-end delay (Fig. 5), and packet drop rate (Fig. 6), is less compared to other protocols. Based on the simulated results, our proposed protocol is more efficient compare to AODV and DSR protocol.

5 Conclusion

We addressed many current routing protocols for precision agriculture based on IoT in this article. To monitor the agricultural land, it is important to keep excellent network coverage. In WSN, minimizing power usage and improving the network's lifetime is essential. Here we have developed an IoT-based PA routing protocol that minimizes energy consumption and minimizes transmission rates by distributing data and thus improving the network's lifetime. The proposed EERP protocol is compared with the existing protocols AODV and DSR and our proposed protocol outperform the existing protocol in terms of energy consumption, network lifetime, end to end delay, packet drop rate and throughput.

Acknowledgement. We would like to express our immense gratitude to our beloved Chancellor Sri. Mata Amritanandamayi Devi (AMMA) for providing the motivation and inspiration for doing this research work. The authors would like to thank everyone who was instrumental in doing this research work.

References

1. Lerdsuwan, P., Phunchongharn, P.: An energy-efficient transmission framework for IoT monitoring systems in precision agriculture. In: International Conference on Information Science and Applications, pp. 714–721. Springer, Singapore (2017)
2. Rekha, P., Rangan, V.P., Ramesh, M.V., Nibi, K.V.: High yield groundnut agronomy: an IoT based precision farming framework. In: 2017 IEEE Global Humanitarian Technology Conference (GHTC), pp. 1–5. IEEE (2017)
3. Prabha, R., Sinitambirivoutin, E., Passelaigue, F., Ramesh, M.V.: Design and development of an IoT based smart irrigation and fertilization system for chilli farming. In: 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1–7. IEEE (2018)
4. Krishnan, R., Ramesh, M.: A low cost remote cardiac monitoring framework for rural regions. In: Proceedings of the 5th EAI International Conference on Wireless Mobile Communication and Healthcare, pp. 231–236. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2015)
5. Pathinarupothi, R.K., Alangot, B., Ramesh, M.V., Achuthan, K., Rangan, P.V.: H-plane: intelligent data management for mobile healthcare applications. In: International Conference on Mobile Web and Information Systems, pp. 283–294. Springer, Cham (2016)
6. Vhatkar, S., Atique, M.: Design issues, characteristics and challenges in routing protocols for wireless sensor networks. *Int. J. Comput. Appl.* **975**, 8887 (2013)
7. Biradar, R.V., Patil, V.C., Sawant, S.R., Mudholkar, R.R.: Classification and comparison of routing protocols in wireless sensor networks. *Spec. Issue Ubiquitous Comput. Secur. Syst.* **4**(2), 704–711 (2009)
8. Sudha, M.N., Valarmathi, M.L., Babu, A.S.: Energy efficient data transmission in automatic irrigation system using wireless sensor networks. *Comput. Electron. Agric.* **78**(2), 215–221 (2011)
9. Zhou, Y., Yang, X., Wang, L., Ying, Y.: A wireless design of low-cost irrigation system using ZigBee technology. In: 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, vol. 1, pp. 572–575. IEEE (2009)

10. Pantazis, N.A., Nikolidakis, S.A., Vergados, D.D.: Energy-efficient routing protocols in wireless sensor networks: a survey. *IEEE Commun. Surv. Tutor.* **15**(2), 551–591 (2012)
11. Zhu, C., Zheng, C., Shu, L., Han, G.: A survey on coverage and connectivity issues in wireless sensor networks. *J. Netw. Comput. Appl.* **35**(2), 619–632 (2012)
12. Doddapaneni, K., Omondi, F.A., Ever, E., Shah, P., Gemikonakli, O., Gagliardi, R.: Deployment challenges and developments in wireless sensor networks clustering. In: 2014 28th International Conference on Advanced Information Networking and Applications Workshops, pp. 227–232. IEEE (2014)
13. Kanakaris, V., Ndzi, D., Azzi, D.: Ad-hoc networks energy consumption: a review of the ad-hoc routing protocols. *J. Eng. Sci. Technol. Rev. (JESTR)* **3**(1), 162–167 (2010)
14. Kumar, D., Aseri, T.C., Patel, R.B.: EHHC: energy efficient heterogeneous clustered scheme for wireless sensor networks. *Comput. Commun.* **32**(4), 662–667 (2009)
15. Mhatre, V., Rosenberg, C.: Homogeneous vs heterogeneous clustered sensor networks: a comparative study. In: 2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577), vol. 6, pp. 3646–3651. IEEE (2004)
16. Kumar, A., Shwe, H.Y., Wong, K.J., Chong, P.H.: Location-based routing protocols for wireless sensor networks: a survey. *Wirel. Sens. Netw.* **9**(1), 25–72 (2017)
17. Kumar, R.P., Smys, S.: A novel report on architecture, protocols and applications in Internet of Things (IoT). In: 2018 2nd International Conference on Inventive Systems and Control (ICISC), pp. 1156–1161. IEEE (2018)
18. Maurya, S., Jain, V.K.: Fuzzy based energy efficient sensor network protocol for precision agriculture. *Comput. Electron. Agric.* **130**, 20–37 (2016)
19. Maurya, S., Daniel, A.K.: Hybrid routing approach for heterogeneous wireless sensor networks using fuzzy logic technique. In: 2014 Fourth International Conference on Advanced Computing & Communication Technologies, pp. 202–207. IEEE (2014)



Reducing Network Downtime by Intelligent Fault Analysis

B. Bipin^(✉)

Nokia Networks, Bangalore, India
bibinpreethy@gmail.com

Abstract. Fault management system remains as a critical component of any Network Management System present in the telecom industry. The final goal for any telecom service provider is to develop a high availability of service to its customers. For any telecom operator there'll this module Alarm system or even known as Fault Management system to handle the faults in the system. The faults can be ranging anywhere from a hardware fault, a security breach, a software error or anything which can be a possible threat to the high availability of the service. With the number of customers increasing daily, the network in telecom graphs form like an evolving graph. Thus, the complexity of the telecom network also increases with the increase in nodes.

Considering the software faults apart, the amount of hardware faults is increasing in an alarming rate. This is because most of the operators build the hardware infrastructure in a hybrid fashion i.e., with different hardware from different providers. Many of these hardware faults can lead to denial of service to the customers and are of critical severity. As for the service provider, one hardware fault can impact connected nodes in the network and might also bring down a huge part of it. This paper deals with a solution from a service provider's point of view, that when multiple faults are reported by the fault management system, it should prioritize the faults in the order that they need to be resolved so that the loss incurred is minimized.

Keywords: Networks · Telecom · Topology · Fault management · Dependency graphs · Network graphs

1 Introduction

The alarm system or the fault management system is a critical part of a telecom service system which helps in indicating potential faults in the system as well as faults that require corrective actions. After an alarm is raised, the fault causing the alarm must be solved. The solution can be an automatic recovery or a manual corrective action. Alarms typically have instructions for corrective actions in the alarm description, such as replacing a hardware unit. The alarms may be raised due to various events like a software bug, a security breach, potential hardware fault, etc. The alarms usually have a severity level assigned by the operator, which indicates the priority of the alarm. It is typically categorized as Critical, Severe, High, Medium, Low and Warning in the non-increasing order of severities. When an alarm is raised, it is the responsibility of the

operator to check the alarm and decide whether any corrective action is needed or not. Depending on the corrective action taken the level of the alarm may be changed, or the alarm may even be cleared if the fault is fixed.

When comparing the alarms, they are mainly categorized into software issues and hardware issues. The faulty hardware issues can turn out to be more destructive most of the times. For example, say a rack is not working, or say CPU fan has stopped, or a potential fault in the motherboard or say corrupted hard disk or damaged RAM or a connecting wire has been damaged in one node which connects to another node which is situated in another location etc. are some examples of faulty hardware issues. These issues can turn out to cause more loss to the operator as it may indirectly impact the other connected node and which in turn may impact furthermore nodes if they form a connected component. Normally when the faults are reported from the fault management system it is resolved or investigated with direct human intervention. But with the network topology turning to an evolving graph with the number of nodes increasing as a function of time, fault analysis and fault resolution has become more demanding.

If multiple faults are found out in a topology network, for the end operator it might be difficult to decide as to how the faults should be assigned priority which determines the order in which they have to be resolved. The more time it takes to resolve an issue, more will be the loss to the operator. The fault in one network element can impact other connected network elements in some other location if they are connected strongly and due to this connection, it may even bring the service down in some other location.

The preliminary application of this paper is to form priority order for resolving the faults from the topology network of network elements that the operator is controls. The topology network is represented as a dependency graph of the different nodes connected in different locations. This intelligent way of prioritizing the faults will minimize the loss and cost incurred to the operator and will help in avoiding further damage connected nodes if they're in connected loop with faulty node.

The organization of the paper is as follows: In the second section it deals with the Literature review, in the third section it deals with the proposed algorithm, the fourth section deals with the sample results formed from the proposed algorithm and the fifth section concludes with the future scope of the paper for further enhancement.

2 Literature Review

In Telecom domain finding a potential fault in a system is necessary to identify and fix the fault in the system before it causes any downtime to the customer. Kulatunge, Basu, Lee, Prakash [1] presented an idea to predict the fault in a network and take the necessary actions to prevent it using a characteristic pattern of logs which represent the possible abnormalities in the system. These characteristic patterns will be stored in the database and for any possible pattern matching, possible corrective actions should be taken. Kaffine, Rosen, Schmidt [2] proposed different methods to isolate and pin-point for improving the fault isolation in a network. The fault isolator plugin which is connected to all the fault reporting modules centrally communicates, queries, analysis and the faults raised by different modules. The central isolator which in turn runs a series of tests in and predict the fault if it's root cause is from some node and then helps

in isolating the fault in the system. Penido, Nogueira, Machado [3] proposed a paper for fault isolation and methods for automatic fault corrections in heterogeneous networks where many old and legacy components are present in which network supervision is a tedious task for the network operator. Giuseppe Italiano, Luigi, Laura, Alessio Orlandi [4] proposed an algorithm to in 2012 to find the strong articulation points and strong bridges in directed graphs in linear time.

3 Proposed Algorithm

In network topology, the topology can be considered as a topology graph consisting of many interconnected nodes. The connection which forms in the topology graph will get more condensed and complicated as the network grows its size. In other words, with the increase in the customers for each telecom service provider, the topology graph grows with time. It's ever expanding on a day to day basis.

To get a proper order of the nodes in which they should be given the priority in this topology network, 3 major graph theory algorithms are combined in our proposed algorithm. To get a topological order of the nodes, Topological sort can be applied on the graph. But this algorithm can only be used in DAG or directed acyclic graphs. Since the nodes are highly interconnected, there's a very high probability that there will be cycles in the network. So direct Topological sort cannot be applied into this dependency graph. There should be some preprocessing that should be applied to transform the graph so that topological sort can be applied on it.

3.1 Identifying Critical Points

Once the dependency graph has been created, it's important to figure out the critical points in which are of utmost importance. The concept of strong articulation points is applied here. Articulation points in a graph are those points or nodes which are some of the most sensitive nodes in the graph. A strong articulation point is a node in a graph whose removal will increase the number of strongly connected components. Here it means that if network element node is an articulation point, and an alarm has been raised, utmost importance should be given it. A naïve approach to find all the strong articulation points would be like

- Compute the strongly connected components of the topology graph G.
- For each node n in graph G:
 - Delete n from G
 - Calculate the number of strongly connected components of G without n
 - If $\text{SCC}(G(V - \{n\})) > \text{SCC}(G(V))$
- n is a strong articulation point. Map the SCCs generated for node n with the number of obtained SCCs in the above step.

This above naïve approach will result in a time complexity of $O(N(N + M))$ where N is the number of vertices and M is the number of edges (Fig. 3).

In Fig. 1 it shows that topology graph of the network. This will be the initial structure of the dependency graph. From the above figure Node 5 is an articulation

point which means a defect in Node 5 will disrupt the dependency graph and that defect will induce further strongly connected components in the system.

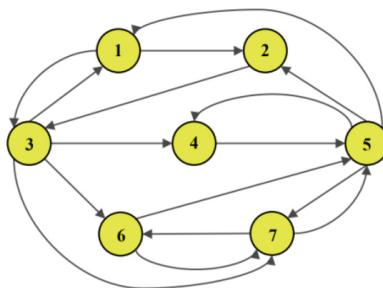


Fig. 1. Dependency graph before removing out articulation points.

From Fig. 2, it brings out that the fact that node 5 is an articulation point. This signifies the fact that removal of node 5, will cause communication breakage from node {4} to {1, 2, 3} and {6, 7} and {6, 7} to {4}. This communication flow was happening via {5} so removal of {5} will increase the strongly connected component and a total of 3 SCCs will be created i.e., {1, 2, 3}, {4}, {6, 7}.

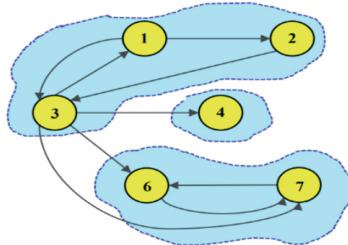
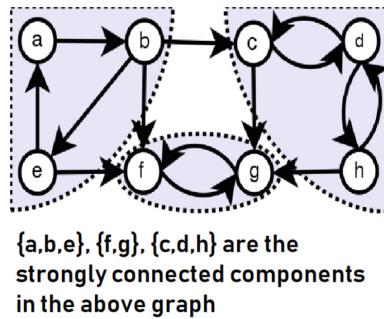


Fig. 2. Removal of node 5 increased SCC by 2

3.2 Removing Cycles and Reconstructing the Graph

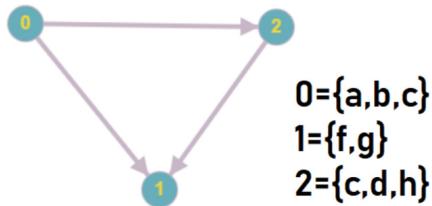
The smaller subgraphs of the topology network may be highly interconnected leading to strongly connected components. A strongly connected component in a graph is a subgraph of the main graph in which there exist a path from all the vertices to all other vertices within the subgraph. In the network topology this strongly connected components play an important role. They are vital parts of the topology network where the nodes are highly dependent on each other. So, a fault in any one node within the

**Fig. 3.** Example strongly connected components

strongly connected components might turn out to be disastrous. So, faults in such nodes may impact that strongly connected component entirely. In other words, if a node inside a strongly connected component is faulty, it can impact the connection to all other connected nodes within the SCC, so all nodes within an SCC needs to be given equal priority. In this part of the algorithm we find out all the strongly connected components in the dependency graph and convert into a single node. This step of converting and condensing is done to remove the cycles in the graph.

If all the strongly connected components are condensed into single node and if a new dependency graph is created using these nodes, it'll form a directed acyclic graph known as component graph or condensed graph. To find the strongly connected components in a graph Kosaraju's Algorithm can be made use of which will have a time complexity of $O(V + E)$ where V is the number of vertices and E is the number of edges.

After the conversion of the above dependency graph the condensed graph will be changed to the following graph. Node 0 represents $\{a, b, c\}$, Node 1 represents $\{f, g\}$ and Node 2 represents $\{c, d, h\}$ (Fig. 4).

**Fig. 4.** Condensed graph after Step A of the algorithm

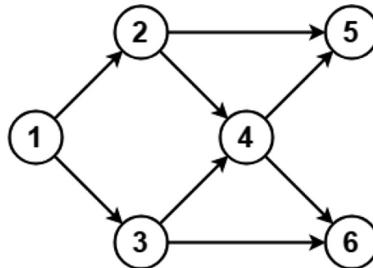


Fig. 5. Dependency graph without priority ordering

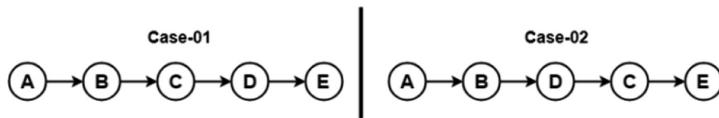


Fig. 6. 2 possible priority orderings of the above graph

3.3 Sorting of the Nodes with the Dependency

After the above-mentioned steps, the dependency graph will be re-generated, and the new dependency graph will not have any cycles in it after Step B. Once such kind of a directed acyclic graph has been obtained then topological sorting can be applied on to the new dependency graph which gives us an order in which for any edge X–Y, X should always be processed before Y. Here X and Y denotes nodes in a graph. The time complexity for topological sort to be run on the new dependency graph will be $O(N + M)$, where N is the number of vertices in the graph and M is the number of edges in the graph (Figs. 5 and 6).

3.4 Pseudocode for the Algorithm

Step 1: Collect the dependency graph G.

Step 2: Identify the articulation points present in the dependency graph.

Step 2.a: For each articulation point in the graph, calculate the number of strongly connected components that have been increased. Map this value for each node

Step 3: Convert the dependency graph to a condensed graph by removing the cycles in the initial G to G'

Step 4: Label these obtained points from step 2 as highly sensitive nodes.

Step 5: Obtain the topological ordering of the graph obtained from step 3 from G'

Step 6: When multiple alarm queries are raised reporting hardware faults at multiple nodes there are 2 main possibilities,

Step 6.a: Higher priority should be given to the node which is having higher value mapped obtained in step 1. Sort the nodes in the query with respect to the mapped value. This step suggests that higher the mapped value, higher will be the breakage of the dependency graph into further strongly connected components.

Step 6 b: If the priority values are same, check with the nodes in the order in which the topological sort is suggesting. Higher priority should be given to the nodes which comes first in the topological order sorted order. This suggests that if a node is placed in a lower position in the topological sorted order, higher will be the dependency of that node.

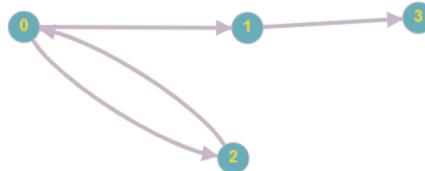
3.5 Working of the Algorithm

Consider the above graph as a dependency graph from the network topology. Find the strong articulation points in the graph and map the value for each node from Step 2 of the algorithm.

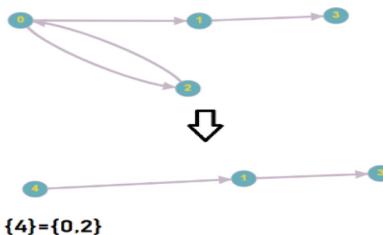
Table 1 denotes the number of strongly connected components that will be generated if node x has been deleted from the graph which is represented in Fig. 7. Once the strong articulation points are found and the number of SCCs formed by the removal of each articulation points are calculated, the graph is condensed with each SCC represented as a single node.

Table 1. Nodes and corresponding SCCs

Node (x)	Number of strongly connected components if deleted
0	3
1	2
2	3
3	2

**Fig. 7.** Dependency graph

From Fig. 8, the subgraph $\{0, 2\}$ is now condensed to a single node. The new condensed node is represented by node 4. So with the new condensed graph, there will be total of 3 nodes only. Topological sort for the above condensed graph is calculated. The possible topological sort ordering for the graph in Fig. 8 is $\{4, 1, 3\}$ where node 4 is a condensed node of $\{0, 2\}$.

**Fig. 8.** Initial dependency graph after condensation

Suppose a query comes as $\{0, 1, 3\}$ where each node in the query signifies that a fault has been detected in that node. Highest priority should be given to the node 0. As suggested from Table 1, node 0 has the possibility to increase the SCCs by 3. So, operator should take necessary steps to fix the fault in node 0 as soon as possible without disconnecting the topology network. Node 1 and node 3 has the same value from the table. It means deleting 1 or 3 disconnects the graph into 2 components. So here a decision cannot be taken with the concept of articulation point alone. For this scenario, we take use of topological sort. Node 1 occurs before node 3 in the topological sort. This order suggests that, node 3 has a dependency on node 1. So, delaying the fault in node 1 can further impact node 3 since there's a direct dependency.

4 Experimental Results

The proposed model is tested with Intel(R) Core (TM) Core i5 8300H CPU@2.3 GHz, with 8 GB RAM with Windows 10 as the operating system (Table 2).

Table 2. The above table represents the time taken for various datasets of graph models

Experiment no			
	No of nodes	No of edges	Time taken (sec)
1	10	10	0.000
2	100	100	0.001
3	500	500	0.191
4	1000	1000	0.192
4	1000	10000	0.651

The obtained quantitative results clearly show that the algorithm runs in a reasonably small time even with large number of nodes. Since the algorithm is computed offline, every time a new network element is added to the topology the algorithm will have to re-run again.

5 Further Improvements

In this paper we dealt with the scenario where multiple faults occur at the same time and where all the reported hardware faults are of equal severity. This makes the job a lot easier. A harder version of the problem would be when queries come with each alarm having different priority where this can be possibly solved by tweaking with the 3rd part of the algorithm where we can tweak the topological sort part with a priority weight which can be added depending on the alarms that is raised, still human intervention might be required in many cases where faults of varying severity occurs. Another drawback can be that if there's a shortage of engineers to fix the faults, then the lower prioritized alarm might lead to starvation which in effect might lead to downfall of the network element in the long run. A priority inversion protocol can be applied in this scenario where after a regular interval of time, even if the alarm has not been fixed the severity of the alarm can be raised to the next higher state so that operator can take a decision on that.

As mentioned earlier, there may be scenarios where the operator may need to intervene, like at places where the severity of the alarms raised in bulk simultaneously may be different. The operator with his/her experience should take the call as to which fault must be investigated first and rectified as soon as possible. This process can further be studied, and a reinforcement model can be made. Though the underlying problem statement and the algorithm mostly will remain the same, the reinforcement model will be helpful in the long run where the topology network grows on to a higher level where the number of nodes is so high, that it gets tougher to make a human intervention every time.

6 Conclusion

This paper was intended to provide an efficient approach by which the operators can decide which fault needs to be taken into priority to be solved first when multiple alarms are raised at same time or during a short interval. This approach will help the operator from incurring too many losses in terms of revenue. The down time of the network topology can also be reduced. As mentioned in Sect. 5, research is being done, to reduce the further intervention even more, when faults of varying severity are raised.

References

1. Kulatunge, A., Basu, K., Lee, H.C., Prakash, M.: Network fault prediction and proactive maintenance system. Nortel Networks Limited, St. Laurent & Patterson, L.L.P US Patent 6,353,902 B1, 5 Mar 2002
2. Kaffine, D.M., Rosen, J.S., Schmidt, P.H.: Network fault isolation. Teradyne, Inc., Boston, MA, USA, US Patent 6,654,914 9 9 B1, 25 Nov 2003
3. Lutz, C., Nall, N.L., Spain, D., Sexton, O.R.: Proactive analysis of communication network problems. AT & T Intellectual Property I, L.P., Atlanta, GA, USA, US Patent 7,974,387 B2, 5 July 2011
4. Penido, G., Nogueira, J.M., Machado, C.: An automatic fault diagnosis and correction system for telecommunications management. Published in Integrated Network Management VI. Distributed Management for the Networked Millennium. Proceedings of the Sixth IFIP/IEEE International Symposium on Integrated Network Management. (Cat. No.99EX302) (1999)
5. Raman, L.G.: Fundamentals of Telecommunications Network Management Wiley/IEEE Press (1999). ISBN: 978-0-7803-3466-3
6. Aghasaryan, A., Jard, C., Thomas, J.: UML specification of a generic model for fault diagnosis of telecommunications networks. In: ICT (2004)
7. Liebowitz, J. (ed.): Expert System Applications to Telecommunications. Wiley, New York (1988)
8. Bouloutas, A., Calo, S., Finkel, A.: Alarm correlation and fault identification in communication networks. IEEE Trans. Commun. **42**, 523–533 (1994)
9. Ensel, C., Keller, A.: An approach for managing service dependencies with XML and the resource description framework. J. Netw. Syst. Manag. **10**(2), 147–170 (2002)
10. Enhanced Telecom Operations Map. TeleManagement Forum. <http://www.tmforum.org>
11. <https://www.geeksforgeeks.org>
12. Fitzgerald, J., Dennis, A.: Business Data Communications and Networking, 5th edn. Wiley, Hoboken (1996)
13. Wolfe, A.: IBM sets its sights on ‘autonomic computing’. IEEE Spectr. **39**, 18–19 (2002)
14. Jacobson, G., Weissman, M.D.: Alarm correlation. IEEE Netw. **7**(6), 52–59 (1993)
15. Sterritt, R., Curran, E.P., Song, H.: HACKER: human and computer knowledge discovered event rules for telecommunications fault management. In: Proceedings of IEEE International Conference on Systems, Man & Cybernetics, October 2002



A Novel Access Control for Cloud Services Using Trust Based Design

Manikonda Aparna^{1(✉)} and N. Nalini²

¹ VTU, Bangalore, India

aparna.subhadra@gmail.com

² Department of CSE, NMIT, Bangalore, India

nalinirajan@hotmail.com

Abstract. In recent years the progress of cloud computing has become a complex system with diverse set of services and its user requirements. Access control plays a crucial role for accessing these services and assets of an organization via cloud servers. In, this paper we presented a novel access control technique known as Trust-RBAC which is based on non-security-oriented trust that provides a new dimension to prevent from unauthorized access to the cloud resources. To prove the efficiency of our approach, extensive simulations are been carried out in a cloud environment to show its effectiveness in controlling the malicious requests to the resources.

Keywords: Access control · RBAC · Trust-RBAC · CloudSim

1 Introduction

Cloud computing is also known for its on-demand computing feature that provide any service at any time. Basically, cloud allows to share information with various entities that has different degree of sensitivity. However, the sharing of resources with different users at varied times arises to major issues such confidentiality and delegation. These issues get more complicated when there is potential heterogeneity in the technology by various service providers. As more and more application are transitioned into the cloud computing platforms, it is important to ensure healthy isolation of data by monitoring the access mechanisms in the cloud platform. Hence access control is one the prime concern to cloud service providers. Over years many access controls models have been devised by different researchers, but these conventional models cannot support characteristics features of cloud. First, the access control must adapt itself for the cloud resources joining and leaving. Second, access control should accede itself with available security policies for the cloud. Finally, identity-based security cannot be used.

Many scholars modified the conventional access control [1] to support and enhance the security in cloud via key generation, encryption, authentication mechanisms. The projected models have a number of short comes. First, encryption and decryption techniques are costly in terms of computation and implementation. Second, lack of integration in the authentication and authorization mechanisms. Therefore, developing a novel and efficient control model is the prime investigation of this study. This paper aims at addressing some of the issues discussed thereby reviewing and assessing in

terms of authenticating and authorizing the services provided by the cloud. Our proposed approach is novel access control based on trust design which is an adaptive technique to the resources based on the contextual data such as security and time. The remaining articles is organized as follows. Section 2 Related work on existing access control models in cloud. Section 3 discusses about trust in cloud computing. Section 4 fuses the thoughts considered in the previous sections and propose a technique on access control based on trust design. Finally, Sect. 5 presents the analysis of the proposed work and discussion related to the approach.

2 Related Work

In storage as a service of the cloud providing an access ability is a challenge for holding the data security. Data in cloud are of two types public data and private data. Public data, data owner uses access control methods provided by service providers, whereas for private/secret data the data owners uses the encryption and decryption techniques to secure the data accessibility. Access control abilities are offered to target users by Zhu et al. [2] by proposing a role-based access control (RBAC). But this technique is not suitable for broadcasting messages as this involves the uses of frequent encryption procedures for submitting one file to numerous receivers. Kuhn et al. [3] proposed an approach for securing information by role assignment with permissions. However, its drawback is in structuring the initial role setting and also limits the capability of dynamic attributes which leads to role expansion. Li et al. [4] proposed an access policy that addresses the problem of illegitimate sharing of keys between colluding users. Ruj et al. [5] suggested that the data privacy can be preserved with use of trust tokens for authenticated users, where they can later perform read, write and execute operations on a file in the cloud. Goyal et al. [6] suggested a fine-grained access level for data stored in cloud by developing a key policy-based encryption KP-ABE, that uses secret key for encryption and decryption, but it has problem while setting audit logs. Bethencourt et al. [7] developed a method that combines access rules into the encrypted data and is widely distributed among unknown users and named as ciphertext-policy attribute-based encryption (CP-ABE). According to Andal et al. [8] task-role -based access control for separation among tasks and roles. The technique uses a workflow authorization model to differentiate task based on active access control and passive access control. Tsai et al. [9] proposed a framework based on RBAC known as O-RBAC that provides a suitable policy with a precise role for every tenant. But it does not provide level of sensitivity to the information. Mon et al. [10] suggested an Attribute Role based access control (ARBAC) that combines RBAC and ABAC techniques to support user's privacy and security. But it does not provide any information about data protection. Wang et al. [2] suggested a trust based access control model to monitor the user behaviour. However, the scheme does not provide any information about granting of cloud resources. Tianyi et al. [11] scheme inherits the features of RBAC and dRBAC and named as cloud optimized RBAC model. The scheme uses condition expressions to manage roles with in the network (inner network).

3 Trust and Cloud Computing

In 1996 Blaze [12] proposed the theory of trust management, which designates and enlightens a unique method for security policies, the credentials and its operations that can be authorized and executed directly. Trust management includes admittance to security credentials, advancement in security policies for the pertinent safety plans. Later these policies are introduced in the web to restrict the user's malicious activities.

Trust comprises of a subjective measures and involvement and therefore it is wider conception than security. There are security-oriented trust (hard) and Non-security-oriented trust(soft) solutions [13]. Security oriented trust features about encryption, security and authenticity in transactions, however Non-security-oriented trust comprises of loyalty, user friendliness and human psychology [14]. For instance, soft trust can be Company reputation and is most valuable asset [15].

Users often find it difficult to trust on-line services than off-line, as there is absence of centralized authority and physical cues. The suspicion of on-line services can be a negative effect to the organizations and hence they can no longer be respected as trustworthy. When assessing trust relevance to cloud computing persistent and dynamic trust [16] comes into forefront to differentiate the social and technological means.

Cloud can be said as distributed resource management system, as the resources are dispersed to every resource owner. The relationship of trust is built between one cloud and another cloud. Which means, the evaluation of one cloud is done by other based on the user behaviors of that cloud, and hence called comprehensive reflection of user.

4 Trust – Role Based Access Control

RBAC is a traditional access control model and cannot be directly applied to the cloud environment for security purpose due to its subject-centric nature. The Trust-RBAC model presented in this segment addresses some of the limited benefits by incorporating trust into the existing model. Our approach is focused on providing secure access management to the SAAS in the cloud where requests are delivered as service to the end user. Trust-RBAC comprises of three different roles USER, OWNER, SERVICE PROVIDER, and a certain level of trust is associated with each role. Upon the completion of each transaction, Virtual Machines (VM) evaluate each other for the requests delivered. The Cloud Server (trust management system) automatically apprises the value of trust for each VM.

4.1 Important Definitions

The Trust-Role based access control consists of three roles and the definitions are listed below:

4.1.1 User Role: User is an individual of an organization/enterprise who gets access permission according to the role assigned to him/her. Each user is associated with some trust value.

4.1.2 Owner Role: Owner of the resource who has the right to give access permissions to the User for a particular resource. Data owner updates the cloud resources.

4.1.3 Service Provider Role: Service Provider is an VM which authenticates the user credentials associated with the resource. Key is shared between Owner and Service Provider for decryption and encryption purposes.

4.2 Access Control Management

As our technique is based on trust so the server assigns a trust value to the user of the resource, whenever the data is requested for the resource the server automatically updates the trust value so that it can be able to keep control of any malicious activities from happening. This technique includes authentication between the user and owner of the resource, whereas authorization is between user and the service provider. There are two constraints while assigning a role to the user (1) no two roles can be assigned to the user (2) role and trust value is been tagged to the user.

4.3 Computation of Trust Value

The trust value is in between (0, 1). Upon each successful attempt the trust value increases once it reaches the upper limit i.e. ‘1’ then the server initializes the $T_{RST}VAL$ of that particular user to ‘0’ (Fig. 1).

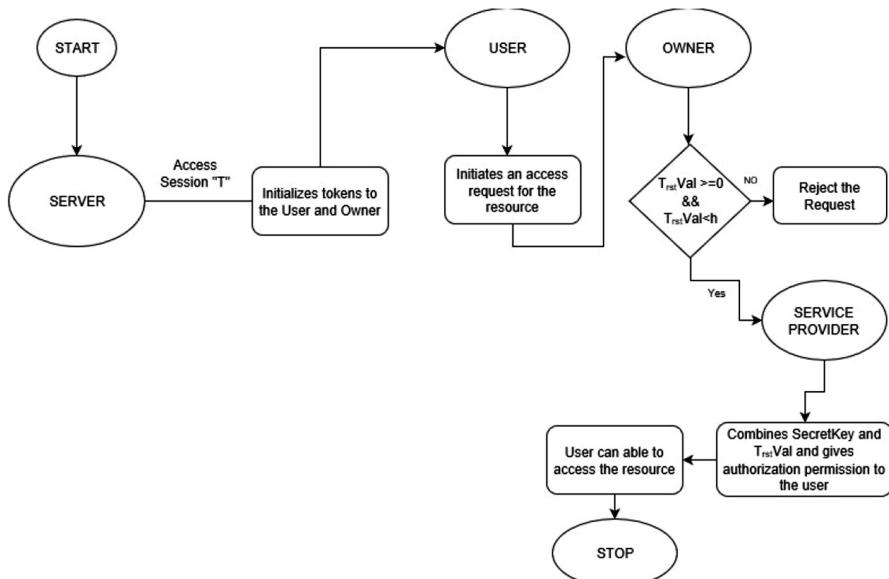


Fig. 1. Authentication and authorization procedure for Trust-RBAC

4.4 Algorithm for Access Control

Authentication Procedure

Step-1 Initially the server assigns authentication token to the user and owner of the resource. Authentication token consists of $\langle \text{USERID}, \text{SCRTKEY}, \text{ROLE}, \text{T}_{\text{RSTVAL}} \rangle$

Step-2 In an access session ‘T’ whenever a user sends data access request. The Request is processed by owner of the resource.

Step-3 The received request gets validated by the owner of the resource with help of the Trust value associated with the request. The Trust value helps to determine the intention of the user access request. The owner checks the trust value from the token of the user, to confirm whether the user has right to access the resource.

Authorization Procedure

Step-1 After validation the owner will respond to the user via permission packet. Packet contains essential information such as request-id, user-id, trust value and secret key which is shared among owner and the service provider.

$\text{P}_{\text{RM}}\text{-Pack} \langle \text{REQID}, \text{USERID}, \text{T}_{\text{RSTVAL}}, \text{SCRTKEY} \rangle$

Step-2 The received request is then redirected to the service provider. By combining T_{RSTVAL} and SCRTKEY the service provider gives authorization permission to the user.

Step-3 The user then will be able to access the resource with the successful response from the service provider.

Step-4 The server calculates and updates the trust value of the user. And this process can control the user malicious behaviour.

5 Analysis and Discussion

For the evaluation of proposed scheme Trust-RBAC model, a simulation environment of 30 nodes is developed using CloudSim [17]. We established two important cloud applications on the computing nodes i.e. file access and document retrieval. The resources of the cloud are accessed through the Trust-RBAC model.

Meanwhile, we assumed 300 accesses from 10 different hosts of cloud, we keep on sending file access or document retrieval request from the cloud. we randomly added a noise such as unauthorized user and mismatching.

From Figs. 2 and 3, it has been observed that for $\lambda = 0.4$ the percentage of file access and document retrieval dropped much faster as and when the percentage of suspected hosts rises. On the contrary, file access has shown better results than document retrieval.

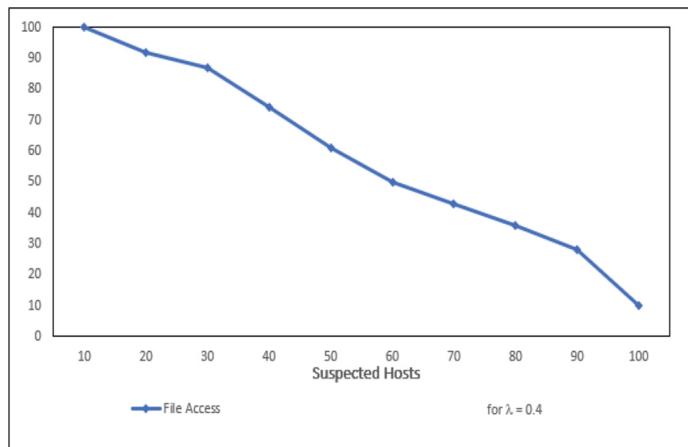


Fig. 2. For $\lambda = 0.4$: suspected hosts versus file access

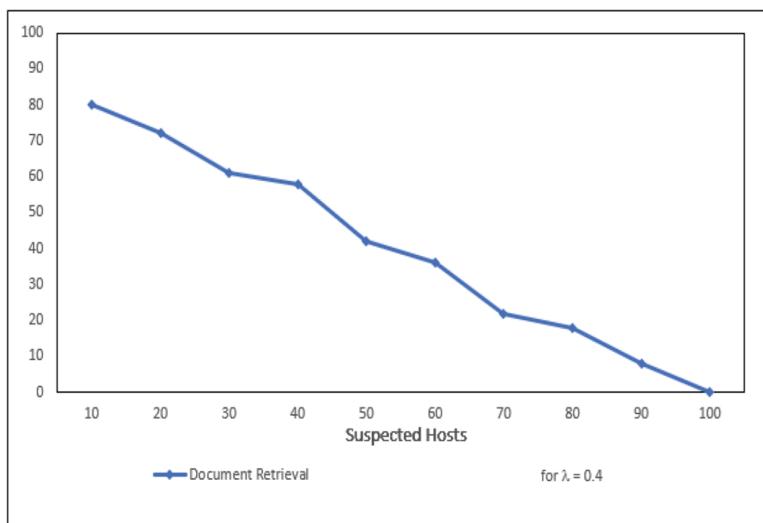


Fig. 3. For $\lambda = 0.4$: suspected hosts versus document retrieval

From Figs. 4 and 5, we observed that there was more rejection of legal access for higher value of λ . Hence from the experiments and figures the proposed scheme Trust-RBAC can effectively control the malicious requests from unauthorized accesses.

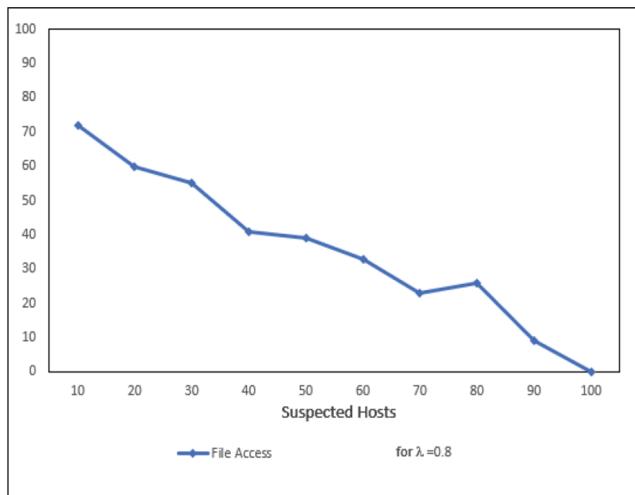


Fig. 4. For $\lambda = 0.8$: suspected hosts versus file access

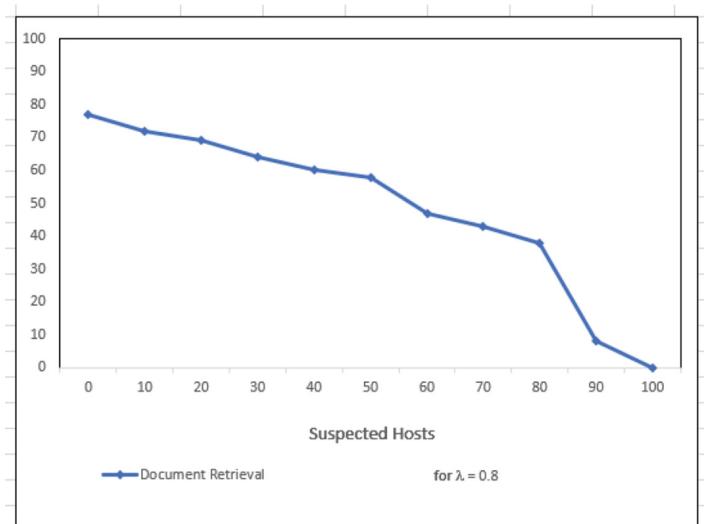


Fig. 5. For $\lambda = 0.8$: suspected hosts versus document retrieval

6 Conclusion

In this paper, we proposed a Trust-RBAC that integrates non-security-oriented trust in RBAC to increase the effectiveness in authentication and authorization process in cloud computing. In Trust -RBAC model, the trust value of a user is considered before giving the authorization rights to the requested data unit. The results of the experiments show

the model can effectively secures the data access there by controlling the unauthorized requests. Because of resource limitation we evaluated our method in simulation environment. In near future, we try to implement our method in a real cloud environment for verification.

References

1. Younis Y, et al.: An access control model for cloud computing. *J. Inf. Secur. Appl.* (2014). <http://dx.doi.org/10.1016/j.jisa.2014.04.003>
2. Tianyi, Z., Weidong, L., Jiaxing, S.: An efficient role based access control system for cloud computing. In: IEEE 11th International Conference on Computer and Information Technology (CIT), pp. 97–102 (2011)
3. Kuhn, D.R., Coyne, E.J., Weil, T.R.: Adding attributes to role-based access control. *Computer* **43**(6), 79–81 (2010)
4. Li, J., Zhao, G., Chen, X., Xie, D., Rong, C., Li, W., Tang, L., Tang, Y.: Fine-grained data access control systems with user accountability in cloud computing. In: Proceedings of 2nd IEEE International Conference on Cloud Computing Technology and Science. IEEE Computer Society (2010)
5. Ruj, S., Stojmenovic, M., Nayak, A.: Privacy preserving access control with authentication for securing data in clouds. In: 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 556–563 (2012)
6. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: ACM CCS 2006, Alexandria, Virginia, USA, 30 October–3 November 2006 (2006)
7. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP 2007, Washington, DC, USA, pp. 321–334 (2007)
8. Andal Jayaprakash, H., Hadi Gunes, M.: Ensuring access control in cloud provisioned healthcare systems. In: Consumer Communications and Networking Conference (CCNC), pp. 247–251. IEEE (2011)
9. Tsai, W.-T., Shao, Q.: Role-based access-control using reference ontology in clouds. In: 2011 10th International Symposium on Autonomous Decentralized Systems (ISADS), pp. 121–128 (2011)
10. Mon, E.E., Naing, T.T.: The privacy-aware access control system using attribute-and role-based access control in private cloud. In: 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, pp. 447–451. IEEE (2011)
11. Wang, C., Wang, Q., Ren, K., Lou, W.: Ensuring data storage security in cloud computing. In: 2009 17th International Workshop on Quality of Service, pp. 1–9. IEEE (2009)
12. Tianyi, Z., Weidong, L., Jiaxing, S.: An efficient role based access control system for cloud computing. In: 2011 IEEE 11th International Conference on Computer and Information Technology, pp. 97–102. IEEE (2011)
13. Blaze, M., Feigenbaum, J. and Keromytis, A.D.: KeyNote: trust management for public-key infrastructures. In: Christianaon, B., Crispo, B., Willian, S., et al. (eds.) Cambridge 1998 Security Protocols International Workshop. Springer, Berlin (1998)
14. Pearson, S., Mont, M.C., Crane, S.: Persistent and dynamic trust: analysis and the related impact of trusted platforms. In: Herrmann, P., Issarny, V., Shiu, S. (eds.) Trust Management, Proceedings, iTrust 2005, LNCS, vol. 3477, pp. 355–363 (2005)

15. Wang, Y., Lin, K.-J.: Reputation-oriented trustworthy computing in e-commerce environments. *IEEE Internet Comput.* **12**(4), 55–59 (2008)
16. Singh, S., Morley, C.: Young Australians' privacy, security and trust in internet banking. In: Proceedings of the 21st Annual Conference of the Australian Computer-Human interaction Special interest Group: Design: Open 24/7 (2009)
17. Goyal, T., Singh, A., Agrawal, A.: Cloudsim: simulator for cloud computing infrastructure and modeling. In: International Conference on Modelling Optimization and Computing, vol. 38, pp.3566–3572 (2012)



An Intelligent Recommendation Engine for Selecting the University for Graduate Courses in KSA: SARS Student Admission Recommender System

Zeba Khanam^(✉) and Salwa Alkhaldi

College of Computing and Informatics, Saudi Electronic University,
Riyadh, Saudi Arabia
{z.khanam,s130108247}@seu.edu.sa

Abstract. Completing the school degree and selecting an appropriate university/college for graduation could be a stressful and a confusing venture. Searching for an appropriate college online in a specialized field is a challenging task. This research focusses on building a recommender engine which can classify KSA universities according to the preferences of students and voting from others. The proposed system is a recommender system that depends on differentiating between the preferences/voting of the college and a student profile. The preference/voting of each college is represented as a corpus (dataset) of features (embedded in raw files), specifically the words appearing in the file/document. The student profile is depicted using the same terminology and is constructed by performing the analysis of the content that have been done by the user. In order to propose the model for the Recommendation engine research is conducted on the used algorithms and comparison has also been made of various algorithms in this paper, so as to choose ours, which is random forest with regression.

Keywords: Recommender engine · Machine learning · Random forest · WEKA · Weighted clustering · Nearest neighbor

1 Introduction

Recommender system is an automated filtering system that tries to predict the “rating” or “preference” that a customer or in our case previous academic users would give to an education institute. The proposed system is a recommender system that depends on differentiating between the preferences/voting of the college and a student profile. The preference/voting of each college is represented as a corpus (dataset) of features (embedded in raw files). The student profile representation is done using the same terminology and is developed by analyzing the content that have been done by the user.

The programmers use different kind of programing language EX: java and python. Python is more common in Building a Recommender System EX: Google Recommender System.

We are going to manipulate the process of creating a model that can classify KSA universities according to the preferences of students and voting from others, in order to do that, we have made researches in the following section of literature review, on the used algorithms and made comparison between them, so as to choose ours, which is random forest with regression.

The problems of existing system are the deficiency of information about the universities specialties and future aspects, as to find appropriate places, quality of college education, popularity, suitability for student's qualification, suitability of future jobs ... etc. Student's admissions have increased and huge number of students strive for better future colleges other than just a degree or certificate. But for now, they just fill the admission form with choices of specialties according to their popularity. The case ends in enrolling and admit to any college not suitable for them. The proposed recommender system, will make it available for students to enroll in the appropriate colleges based on their capabilities and suitability with popularity and offer them a prioritized list of best options for them, also, it will give information of the colleges e.g. location, voting from previous users, infrastructure etc. The application will have all the colleges and universities available in the corpus or dataset that will be gathered. The approach of our SARS (Student Admission Recommender System) is based on priority and rating of educational institutions that is built from downloaded and gathered corpus, then will apply data pre-processing (noise clean, normalization and conversion to suitable format for classification). It recommends colleges based on a comparison between the college preferences (features)/ratings and a user profile by using an unsupervised approach for classification using WEKA (Waikato Environment for Knowledge Analysis) [11].

It's important to choose the right algorithm for the an efficient model. Therefore like the test driven development [23] is about drafting tests for small code samples before actually coding it similarly a test driven algorithm development applies the same technique on a higher level. Before developing or choosing an algorithm a through plan to test its applicability is a good idea.

There will be experiments to be done by utilizing feature selection on many known algorithms like decision tree, random forest and clustering in order to obtain the optimal model for classification. The scope of SARS (Student Admission Recommender System) is that the application is standalone in JAVA, specifically designed for students who would like to enroll in a college, the student can register, login and add his preference data and his desired specialty or category of education.

The activities of the application are limited for students' admission recommender system, and not colleges as a user's to accept students as a recommendation from the system. Teachers or administrators may use the application for recommendation to their students.

The target customer is the student, teacher, and administrator of Saudi colleges who can download the application, and fill his profile, grades or GPA (Grade Point Average), and demand a recommendation for a certain branch of education.

The query will be on big Saudi universities Kfupm.edu.sa-Dhahran, Seu.edu.sa, Imam Abdurrahman bin Faisal university - Dammam etc. The major aim of the Student Admission Recommender System (SARS) is to

- Help the students to find a list of colleges suitable for his preference.
- Offering the best colleges based on voting for certain aspect.
- Help in career choice, course suggestions according to the student profile and choice with respect to college suitability and vote.
- Saves time and reduces student selection errors.
- The system is to be interactive, attractive, easy and secured to be used.
- The system can be proposed for selling, thus gain profit.

2 Related Research

This section highlights the research performed by various researchers in the same area. The comparison of various machine learning algorithm has been done and many ideas are discussed that relates to the project. The practical applications to help the research in aspects of precision, voting and preferences have been discussed. In the present scenario such systems are not available frequently to benefit the students from their aspect in selection of a good university in KSA. In this project research has been performed on various algorithms that are used in building a recommendation engine. This project addresses and chooses the algorithm, depending on the objectives that needs to be fulfilled.

2.1 A Hybrid Approach for Recommendation System with Added Feedback Component [1]

A recommender application built using hybrid approach using customer based and product based collaborative filtering, depicts a recommender environment containing a feedback analysis support. This model assists the users in decision support. For hybrid approach, a need of huge corpus of feedback is acquired to enhance results. Utilizing this approach of collaborative filtering and the feedback section, they can design a model which can benefit the users to make decisions in return of the feedback that is proclaimed by the other customers like cadets, universities, etc. [1].

2.2 An Answer Recommendation Algorithm for Medical Community Question Answering Systems [2]

In this recommendation engine, the research is done to recommend feedback for a medical question and answer system [2]. The question and answers frequency along with their similarity is assessed together to depict the final evaluation of the question-answer couple. The applied algorithm is evaluated on the feedback score and corpus shows a higher result in answer recommendation. They faced a lexical spot problem that appeared, it's so hard for these old information acquiring data models to get the semantic frequent history samples according to users' opinion or view. Utilizing this technique for recommendation can be applied based upon answer performance and question-answer coupling.

2.3 A Personalized Recommendation Strategy Based on Trusted Social Community

Another research [3] focused on, a new personalized recommendation methodology depending on collaborative filtering approach, a technique used for confident relationship result has been established. Customers can give some thoughts for their confident relationship after every process or buying. Tests appeared the results that recommendation built on confident relationship in internet community can enhance the recommendation precision and get better user satisfaction. This technique proposed a better method to fix change of preference. Tests resulted in the algorithm can better enhance the precision of recommendation, and upgrade scoring of customer satisfaction [3].

2.4 Music Recommendation System Based on User's Sentiments Extracted from Social Networks [4]

Music/melodic recommendation engines are also quite prevalent. The research [4] focused on showing a music recommendation system built on a sentiment intensity metric, called enhanced Sentiment Metric (ESM) which is followed by lexicon-based sentiment metric that has a correction factor developed on the customer's preference. The model does not contain a hard sophisticated programming tools; devoirs little resources from appliances. Machine learning acquire a huge dataset or corpus, because an un-learned sentence may introduce noise and cause errors in the algorithms calculus of the sentiment. Utilizing this recommender model can be applied depending on customers' emotions and their peripherals on social site.

2.5 FSOS: A Tool for Recommending Suitable Operating Systems to Computer Users

FSOS (Find Suitable Operating Systems), analyzes multiple environment systems used at local, business and industrial scopes and proclaims adequate environment systems to the customers according to their needs. This application is acquired for recommendation of multiple operating system depending on user's requests and comments given by history reviewed users [5].

2.6 Online Book Recommendation System by Using Collaborative Filtering and Association Mining [6]

Another recommendation engine described for recommending books [6] uses Collaborative filtering and Association Mining. It offers customer with informative data to support him to make a decision, as which products to buy. The requests of information from internet have shown the path to create some new methods for making a list of priorities and showing products that makes interest to customers. The feedback due to frequent similarity math shown a better quality of accuracy [6].

2.7 A Restaurant Recommender System Based on User Preference and Location in Mobile Environment

Another related work shows food court recommender system in smartphone operating system. Application adopts a customer profile and preference model by utilizing the feature selection of customer's experienced certain restaurants, not to mention the geographical coordination information of customer and restaurants to precisely and automatically offer the recommendation lists [7].

2.8 HyredHYbrid Job Recommendation System

HYbrid Job is a Recommendation System is a mixing of Job Opportunities Recommendation engine that makes use of the social interactions (collaborative filtering) and user model (content-based filtering) and to enhance the accuracy of its recommendations [8].

2.9 Development of Location-Aware Place Recommendation System on Android Smart Phones

Location-Aware Place Recommendation System on Android Smart Phones is also a significant project whose objective is to create a location-aware place recommender system. For predicting the location, user-based collaborative filtering scheme is used that is as near as possible to the customer depending on his/her location obtained from internet or GPS from a smartphone appliance. The results show that the system achieves both satisfying precision and recall of recommended places on the corpus [9].

2.10 Recommendation System for Alternative-Ingredients Based on Co-occurrence Relation on Recipe Database and the Ingredient Category

Recommendation System for Alternative-ingredients depending on already occurred link on Recipe dataset and the Ingredient dataset shows a recommendation system for some replaceable ingredients. The outcome of the multiple subjective experiments appeared that 88% suitable for alternative-ingredients recommendation. This paper suggests a recommendation system for alternative-ingredients using founded data frequent of ingredients and cooking ontology [10].

2.11 A Bayesian Approach to Predict Performance of a Student (Bapps) and a Quality Based Recommender System to Disseminate Information in a University Digital Library

Supporting of career suggestion services is one of the most important objective acclaimed by students' academic success. The most recommender tool of student utilities is to offer them a better course, suitable for their career and brings his qualification and aptitude. Students always prefer, particular courses of study hoping of

better job opportunities, their interests and the dreams of his career developments at the time of his graduation.

The main issue here, came up, if a student doesn't like the course or if his requested future is not perfectly matching the qualifications [12–15].

2.12 Machine Learning in Automated Text Categorization

Text categorization can performed either through text clustering and text classification. Text clustering explores a structure of groups among the dataset, whereas in the latter each text is assigned to the most suited group. The classification of text could be conflicting sometimes as the humans and machine might not concur on the classification of the data. Text classification can either be single-labelled or multi labelled. The former refers to the case where every document is assigned a single category, in the latter case a document can be assigned to several possible categories. This benefit of this method is that the user has an edge of taking the final decision as per their own understanding and opinion as several texts might be allocated to multiple categories. Different applications such as genre classification, webpage classification, authorship attribution, spam filtering can be decided with text classification. There are many machine learning algorithms that are utilized for building classifiers, the researchers [16] have proved that one the most successful are support vector machines (SVM) and boosting. Boosting algorithms works to reduce the bias and incorporates the decisions of a group of classifiers in order to achieve a better classification results [16, 17].

For recommendation engines we need to identify the products, similar to the one that is of our interest, the similarity between pairs needs to be computed. In this scenario MapReduce also serves as a powerful framework for a large and sparse dataset to implement the data mining algorithms [22–24]. Recommendation engines are quite common in movie recommendations, they compare the similarity between two movies. One way to achieve this is by computing the correlation between pairs of items. But if the dataset is very huge, say around 500,000 products that would amount to 250 billion computations. Therefore to handle very large, temporal and sparse dataset, we need the correlation calculation done periodically. For these reason one of the best way to handle it using Map reduce making use of divide and conquer pattern.

3 Comparison of a Few Related Algorithms

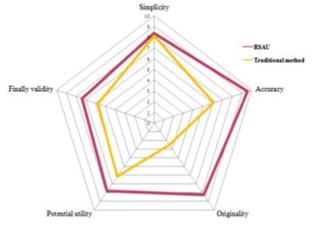
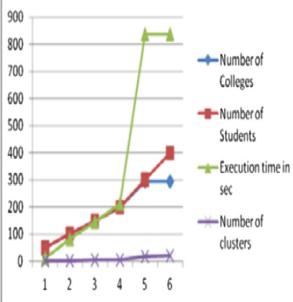
The following table shows a comparison between different recommender algorithms for different applications like university admission recommender, college recommender system using student preference/voting, college recommendation system for admission and our system SARS (Table 1).

Table 1. Comparison of SARS (our proposed system) with college recommendation engine

	University Admission Recommender [18]	College Recommender system using student' preferences/voting [19]
Classifier algorithm	<p>The recommender employs a Decision tree, to model the rules for the admission process of the university. IT also manages a knowledge base for storing up the decision-making rules.</p> $\text{Precision}(\text{for predicted Class}_j) = \frac{C_{jj}}{\sum_{i=1}^m C_{ij}}$ $\text{Recall}(\text{for real Class}_i) = \frac{C_{ii}}{\sum_{j=1}^m C_{ij}}$ $F1\text{-Measure} = \frac{2 \times \text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}}$ <p>C4.5 algorithm: Entropy (Decision) = $\sum - p(I) \cdot \log_2 p(I)$ $= - p(\text{Yes}) \cdot \log_2 p(\text{Yes}) - p(\text{No}) \cdot \log_2 p(\text{No})$</p> $\text{GainRatio}(A) = \text{Gain}(A) / \text{SplitInfo}(A)$ $\text{SplitInfo}(A) = -\sum D_j / D \times \log_2 D_j / D $	<p>This system uses the Weighted clustering process WCLUSTER. R-tree data structure is used, top-k queries are applied for clustering the college data. Based on students' preferences /voting.</p> <p>Using score function:</p> $f(\text{object}) = \sum_{i=1}^n \text{voting}(i) * \text{object}(i)$ <p>ALGORITHM WCLUSTER (Threshold, Root, D)</p> <p>INPUT Threshold:user-specified similarity limit Root: indexed tree D: the dataset</p> <p>OUTPUT Set of clusters</p> <ol style="list-style-type: none"> 1. Initialize cluster number i = 1 2. While D is not empty do 3. Object = first object in the D 4. Cluster set c_i = Theta-Similarity-Query (Root, Threshold, Object) 5. i = i + 1 6. update input dataset D = D - c_i 7. End-While
Objective	Improved recommendation output. The recommender system follows a novel approach to provide recommendations to apply and get admission in the universities by taking the student's secondary school scores into consideration and also other factors into account.	An automated system to do all the work for helping the students to select college. Weighted approach can provide better information by an efficient grouping of related items (colleges). Using this weighted groups of colleges with related profile attributes, can suggest a better list of colleges that meet the preferences given by the students.
Methodology	Hybrid model of neural network and decision tree classifier	Weighted clustering with r-tree and top-k queries

(continued)

Table 1. (continued)

<p>Result</p>	 <p>The experiments shown that the hybrid decision tree and neural network approach improved accuracy in classification task.</p>	 <p>The results prove that the proposed system is reliable, faster, intelligent and more apt for selecting the colleges for admissions.</p>
	<p>COLLEGE RECOMMENDATION SYSTEM FOR ADMISSION [20]</p>	<p>STUDENT ADMISSION RECOMMENDER SYSTEM (SARS) OUR PROPOSED SYSTEM</p>
<p>Classifier algorithm</p>	<p>Combine Naive Bayes and Adaboost algorithm (Adaptive Boosting).</p> $F(x) = \text{sign}(\sum_{m=1}^M \theta_m f_m(x)),$ $P(x_1, \dots, x_n) = \prod_{i=1}^n P(x_i \text{Parents}(Y_i)),$ <p>Where $P(x_1, \dots, x_n)$ is the probability of a particular combination of values of X, and the values for $P(x_i \text{Parents}(Y_i))$ correspond to the entries in the CPT (conditional probability table) for Y_i.</p> <p>Algorithm:</p>	<p>A new hybrid method using supervised random forest + Multivariate Adaptive Regression Splines (MARS). Random forests is an ensemble learning algorithm. Two or more trees can be combined to form a single, strong learner by taking the average or the majority vote. It has been found that the random forests serves as an accurate learning algorithm. The pseudocode is illustrated.</p> <p>Precondition: A training set $S := (x_1, y_1), \dots, (x_n, y_n)$, features F, and number of trees in forest B.</p> <pre> 1 function RANDOMFOREST(S, F) 2 $H \leftarrow \emptyset$ 3 for $i \in 1, \dots, B$ do 4 $S^{(i)} \leftarrow$ A bootstrap sample from S 5 $h_i \leftarrow$ RANDOMIZEDTREELEARN($S^{(i)}, F$) 6 $H \leftarrow H \cup \{h_i\}$ 7 end for 8 return H 9 end function 10 function RANDOMIZEDTREELEARN(S, F) 11 At each node: 12 $f \leftarrow$ very small subset of F 13 Split on best feature in f 14 return The learned tree 15 end function </pre> <p>Regression: is defined as a method used to model the linear relationship between a dependent variable (target) and one or more independent variables</p>

(continued)

Table 1. (*continued*)

		<pre> 1. Start 2. For i=1 to Na 3. Get_alumni_details(Nai); 4. i++; 5. End for. 6. For i=1 to Na*Nb*Nc. //for each alumni student 7. Send_login_details(Nabc); 8. i++; 9. End for. 10. Login 11. Flag=Check_if_Eligible(Nai.Nbi.Nci); 12. If(flag==true) 13. Rtb=Rtm+Rttc+Rtp/3 //Give_Rating(Rtb) 14. Give_Review(Rvb) 15. ORb=(ORb*ORu)+Rtb/ORu+1; //Overall Rating 16. ORvb=PRb-NRb/ORu; //Overall Review 17. ARb=ORb+ORu; //Overall Rating review 18. Let ORa=0; 19. For i=1 to Nb 20. ORa=ORa+ARbi; 21. i++; 22. End for 23. ARA=ORa/Nb; 24. Rank_colleges_based_on_rating(ARA) 25. Save_this_rating_for_college as a historical record. 26. End. (obs predictors). </pre> $\text{observed data} \rightarrow y = b_0 + b_1 x_1 + b_2 x_2 + \dots + b_p x_p + \varepsilon$ $\text{predicted data} \rightarrow y' = b_0 + b_1 x_1 + b_2 x_2 + \dots + b_p x_p$ $\text{error} \rightarrow \varepsilon = y - y'$
Objective	In this recommendation system, student gets a clear picture about the options that he has to choose a branch or college for admission.	Predicting a list of best colleges, for admissions of the new students, and classifying colleges according to specialties, location, prices and vote.
Methodology	In this system, rating is computed using the bottom up approach. The positive and negative comments are assessed using semantic algorithms. The system gets combination of Naive Bayes and Adaboost algorithm which will add result information to the database according to rating parameter to college.	SARS exhibits three main components, namely Data Analyzer, Classifier and Visualization that provides an efficient interface to be used by the users. The classifier will use the train portion of dataset to build a model with the hybrid system (Random forest + Regression).
Result	Colleges are ranked on the basis of alumni reviews and rating. User can choose college as per his requirements, such as he can choose college on the basis of his priority, near to user location, fees,	An experiment will be performed in order to produce a high precision model with F-measure as best as we can and accuracy over 90% for predicting the best college for the student user, through an interactive easy interface.

4 Result

Our system will use a different approach to make a better precision classification. The proposed methodology of SARS has three main components, namely Data Analyzer, Classifier and Visualization depicted in Fig. 1(b). The data processing flow is depicted in Fig. 1(a). The classifier will use the train portion of dataset to build a model with the hybrid system (Random forest + Regression), aiming for predicting a list of best colleges, for admissions of the new students, and classifying colleges according to specialties, location, prices and vote.

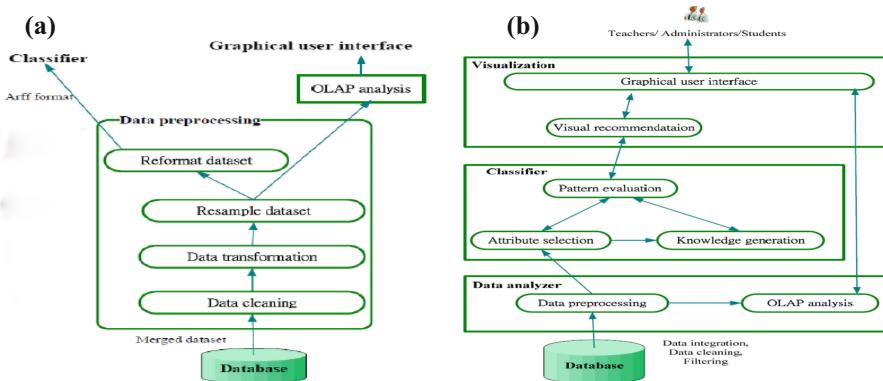


Fig. 1. (a) Data processing flow of Data Analyzer (b) Data Analyzer, classifier and visualization

5 Conclusion

Student Admission Recommender System (SARS), is specialized to analyze various datasets/corpora of previous high school students, their voting on multiple universities they used to learn in, and their colleges characteristics, for predicting a list of best colleges, for admissions of the new students, and classifying colleges according to specialties, location, prices and vote.

The data preprocessing is an essential part, corpus/dataset is merged, cleaned, transformed, resampled and reformatted to ARFF (Attribute-Relation File Format) to be in the form suitable for the classifier or WEKA to work on, on the other hand the OLAP (Online analytical processing) analysis may be used for the graphical representation part after classification and analysis.

The user will download the java application, give only his formatted information, which will be filled in a specific form, along with his ambitious requirement of education specialty. The system will recommend colleges based upon various profile/ratings and data entered by the user, the application will list out number of colleges suitable for the user, later the system will also provide information such as education roles, prices, location etc.

References

1. Kavinkumar, V., Reddy, R.R.: A hybrid approach for recommendation system with added feedback component. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI) (2015). 978-1-4799-8792-4.com/2015/\$31.00_c IEEE
2. Wang, J., Man, C.: An answer recommendation algorithm for medical community question answering systems (2016). 978-1-5090-2927-3/16/\$31.00©2016 IEEE

3. Wu, W., Lu, Z.: A personalized recommendation strategy based on trusted social community. In: The 10th International Conference on Computer Science & Education (ICCSE 2015), 22–24 July 2015. Fitzwilliam College, Cambridge University, UK (2015)
4. Rosa, R.L., Rodríguez, D.Z.: Music recommendation system based on user's sentiments extracted from social networks. *IEEE Trans. Consum. Electron.* **61**(3) (2015). 00983063/15/\$20.00©2015 IEEE
5. Lath, B.R., Liu, H.: FSOS: a tool for recommending suitable operating systems to computer users. In: SAI Computing Conference 2016, 13–15 July 2016. IEEE, London, UK (2016). 978-1-4673-8460-5/16/\$31.00©2016 IEEE
6. Parvatikar, S., Joshi, B.: Online book recommendation system by using collaborative filtering and association (2015). 6/15/\$31.00©2015 IEEE
7. Zeng, J., Li, F.: A restaurant recommender system based on user preference and location in mobile environment. In: 2016 5th IIAI International Congress on Advanced Applied Informatics. <https://doi.org/10.1109/iai-aaai.2016.126>. 978-1-4673-8985-3/16 \$31.00©2016 IEEE
8. Coelho, B., Costa, F.: HyredHYbrid job recommendation system. Project Work in Team, Portuguese National Strategic Reference Program (QREN 2007–2013), pp 2013/38566
9. Jueajan, B., Naleg, K.: Development of location-aware place recommendation system on android smart phones. In: 2016 Fifth ICT International Student Project Conference (ICT-ISPC) (2016). 978-1-5090-1125-4/16/\$31.00©2016 IEEE
10. Shino, N., Yamanishi, R.: Recommendation system for alternative-ingredients based on co-occurrence relation on recipe database and the ingredient category. In: 2016 5th IIAI International Congress on Advanced Applied Informatics (2016). <https://doi.org/10.1109/iai-aaai.2016.187>. 978-1-4673-8985-3/16\$31.00©2016 IEEE
11. Frank, E., Hall, M.A., Witten, I.H.: The WEKAWorkbench. Online Appendix for Data Mining: Practical Machine Learning Tools and Techniques, Fourth edn. Morgan Kaufmann, Burlington (2016)
12. Tejeda-Lorente, A., Porcel, C., Peis, E., Sanz, R.: A quality based recommender system to disseminate information in a university digital library. *Inf. Sci.* **261**, 52–69 (2014)
13. Bobadilla, J., Serradilla, F., Hernando, A.: Collaborative filtering adapted to recommender systems of E-learning. *Knowl.-Based Syst.* **22**, 261–265 (2009)
14. Bell, R.M.: Scalable collaborative filtering with jointly derived neighborhood interpolation weights. In: Proceedings of the 7th IEEE International Conference on Data Mining (ICDM 2007), pp. 43–52. IEEE CS, Washington, USA (2005)
15. Bekele, R., Menzel, W.: A Bayesian approach to predict performance of a student (BAPPS): a case with Ethiopian students. In: Artificial Intelligence and Applications, Vienna, Austria, pp. 189–194 (2005)
16. Sebastiani.: Machine learning in automated text categorization. *ACM Comput. Surv.*, **34** (1):1–47, Mar. 2002. ISSN 0360-0300. doi:10.1145/505282.505283. (2005)
17. Sebastiani: Text categorization in Encyclopedia of database technologies and applications, pp. 683–687. IGI Global (2005)
18. Fong, S., Robert, P.: Automated university admission recommender. ICITA (2009)
19. Reddy, Y.S., Govindarajulu, P.: College recommender system using student' preferences/voting. *IJCSNS* **18**, 87–98 (2018)
20. Monali, D., Dhanashri, G.: IRJET. College recommendation system for admission. SVPM's College of engineering Malegaon, Department of Information Technology, Maharashtra, India (2018)
21. Khanam, Z., Agarwal, S.: Map-reduce implementations: survey and performance comparison. *Int. J. Comput. Sci. Inf. Technol.* **7**, 119–126 (2015). <https://doi.org/10.5121/ijcxit.2015.7410>

22. Agarwal, S., Khanam, Z.: Map reduce: a survey paper on recent expansion. *Int. J. Adv. Comput. Sci. Appl.* **6** (2015). <https://doi.org/10.14569/ijacsa.2015.060828>
23. Khanam, Z., Ahsan, M.N.: Evaluating the effectiveness of test driven development: advantages and pitfalls. *Int. J. Appl. Eng. Res.* **12**, 7705–7716 (2017)
24. Khanam, Z.: Analyzing refactoring trends and practices in the software industry. *Int. J. Adv. Res. Comput. Sci.* **10**, 0976–5697 (2018)



Smart Cloud: A Self-organizing Cloud

Gayatri Hegde^{1,2(✉)} and Madhuri Rao¹

¹ Thadomal Shahani Engineering College, Mumbai, India

ghegde@mes.ac.in, my_rao@yahoo.com

² Faculty Pillai College Engineering, Mumbai, India

Abstract. The Self Organizing Cloud aims to provide efficiency i.e. robust and scalable solutions. Self organization can be provided through providing interactions among individuals. This paper proposes a self organizing architecture which predicts number of VMs using Kohonen algorithm and balances the load inheriting the convection process of molecules. The Kohonen algorithm is usually used for clustering. In this paper we apply Kohonen algorithm, an artificial neural network algorithm for prediction.

Keywords: Cloud computing · Convection process · Kohonen algorithm · Priority based algorithm · Self organizing cloud

1 Introduction

Cloud Computing in simple words means storing and accessing data over the Internet. Cloud computing has become highly demanded service since one can access the service from a remote server rather than accessing it from a local server. It has become advantageous because of its features like accessibility, scalability, low cost management, and availability anytime, anywhere. It has now provided the customer the on-demand affordable services.

The Self Organizing Cloud aims to provide efficiency i.e. robustness and scalability. The aim of this solution is to minimize the required cloud resources and minimize the time required to transfer the required processed data which is scattered all over. To meet these aims we can go for providing a hardware solution which acts as a media for self organizing systems or can be a software solution which benefits from the agility and scalability provided and these goals can be achieved by providing interactions among the virtual machines.

With this idea in mind, this research heading towards software solution to self organizing cloud. In this approach an intelligent system is used to predict the number of virtual machines required in a day before and will help to make decisions and may keep those virtual machines ready. Than these virtual machines are fed to convection module where virtual machines are arranged in a way as to resemble convection molecules. This module applies priority to each virtual machine. The level of VM increases with increase in no. of users and decreases priority.

2 System Architecture

Figure 1 here is the proposed architecture for smart self organizing cloud, where the big data is fed into Kohonen model for predicting number of virtual machines required for the day. These virtual machines are fed further into convection model which is arranged in layers depending on number of users. Than priority model is used to choose virtual machine among the few to keep them balanced.

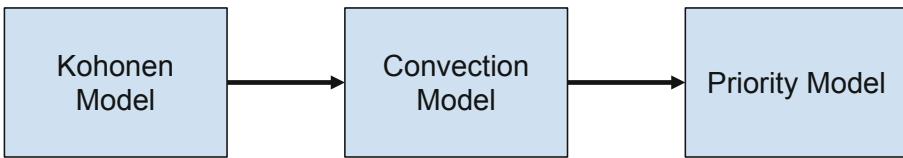


Fig. 1. System architecture for smart self organizing cloud

2.1 Kohonen Model

This model is used to predict the number of virtual machines required to keep them ready for the users. The decision to keep the Virtual Machines ready, play a vital role for the cloud provider, which decreases the energy, hence cost and hence meet service level agreement (SLA). Here we use Kohonen network for pattern recognition i.e. forecasting number of VMs everyday for a particular user.

2.1.1 Adapting Kohonen Algorithm to the Banking Data for Predicting the Load

Before modeling the Kohonen model for the required data set, a thorough study of our data set is made. Going through the data set for banking, following conclusion has been drawn,

- The load has a nonlinear and complex function.
- Everyday has different curve depending on different factors.
- It was observed that the load on the day before the holiday and a day after the holiday and the day of holiday was different from other days.
- It is also observed that due to increase in population and digitization the load has been increasing yearly.

2.1.2 Kohonen Load Predicting Model

This model consists of 10 submodels.

- 7 submodels for each day of the week
- 1 for day of holiday.
- 1 for day before holiday
- 1 for day after holiday

Each of this model is firstly trained and than used for prediction.

When training the network is completed, the transaction data is used and than the neural network output generates the average transaction for the day of training and also generates the number of transactions for next day of training. This acts as the input to the neural network. Then using this, load for next day is predicted by the network.

To get most appropriate result samples should be wisely chosen. The sample data can be 15 days from the day of prediction from recent years and a month sample data each of past years.

For holidays other than saturday and sunday, the samples are specially of the same day for previous years. Figure 2 depicts the Kohonen Model architecture for the banking data.

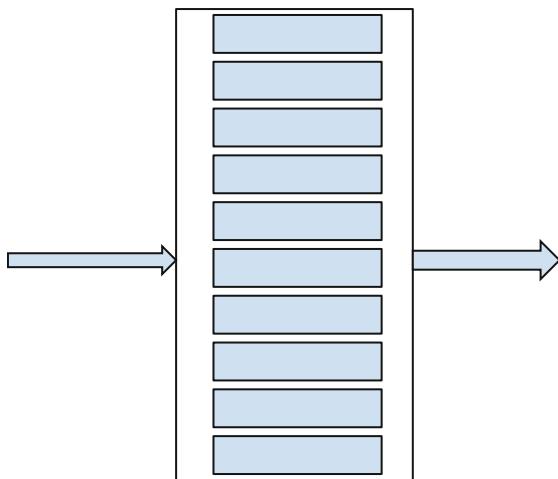


Fig. 2. Kohonen model for predicting load

2.2 Convection Process for Self Organization System

2.2.1 What Is Convection Process

Convection [2] cell in fluid dynamics is the process which occurs when there is a difference in density exists in liquid or gaseous material. As a result of this difference in density there is a rise and fall in the molecules within. And this is the main characteristics of a convection cell. When any liquid for example water is heated, it gets expanded and the density goes on decreasing and hence becomes more light than the surrounding liquid. This means that the colder the molecules higher the density and warmer the molecules lower the density. Hence the colder molecules with higher density tends to move lower which causes the warmer molecules with lower density to move upward. This movement of molecules called convection, and the moving cell of liquid is called a convection cell (Figs. 3 and 4).

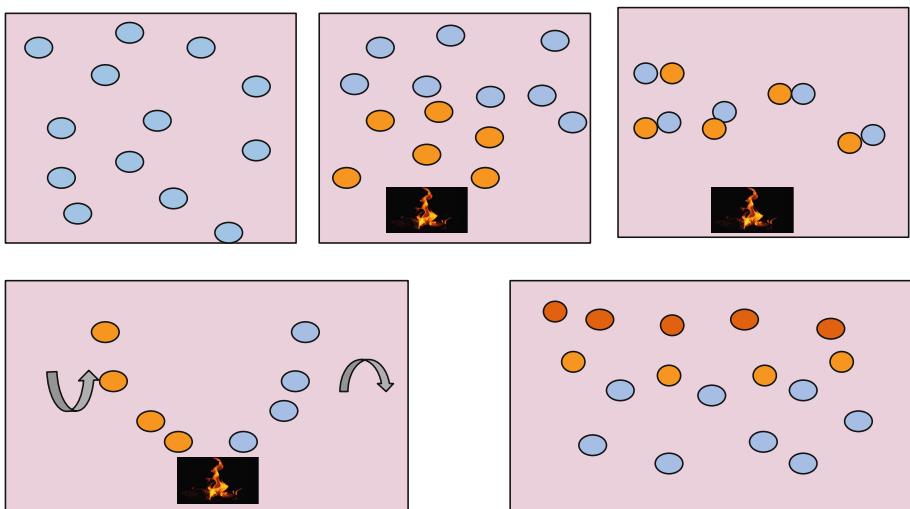


Fig. 3. Convection process in water

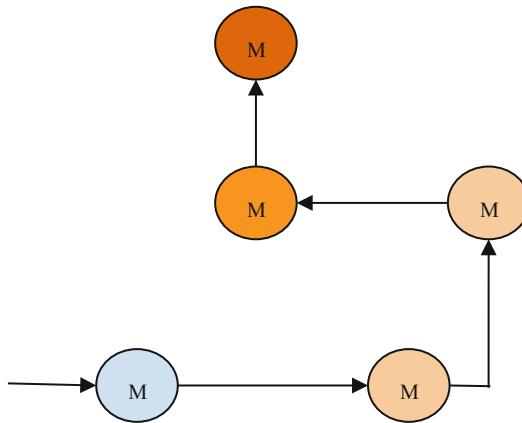


Fig. 4. Flow diagram for convection process

2.2.2 Proposed Model of Convection for Smart Self Organization Cloud

Consider the molecules within the water as VM which are requested by the customer. The heat which rises the molecules from lower level to the higher level, are the request from customer. Cooling of water is considered as releasing of resources by the customer.

Rising of molecules from bottom to the top layer when heated refers to the rising of the resources to the top layer when requested by the customer. Rising to the top here means allocating the resource a level. All the resources having the same number of requests will be allocated the same layer. Higher the number of request higher the level.

Cooling of molecules in convection cell reduces the density and the upper layer of the water is pushed back to lower level, similarly the resources released by the

customer after use reduces its level and put back to the lower layer ready to get requests from other customers (Fig. 5).

Algorithm for Convection process:

1. Initially all VM's are in level 1
2. As user request for the resource,

Get the higher priority VM,

If $VM[i]$ has the highest priority

Allocate this $VM[i]$ to user

$$\text{level}[VM[i]] = \text{level}[VM[i]] + 1$$

3. Repeat Step 2 for next user request

4. As user release the resource of $VM[j]$

$$\text{level}[VM[j]] = \text{level}[VM[j]] - 1$$

5. Repeat Step 4 for the next user release resource

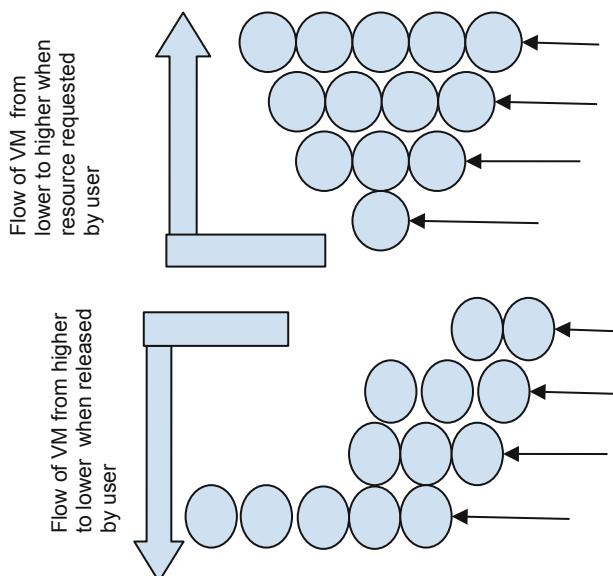


Fig. 5. Convection model

2.3 Priority Model

To choose among one of the virtual machines from a chosen level by convection model is also an important task. This is required for load balancing. This is done through priority based algorithm. The virtual machines can be prioritized according to the available resource and speed in a given level.

Priority based Algorithm for allocation of Priority to the VM

For all VM at level 1 to i

For all VMs 1 to j at level i

If Memory space is largest and Speed is high for VM[j]

high=VM_{ij}[priority]

2.4 Integration of the Models

Kohonen Model predicts the number of transactions for a particular day. By which the service provider can easily predict the number of VMs required by the user. This helps both the user and the service provider. Service provider can assure robust and fault tolerant service with low cost and also ensuring QoS. The number of VMs can be kept ready for the user in the initial layer. The Convection Model and Priority Model work together. As the user request arrives for the VMs depending on the priority VMs are allocated to the user and depending on no. of users the VM moves from one layer to another. This helps in load balancing. Any VM is not overloaded or underloaded.

3 Conclusion

Smart Self organizing cloud can be used to manage the service in any changing requirements of the user. It calculates the load required by the user per day and can reserve the space for their regular user without any intervention. This is also provided with load balancing due to priority module, which helps the service provider to avoid Virtual Machines to be overloaded or underloaded.

References

1. <https://www.cairn.info/revue-internationale-de-philosophie-2004-2-page-151.htm>
2. <https://en.wikipedia.org/wiki/Self-organization>
3. Xu, L., Chen, W.J.: Artificial neural network short – term electrical load forecasting techniques. In: Proceedings of IEEE, pp. 1458–1461 (1999)

4. Farhadi, M., Moghaddas-Tafreshi, S.M.: A novel model for short term load forecasting of Iran power network by using Kohonen neural networks. In: Proceedings of IEEE, pp. 1726–1731 (2006)
5. Andina, D., Pham, D.T. (eds.): Neural Networks Historical Review. Computational Intelligence, pp. 39–65. Springer (2007)
6. Farhadi, M., Tafreshi, S.M.: Effective model for next day load curve forecasting based upon combination of perceptron and kohonen ANNs applied to Iran power network. In: INTELEC 2007 - 29th International Telecommunications Energy Conference. IEEE (2008)
7. Lendasse, A., Cottrell, M., Wertz, V., Verleysen, M.: Prediction of electric load using Kohonen maps - application to the Polish electricity consumption. In: American Control Conference. IEEE (2002)
8. Senju, T., Tamaki, Y., Uezato, K.: Next day load curve forecasting using self organizing map. In: PowerCon 2000, 2000 International Conference on Power System Technology, IEEE (2000)



A High Linearity Shunt Capacitive Feedback LNA for Wireless Applications

Gaurav Srivastava and Malti Bansal^(✉)

Department of Electronics and Communication Engineering,
Delhi Technological University, Delhi 110042, India
maltibansal@gmail.com

Abstract. In this paper, CMOS LNA with low noise and high linearity with shunt capacitive and CS with inductive degenerate topology is presented. LNA is implemented in ADS on 0.18 μm TSMC technology. The LNA is designed for RF Front end so the important parameters are gain, linearity and noise figure. The circuit designed exhibits good I/P and O/P reflection coefficients with low power consumption which is crucial for LNA designing. The circuit attains $S_{11} = -22.06 \text{ dB}$, $S_{12} = -2.77 \text{ dB}$, $S_{21} = 9.4 \text{ dB}$, and $S_{22} = -104.85 \text{ dB}$ and $\text{NF} = 1.23 \text{ dB}$ and $\text{IIP3} = 56.86 \text{ dBm}$ for 6 GHz frequency band, used for future mobile communication or 5G technology.

Keywords: Cascode topology · LNA · Pie matching · Shunt capacitive feedback · Source degenerate topology

1 Introduction

Wireless communication is the procedure of information transmission over a distance without the need for cables, wires and other electrical network. In RF domain the wireless communication occurs through electromagnetic spectrum ranging from 30 Hz to 300 GHz. In modern era the wireless communication involving RF front end circuits are designed for applications like IOTs (internet of things), LTE and 5G connectivity [1]. Modern and future mobile devices need to support increasing number of frequency band and wireless standards and the applications like Bluetooth, Wi-Fi (802.11/a/b/g/n) standards ranging in 2.4 and 5 GHz band and mobile television. It should also support 4G LTE networking [2] consisting of 40 frequency band globally ranging from 700 MHz to 6 GHz. Other wireless application lies in UWB which is defined as data transmission in the form of radio energy spreaded over the entire bandwidth with a low power spectral density. The frequency range of UWB ranges from 3.1–10.2 GHz. In [3] a wideband amplifier with a resistive feedback topology is implemented for UWB applications the LNA consist of input-matching network and single to differential amplifier acting as a voltage buffer for improving power gain. However, it faces challenges like pulse shape distortion (low powered signal distorted by transmission link), low transmission power, channel estimation and high frequency synchronisation. As compared to 4G network 5G network requires to be versatile, scalable and energy smart for the hyper connected IOE world. In [4] By using advanced modulation methods massive MIMO and beam forcing techniques 5G

connectivity are expected to achieve data rate of (10 Gbps) with universal coverage having high efficiency and spatial diversity. [5] 5G spectrum has three key frequency for widespread coverage capable of supporting all users and cases. Three frequency ranges are sub-1 GHz, 1–6 GHz and above 6 GHz. 6 GHz radio (LANs) are less prone to interfere with the spectrum for fixed microwave, satellite digital radio, telecom backhauls. Therefore, 6 GHz draft plan is under study with a goal of ensuring its use in wideband channel applications. The LNA designed for such wireless applications are required to have matching network for selecting specific range of frequencies, good linearity flat gain with low noise figure. The LNA designed should have low power consumption and area occupied should be less. Organisation of the content for this paper is as follows: Sect. 2 gives the brief description of the topologies, shunt capacitive feedback topology and matching circuits. Section 3 description of the circuit followed by simulation results. Section 4 conclusion and comparison of work is made.

2 Design Methodology

LNA implementation involves three basic topologies like common source, common gate and cascode topology. The choice of the CS or CG is determined by the robustness of the I/P and O/P matching network or low noise figure in the circuitry. CS stage provides low noise figure as compared to CG stage. In the present circuit common source stage is cascaded with the common gate stage which provides better I/P and O/P matching, isolation, better stability and low noise figure [6]. The capacitance feedback topology provides additional optimization of NF. However, this topology provides high linearity, low noise figure and gain. The present circuit is implemented with pie matching network providing two degrees of freedom in the form of quality factor of the circuit and For attaining the ideal resistance of 50Ω a common source with inductor degenerate is implemented.

3 Circuit Design

In the given circuit C1, C2 and inductor L2 forms a pie matching network. The shunt capacitance C3 along with source degenerate inductor L3 attains I/P impedances of 50Ω . The mosfet M1 with common source and M2 with common gate topology forms a cascaded stage providing isolation between input and output and circuit attains high linearity with low noise figure. The feedback capacitor C3 is in shunt configuration. Thus, the circuit attains negative feedback causing the system to become unconditionally stable which improves the gain lower noise figure and causes the circuit to attain high linearity. The DC blocking is obtained through capacitor C4. The series network of L3 and resistance R2 acts as a loading element of the cascode stage and for further increasing the gain and bandwidth the second stage of source follower M3 is used (Figs. 1 and 2).

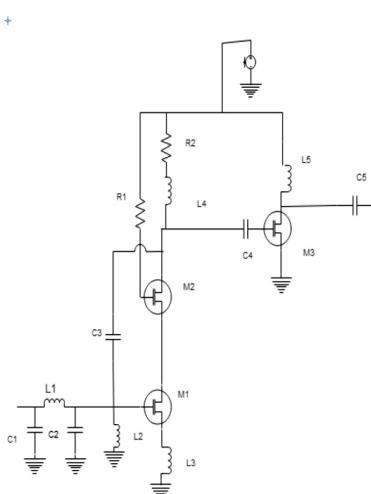


Fig. 1. Circuit diagram for proposed LNA

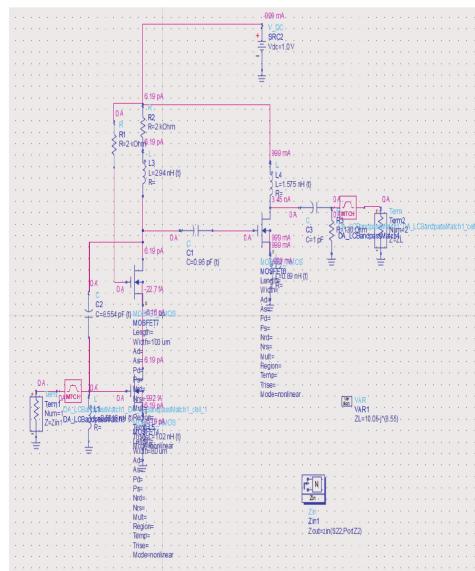


Fig. 2. Schematic for proposed LNA

4 Results and Comparative Analysis

The parameter S_{11} denotes the input return loss or reflection coefficient. For measuring S_{11} , at I/P port signal is injected and reflected signal at the same port is measured for this no signal is coupled to the output port so, it denotes the matching between the input and characteristics impedance or reference impedances. For 6 GHz the S_{11} obtained is -22.09 dB as shown in Fig. 3.

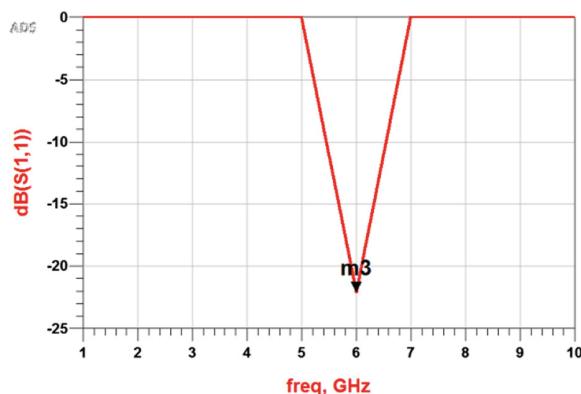


Fig. 3. Input return loss

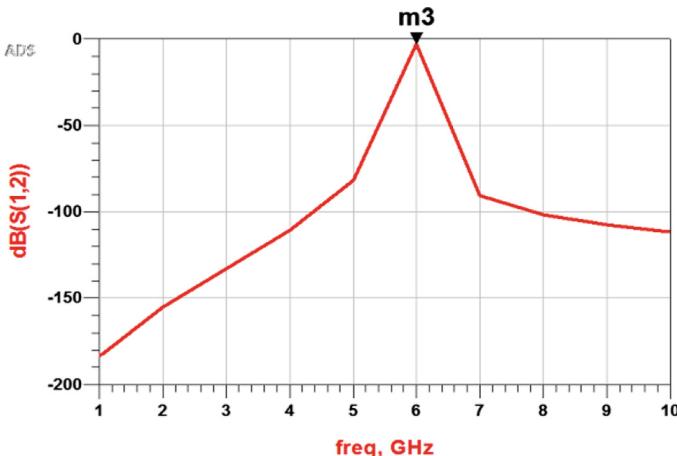


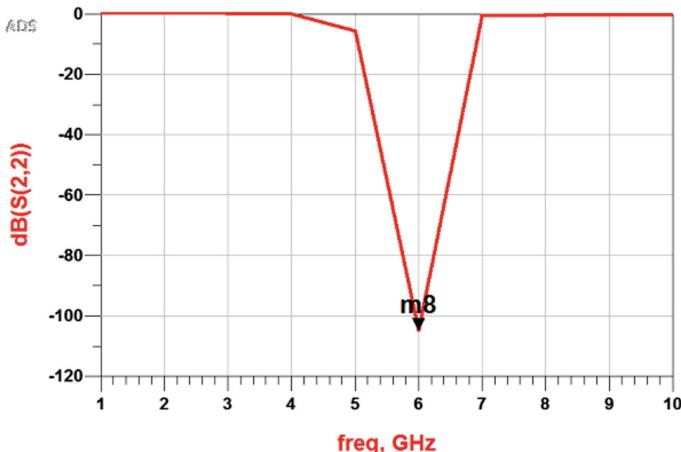
Fig. 4. Reverse transmission coefficient

S_{12} is also called as reverse transmission coefficient. It calculates the I/P signal reflected back or measures the isolation b/w the I/P and O/P port. The S_{12} parameters for this circuit is -2.75 dB (Fig. 4).

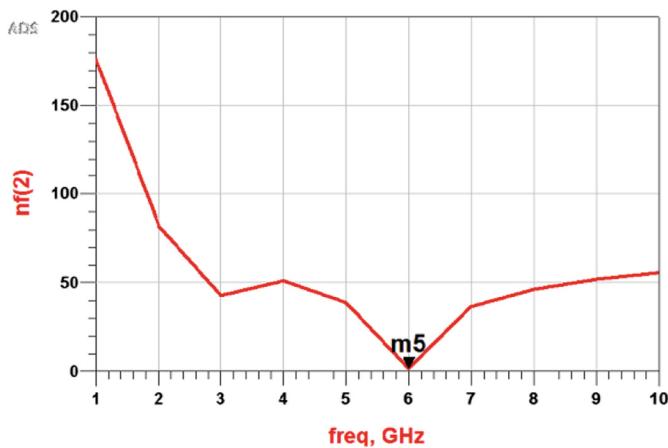


Fig. 5. Forward transmission coefficient

S_{21} is also called as forward voltage gain or forward transmission coefficient it measures the signal transmitted from the I/P to the O/P or the intensity of the signal reaching the O/P for this circuit the S_{21} obtained is equal to 9.4 dB as shown in Fig. 5.

**Fig. 6.** Output reflection coefficient

The S_{22} is also called as output voltage reflection coefficient or output return loss. For measuring S_{22} at O/P port signal is injected and the reflected signal at the same port is measured for this no coupling of signal takes place so, it denotes the matching between the output and the reference impedances. For 6 GHz the S_{22} obtained is equal to -104.85 dB (Fig. 7).

**Fig. 7.** Noise figure

The parameter NF (noise Figure) is a measure of SNR. It calculates the degradation in the signal to noise ratio. The small value of the NF denotes the performance of the circuit is better for the present circuit $NF = 1.23$ dB as shown in the Fig. 6.

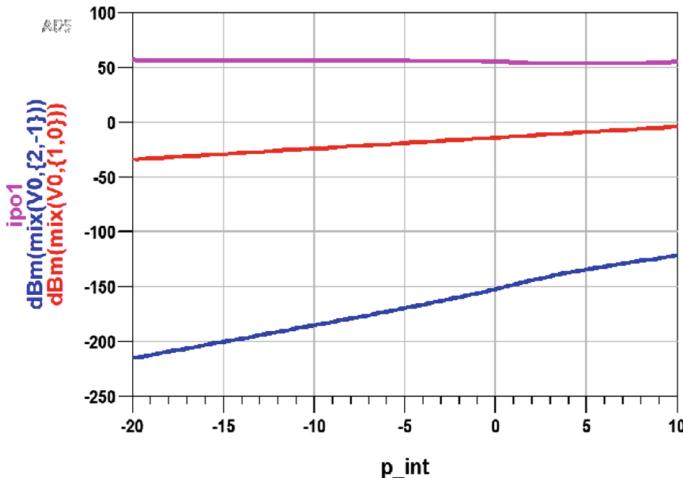


Fig. 8. Third order intercept point

The characteristics of LNA are determined by high amplification factor and low noise figure along with it circuit should have high linearity. Linearity of the circuit is measured by third order intercept point. In this circuit the IIP_3 is found to be 56.89 dBm which denotes the circuit with low noise figure attains high linearity causing system to become relatively more stable. Thus, it implies that [7] from the fact that circuit can either have moderate gain, low noise figure or high linearity or moderate gain with high noise figure and low linearity (Figs. 8 and 9).

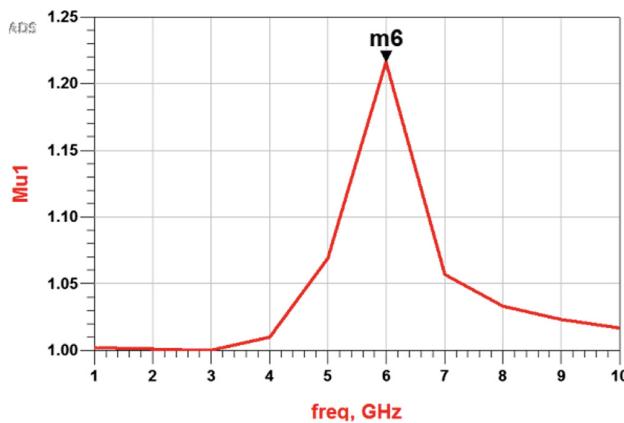


Fig. 9. Stability

Stability of an LNA [7] measures the tendency of an amplifier to oscillate. It is defined as immunity against spurious oscillations. The circuit becomes unstable for

specific combination of source and load impedances. An LNA designed oscillate at extreme of voltage variation for low or high frequency. Therefore, the stability of an amplifier is given by two factors K and Δ where K denotes Rollett's stability factor or Stern stability factor. The stability factor of this circuit is 1.21.

Rollett stability factor or $K > 1$ for unconditionally stability.

$$k = \frac{1 - |s_{22}|^2 - |s_{11}|^2 + |\Delta|^2}{2|s_{12}s_{21}|} > 1$$

$$\text{Where } \Delta_s = S_{11}S_{22} - S_{12}S_{21}$$

Table 1. Comparison of proposed LNA with other published works

Ref. no.	[8]	[9]	[10]	This work
Tech (μm)	0.13	0.18	0.18	0.18
NF (dB)	1.8	2.7–3.38	2.5–3.5	1.23
S_{11} (dB)	-1.3	-10.61	-12.6	-22.06
Pdc (mW)	-	8.65	8.14	0.035
IIP ₃ (dBm)	3	-	-	56.89
Supply (V)	1.2	1.2	1	1
Freq (GHz)	3.1–10.6	3–11	2–6	6

5 Conclusion

The proposed CMOS LNA is implemented using cascode topology for input and output isolation and shunt capacitive feedback topology providing high linearity to the circuit it is implemented with source degenerate inductor topology to achieve matching circuit of 50Ω . The circuit is found to consuming 0.035 mW of power and noise figure of 1.23 dB at 6 GHz band for wireless application. The circuit is found to attain IIP₃ of 56.82 dBm and stability factor of 1.21 with output return loss or $S_{22} = -104.85$ dB which is best so far (Table 1).

References

1. Hindawi Wireless Communication and Mobile Computing (2018). Article Id 1438060, <https://doi.org/10.1155/2018/1438060>
2. Mudavath, M., et al.: Design of CMOS RF front-end of low noise amplifier for LTE system application. Asian J. Inf. Technol. **20**(15), 4040–4047 (2016)
3. Jha, P., et al.: Design of RF front end LNA for an ultra wideband receiver. J. Electron. Devices (13), 1006–1011
4. Hindawi Wireless Communication and Mobile Computing (2018). Article Id 6793814, <https://doi.org/10.1155/2018/6793814>

5. GSMA 5G spectrum position offer a Roadmap for Regulations. <https://www.gsma.com/spectrum/resources/5g-spectrum-positions/>
6. Taylor and Francis: High performance capacitive shunt feedback LNA. *J. Electromagn. Waves Appl.* **30**(5), 612–625
7. Liao, H.Y., Lu, Y.T., Deng, J.D.S., Chiou, H.K.: Feed-forward correction technique for a high linearity WiMAX differential low noise amplifier. In: International Conference on Radio-Frequency Integration Technology, December 2007, Singapore (2007)
8. Ragheb, A.N.: A 3.1-10.6 GHz low power high gain UWB LNA using current reuse technique. In: International Conference on Intelligent and Advanced System, no. 2, 741–744 (2012)
9. Aditi, Bansal, M.: A- high linearity and low noise shunt resistive feedback UWB LNA. In: International Conference on Information and Communication Technology, April 2018
10. Chang, C.-W.: A 1-V 14.6 dB gain LNA for Wi-Max 2-6 GHz applications. In: International Conference on Symposium Circuits and Systems, pp 1039-1041, September 2009
11. Visweswaran, A., Serdijn, W.A.: A low power UWB-LNA using active dual loop negative feedback in CMOS 0.13 μm . In: Proceedings of IEEE International Symposium on Circuits and Systems, Taipei, pp. 225–228 (2009)
12. Vishwakarma, S., Jung, S., Joo, Y.: Ultra wide band CMOS low noise amplifier with active input matching. In: Proceedings of International Conference on Ultra Wideband Systems and Technology, pp. 415–419, May 2004
13. Bevilacqua, A., Niknejad, A.M.: An ultra-wideband CMOS LNA for 3.1 to 10.6 GHz wireless receiver. In: Proceedings of IEEE ISSCC Digest, pp. 382–383 (2004)
14. Hirt, W.: Ultra-wideband radio technology: overview and future research. *Comput. Commun.* **26**(1), 46–52 (2003)
15. Wheeler, A.: Commercial applications of wireless sensor networks using ZigBee. *IEEE Commun. Mag.* **45**(4), 70–77 (2007)



Transparent Watermarking QR Code Authentication for Mobile Banking Applications

Saiteja Ityala^(✉), Oshin Sharma, and Prasad B. Honnavalli

Department of Computer Science and Engineering,
PES University, Bangalore, India
saiteja2208@gmail.com

Abstract. Mobile banking is a service provided by the bank and other financial institutions, which accepts their users to do a remote online transactions by using smart devices such as mobile or tab. With the help of Mobile Banking, customer can pay bills, check account balance and recent transaction details. To keep mobile banking application secure in E-commerce transaction or a banking transaction, we require proper Authentication so that the intruder or attacker cannot do Eavesdropping.

This paper provides a novel approach of watermarking QR Code authentication for mobile banking applications. The idea is to develop an Android Mobile Banking Application which will give Authentication at Sign-in part & Transaction part. This proposed method will provide high security while doing online transactions along with HTTPS Protocol.

Keywords: Mobile banking · Watermarking · QR Code · Authentication · DWT · OTP

1 Introduction

Mobile Banking was started in the year 1999 by Deutsche Bank. Past 10years, the cost of mobile phones is very high with limited functionality and also cost of data plans are also very high. The technology has been improved in hardware & software and the cost of mobile phones are also reduced. In Sep 2007, Alite company predicted that mobile banking users in the US were 1.6million and will increase to 35million by 2010. In Mobile Banking, the main concern is the security issues, when more users are using mobile banking there is a chance for the attackers for a financial gain.

Mobile Banking Security requirements are (i) Confidentiality, (ii) Integrity, (iii) Authentication& (iv) Non-Repudiation.

Mobile banking is very fast while compared to online banking. This requires an application & consists of a nice user- interface and user-friendly, so that the user can understand easily & make payments. SMS were the earliest mobile banking services in the 90's. Multi-factor authentication provides double security example: If an attacker tries getting in with other user's credential's, he gets structs in one or another

authentication process or it takes some time for attacker to get in or it's impossible for him to think about each module.

Online Banking services are increasing day-by-day in-terms of easy of use & time saving. This banking services can be used anywhere & anytime which is used to solve the problem of going to a bank and wait in a queue. Mobile banking is easy for a user for doing online transactions but providing proper security is the important concern. When a user sign-in with his/her credentials the server requests for username & password to check for a privileged user. And there is a chance for an attacker to do phishing in which he tries to steal the bank details of a user. This will propose a Multilevel Authentication where QR Code Watermarking Authentication is used at the Sign-in part and multiple OTP Authentication at the payment part.

2 Related Work

Mobile Banking Services provides free of cost services. Authentication gives the more security for any application. This paper is mainly discussed about a proper multilevel authentication by using a passcode as a key. This passcode will hide in a QR Code for Scanning. This Scanning will be fast, the server will check's the passcode. Some of the papers related to Authentication are discussed below:

Nuakoh [1] presented a novel approach by developing a mobile application which will watch user's activities and control of their account login & usage. This application will find the fraudulent user by sending notification reports to legitimate users for avoiding malicious activity. This application will collect information such as location account, OS, date & time. This will allow user to set own security policies.

Islam [2] proposed a stenographic technique called DNT-SVD. This technique will hide the payload by using a QR Code image generator as a cover image & payload is a key for hiding in a QR Code. This method has been done in an iterative manner i.e., if we cannot recover the exact data in the first time, it will re-implement the process on steno-image to get the exact payload.

Mbungo [3] author proposes a strong & scalable four factor authentication structure to provide more security for online transactions. This will used to prevent from active & passive attacks. Token generation algorithm were used to generate a session token which will retrieve IMEI, IMSI, current time from the bank server side and also from client application & it will synchronize time.

Venugopal [4] proposed a multimodal bio-metric (face & fingerprint) for financial transaction. Single authentication can be easily breached when user reveals his credentials & his cards were stolen. To avoid these, both (face & fingerprint) were used for log-in process & one biometric used for financial transaction process. By using this authentication, hacking & phishing can be avoided.

Ahvanooy [5] presented Social media has become a part of people's life. When user sends a text message from social media, the data present in the text message transmits in a plaintext, which inclined to attacks. To prevent these attacks, the author proposes a novel based stego technique known as AITSteg, which gives a secure transmission from end-to-end.

Sharma [6] presented Fingerprint authentication is an important module after multifactor authentication when doing mobile banking transactions. The author created a java based mobile banking application which will give an access to a mobile banking sign-in and payment modules which gives 100% very secure. Fingerprint recognition system is a reliable authentication for a mobile banking application.

Thomas [7] presented a mechanism by taking a QR Code as a cover image and OTP as a key to hide in a QR Code. For hiding a key, a technique called watermarking are used with Hadamard transformation. OTP is the first level authentication & water marking sequence for hiding the OTP is a second level authentication. Multilevel authentication will enable's more security when doing online transaction.

Kaka [8] proposed a MITM vulnerability in many banking applications, when the user information travels from banking application to the server. Some banking application were using a HTTP protocol which is not secure, even if they are using HTTPS also its not secure because no proper SSL/TLS handshake which leads to MITM attack.

Lee [9] to implement a strong authentication, the author proposes a authentication system by using mobile otp with the help of QR Code so that legitimate user can access it, so this will give first level of authentication. Second level of authentication will send otp to a mobile user from a server. It will check that the both otps are matched or not and also author used an SSL/TLS handshake for secure transactions.

Kakade [10] author proposed a steganographic technique where it will hide the data in a QR code by using DWT technique & LSB Steganography & used AES Encryption algorithm to secure the information hiding mechanism. This is used for hiding the criminal data of a particular criminal in a QR code.

Shaju [11] author proposed a three factor authentication by using a BISC authentication algorithm. This consists of a 3 different categories for authentication factors like Knowledge, Possession & inherent. This proposed system will merge the device & used based authentication which provides a security for user privacy details.

Mulliner [12] author proposed a SMS based OTP's is used to secure from phishing attacks when doing online banking. In this they proposed a mechanism for securing OTP's against attacks for smartphone Trojans. This OTP is used as another factor for authentication after sign-in with their username & password. These OTP's are used for mobile transactions as a trusted user.

Rathod [13] Online Banking is used for bank clients to access their transactions from a work places via internet. To take care for a user verification for unstoppable hacking of the databases on the internet, the author proposes an authentication mechanism like Visual Cryptography & Steganography. These techniques are used to hide the data or key embedded in an image. This image is divided into two shares, one is saved in a database & another is at client side. These shares are used to validate the users.

Mishra [14] author proposed a secured authentication mechanism by using QR Code & digital watermarking. The visible watermarked data is embedded in a QR Code as a cover image using DWT technique. By using this technique the data cannot be changed or modified of the information from an intruder. The data will be safe when it is transmitted.

Mendhe [15] author proposed a 3-layer architecture for secure message transferring mechanism by using QR Code as a one layer. In first layer they have used a RSA

Encryption to encrypt the secret data. In second layer, the encrypted data is embedded in a QR code. In the third layer, the QR Code image is encoded with a mask image by using a proposed encoding algorithm.

3 Proposed Methodology

According to OWASP (Open Web Application Security Project), insecure authentication is the fourth most exploited vulnerability by phishing or bypassing authentication in mobile authentication. If a mobile application trying to execute a backend API anonymously without giving any access token, it leads to insecure authentication. An attacker will reveal sensitive information & encrypted communications if and only if he encounters unencrypted communications & insecure authentications. To provide secure authentication for mobile banking applications, a proper HTTPS protocol with proper SSL/TLS handshake should be provided.

In this proposed system, a QR Code Watermarking is used which will give strong authentication mechanism at the Sign-in part where the attacker unable to scan the QR Code which consists of a passcode. A passcode will be generated at the time of registration. When the user scans the QR Code it will check for the generated passcode. Only Privileged user can scan that QR Code. Watermarking is used to hide a data inside a QR Code Cover Image.

In this a powerful technique called Discrete Wavelet Transform (DWT) are used to hide the data inside a QR Code Image. This will decompose the image into different frequencies like High Frequency, Middle Frequency, Low frequency. It performs in 1-D & 2-D. It is more accurate model when compared to Discrete Fourier Transform (DFT) & Discrete Cosine Transform (DCT). This model is based on four sub-bands LL, LH, HL & HH. This four sub-band will obtain by using two filters are Low pass filter and High pass filter. This technique will apply Watermarking & de-watermarking. Here we are using 2-level image decomposition for better result (Fig. 1).

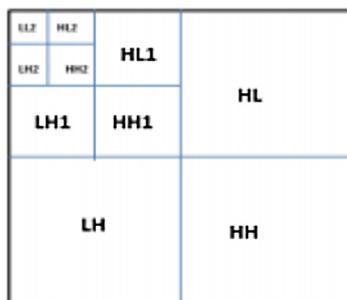


Fig. 1. Image decomposition

This DWT will use LL Subband for high frequency to get exact result. For every level of decomposition LL band will be used as the input for a previous level. In this first we will perform Vertical direction followed by Horizontal direction.

Watermarking image has given a bit sequence of watermark S & secret key i. The background values are set to -1 & 1

$$S = \{s_i, 1 \leq i \leq N\}, s_i \in \{-1, 1\}$$

Where N will be the No. of Pixels for watermarking image (Figs. 2 and 3).

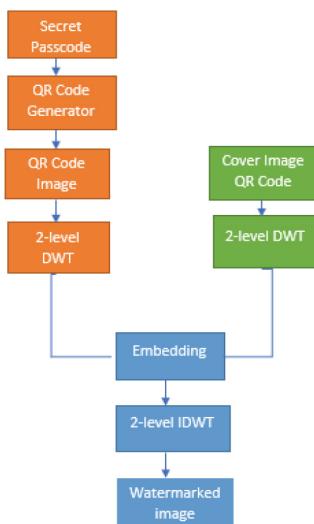


Fig. 2. Embedding process

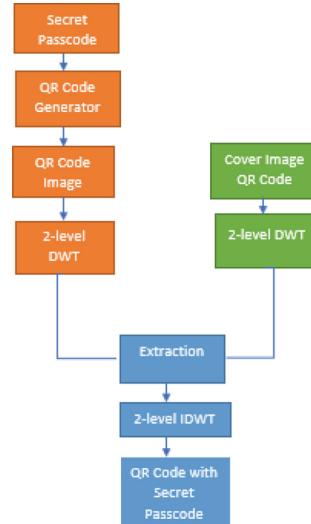


Fig. 3. Extraction process

Embedding Process

- Step 1: Secret data will be hide in a QR Code.
- Step 2: QR Code image will be generated with a secret passcode & cover image is used as a watermarking technique.
- Step 3: Applying DWT algorithm for both Cover image QR Code & QR Code image
- Step 4: IDWT will be used for reconstruction of cover image.
- Step 5: Watermarked image will be same as QR Code Image.

Extraction Process

- Step 1: In this the QR Code & watermarked QR Code is extracted
- Step 2: The QR Code consists of a passcode is used for scanning
- Step 3: QR Code will have a secret passcode is extracted from watermarked image.

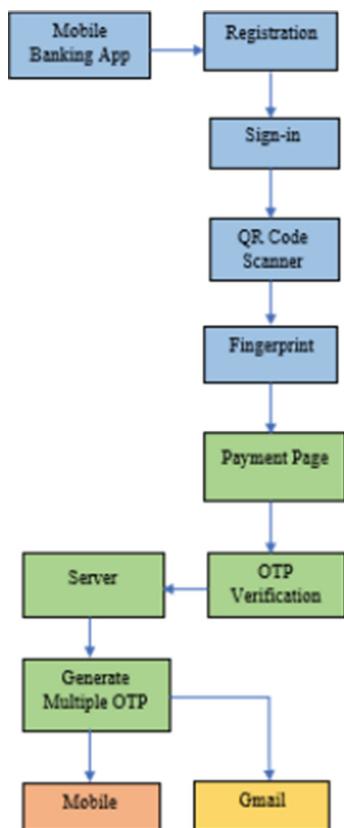
For generating a QR Code a Zxing is an image processing library developed in java & used for mobile application. QR Code is a 2-D which uses version 1 (Fig. 4).

Below is the architecture diagram which will describe all modules for banking application (Fig. 5):



Fig. 4. QR Code comparison

Following are the steps used in the proposed architecture:



Step 1: The user has to register with his/her details like Email, mobile number, password, username.

Step 2: After Registration, the user will go to the Sign-in page where he has to give his Email & Username. With that username the server will generate watermarking QR Code

Step 3: The user has to scan the QR Code for the Proper Authentication to prevent attacks.

Step 4: After scanning the QR Code, the user has to give his Biometric Authentication to access the app.

Step 5: After Fingerprint it will go to the Payment page to do the Mobile Transaction.

Step 6: After giving the bank credit/debit card details it will ask for multiple authentication for checking the privileged user.

Step 7: The mobile app requests to the server to generate OTP for OTP Verification

Step 8: The server will generate OTP to a Registered mobile Number i.e., First Authentication

Fig. 5. Flowchart for proposed methodology

Step 9: Second it will send to a Registered Gmail i.e., Second Authentication By using QR Code Watermarking at the sign-in part & multiple OTP Authentication at the payment side will secure the mobile Banking Application from intruder/attacker.

Comparison Factors for Cover-Image with Steno Image

In Existing methodologies there were used QR Code OTP which will take more time for authentication. In this proposed mechanism, the accuracy will be fast in this we were using a passcode authentication which will be generated based on user details & hide in a QR Code. The server will check the QR Code which consists of a same passcode or else it won't scan the QR Code. The server will send an QR to a registered email id.

- (1) Peak Signal to Noise Ratio (PSNR): When the data has been hidden in an image so that the quality of image should not be changed. PSNR is used to check lossy compression. Higher the PSNR value indicates the better the quality of image.

$$\text{PSNR} = 20 * \log_{10}(255/\sqrt{\text{MSE}})$$

- (2) Mean Square Error (MSE): It will perform byte by byte comparison for the two images. The distortion of the image can be calculated by using MSE.

$$\text{MSE} = \frac{1}{MN} \sum_{y=1}^M \sum_{x=1}^N [I(x,y) - I'(x,y)]^2$$

Where $I(x, y)$ will be the original image & $I'(x, y)$ is the decomposed image. M & N is the image dimensions.

- (3) Imperceptibility: It means the data in an image to be unnoticed by a Human eye.
- (4) Robustness: It means the ability of embedded data remain undamaged if the image has cropping, blurring Normalized correlation (NC) is calculated between the Original Watermark & Extracted Watermark (Figs. 6 and 7).

$$NC = \frac{\sum_{i=1}^M f(i) \times f'(i)}{\sum_{i=1}^M f(i)^2}$$

Type of Noise	MSE	PSNR	NC
Salt & pepper (0.02)	0.05	45.32	0.98
Gaussian (0.05)	0.06	41.24	0.88

Fig. 6. Comparing noise for proposed methodology

Type of Noise	MSE	PSNR	NC
Salt & pepper (0.02)	0.03	40.88	0.8
Gaussian (0.05)	0.04	37.14	0.75

Fig. 7. Comparing noise for existing methodology

- Imperceptibility & Robustness are high
- MATLAB is used for running these test-cases.

[16] Good PSNR value will be 30–50 db provided bit depth is 8bits for lossy image.

[16] MSE is non-negative & values are closer to Zero are good. Lesser the MSE value will give accurate result.

4 Results and Discussions

This section consists of an implemented Secure App Screens.

- Front Page Activity
In a Fig. 8: In this Activity, the screen consists of a Registration Phase & Login Phase.
- In a Fig. 9: the user has to register by his details like Email Id, Name, Password, Mobile Number.
- In a Fig. 10: After Registration, the user will go to the Sign-in page where user has to give his Registered Email & Username. The QR Code with Watermark will generate at the server side with registered username.



Fig. 8. Front page



Fig. 9. Registration

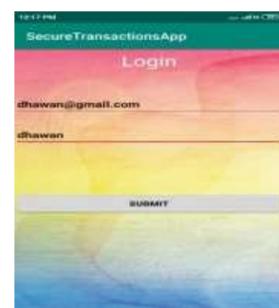
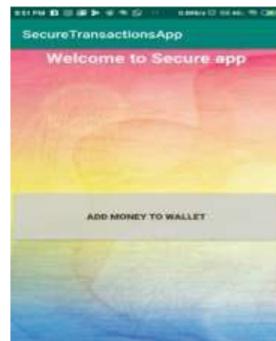
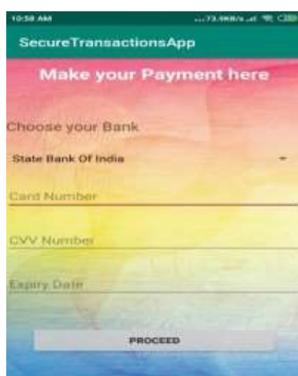
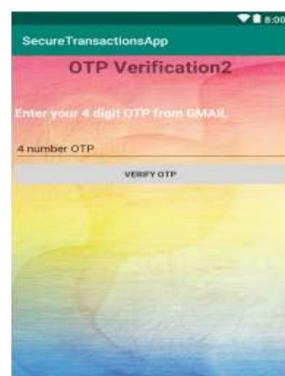


Fig. 10. Sign-in page

- (d) In a Fig. 11: After sign-in, the user will scan the QR code which consists of a Watermarking. The scanner will check the QR Code which consists of a passcode. The passcode will be generated inside the QR Code in the server at the time of registration. And watermarking technique will be applied when user presses the sign-in button. A library called Zxing is used for creating a QR Code
- (e) In a Fig. 12: After scanning the QR Code, the user will give the Fingerprint for accessing the Application which gives another layer of security.
- (f) In a Fig. 13: After Fingerprint, the user can make the transactions by adding money to a wallet.

**Fig. 11.** QR Code scanner**Fig. 12.** Fingerprint authentication**Fig. 13.** Payment page

- (g) In a Fig. 15: After adding amount it will go the credit/debit cards payment page where the user has to give his/her card details for making a transaction.
- (h) In a Fig. 16: After giving the card details it will go for multiple OTP Verification i.e., (a) mobile, (b) Gmail (Fig. 14).

**Fig. 14.** Adding card details**Fig. 15.** Mobile OTP**Fig. 16.** Gmail OTP

5 Conclusion and Future Scope

Mobile Banking will play a vital role for a Customers to do a Paperless Transactions by using an application. In banking Application, Authentication will give an access to the privileged user for doing the transactions. In this proposed method a multiple OTP Authentication & QR Code based authentication are used. Watermark Technique has been used for hiding a key in QR Code cover page. These will give strong authentication by using an HTTPS Protocol.

This application will be used were the users consist of a private data or images & videos in a mobile application. This proposed application will be more secure because the watermarking QR Code can be scanned by a privileged user. It also provides a user experience by making QR Code Authentication more user friendly. Future scope will work on payment gateways & message gateways which will be the real banking application.

References

1. Nuakoh, E.B., Coffie, I.: MonitR: a mobile application for monitoring online accounts security. In: Southeastcon, st.petersberg, FL, USA, April 2018
2. Islam, Md.W., Alzahir, S.: A novel QR Code guided image stenographic technique: In: International Conference on Consumer Electronics (ICCE), pp. 586–587, Las Vegas, NV, USA, January 2013. ISSN: 2158-4001
3. Mbunge, E.: A robust & scalable four factor authentication architecture to enhance security for mobile online transaction. *Int. J. Sci. Technol. Res.* **7**(3) (2018)
4. Venugopal, H.: A robust and secure authentication mechanism in online banking. In: Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, India, November 2016
5. Ahvanooey, M.T., Li, Q., Hou, J., Mazraeh, H.D., Zhang, J.: AITSteg: an innovative text steganography technique for hidden transmission of text message via social media. *J. IEEE Access*, 65981–65995 (2018). ISSN: 2169-3536
6. Sharma, L.: Mobile banking transaction using fingerprint authentication. In: Second International Conference on Inventive Systems & Control (ICISC), Coimbatore, India, pp. 1300–1305, January 2018
7. Thomas, J., Goudar, R.H.: Multi-level authentication using QR code based watermarking with mobile OTP and Hadamard transformation. In: International Conference of Advances in Computing, Communications & Informatics (ICACCI), Bangalore, India, pp. 2421–2425, September 2018
8. Kaka, S., Sastry, V.N., Maiti, R.R.: On the MITM vulnerability in mobile banking applications for android devices. In: International Conference on Advanced Networks & Tele Communications Systems (ANTS), Bangalore, India, November 2016
9. Lee, Y.-S., Lee, H.: Online banking authentication system using mobile OTP with QR code. In: 5th International Conference on Computer Sciences & Convergence Information Technology, Seoul, South Korea, pp. 644–648, December 2010
10. Kakade, R., Kasar, N.: Image steganography & data hiding in QR Code. *Int. Res. J. Eng. Technol.* **4**(5), 2926–2928 (2017)

11. Shaju, S., Panchami, V.: BISC authentication algorithm: an efficient new authentication algorithm using three factor authentication for mobile banking. In: Online International Conference on Green Engineering and Technologies, Coimbatore (2017)
12. Mulliner, C.: SMS based OTP's: attacks & defense. In: 10th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Germany, pp. 150–159 (2013)
13. Rathod, P.D., Kapse, S.R.: Secure bank transaction using data hiding mechanism. In: International Conference on Innovations in Information, Embedded and Communication Systems. IEEE Press, Coimbatore (2017)
14. Mishra, A., Mathuria, M.: Multilevel security feature for online transactions using QR Code & digital watermarking. In: International Conference on Electronics, Communication and Aerospace Technology, pp. 48–51. IEEE, Coimbatore (2017)
15. Mendhe, A., Gupta, D.K.: Secure QR-Code based message sharing system using cryptography & steganography. In: First International Conference on Secure Cyber Computing and Communication. IEEE, Jalander (2018)
16. Best PSNR & MSE value. https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio



Network Intrusion Detection System Using Two Stage Classifier

Devakunchari^(✉), Sourabh, and Prakhar Malik

Department of CSE, SRMIST, Chennai 603203, India

devakunr@srmist.edu.in,

sourabhcse23@gmail.com, prakhar2609@gmail.com

Abstract. A Network Intrusion Detection System (NIDS) is a mechanism that detects illegal and malicious activity inside a network. Anomaly based Intrusion detection systems use machine learning techniques to detect novel attacks. Classifiers are predictors that estimate the class label of an attack based on prior training and learning models. While it can be seen that DoS (Denial of Service) and probe attacks are filtered with reasonable accuracy, the detection rate fails miserably for R2L (Remote-to-Local) and U2R (User-to-Root) attacks. This paper aims to improve the accuracy of the above-mentioned attacks by proposing a two-stage classifier with feature selection used in the second stage of classification. The first stage uses a simple NB classifier with all the trained features. The proposed feature selection technique is based on Genetic Algorithm with entropy-based weights used for giving importance to each feature in the fitness function. Experiments were conducted on the NSL-KDD dataset using the WEKA machine learning tool. It can be seen that the detection rate of R2L and U2R improves significantly with 86.2% and 95% enhancement in the second stage of classification. This paper also compares the proposed feature selection technique with the existing filter methods and inspects the accuracies of other classifiers.

Keywords: Intrusion Detection System · Anomaly detection · Machine learning · Naïve Bayes classifier · Genetic Algorithm

1 Introduction

With the advancement in network-based services and information transfer, it is highly imperative to provide security. An intruder masquerading as a legitimate user tries to steal information and compromise the security. According to [1], Intrusion Detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the integrity, availability and the confidentiality of information or to bypass the security mechanisms of a computer or network. With the ever-increasing dependence on information systems and the use of intra-network connectivity within the organizational network, an Intrusion Detection System (IDS) protects the system from threats. It raises alarms when any suspicious activity is found which can then be supervised upon by the network security administrator or the Intrusion Prevention System (IPS). With bulky

data commonly traversing across the network, the amount of alerts generated by these systems is very high. Moreover, these systems are not perfect in detecting attacks with increasing number of novel attacks found every day. They are also optimized with latest state of the art techniques [2, 3] to automate and mitigate the task of the security expert. The attacks considered for our proposed work are explained below,

Denial of Service (DoS). In this type of attacks, legitimate users are denied access to a particular resource or service. However, anomaly detectors can easily keep a track on these attacks since most of these attacks require analysing the temporal based features. Many packets will occur with a short period of time. It is the Distributed Denial of Service (DDoS) that is a cause for concern for security experts.

User-to-Root (U2R). A normal user trying to gain super-user privileges for malicious purposes. For example buffer overflow, loadmodule or by guessing the administrator password.

Remote-to-Local (R2L). A remote attacker who does not have access to the local machine tries to gain local access. For example, anomalies can be in the form of incorrect password guessing for more than 5 times, gaining FTP root directory access through FTP commands and writing malicious scripts so that users download them etc. These attacks are the most difficult to detect since they require a thorough inspection of the payload.

Probe Attacks. Stealth scanning and surveillance of the hosts on the network for open IP addresses and ports. They are not malicious in nature but network reconnaissance will help an attacker to gain insider information of the network.

2 Related Work

Over the last 10 years, there has been a flurry of research into machine learning algorithms' effectiveness at network traffic classification. This was due to a combination of static network classification techniques, which became outdated due to more dynamic IP addressing and the continued expansion of internet users and internet growth. Many of the works examine the effectiveness between varying machine learning techniques, comparing Naïve Bayes, bayes net, neural networks, C4.5, and others. Singh, et al., found that bayes net, combined with a correlation based feature selection algorithm, was the highest performing classifier [4]. However, this classifier struggled with long training times, but was still sufficient for near real-time classification. Limthong, et al., meanwhile found that k-nearest neighbors had the best performing accuracy, but were comparing it against a more limited set of algorithms, namely the Naïve Bayes model [5]. In both cases, the researchers collected their own data off a set of controlled ‘clean’ machines or through open access packet sniffing programs. We expand on these works by taking a deeper dive into the C4.5 algorithm [6] and by using a dataset that contains a high volume of ‘attack’ data as opposed to a heavy percentage of normal traffic. Li, et al. [7], and Casas, et al. [8], took an approach

focusing on decision tree classifiers, distributed machine learning algorithms, and random forest classifiers as compared to traditional intrusion detection techniques, such as part of application based.

3 Feature Selection Using Genetic Algorithm

The proposed feature selection technique is based on evolutionary computing. Genetic Algorithm [9, 10] combines the searching and evaluation of a feature subset thereby requiring no additional effort in finding the optimal subset for R2L and U2R attack class. Genetic Algorithm requires a set of initial solutions through which it can work with. These solutions are arbitrary and provided through the training dataset. Since, feature must be selected for each class; the initial solutions for GA are the set of R2L and U2R attack instances [11]. For calculation of feature subset for R2L attacks, the initial solutions are the 995 record connections whereas for U2R attacks, the initial solutions are the 52 records. Since feature number 2, 3 and 4 (protocol, service and flag respectively) are nominal values; they are removed from the algorithmic process and considered later on in the feature subset. The first step in a Genetic Algorithm is the encoding [12]. In the proposed approach, for each record connection, the value of a feature was converted to a bit binary gene value 1 or 0 indicating that a feature was selected or rejected respectively. If the value of the feature is non-zero, then the gene value is 1 otherwise it is 0. An ideal initial population size of about a 100 chromosomes gives a good solution to any optimization problem. Increasing the population size will only increase the computational overhead. However, since there are 8 attacks in R2L contributing to 995 record connections, it was necessary to consider each attack separately and find an approximate solution representing the aggregated feature subset for R2L attack class. Hence using each record connection as an initial solution is important. Population size for R2L attack = 995 and Population size for U2R attack = 52.

4 NIDS Using Two-Stage Classifier

The proposed methodology is built on two stages with the Naïve Bayes classifier as shown in Fig. 1. In the first stage, the filter is trained with all features present in the NSL-KDD dataset. The trained filter is tested against the test dataset consisting of 22544 records. The output of stage 1 classifier will be:

1. Records which are correctly classified. (actual class == predicted class).
2. Records which are misclassified. (actual class != predicted class).

In order to improve the detection rate of R2L and U2R attacks, the misclassified R2L and U2R records are applied to the next stage of filtering. It is expected that at least some incorrectly classified instances will be caught by the trained filter in the second stage. The second stage filter is trained for only R2L and U2R attacks and is run in parallel. Training is provided by dividing the training dataset into 2 classes:

1. For R2L attacks, training set is divided into classes: R2L and others.
2. For U2R attacks, training set is divided into classes: U2R and others.

The filter is trained with only the selected features from the proposed feature selection algorithm. It is tested against the misclassified instances obtained from stage 1.

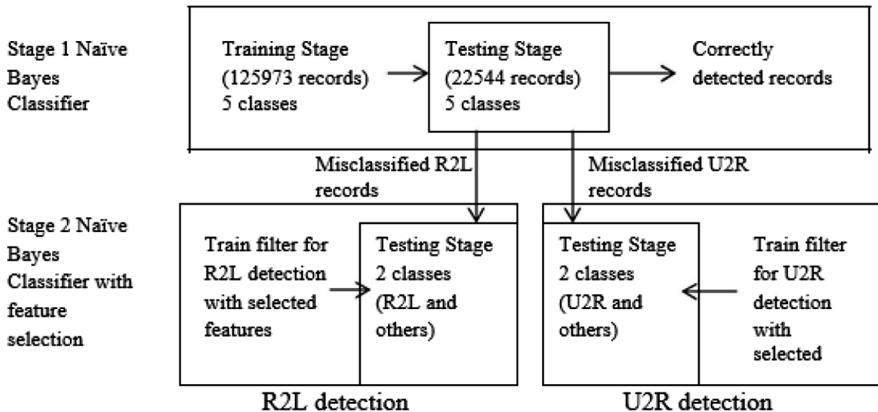


Fig. 1. NIDS two-stage classifier

5 Experimental Results

5.1 Dataset

The KDD99 cup dataset is a benchmark for testing many anomaly detection algorithms. Though it is mostly used by researchers, it suffers from several problems. On account of these problems, KDD99 is not a suitable dataset for research purposes. The NSL-KDD [13] is a dataset which solved the shortcomings [14] of its predecessor. The NSL-KDD dataset consists of 125973 records in the training set and 22544 records in the test set with WEKA [15], and each record connection having 41 features (or attributes) divided into four categories: Basic features (Features 1–9), Content Based features (Features 10–22), Time-based Traffic features (Features 23–31) and Host-based Traffic features (Features 32–41). The detailed names of the features are given in Table 1.

Table 1. List of features in datasetes

ID	Name	ID	Name
1	Duration	22	is_guest_login
2	protocol_type	23	Count
3	Service	24	srv_count
4	Flag	25	serror_rate
5	src_bytes	26	srv_serror_rate
6	dst_bytes	27	rerror_rate
7	Dos	28	srv_rerror_rate
8	wrong_fragment	29	same_srv_rate
9	Urgent	30	diff_srv_rate
10	Hot	31	srv_diff_host_rate
11	num_failed_logins	32	dst_host_count
12	logged_in	33	dst_host_srv_count
13	num_compromised	34	dst_host_same_srv_rate
14	root_shell	35	dst_host_diff_srv_rate
15	su_attempted	36	dst_host_same_src_port_rate
16	num_root	37	dst_host_srv_diff_host_rate
17	num_file_creations	38	dst_host_serror_rate
18	num_shells	39	dst_host_srv_serror_rate
19	num_access_files	40	dst_host_rerror_rate
20	num_outbound_cmds	41	dst_host_srv_rerror_rate
21	is_host_login		.

Each connection has a class label representing the attack type of the class and there are five attack types: Normal, DoS, U2R, R2L and Probe. In the NSL-KDD dataset there are 23 attack types belonging to these 4 classes with an additional 17 attack types in the test set. Table 2 all the different R2L and U2R attack types in the train and test set. Table 3 lists the number of records for each class.

Table 2. R2L and U2R attack types in the dataset

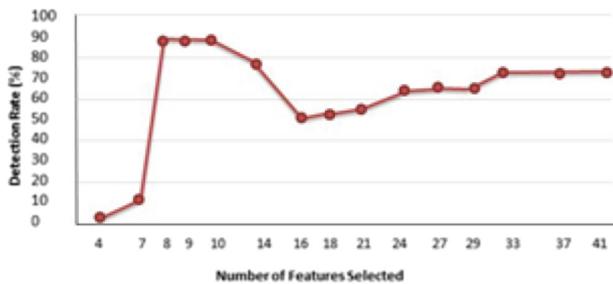
Attack Type	List of Attacks in Training Set	List of new Attacks in Test Set
R2L	FTP Write, Guess Password, Imap, phf, spy, multihop, warezclient, warezmaster	Sendmail, named, snmpgetattack, snmpguess, xlock, xsnoop, worm
U2R	BufferOverflow, Loadmodule, perl, Rootkit	Httpunnel, ps, xterm, sqlattack

Table 3. Number of records for each attack types

Class Type	Number of records in Training Set	Number of records in Test Set
Normal	67343	9711
DoS	45927	7458
U2R	52	200
R2L	995	2754
Probe	11656	2421
Total	125973	22544

5.2 Results

Analysing the trends in Fig. 3, the number of features selected to the detection rate of R2L attacks, it can be seen that the detection rate is maximum (88.6%) when 8 features are selected i.e. features 11, 22, 10, 9, 5, 1, 6, 23.

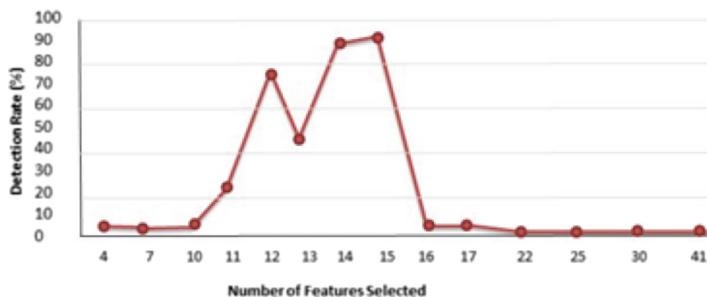
**Fig. 3.** Number of features selected by gain ratio vs detection rate of R2L

The detection rate climbs from a miserable 13.5% when 7 features are selected to a maximum of 88.6% with the addition of feature no. 23. Thereafter, with the addition of features in the order of relevance, the detection rate decreases steadily. When all the features are selected and the 2nd stage Naïve Bayes Classifier is tested, the detection rate is 72.14%. Hence, we conclude that when the classifier is trained to detect only R2L attacks in the 2nd stage, 72.14% of the misclassified records are detected correctly when all features are selected. The most important feature for R2L attack is found to be feature no. 23. i.e. count which advocates the conclusions obtained. The GainRatio AttributeEval + Ranker search feature selection technique is found to be better than the proposed algorithm for finding relevant features for R2L attacks. The accuracy of the proposed algorithm is 86.2% as compared to this technique which is 88.6%. The accuracy is 2.4% lower than GainRatioAttributeEval. Table 4 shows the number of U2R records detected correctly using a NB classifier in stage 2 using different selected features in the order of ranks.

Table 4. Number of records detected by NB classifier wrt features selected for U2R attacks

No. of feature selected	U2R records detected (out of 149)	Detection rate (%)
4	9	6.04
7	8	5.36
10	9	6.0403
11	37	24.83
12	119	79.86
13	74	49.66
14	135	90.60
15	140	93.95
16	8	5.36
17	8	5.36
22	1	0.6711
25	2	1.34
30	1	0.6711
41	1	0.6711

As shown in Fig. 4, the detection rate achieves maxima (93.95%) when 15 features are selected. i.e. 14, 18, 17, 9, 16, 13, 10, 1, 32, 5, 6, 33, 36, 23, 24. Thereafter, with the addition of features in the order of relevance, the detection rate dips to 5.36% when 17 features are selected and 0.6711% when all 41 features are selected.

**Fig. 4.** Number of features selected by gain ratio vs detection rate of U2R

The proposed approach for feature selection performs better in this case with the detection rate of 95%, almost 1.05% higher than GainRatioAttributeEval + Ranker algorithm. It detects 3 more U2R records correctly than GainRatioAttributeEval. In general, after the analysis of the results, it was concluded that a two-stage or a multi-stage classifier improves the detection rate as compared to a single stage classifier. Usage of feature selection at different stages even enhances the detection rate further. The proposed feature selection algorithm gives the best results for U2R attacks with the detection rate reaching 95% in the second stage. However, its detection rate is lower than the GainRatioAttribute evaluator which classifies 88% of the records correctly.

6 Conclusion

A novel two-stage Naïve Bayes classifier was proposed to enhance the detection rates of R2L and U2R attacks. Feature selection is the proposed solution to improve detection rates of R2L and U2R attacks. Meta-heuristic based evolutionary computing algorithm is used as the feature selection technique. Fitness function in GA is based on entropy based weight calculation. Feature selection is run over 300 generations to find 21 relevant features for R2L attacks and 22 relevant features for U2R attacks. Two-stage Naïve Bayes classifier is tested on the NSL-KDD dataset. NSL-KDD dataset was used since it removes the redundant records in the KDD99 dataset so that classifiers do not produce biased results towards the more frequent records. The second stage classifier is run in parallel to detect both attacks, thereby increasing speed of execution. The proposed method was compared with existing techniques, feature selection techniques were also compared. It can be seen that the proposed method is better than most other existing techniques, improving the detection rate significantly. Overall detection rate of the proposed algorithm is 86.2% for R2L attacks and 97% for U2R attacks. This is compared with the performance of backpropagation based neural networks and it is seen that the proposed method significantly improves results.

References

1. Liao, H., Lin, R.C., et al.: Intrusion detection system: a comprehensive review. *J. Netw. Comput. Appl.* **36**, 16–24 (2013)
2. Cano, J.: Cyberattacks-the instability of security and control knowledge. *ISACA J.* **5**, 1–5 (2016)
3. Hollingsworth, C.: Auditing from FISMA and HIPAA: lessons learned performing an in-house cybersecurity audit. *ISACA J.* **5**, 1–6 (2016)
4. Singh, K., Agrawal, S., Sohi, B.S.: A near real-time IP traffic classification using machine learning. *Int. J. Intell. Syst. Appl.* **5**(3), 83–93 (2013)
5. Limthong, K., Tawsook, T.: Network traffic anomaly detection using machine learning approaches. In: IEEE Network Operations and Management Symposium, Maui, HI, pp. 542–545 (2012)
6. Anon: Decision Trees – C4.5. <https://octaviansima.wordpress.com/2011/03/25/decision-trees-c4-5/>
7. Li, W., Moore, A.W.: A machine learning approach for efficient traffic classification. In: 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, Istanbul, pp. 310–317 (2007)
8. Casas, P., Fiadino, P., D'Alconzo, A.: Machine-learning based approaches for anomaly detection and classification in cellular networks. In: Network Traffic Measurement and Analysis Conference, TMA (2016)
9. Benaicha, S.E., Saoudi, L., et al.: Intrusion detection system using genetic algorithm. In: Science and Information Conference, pp. 564–568, London, UK (2014)
10. Pal, D., Parashar, A.: Improved genetic algorithm for intrusion detection system. In: Internationl Conference on Computational Intelligence and Communication Networks (CICN), USA, pp. 835–839 (2014)

11. Guo, Y., Wang, B., et al.: Feature selection based on rough set and modified genetic algorithm for intrusion detection. In: 5th International Conference on Computer Science & Education, China, pp. 1441–1446 (2010)
12. Hu, Y.J., Ling, Z.H.: DBN-based spectral feature representation for statistical parametric speech synthesis. *IEEE Signal Process. Lett.* **23**(3), 21–325 (2016)
13. NSL-KDD Dataset. <http://nsl.cs.unb.ca/NSL-KDD/>
14. Ibrahim, L.M., Basheer, D.T., Mahmood, M.S.: A comparison study for intrusion database (KDD99, NSL-KDD) based on Self-Organization Map (SOM) Artificial Neural Network. *J. Eng. Sci. Technol.* **8**, 1107–1119 (2013)
15. WEKA machine learning tool. <http://www.cs.waikato.ac.nz/ml/weka/>



Priority Queue Scheduling Approach for Resource Allocation in Containerized Clouds

Madhumathi Ramasamy^(✉), Mathivanan Balakrishnan,
and Chithrakumar Thangaraj

Department of CSE, Sri Ramakrishna Engineering College, Coimbatore, India
{madhumathi.r.mathivanan.bala,
chithrakumar.thangaraj}@srec.ac.in}

Abstract. Finding the appropriate resources and allocating them for executing software applications in cloud environments is very challenging because of its dynamic nature. Cloud service and resource providers do not render any performance assurance. Bare Metals, Virtual Machines and containers are being statically assigned to users' workloads. This leads to a lot of resource wastage. The dynamic allocation of resources is sorely missing in the current and conventional cloud centers. This paper tackles the problem of static resource allocation inside a cloud center for running heterogeneous applications in a high-performance manner. This specifically focuses on how to accurately identify the various resources such as the memory (RAM), the number of cores, the amount of storage, the input/output requirements, etc. and dynamically allocate the identified resources to execute the different tasks of workloads to ensure the mandated performance requirements. In this work, we have focused a priority queue scheduling (PQS) algorithm in cloud environment and fair share policies are defined at each queue to deal with the dynamic priority of the requests submitted by users. According to the dynamic priority of user requests, they are scheduled at two levels on the basis of their resource accessibility. The proposed scheduling algorithm hosts the containers on cloud nodes to utilize the resources in a well-organized manner and the performance is evaluated and compared with the conventional scheduling methods.

Keywords: Cloud computing · Resource allocation · Scheduling · Docker · Containers

1 Introduction

Cloud computing (CC) represents the IT industrialization. Tens and thousands of computing machines along with storage appliances and network solutions are being clubbed and centralized in order to enable enterprise computing in a distributed manner. Physical machines are partitioned into a collection of virtual machines and containers and on a need basis, virtual machines and containers are allocated for workload execution [1]. There are virtual machine monitors (VMMs) (alternatively touted as hypervisors) and the Docker platform for crafting and running virtual machines and containers. The hypervisor software mediates the access to the physical hardware. Similarly, the faster maturity and stability of the Docker platform has led to

the proliferation of containers, which is being proclaimed as the next-generation resource and runtime for micro services. The virtualization and containerization have opened a stream of fresh possibilities and opportunities. There is a need for dynamic provisioning of cloud resources in order to bring down the overall cloud costs. With an appropriate allocation of various resources for running workloads, there are other benefits also. That is, achieving higher performance in an affordable pricing delights cloud users and consumers [2, 3].

The paper is organized as follows. Section 2 deals with the related work, Sect. 4 describe the proposed model using priority based linear programming method. Section 5 reviews the experimental results and Sect. 6 concludes the paper.

2 Related Work

A number of resource allocation and scheduling algorithms have been made available in the literature. However, several research works have not considered about the memory (RAM) and CPU requirements to optimize the computing performance of VMs and containers. Therefore, a proper utilization of the expensive resources such as the available memory and CPU on the host machines is needed to ensure a better placement of the user requests and running workloads on proper VMs and containers.

The utilization of servers and consumption of the electric power has been investigated. The power consumption of the container host is estimated. The user's service requests, and the services available in the container host, are evaluated by units. The total cost was comparatively higher than the Docker Swarm scheduler. This can be integrated with the open-source orchestration framework container [4]. Bernstein introduced DOCKERFINDER, a prototype which provides multiple attributes for searching images [5]. These web-based cloud services are exposed for Cloud Portal (CP) execution.

ELASTICDOCKER makes container live migration and improves resource utilization for container providers. It also helps to reduce expenditures for customers [6]. Adam et al. used two-stage Stochastic Programming Resource Allocator (2SPRA) to reduce the total resources provisioned [7]. To minimize deployment cost in DCs application oriented Docker container (AODC) resource allocation framework was introduced. This method provides automatic scaling for cloud applications [8]. Morabito aimed to show the performance evaluation for container-virtualized instances for several low-power devices [9].

3 Problem Specification

3.1 Problem Formulation

Dynamic allocation of various resources such as memory and the processing core for the container creation on specific hosts is discussed. $R = \{r_1, r_2, \dots, r_n\}$ are the set of

resource instances available in a cloud system, where each r_j ($1 \leq j \leq n$) is an identifier of a specific resource.

The user sends a request with required memory which will not exceed the maximum capacity of any of the host nodes in the cloud system i.e. $r_{ui}(m) < (rs_i^0 + rs_i^1 + \dots + rs_i^n)$ and it is the same for the VCPU i.e. $r_{ui}(CPU) < (rs_i^0 + rs_i^1 + \dots + rs_i^n)$. The maximum resource utilized in all the hosts for all the requests is calculated as,

$$RU = \sum_{i=0}^m r_{ui} \quad (1)$$

Hence, the waiting time of the request is defined as by adding the time required for processing the accepted tasks in the queue with its service rate. That is,

$$W = W_q + \frac{1}{\mu} \quad (2)$$

$$W_q = \frac{L_q}{\lambda} \quad (3)$$

Where λ denotes mean arrival rate and μ denotes mean service rate. Average number of users in queue is denoted by L_q and W_q denotes the expected waiting time of the users.

The makespan of the task is the maximum time taken for the completion of all the tasks in a given application. If resources are assigned to requests of a queue with the FCFS scheduling individually regardless of fair-share policies, then the share assignment is not properly used. Hence, the fair-share policy is defined at queue level as in the form of,

$$\text{Queue_Fairshare} = \text{USER_SHARES}[[r_{ui}, \text{number_shares}], \dots] \quad (4)$$

Where, r_{ui} is the request from the user and `number_shares` denotes the number to indicate the share assignment to the r_{ui} . When each user request has come up with the different requirement at regular intervals, they are assigned with priority 'P' for getting the host instantly for container creation. Based on the availability of the memory (C_m) and the processing core (C_{CPU}), the priority has rated as low ' P_L ' or high ' P_H ' for all the requests. Initial placement of the container on any container host is to be done without any priority assignment since the resource availability is more for the first request. Then each upcoming request r_{ui} is placed at first level of queue as it has come with all resource requirements such as memory, CPU and disk size etc., when the request $r_{ui}(r_{ui}(m) \& r_{ui}(CPU))$ is put into the second queue as it need to assign either low or high priority according to both the user demand and current availability of the resources in the cloud system [10].

4 System Model

The cloud framework for allocation of containers to physical host nodes is shown in Fig. 1. The proposed system consists of a Node Performance Analyzer, container fair share scheduler and container Allocation Control Manager. This work considers an IaaS cloud system, which delivers a basic on-demand storage and compute capacities. These resources are provided in the form of containers, which are deployed in a provider's cloud center without the loss of generality. In the proposed cloud resource allocation mechanism, every provider has container scheduler software running in its cloud center. The container scheduler's role is to direct incoming instance requests to suitable compute nodes that in turn will serve the requests by launching and making available new containers. Based on the incoming user requests, the scheduling policy (fair-share) is defined. All the host state information has been sent to the compute nodes to take scheduling decisions periodically.

Algorithm 1: Queue Scheduling based on Requests

```

Input      : Requests  $r_{ui}, \dots, r_{ui}$  server s,  $s_{current}(C_m)$  &  $s_{current}(C_{CPU})$ 
Output     : Resources allocation results in terms of task
foreach  $r_{ui}$  in Queue  $Q^1$  do
    if not initial request then
         $s_{current} \leftarrow$  current available state of server by last n requests
    if  $s_{current} > r_{ui}$  then
        return priority  $\leftarrow Q^1(r_{ui})$ 
    else
        return  $Q^2 \leftarrow Q^1(r_{ui})$ 
    end if //  $s_{current} > r_{ui}$ 
    else
        return  $s_{current} \leftarrow$  current available state of server by new requests
    end if
end

```

4.1 Dynamic Priority Queue Scheduling Algorithm

The priority is allocated dynamically for all the user requests for adopting the changes in the resource state in the cloud environment using Load Sharing Facility (LSF). Here, only memory and the processing core of the host machines are considered. So, the priority assessment is done according to the changes in the memory and the processing core. Usually, the request's dynamic priority decreases once the request starts, and then it increases when the request turns to be an instance. In this work, both memory and the processing core based dynamic priority adjustment are implemented. Current availability of each server is calculated as $s_{current}(C_m) = C_m - r_{ui}(m)$ and $s_{current}(C_{CPU}) =$

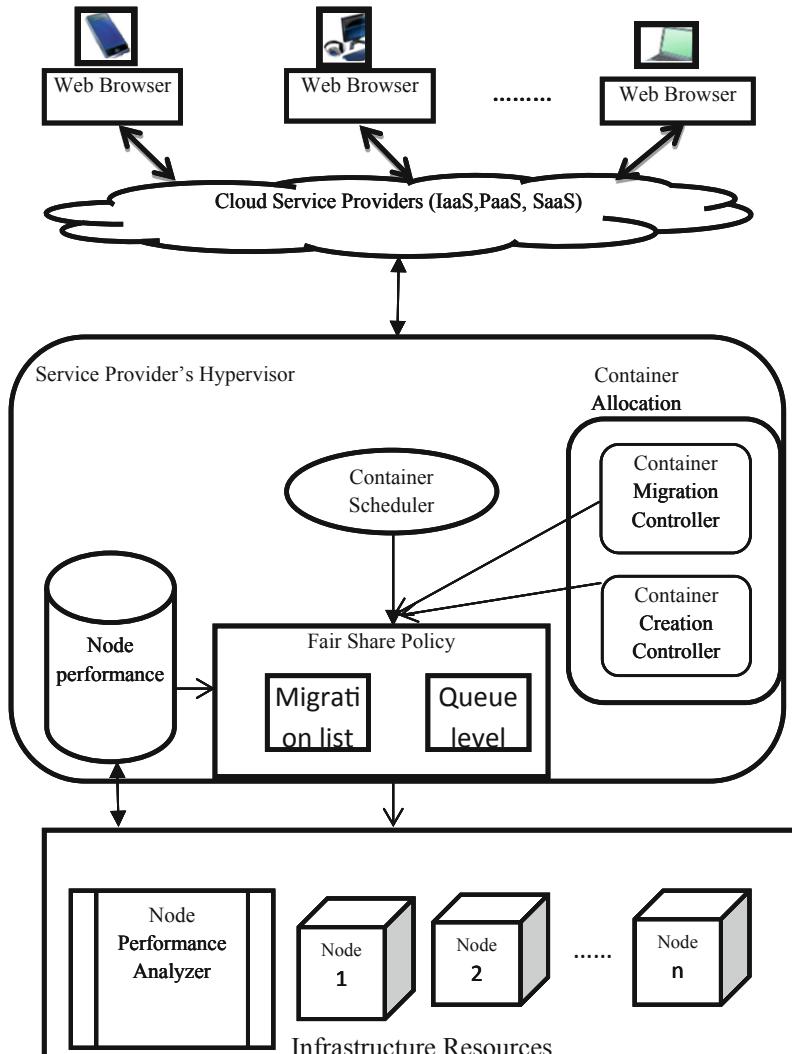


Fig. 1. System model for container allocation

$C_{CPU} = r_{ui}(CPU)$ respectively. The total number of request received by the server is denoted as $\sum r_{ui}$

$$fairshare_{finetune}(RAM) = (1 + r_{ui}) * \left(\frac{s_{current}(C_m)}{\sum r_{ui}} \right) / (r_{ui}(m) * r_{smax}) \quad (10)$$

$$fairshare_{finetune}(VCPU) = (1 + r_{ui}) * \left(\frac{s_{current}(C_{CPU})}{\sum r_{ui}} \right) / (r_{ui}(CPU) * r_{smax}) \quad (11)$$

$$fairshare_{finetune}(u) = fairshare_{finetune}(RAM) + fairshare_{finetune}(VCPU) \quad (12)$$

This algorithm automatically allocates resources as well as monitor infrastructure properties for an on-demand user request based on the fair share policies defined by the cloud infrastructure manager. Here PQ scheduler is aware of the present status of containers in the cloud and their communication to make scheduling decision appropriately.

Algorithm 2 : Priority Assignment Algorithm

```

Input:  $Q^2(r_{ui})$ 
Output: Low priority ( $P_L$ ) or High priority ( $P_H$ )
foreach  $r_{ui}$  do
    if  $r_{ui} < fairshare_{finetune}(u)$ 
         $r_{ui} \leftarrow P_H$ 
        return  $P_H$ (Request)
    else
         $r_{ui} \leftarrow P_L$ 
        return  $P_L(r_{ui})$ 
    endforeachPriority( $r_{ui}$ ) do
        if  $P_H$  then
            put[ $P_H$ ] inUpperLevelQueue( $Q^1$ )
        else
            put[ $P_L$ ] in SameLevelQueue( $Q^2$ )
        end if
    end
end if
end

```

5 Results and Discussions

The proposed model is simulated using ContainerCloudSim toolkit wherein the performances of the proposed Priority Queue approach and the existing algorithms are evaluated [11]. This tool provides basic classes that describe data center, virtual machine, computational resources and policies for scheduling and provisioning of resources. The tasks are submitted to the container for their execution. The bandwidth of the containers varies with respect to the system model. Existing scheduling algorithms such as First Come First Serve and Random Scheduling (RS) are considered for the evaluation of the proposed PQS technique.

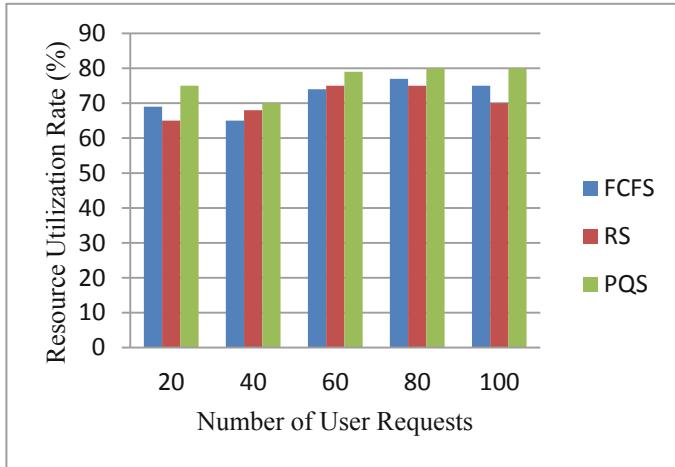
**Fig. 2.** Resource utilization rate

Figure 2 shows the resource utilization rate for the proposed and the existing scheduling algorithms. The resource utilization of PQS is high when compared to other scheduling algorithms. Moreover, the processing speed of containers is fully utilized in PQS due to the deployment of VM scheduler.

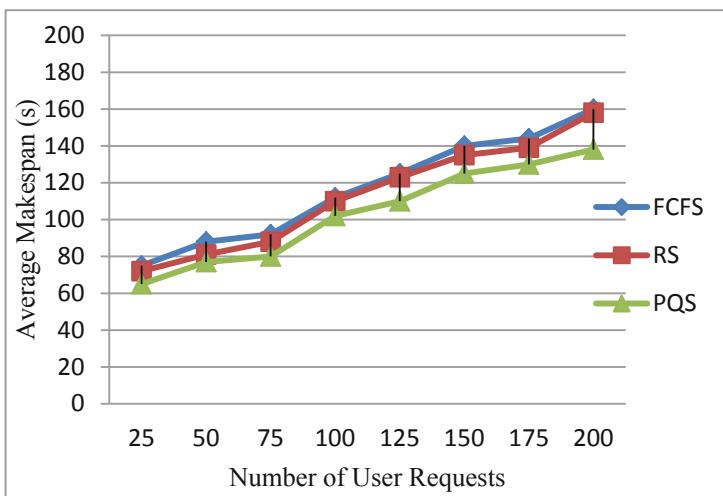
**Fig. 3.** Average Makespan for various methods

Figure 3 shows the average makespan of the various scheduling. It is clearly observed that, with the increase in the number of tasks, the average makespan also gets increased, but the average makespan of PQS approach is low when compared to FCFS and RS techniques.

6 Conclusion

The proposed PQS algorithm multiplexes virtual to physical resources relatively based on the varying needs. The main goal of this algorithm is to attain utilization of available cloud resources as much as possible. Both memory and the processing core are considered as cloud resources for the experimental purpose. The resources are utilized significantly with lesser response time and average makespan due to the efficiency of the proposed algorithm. The overall performance of the containerization is improved with the fair share technique. Extended PQ scheduler can be designed for processing both dependent and independent tasks.

References

1. Leivadeas, A., Papagianni, C., Papavassiliou, S.: Efficient resource mapping framework over networked clouds via iterated local search-based request partitioning. *IEEE Trans. Parallel Distrib. Syst.* **24**(6), 1077–1086 (2013)
2. Vasile, M.A., Pop, F., Tutceanu, R.I., Cristea, V., Kołodziej, J.: Resource-aware hybrid scheduling algorithm in heterogeneous distributed computing. *Future Gener. Comput. Syst.* **51**, 61–71 (2014)
3. Lee, Y.C., Zomaya, A.Y.: Energy-efficient resource utilization in cloud computing. *J. Supercomput.* **60**, 268–280 (2012)
4. Zhang, R., Li, M., Hildebrand, D.: Finding the big data sweet spot: towards automatically recommending configurations for hadoop clusters on docker containers. In: *IEEE International Conference on Cloud Engineering* (2015)
5. Bernstein, D.: Containers and cloud: from LXC to docker to kubernetes. *IEEE Trans. Cloud Comput.* **1**(3), 81–84 (2014)
6. Rosenblum, M., Garfinkel, T.: Virtual machine monitors, current technology and future trends. *IEEE Trans. Comput.* **38**(5), 39–47 (2005)
7. Adam, O.: Stochastic resource provisioning for containerized multi-tier web services in clouds. *IEEE Trans. Parallel Distrib. Syst.* **28**(70), 2060–2073 (2017)
8. Guan, X., Wan, X., Choi, B.-Y., Song, S., Zhu, J.: Application oriented dynamic resource allocation for data centers using docker containers. *IEEE Commun. Lett.* **21**(3), 504–507 (2017)
9. Morabito, R.: Virtualization on internet of things edge devices with container technologies: a performance evaluation. *IEEE Trans. Content Min.* **5**, 8835–8850 (2017)
10. Madhumathi, R., Radhakrishnan, R.: Priority queue scheduling approach for resource allocation in cloud. *Asian J. Inf. Technol.* **15**(3), 472–480 (2016)
11. Piraghaj, S.F., Dastjerdi, A.V., Calheiros, R.N., Buyya, R.: ContainerCloudSim: an environment for modeling and simulation of containers in cloud data centers. *Softw.: Pract. Exp.* **47**, 205–521 (2017)



Hybrid Evolutionary Approach for IDS by Using Genetic and Poisson Distribution

Riya Bilaiya^(✉) and Priyanka Ahlawat

Department of Computer Science and Engineering, National Institute of Technology, Kurukshetra, Kurukshetra, India
sweetriya.bilaiya@gmail.com

Abstract. As Intrusion detection system (IDS) are obvious class under safety layout, therefore it may manage capacity with support to determine safety points in a framework. Numbers of several system supports under intrusion detection. Given research studying distinguishing in middle of hybrid documents opening approach & mono approach. Primary objective of the research are representing i.e. with support to hybrid document opening approaches may minimize duration difficulty in process as compared to mono approach. Particular structures were certified with support to kdd'99 document pair. An observational outcome significantly describing i.e. hybrid approaches with support to GA & Poisson distribution may uniquely minimize structure practicing duration of the framework & balancing perfectness of detections.

Keywords: IDS · Data mining · Genetic algorithm · Poisson distribution · Intruder

1 Introduction

With simultaneous encapsulation of the Internet over the society, the Internet is lead to upgrade individuals living, study and Work standard. However, numerous security challenges that we face are winding up increasingly genuine. Step by step instructions to distinguish different system assaults, particularly unexpected assaults, is a certain key specialized issue. An Intrusion Detection System (IDS), a vast research accomplishment in the data security field, can distinguish an attack, which could be a progressing intrusion or an interruption that has just happened. As the beginning of twenty-first century, PC framework describing improving Updation in form of network efficiency, several hand holders & kind of operations which achieve on the system. As progressing accompanied by latest generation under comfortable machines for ex: Internet mobile, tabs, smart instruments i.e. updated machines & software also several calculating devices, no. connected hand holders progressing most & most. Therefore, safety on connection has been key process which support complete hand holders. Intrusion detection has been procedure in protecting intrusion. Process of going to a system unable to take agreement termed as intrusion. An intrusion detection technique may predict complete upcoming & on - going intrusion at a structure. Intrusion detection technique may investigate complete priority under safety procedure with the help of managing infrastructure movement. In fact, user interruptions are often

responsible for reporting problems, such as binary or multiclass problems, that is, the identification of network traffic patterns is either negative or abnormal, or classification problems of five categories, or not, whether it makes sense or not. of the other four attacks: Operational Dissociation (DOS), User to Citizens (U2R), Scanning (Sensing), and Root up to Local (R2L). In short, the main purpose of intrusion detection is to improve the class's accuracy to accurately detect intrusion behavior [1].

2 Intrusion Detection System

The Intrusion Detection System (IDS) is an important diagnostic or testing tool that uses traffic management systems, such as switching units, channels, light switches, and more. Most people use IDS to indicate ordering. At a time when people are using the call list or desktop operating system screen, they can monitor intrusions with IDS. For example, record systems and operating systems contain a large volume of knowledge and programs. Unexpected changes in records and records, especially those encountered, may be the result of the attack. The change may include alteration, creation or deletion of records and documents. The reason for such a failure may depend on who is changing it and where, when and how it goes. IDS is a PC operating system developed by PCs to access social injustice and systems to move forward with IT assets, split data, and respond to pre-defined security conditions [3]. Assault can be defined as movement of a job that requires trust, classification or resource availability of a system. The attack can be in many aspects, such as malicious, unwanted, and attempted attacks that seek to increase other benefits [4].

Intrusion Detection System working with various types such as Host Based, Network-based Hybrid and Distributed.

Host Based: In this type, the IDS mechanism was installed on the server system to monitor and audit the information received from the operating system to identify the intrusion. It can deal with the encrypted environment at the transport layer—no need for additional hardware.

Network-Based: In this type of IDS mechanism, observing the network traffic and application protocol activities between two systems. It is able to handle the attacks which are missed at Host Based model, Faster response and easy to deploy. Need full-time monitoring and unable to detect encrypted packets.

Hybrid Model: It is the combination of above to type's, i.e. Host and Network-based models. It uses mobile agents and combined anomaly and misuse based approaches. Log file checked by the mobile agent.

Distributed Type: Different IDS are combined by working as faraway sensors and generate a report about intrusion at the end send to a centralized system treated as distributed IDS. In this centralized model system able to monitor intrusion detection and responses. Able to analyze the incident and instant attack data.

3 Related Work

The first network intrusion detection system was developed in 1990 by Heberlein [14]. Particular research objective provides analysis of continuing interruption detection framework with support to hybrid approach i.e. document opening accompanied by flexible evaluating procedure. Numbers of several system applied under interruption found out procedure however every procedure are unable to become fully unique. Given published researches revised some published article related to the concept of interruption detection framework, procedures, & best fuzzy categorizers with support to hereditary code & document processing approaches that provides medium with support to the issues regarding interruption detection framework [1]. Additionally, a conversation on future information creativity & several approaches that assurance for progressing efficiency for computer framework in predicting interruptions are proffer [2, 3]. Given research describing observational outcomes under altogether approaches for ex: release, super charging & on analyzing the achievement accompanied by std. J-forty eight categorization code build under the categorization of ten % document pair. Benefits under altogether are analyzed accompanied by earn outputs [4]. Given articles also describes profits with support to anomaly detection recommend accompanied by exploitation found out procedure under finding unspecified interruption infrastructure. Under exploitation find out approaches, 4 dissimilar categorizers (Formula induction, baye, judgment tree & closest acquaintance) which support for find out acknowledged assaults. Although that codes got unsuccessful in finding out unspecified interruptions [5]. Main aim of published research has been primarily choose 10 categorization codes build according to his capacities for ex: velocity, build under the observational analysis, complete better outcomes under perfectness & F-score were collected by Random tree code, however large find out speed & below wrong signaling device speed was collected through formulation-One R, J48 & Random Forest codes [6] Device studying approaches are process with support to interruption detection. Under previous years, many procedure build for device studying codes which support to interruption detection framework although it is powerless under find out perfectness & duration also gap difficulty for continuation also with support to implemented application which choose a sub pair for categorizing that minimize duration difficulty & mind necessities. His approaches presenting up to 98% perfect & detection extent [7]. Given research with support to kmeans & NB to find out interruption [11, 12].

4 Proposed Methodology

This paper introduced a Hybrid Probabilistic intrusion detection system that encapsulate feature extraction with pattern detection and probabilistic classification model to identify intruder. Proposed methodology is based on framework i.e. shown in Fig. 1. In this framework initially data are acquired then similarity and negative feature are extracted. These negative and similarity feature act as key for pattern detection. Proposed framework use passion distribution to explore negative feature and examine intruder data in KDD 90 Cup data set.

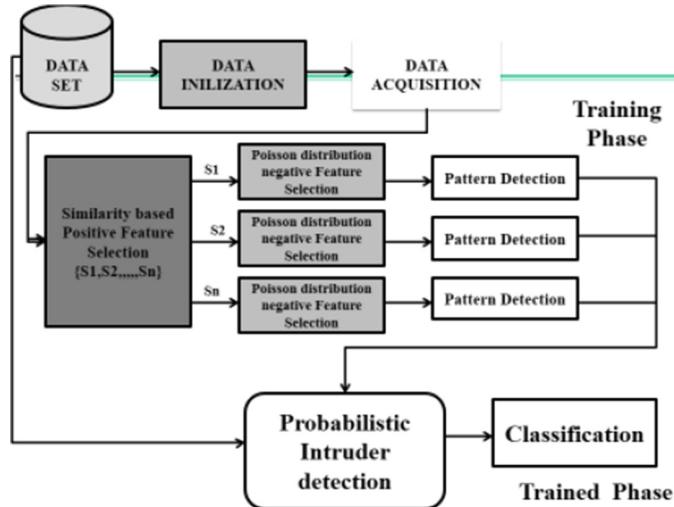


Fig. 1. Hybrid Probabilistic IDS framework

Proposed framework initialized with KDD 99 intruder data set with random partition for training then generate randomized negative feature for intruder in system. Then data acquisition lead passion distribution to extract negative feature for intruder. Passion distribution is recertifying negative feature through randomization. If relevancy of negative feature is high then its accepted otherwise ignore. If intruder detection have high false negative rate then whole process is initialed by random partition and if intruder detection have low true positive rate then new feature is generated on same partition.

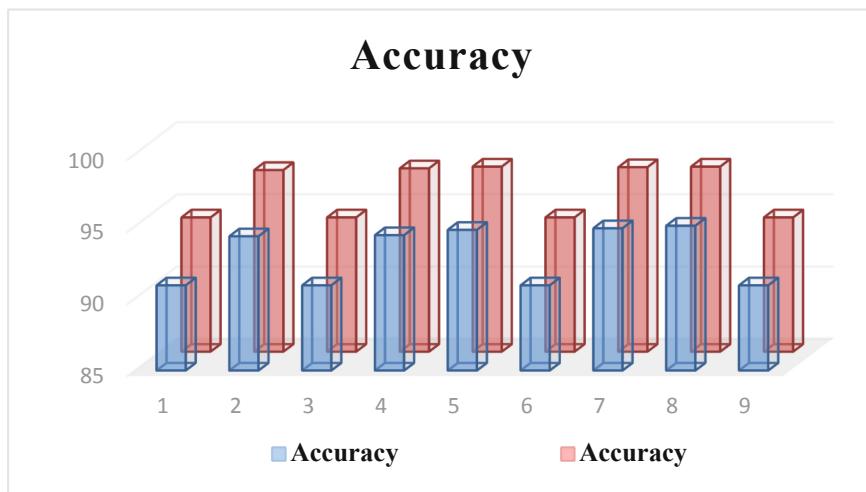
5 Exponential Setup and Result Analysis

In this paper performance evaluation is done over Matlab with 64-bit 10-bit windows, 8 GB of RAM and a 2.4 GHz Intel i3-4010U CPU. This data is from the MIT Lincoln Laboratory of the KDDCup99 Information Index. We selected a 10% message bank with a 494021 link directory, each directory with 41 locations, 7 parts represented, and a 34-bit unit to test based on the information's size. This message template has four types of intrusions: DoS, scanner, U2R, and R2L, for example. The IDS scanner model does not use the KDD Cup 99 data and the new test for CID is better. We used flour and 10% KDD CUP 99 in two ways to achieve normal information in the sample. Knowledge of these two approaches is given in Tables 1, 2, 3.

Performance of GA based IDS system is significantly bust-up after incorporate Poisson distribution with it. As shown in Fig. 2 proposed GA based PD lead the performance then GA alone.

Table 1. Comparison between Accuracy Rates

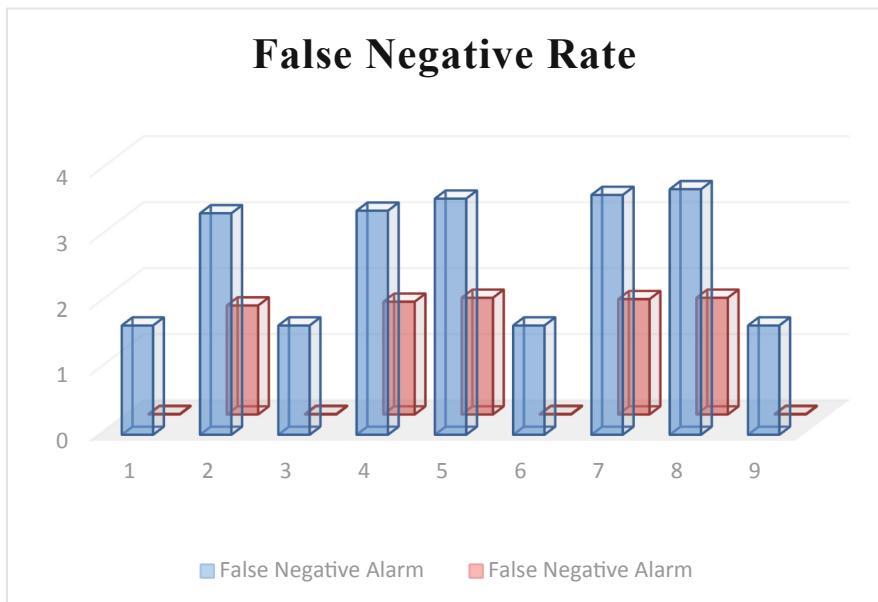
Data initialization rate	Accuracy (GA)	Accuracy (GA-poisson distribution)
0.1	90.92580	94.318111
0.2	94.32401	97.601720
0.3	90.92581	94.318111
0.4	94.40173	97.716320
0.5	94.76857	97.836310
0.6	90.92580	94.318111
0.7	94.88023	97.794040
0.8	95.05276	97.836310
0.9	90.92580	94.318111

**Fig. 2.** Accuracy Compersion

Along with that proposed GA + PD approach achieve higher true positive rate and lower false negative rate for IDS system over GA approach. Proposed framework acquire higher degree of filtering suspicious data that lead to improve performance as shown in Fig. 3 and Table 2.

Table 2. Comparison between FNR Rates

Data initialization rate	False negative alarm (GA)	False negative alarm (GA + PD)
0.1	1.65520	0.0087105
0.2	3.35431	1.6505200
0.3	1.65520	0.0087105
0.4	3.39313	1.7078200
0.5	3.57657	1.7678100
0.6	1.65520	0.0087105
0.7	3.63243	1.7466400
0.8	3.71866	1.7678100
0.9	1.65520	0.0087105

**Fig. 3.** Comparison between FNR Rates

Along with that proposed GA + PD approach achieve higher Detection rate for IDS system over GA approach. Proposed framework acquire higher degree of filtering suspicious data that lead to improve performance as shown in Fig. 4 and Table 3.

Table 3. Comparison between Performance Evaluations

Data initialization rate	Detection rate (GA)	Detection rate (GA + PD)
0.1	89.2706	94.3094
0.2	90.9697	95.9512
0.3	89.2706	94.3094
0.4	91.0086	96.0085
0.5	91.192	96.0685
0.6	89.2706	94.3094
0.7	91.2478	96.0474
0.8	91.3341	96.0685
0.9	89.2706	94.3094

**Fig. 4.** Comparison between Performance Evaluations

6 Conclusion

Intrusion detection is doing recognition acquire start picking up reliability in the network, a few techniques have thought about fulfilling the issue. IDS acquire accurate information and strategies they use to investigate this information. Every methodologies has benefits and impediments. Flawless following like impeccable security, isn't a reachable objective given the intricacy and advancement of a advance system. The exploration displayed in this paper is to examine the job of information mining calculations in an IDS. Test results demonstrate that the participation intrusion recognition show dependent on GA and Poisson distribution is better than the identification system with a solitary GA in term of time multifaceted nature.

References

1. Patel, A., Qassim, Q., Wills, C.: Survey of intrusion detection and prevention systems. *Inf. Manag. Comput. Secur.* **18**, 277–290 (2010)
2. Beigh, B.M., Bashir, U., Chahcoo, M.: Intrusion detection and prevention system: issues and challenges. *Int. J. Comput. Appl.* (2013)
3. Aung, Y.Y., Min, M.M.: A collaborative intrusion detection based on K-means and projective adaptive resonance theory, pp. 1575–1579 (2017)
4. Kulkarni, R.D.: Using ensemble methods for improving classification of the KDD CUP '99 data set. *IOSR J. Comput. Eng.* **16**, 57–61 (2014)
5. Syarif, I., Prugel-Bennett, A., Wills, G.: Unsupervised clustering approach for network anomaly detection (2012)
6. Alblawi, U., Suh, S.C., Kim, J.: Incorporating multiple supervised learning algorithms for effective intrusion detection (2014)
7. Choudhury, S., Bhowal, A.: Comparative analysis of machine learning algorithms along with classifiers for network intrusion detection. In: 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Chennai, pp. 89–95 (2015)
8. Ariaifar, E., Kiani, R.: Intrusion detection system using an optimized framework based on datamining techniques. In: 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, pp. 0785–0791 (2017)
9. Pal, S.: An integration of clustering and classification technique in software error detection. *Afr. J. Comput. ICT* **8**, 11–20 (2015)
10. Malviya, V., Jain, A.: An efficient network intrusion detection based on decision tree classifier & simple k-mean clustering using dimensionality reduction – a review. *Int. J. Recent Innov. Trends Comput. Commun.* **3**(2) (2015). ISSN 2321-8169
11. Foroushani, Z.A., Li, Y.: Intrusion detection system by using hybrid algorithm of data mining technique. *Int. J. Innov. Res. Electr. Electron. Instrum. Control. Eng.* **3** (2018). Special Issue 1
12. Rishabh, G., Soumya, S., Shubham, V., Swasti, S.: Intrusion detection system using SNORT. *Int. Res. J. Eng. Technol. (IRJET)*. e-ISSN 2395-0056
13. Suricata rules. <https://redmine.openinfosecfoundation.org/projects/suricata/wiki/SuricataRules>. Accessed 12 Jan 2019
14. Ghafir, I., Prenosil, V., Svoboda, J., Hammoudeh, M.: A survey on network security monitoring systems. In: IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, pp. 77–82 (2016). <https://doi.org/10.1109/w-ficloud.2016.30>



A Novel Approach to Overcome the Limitations of Power Iteration Algorithm Designed for Clustering

D. Jayalatchumy^{1(✉)}, P. Thambidurai¹, and D. Kadirvelu²

¹ Perunthalaivar Kamarajar Institute of Engineering and Technology,
Karaikal, India

d.jpkiet@gmail.com, ptdurai@gmail.com

² Sunshine Institution, Pondicherry, India

Abstract. The rise of Big Data has generated a new challenge to develop and refine algorithms to process and extract useful information. Power Iteration Clustering is the most efficient and scalable algorithms that can deal with larger datasets. It uses the power method for finding the eigen values and vectors. Despite its advantages the main disadvantage is that the convergence of this method relies on the magnitude of the leading eigen values that do not guarantee convergence. Moreover, it gives only one pseudo eigen value and it seems to be difficult when it is multideimensional. Hence, the algorithm has been refined using various acceleration techniques to make it more efficient to handle larger datasets. Various experiments was conducted to check its validity and it has been proved that the power method modified is efficient and suitable for processing larger datasets more accurately.

Keywords: PIC · Aitken · Steffensen · Banach fixed point · Cauchy theorem

1 Introduction

The advantage of the power method is that the eigen value is generated for every eigen vector. The eigen values are ordered and the largest eigen value becomes dominant. Power method in used as a solution in many practical problems and is more effecient. Unfortunately, this method do not work always. PIC is one of the powerful clustering machine learning algorithm that uses the power method to cluster larger datasets. The drawbacks of power method is its convergence depends on the magnitude of the highest eigenvalue and the next largest eigenvalue [9]. If the ratio is small then convergence become slow or even diverge. It generates a single pseudo eigenvalue and its difficult when its dimensionality is more than one. Its becomes complex in the case of many eigen values. So, acceleration techniques can be induced to make it more effective. Also, the error between the iterations has to be minimised leading to faster convergence.

Power Iteration Clustering. It's an algorithm that uses the power technique $v^{t+1} = cWv^t$ where v^t is the vector at the t^{th} iteration to find its eigen values [2] where W is Square matrix and c is the normalizing constant to keep v^t to become very large or small. The convergence of this technique relies on the magnitude of the highest

eigenvalue λ_1 and the magnitude of next highest eigenvalue. If the ratio is small then convergence can even fail on condition $|\lambda_1| = |\bar{\lambda}_1|$. It generates a single pseudo eigenvalue and its not easy for multidimension. It is more difficult for many eigen values. The power method uses a initial guess. PIC requires both the data matrix and the similarity matrix to fit into the memory and it is not feasible for big datasets. Its calculation and storage of larger matrices is itself a big challenge [1, 4]. Since PIC finds only a single eigen vector it can lead to inter collision problem.

Lin and Cohen in paper [1] have found that before v^t converge to the constant value, they first converge to local centers that relates the clusters. For a slowly convergent sequence, some acceleration techniques has to be induced to generate a new sequence that converges faster. Also, there is a need to deal with a sequence that converges slowly because it loses its effectiveness. Extrapolation techniques have paved a way for it, solving such problems by accelerating its convergence. Mostly, power method uses some displacement techniques for acceleration, but it is difficult since there is a need to know the amount of displacement. So, some quadratic extrapolation methods are being used to increase the convergence.

Aitken's Delta Square Method. It is a method that improves the convergence of any sequence that can converge linearly. Aitken's method is based on a recursive computation, in which each term in the sequence is found by three terms that is found using fixed point iteration. The advantage of this method is that it is very powerful and it can accelerate the linear convergent of any iterative sequence. Its convergence power can be increased by iterating it. The Aitken's method is induced to the power method to increase its speed. The Aitken's method is derived [6] for the following sequence for higher values of n.

$$\frac{x_{k1+1} - r}{x_{k1} - r} = \frac{x_{k1+2} - r}{x_{k1+1} - r} \quad (1)$$

Here r is the root or solution of $f(x) = 0$. Rewriting (1),

$$(x_{k1+1} - r)^2 = (x_{k1+2} - r)(x_{k1} - r) \quad (2)$$

On expanding (2),

$$r(x_{k1+2} + x_{k1} - 2x_{k1+1}) = x_{k1+2}x_n - x_{k1+1}^2 \quad (3)$$

Solving for r in (3),

$$r = \frac{x_{k1+2}x_n - x_{k1+1}^2}{x_{k1+2} + x_n - 2x_{k1+1}} \quad (4)$$

On adding and subtracting the same [9]

$$x_{k1+2}x_{k1} - x_{k1+1}^2 = x_{k1+2}x_{k1} - x_{k1+1}^2 + 2x_{k1+1}x_{k1} - 2x_{k1+1}x_{k1} + x_{k1}^2 - x_{k1}^2 \\ x_{k1}(x_{k1} - 2x_{k1+1} + x_{k1+2}) - (x_{k1}^2 - 2x_{k1}x_{k1+1} + x_{k1+1}^2)$$

Sub in (4) we get,

$$\hat{x}_{k1} = x_{k1} - \frac{(x_{k1+1} - x_{k1})^2}{x_{k1+2} - 2x_{k1+1} + x_{k1}}$$

This method depends on the recursive computation and it accelerates towards linear convergence, though it isn't accelerative for logarithmic convergent sequence. The convergence can be increased by iterating it continuously. The Aitken's method is embedded now to accelerate its convergence and the Aitken power. The pseudo code for Aitken Power Iteration Clustering is shown in Algorithm 1. The advantage of quadratic extrapolation is that the first eigenvalue is kept to be one to find the other eigenvectors of the next iterations. This can be obtained using power method [3].

```

function  $x_k$ =Aitken power Method ( )
{
     $x_0=\vec{v}$ ;
     $k1=1$  ;
repeat
     $x_k = Wx_{k1-1}$ ;
     $\delta_t = ||x_{k1} - x_{k1-1}||$  ;
    // $\vec{x}_k$ =Aitken( $\vec{x}_{k1+2}$   $\vec{x}_{k1+1}$ , $\vec{x}_{k1}$ )
    // Calculate  $x_0, x_1, x_2$  using any linear iteration method
     $\vec{x}_{k1} = x_{k1} - \frac{(x_{k1+1} - x_{k1})^2}{x_{k1+2} - 2x_{k1+1} + x_{k1}}$  ;
     $k1 = k1 + 1$ ;
     $\delta_t = ||\delta_t - \delta_{t-1}||$  ;
Until  $\delta_t \approx 0$ ;
}

```

Algorithm 1. Aitken Power Iteration Clustering

2 Steffesen Power Iteration Clustering Algorithm

The fixed point iteration [11] determines the fixed point of any function. It finds the roots and converges to any fixed point. This technique can be applied to fixed point iterative methods for any nonlinear equations. The Aitken's method accelerates the linear convergence of an iterative sequence. It does not accelerate the logarithmic convergent sequence. A combination of fixed point iteration and the Aitken's method leads to Steffensen's method [7] and when induced in the power method leads to Steffensen PIC. Steffensen's method is the method of applying Aitken's acceleration to the second iteration of fixed point method [13]. The properties of Steffensen's method [14] are that it has two function evaluation and a complicated algebraic expression without any derivative. To guarantee quadratic convergence in Steffensen's method, the function f is continuously differentiable three times. The pseudo code for

Steffensen PIC is shown below in Algorithm 2.

```

function  $\vec{x}^k = \text{Steffensen Power Method}()$ 
{
     $x_{(0)} = \vec{v}; k1 = 1;$ 
repeat
     $x_{(k1)} = Wx_{k1-1};$ 
     $\delta_t = ||x_{k1} - x_{k1-1}||;$ 
    // function  $\vec{x}_k = \text{Steffensen}(\vec{x}_{k1+2}, \vec{x}_{k1+1}, \vec{x}_{k1})$ 
     $x_{k1+1} = g(x_{k1}); \vec{x}_{k1} = x_{k1} - \frac{(x_{k1+1} - x_{k1})^2}{x_{k1+2} - 2x_{k1+1} + x_{k1}};$ 
    //Restart fixed point Iteration with the computed values
     $k1 = k1 + 1;$ 
     $\delta_t = ||\delta_t - \delta_{t-1}||;$ 
Until  $\delta_t \approx 0;$ 
}

```

Algorithm 2. Steffensen PIC

3 Proposed Steffesen Power Iteration Clustering Algorithm

This algorithm is based on the Banach fixed point theorem to overcome the drawbacks of the proposed algorithm. The drawback of Steffensen's method lies in choosing the value of x_0 , which, if not chosen precisely, can even lead to divergence. To overcome this drawback, we apply the Banach fixed point theorem [8, 12] guaranteeing the procedure of iterating a function yields a fixed point if it is satisfied.

```

function  $\vec{x}_k = \text{Modified Steffensen Power Method}()$ 
{
    pick initial vector  $v_0$ ;
     $x_0 = \vec{v};$ 
repeat
     $x_{k1} = Wx_{k1-1};$ 
     $\delta_t = ||x_{k1} - x_{k1-1}||;$ 
    // choose the Cauchy sequence
    function  $\vec{x}_{k1} = (\text{Steffensen}(\vec{x}_{k1+2}, \vec{x}_{k1+1}, \vec{x}_{k1}))$ 
     $x_{k1+1} = g(x_{k1});$ 
    // convert to the Cauchy sequence
     $x_{k1+1} = g(x_{k1}) = \cos(x_{k1});$ 
     $\vec{x}_{k1} = x_{k1} - \frac{(x_{k1+1} - x_{k1})^2}{x_{k1+2} - 2x_{k1+1} + x_{k1}};$ 
     $\delta_t = ||\delta_t - \delta_{t-1}||;$ 
    increment  $k1;$ 
until  $\delta_t \approx 0;$ 
}

```

Algorithm 3. Modified Steffensen PIC.

The Banach fixed point theorem is performed by choosing a Cauchy sequence. Cauchy sequence [10] is a sequence where its elements become arbitrarily close to each other as the sequence progresses. The iteration sequence for a function starting at any value of x_0 will converge to a fixed point of Cosine [15]. Hence, we choose a sequence $x_{n+1} = \cos(x_n)$ that converges to the distinct fixed point of the function $f(x) = \cos(x)$ for any starting point x_0 . The pseudo code for Modified Steffensen PIC is shown in Algorithm 3. The three algorithms have been evaluated using five criteria namely (1) Efficiency (2) Number of iterations (3) Error rate (4) Relative error and (5) Accuracy to analyze the rate of convergence achieved using different datasets.

The efficiency of the algorithm is measured in terms of its execution time. Let $T(n)$ be the number of units of time taken by an algorithm of size ‘ n ’. The running time is proportionate to the input size on which it is run. Based on the concept of linear running time the algorithm has been analyzed for inputs of varying sizes. Iteration is done to improve the accuracy of the algorithm since, it is the process of continuously calculating the function over the value of a fixed point. The comparison of number of iterations vs. execution time is shown in Fig. 1a., the number of iterations in Fig. 1b. The running time is computed with the input of varying sizes along X - axis and execution time in seconds and number of iterations along Y - axis.

Table 1. Comparison of Iterations and Execution time of Aitken PIC, Steffensen PIC and Modified Steffensen PIC with PIC.

Dataset (Grid in square matrix form)	PIC		Aitken PIC		Steffensen PIC		Modified Steffensen PIC	
	No. of iterations	Execution time (sec)	No. of iterations	Execution time (sec)	No. of iterations	Execution time (sec)	No. of iterations	Execution time (sec)
2	19	2.33	8	1.738	6	0.978	5	0.812
3	22	4.366	13	2.11	10	1.407	8	1.3
5	24	4.079	10	2.783	10	1.95	10	1.973
7	28	3.986	17	2.175	14	2.1	12	1.75
10	32	6.778	22	4.384	18	2.719	16	1.8
20	39	8.326	26	6.982	22	4.491	21	4.593
50	48	13.243	37	10.372	33	8.021	31	7.95

Table 1 and Fig. 1 infers that for a given dataset of varying grids, power method takes approximately 6.2 s, Steffensen power method takes about 3.1 s and Modified Steffensen PIC takes only 2.8 s. The performance of Modified Steffensen PIC is improved by 54.9% when compared to PIC. Since, the execution time decreases, performance increases attaining higher efficiency. The Modified PIC effectively decreases the iterations of PIC at the rate of 52% and the convergence error is determined since the difference among the iteration has an impact on its convergence.

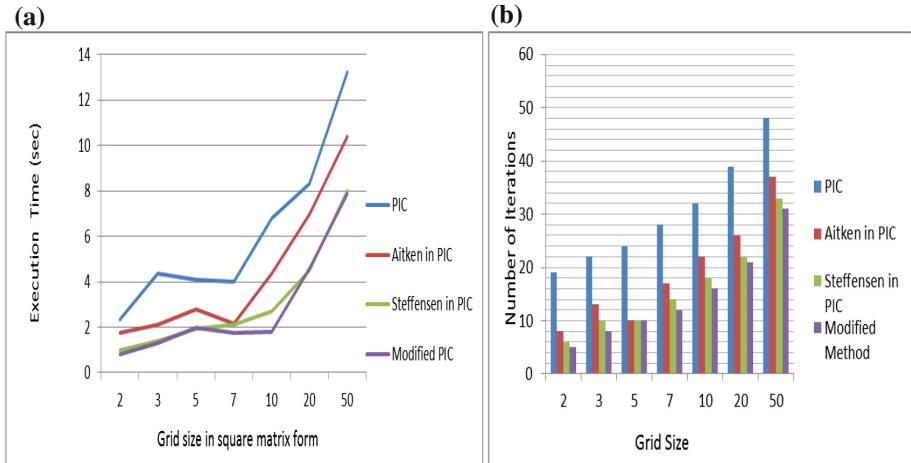


Fig. 1. a. Execution Time. b. Number of Iterations

Error Analysis. The three types of errors are [5] namely (1) Round off errors that occur due to finite arithmetic precision, (2) Convergence error that is given as the difference between the exact and iterative solutions which can be reduced by residual tolerance. (3) Truncation error that results from the neglected terms in the Taylor series. Here, the convergence error is determined since the difference between the iteration has an impact on its convergence. It is the difference between the exact and iterative solutions. Errors can be calculated from both scalars and vectors. The fixed point iteration converges linearly with the order in which they occur, hence they are asymptotic errors. The errors in scalar are measured using the absolute error $|\hat{\alpha} - \alpha|$ and by the relative error $\frac{|\hat{\alpha} - \alpha|}{\alpha}$ if α is non zero. The errors in the vectors are measured by the size or the norm of the vector. Norm is the magnitude of the largest component, $\max_{1 \leq i \leq n} |x_i|$, denoted as

$$\|A_x\| = \max_{1 \leq i \leq n} \sum_{j=1}^n |a_{ij}|.$$

Here, A is the $m \times n$ matrix and $\|A\|$ is norm A . The error values are found. The formula for Aitken error is given as,

$$\alpha - x_n \approx \frac{\lambda_n}{1 - \lambda_n} (x_n - x_{n+1}) [16], \quad \lambda_n = \frac{x_n - x_{n+1}}{x_{n-1} - x_{n-2}}$$

The error rate using Aitken's error estimation is found to be 33% for PIC, 24% for Steffensen PIC and 10% for Modified PIC. It is observed from the results that the error rate of applying Steffensen's power method is less when compared to the power method. (i.e.) The error rate in modified PIC has been reduced by 14% when compared

to Steffensen and by 23% when compared to PIC. The relative error gives the normalized difference between the two values. The relative error tolerance for all the error values has also analyzed. It has been found that the error value is less than the error tolerance. Since, the error value is the less than the error tolerance the amount of error obtained is tolerable. Hence, the results are more accurate as the value of the error itself is almost very less. From the results obtained it is inferred that applying Aitken's and Steffensen's method to PIC accelerates its convergence leading to better performance. Also, applying Bananch Fixed point to Steffensen PIC guarantees convergence. This property of modified Steffensen method gains importance and can be used in all Steffensen type methods to achieve best results.

4 Conclusion

The growth of data is being increasing day by day. Extracting and processing these data need efficient algorithm which is not feasible using existing data mining techniques. Hence PIC is refined using acceleration techniques to overcome its drawback and make it more efficient. The drawback of this refined algorithm is also identified and is overcome using Banach theorem. The developed algorithm is now tested for its convergence and applicability for larger datasets.

References

- Lin, F., Cohen, W.: Power iteration clustering. In: Proceedings of the 27th International Conference on Machine Learning, Haifa (2010)
- Jia, H., Ding, H., Xu, X., Nie, R.: The latest research progress on Spectral Clustering. *J. Neural Comput. Appl.* **24**(7–8), 1477–1486 (2014)
- Kamvar, S.D., Golub, G.H., et al.: Extrapolation methods for accelerating PageRank computations. In: Proceedings of the 12th International Conference on the World Wide Web, pp. 261–270. ACM (2003)
- Yan, W., et al.: p-PIC: parallel power iteration clustering for big data. *J. Parallel Distrib. Comput. Models Algorithms High Perform. Distrib. Data Min.* **73**(3), 352–359 (2013)
- Eyi, S.: Convergence error estimation and convergence acceleration in iteratively. In: Proceedings, Eyi Convergence EE (2012)
- Collomb, C.: A tutorial on the Aitken convergence accelerator
- https://en.wikipedia.org/wiki/Steffensen%27s_method
- https://en.wikipedia.org/wiki/Banach_fixed-point_theorem
- HELM (Helping Engineers Learn Mathematics) Workbooks: Eigenvalues and eigenvectors, Helping Engineers Learn Mathematics, Loughborough (2008)
- https://en.wikipedia.org/wiki/Cauchy_sequence
- Lambers, J.: Fixed Point Iteration. Fall (2009). <http://www.math.usm.edu/lambers/mat460/fall09/lecture9.pdf>
- Rousseau, C.: Banach fixed point theorem and applications (2010). <http://dmuw.zum.de/images/b/bd/Banach2.pdf>
- Lambers, J.: Accelerating Convergence. Numerical Analysis I. Lecture 13 notes MAT460/560 (2009). <http://www.math.usm.edu/lambers/mat460/fall09/lecture13.pdf>

14. Cordero, A., Hueso, J.L., et al.: Steffensen type methods for solving nonlinear equations. *J. Comput. Appl. Math.* **236**, 3058–3064 (2012)
15. <https://math.stackexchange.com/questions/1139021/prove-cosn-does-not-converge-as-n-tends-to-infinity>
16. <http://homepage.divms.uiowa.edu/~whan/3800.d/S3-4.pdf>



Design of Reliable Dense Wavelength Division Multiplexing System for Metropolitan Area Network

K. Sheela Sobana Rani¹(✉), R. Gayathri¹, R. Lavanya¹,
and K. Uthayasuriyan²

¹ Sri Ramakrishna Institute of Technology, Coimbatore, Tamilnadu, India
visitgayathri@gmail.com, yuvsheka@gmail.com

² Sri Manakula Vinayagar Engineering College, Pondicherry, India

Abstract. The optical fiber technology based on the dense wavelength division multiplexing is capable of concurrently transmitting multiple streams of information utilizing a single optical fiber. So this paper details the conception of the networking that is based on the optical transport and multiplexing obtained by the dense wavelength division to enhance the performance of the network. The detail explanation in the paper includes the perception for the optical networking such as the components of the dense wavelength division multiplexing, the components, configuration and the designing of the network along with the routing and the conversion of the wavelength. The rapid growth and the usage of the transport network that overlays on the concept of the dense wavelength division multiplexing enables the proposed system to pave way for meager cost for the deployment by modifying the high scaling traffic entailments. The **DWDM** is further structured with the point to point and a linear topology system utilizing the optical-system to examine the BER under return to zero (RZ) and non-return to zero (NRZ). The forward error correction is utilized to heighten the scalability of the system in the case of the real time implementation. The validation of the system and the results acquired based on the simulation and the comparison from the linear and the point to point topology show that the proffered method ensures the network to cover maximum area with the heightened bandwidth. More over the results acquired evince the performance of the network on the grounds of latency, throughput, availability, redundancy and security.

Keywords: DWDM · Point to point topology · Linear topology · RZ and NRZ modulation

1 Introduction

The explosive usage of internet, increase in data traffic and different forms of data usage has reflected upon the need to improve the bandwidth requirements of wireless communication systems. There is a need for modern communication networks to be able to accommodate the evolving requirements. In these situations optical networks offers higher capacity and a common infrastructure with lesser undesirable effects.

These factors drive the deployment of optical fibers in high speed, high capacity telecommunication networks. Low cost telecommunication and data services now drive the demand for larger bandwidth systems, deploying a new fiber is a costlier option whereas a much viable option is to improve upon the existing network to meet the ever growing demands. In order to increase the bit rate to high data speeds TDM Concepts are used, but complexity, large transmission power, cost and non-linear effects pose as limitations. On the contrary multiplexing multiple wavelengths on a single mode fiber is achieved by Wavelength Division Multiplexing (WDM) where the optical signals to be transmitted are assigned specific lambdas of light within a band of 1530 nm to 1610 nm, a tuner is used to de-multiplex the appropriate signal at the receiver. Dense Wavelength Division Multiplexing is another degree of WDM in which multiplexing of transmitted signals is done with lesser spacing of 0.8/0.4 nm. DWDM also presents notable advantages such as amplification of light signals on the whole, protocol independent multiplexing and ability to carry signals at different speeds. A single optical fiber with this DWDM can reach 400 Gb/s and this can also be increased with increasing channels.

2 Literature Study

Aloisio et al. (2010) proposed the dense wavelength division multiplexing network data transmission system which is used in NEMO underwater neutrino telescope. The parameters like bit error rate and signal to noise ratio measurements at 800/s rate is measured. The network design is tested with NEMO experiment boar. Lai (2005) proposed the transport system based on vertical-cavity surface-emitting lasers injection-locked technique where the bit error rate performance is improved. Fukai et al. (2005) proposed the distributed system undergoing raman amplification transmission characteristic in an optical fiber. By considering nonlinear impairments and signal-to-noise ratio (SNR) characteristics an analysis is made between optical fiber parameters and DRA transmission. Jansen et al. (2006) proposed a system with chromatic dispersion compensation for WDM 40-Gb/s long-haul transmission using OPC system. Here both mixed data rates and mixed modulation formats are used for transmission. By adding an OPC unit to a transmission line using dispersion compensating fiber there is an increase in transmission data rate.

Tonguz et al. (2002) suggested an approximate method for the prediction of power and SNR equalization schemes by applying dense wavelength division multiplexing light wave systems employing EDFA cascades. A comparison is made with two equalization strategies with the maximum number of amplifiers which shows a better equalization. Suzuki et al. (2006) proposed a wavelength division multiplexing transmission systems without dispersion compensation on DWDM technologies with high-wavelength stability. Askarian et al. (2010) improved survivability of the network through a cross layer techniques by decreasing both the blocking probability and the vulnerability of the network to failures.

Huang et al. (2007) proposed a design that is dispersion-free interleaver with inclusion of optical delay lines by pointing the zeros in the transfer function. To achieve bidirectional DWDM transmission the design of interleaver pairs is implemented for return-to-zero DPSK and non-return-to-zero DPSK modulation formats. Gamage et al. (2007) proposed a scheme with upstream transmission using a SOA for Arrayed Waveguide Grating (AWG)-based on dense wavelength-division-multiplexed to improve carrier-to-sideband ratio in the downlink with an yield in improved power budget for the uplink.

3 Practical Design Considerations for DWDM Network

3.1 Estimation of λ Through a Surveyed Data

The estimation of λ plays an important role in DWDM network. So, the optical fiber communication link is carried out for dense wavelength division multiplexing network by considering the number of users and traffic rate. Capacity is obtained for the cost of the equipment, and fiber plant investment is retained. The estimation of λ is taken for various cities like A, B, C and D. For land line users, mobile users, data services, video services λ is estimated. The below Table 1 shows the statistical data collected from four cities.

Table 1. Shown surveyed data of four cities for the estimation of λ

Cities	λ Estimation for land line user		λ estimation for mobile user		λ estimation for land line data services		λ estimation for mobile data services		λ estimation for video services	
	Population	BW (Gbps)	Population	BW (Gbps)	Population	BW (Gbps)	Population	BW (Gbps)	Population	BW (Gbps)
City A	22065	1.4	29420	1.8	7355	35	14710	65	4413	44
City B	11956	0.7	15941	1	3985	19	7970	39	2391	23
City C	12183	0.7	16244	1	4061	20	8122	40	2436	24
City D	12847	0.8	17179	1	4282	16	8564	31	2569	18

For city A the expected total bandwidth required for the whole services is 156 Gbps. Depends on the standard, for 10 Gbps bandwidth the lambda requirement is 1λ . Therefore the required lambda for city A is 14λ . For city B the expected total bandwidth required for the whole services is 82 Gbps. Depends on the standard, for 10 Gbps bandwidth the lambda requirement is 1λ . Therefore the required lambda for city B is 8λ . For city C the expected total bandwidth required for the whole services is 85 Gbps. Depends on the standard, for 10 Gbps bandwidth the lambda requirement is 1λ . Therefore the required lambda for city C is 8λ . For city D the expected total bandwidth required for the whole services is 65 Gbps. Depends on the standard, for

10 Gbps bandwidth the lambda requirement is 1λ . Therefore the required lambda for city D is 6λ . Depends on the customer usage and needs λ is estimated as 36λ . From the analysis it is observed that there is a large demand in the bandwidth specifically for data centric communications.

3.2 Point to Point DWDM Network Design

Point-to-point transmission system is shown in figure below. A laser array is used the transmitter end as the signal source. They are used to set predetermined wavelengths with fixed channel parameters set by the International Telecommunication Union (ITU) standard and has adapted a standard to specify standard frequencies which is used to identify WDM channels. It spans over the 1555 nm C-band (Fig. 1).

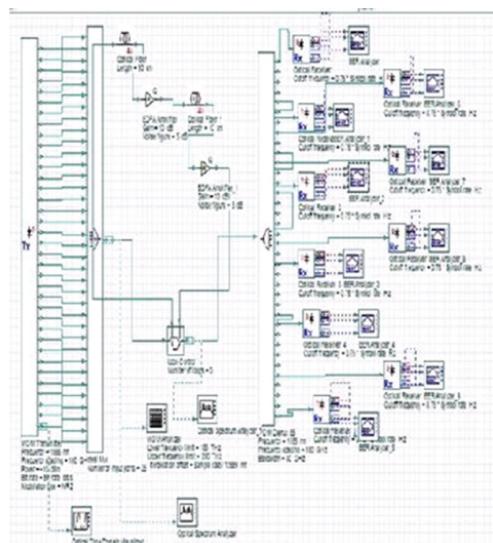


Fig. 1. Design of point to point DWDM Network

Table 2 shows the components and their standard values used in designing a point to point topology.

Table 2. Point to Point Topology Components and their properties

Name	Value
<i>WDM Transmitter</i>	
Frequency	1555 nm
Frequency Spacing	150 GHz
Power	-10 dBm
Extinction ratio	30 dB
Line width	0.1 MHz
No of O/P ports	36
<i>Single Mode Fiber</i>	
Dispersion Coefficient	16 Ps/(nm-Km)
Dispersion Slope	0.076 Ps/(nm ² -Km)
Non Linear Coefficient	0.35 1/(Km.W)
Linear Loss	0.2 dB/Km
Length	50 km
Attenuation	0.5 dBm
<i>Erbium Doped Fiber Amplifier</i>	
Mode of operation	Gain Control
Gain	10 dB
Power	15 dBm
Noise figure	5 dB

3.3 Design of DWDM Network Using Linear Topology

The selection of a suitable modulation format plays a major criteria for the efficiency of the optical system to achieve higher transmission rate. To encode optical pulses in optical networks RZ and NRZ is used and compared.

3.3.1 NRZ Modulation-Linear Topology

Figure 2 represents the design of DWDM network using linear topology under NRZ Modulation.

The signals from the WDM transmitter is send to the multiplexer unit through the fiber channels. The multiplexer synchronizes each input signal and send to the channel for amplification through a booster and power amplifier. Depending on the customer usage the signal is varied in the substations. Figure 3 shows the interior view of subsystem.

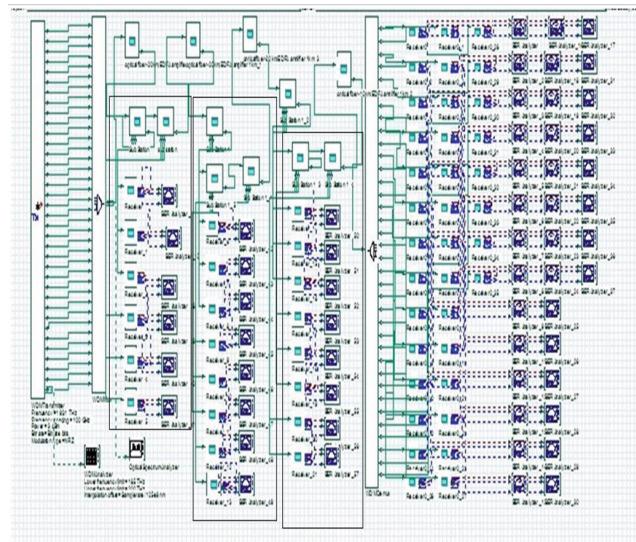


Fig. 2. Design of linear NRZ DWDM network

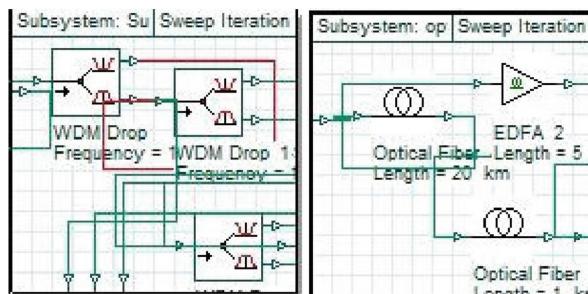


Fig. 3. Subsystems interior view

Add-drop multiplexer is needed for each substation which depends on the requirements of substation components. Table 3 shows the various EDFA amplifier, optical fiber cable and transmissions attributes of WDM transmitter.

Table 3. Linear Topology (NRZ) components and their properties

Name	Value
<i>Transmitter</i>	
Frequency	1555 nm
Frequency Spacing	100 GHz
Power	-5 dBm
Extinction ratio	30 dB
Line width	0.1 MHz
No of O/P ports	36
<i>Single Mode Fiber</i>	
Dispersion Coefficient	16 Ps/(nm-Km)
Dispersion Slope	0.076 Ps/(nm ² -Km)
Non Linear Coefficient	0.35 1/(Km.W)
Linear Loss	0.2 dB/Km
Length	50 km
Attenuation	0.5 dBm
<i>Erbium Doped Fiber Amplifier</i>	
Operation mode	Gain Control
Gain	10 dB
Power	15 dBm

3.3.2 RZ Modulation-Linear Topology

Figure 4 shows the dense wavelength division multiplexing network using linear topology under RZ Modulation (Table 4).

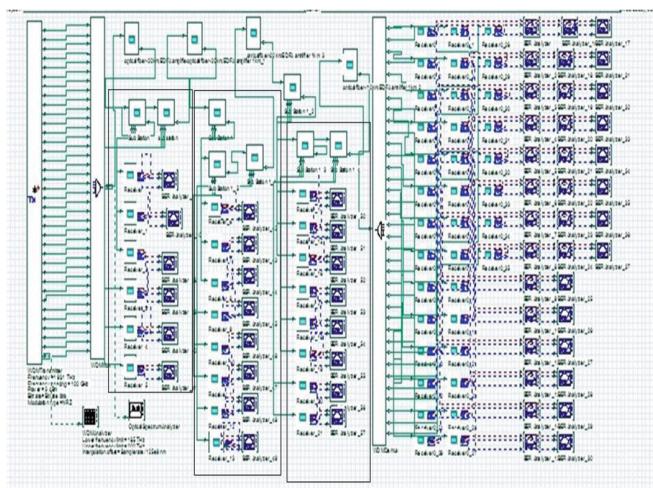
**Fig. 4.** Design of linear RZ DWDM network

Table 4. Linear Topology (RZ) components and their properties

Name	Value
<i>Transmitter</i>	
Frequency	1555 nm
Frequency Spacing	100 GHz
Power	3 dBm
Extinction ratio	30 dB
Line width	0.1 MHz
No of O/P ports	36
<i>Single Mode Fiber</i>	
Dispersion Coefficient	16 Ps/(nm-Km)
Dispersion Slope	0.076 Ps/(nm ² -Km)
Non Linear Coefficient	0.35 1/(Km.W)
Linear Loss	0.2 dB/Km
Length	50 km
Attenuation	0.5 dBm
<i>Erbium Doped Fiber Amplifier</i>	
Operation mode	Gain Control
Gain	10 dB
Power	15 dBm
Noise figure	3 dB
Gain	10 dB

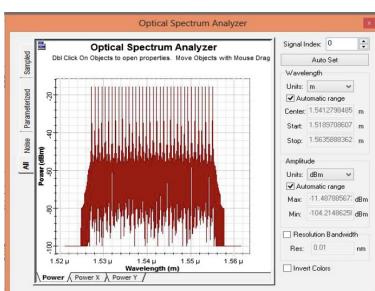
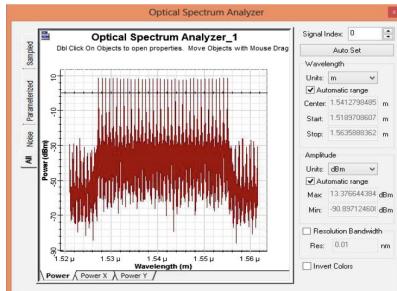
4 Results and Discussions

This research work is implemented in BSNL office, Chennai and for software purpose OPTISIM is used. Thus, the reliable metro DWDM network with the real time statistics of customers usage and traffic rate is designed by referring the telecom division. Four cities were taken into consideration for λ estimation. The lambda value is applicable till 2019 even if the usage scales up for specified MAN. The λ Estimation leads to increase the coverage area and also to provide the Quality of Service. Every year depends upon the customer needs the traffic data rate will vary. Point to point DWDM network which consists of 40 Channels with a negligible dispersion for a distance of 100 km, the result is shown in Table 5. For channel 1 the maximum Q factor is 15.7692 with a minimum bit error rate of 3.68×10^{-9} and for channel 40 the maximum Q factor is 14.7460 with a minimum bit error rate of 4.29×10^{-9} .

Table 5. Point to Point DWDM network

Channels	Maximum Q factor	Minimum BER
Channel 1	15.7692	3.68362e-009
Channel 4	15.8128	4.02815e-009
Channel 8	15.7202	2.89754e-009
Channel 12	15.7100	3.5489e-009
Channel 16	15.9162	5.2694e-009
Channel 20	16.0651	6.0853e-010
Channel 24	15.6028	3.5618e-009
Channel 28	15.1590	1.5894e-009
Channel 32	14.8301	2.5128e-009
Channel 36	14.8560	4.0238e-009
Channel 40	14.7460	4.2925e-009

Figure 5 represents WDM transmitter signal using optical time domain visualize. Time slots is taken in X axis with the time difference of 3 ns and the power is indicated in Y axis with the power difference of 20 μ m. In the transmitter side the center wavelength is found to be 1.54 μ m, with a maximum power of -11.487 dBm and minimum power of -104.214 dBm (Fig. 5).

**Fig. 5.** WDM transmitter signal using optical time domain**Fig. 6.** WDM receiver signal using optical time domain

Wavelength is indicated in X axis with the difference of 0.3 μ s and the power is shown in Y axis with the power difference of -20 dBm. In the receiver side the center wavelength is found to be 1.54 μ m, with maximum power of 13.376 dBm and minimum power of -90.897 dBm.

BER is considered as one of the major criteria for designing optical system. For a point to point DWDM network the typical minimum acceptable rate is 10^{-6} . In substation 1 the eye height is 0.00340274 with a threshold of 0.00355297. The maximum Q factor is 5.90969 and a minimum BER is 1.58465×10^{-9} . The last substation has a minimum bit error of 4.14574×10^{-11} . Hence, BER is less than BER threshold of the

Table 6. Linear NRZ DWDM network with 4 substations

Substations	Threshold	Maximum Q factor	Eye height	Decision instance	Minimum BER
Substation 1	0.00355297	5.90969	0.00340274	0.53125	1.58465e-9
Substation 2	0.00166427	5.10946	0.00125145	0.546875	1.495e-7
Substation 3	0.000348026	4.4924	0.000194441	0.5	3.39119e-9
Destination	0.00310881	6.48445	0.00325969	0.5625	4.14574e-11

receiver. A design of linear NRZ DWDM network with 4 substations is shown in Table 6.

For a linear RZ DWDM network design with 4 substations is shown in Table 7. In substation 1 the eye height is 0.00068473 with a threshold of 0.000586761. The maximum Q factor is 15.0638 and a minimum bit error rate is 1.33569×10^{-51} . The last substation has a minimum bit error of 9.86839×10^{-31} . Typical minimum acceptable rate is 10^{-30} . The linear RZ DWDM network design is shown in Table 7.

Table 7. Linear RZ DWDM network design

Substations	Threshold	Maximum Q factor	Eye height	Decision instance	Minimum BER
Substation 1	0.000586761	15.0638	0.00068473	0.609375	1.33569e-51
Substation 2	0.00160102	11.5034	0.00164867	0.5625	6.06464e-31
Substation 3	0.000492572	11.6074	0.000514127	0.5625	1.81126e-31
Destination	0.000150332	11.4618	0.000152552	0.59375	9.86839e-31

In this paper the estimation of lambda is based on the statistical data from the real data usage and the particular population. One of the challenges in DWDM is nonlinearity. RZ is found to be more tolerant to nonlinearity than the NRZ. While comparing the RZ and NRZ modulations the result shows a better performance when a signal is amplified for a long distance transmission. The RZ and NRZ modulation formats has

**Fig. 7.** Shows the 40-channel DWDM network which handles different types of fiber and loses.

the same performance in the absence of an amplifier. Another comparison between the RZ and the NRZ techniques has been reported in a 4-users WDM system with BER of 2.5 Gb/s per channel. From that it has been observed that RZ modulation format shows a better performance in designing DWDM network (Fig. 7).

This setup is based on the Linear Topology DWDM system. The Fig. 8 shows the overall configuration setting of the single substation. The color obtained in the DWDM system denotes the enabling condition of by the components present in the system.

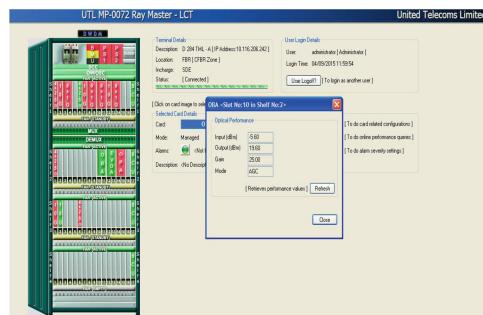


Fig. 8. DWDM network

The configuration of components or slots in the system can be changed card settings. The card setting has optical setting, port setting and performance threshold setting. Here the 4*2.5G slot has been chosen and fixed the performance threshold setting in source side as 1×10^{-5} and destination side as 1×10^{-7} . Here, the automatic laser source has been fixed because of no loss in transmission medium means it will indicate to transmitter side to cut off the laser source by giving acknowledgement from receiver. The input power is fixed as -5.60 dBm and the estimated output power is 19.60 dBm and this is done by using automatic gain control mode.

The client side optical performance are: transmitter optical power is 0.46 dBm, the receiver optical power is -12.503 dBm and the transmitter bias current is 20.064 mA with a temperature of 46.250° . The result obtained for line are: transmitter optical power is -0.31 dBm, the receiver optical power is -9.93 dBm and the transmitter bias current is 77.74 mA with a temperature of 34.313° .

5 Conclusion

The technologies in metropolitan area network such as SONET, ATM, and FDDI are meant only for voice transmission. But DWDM is not only used for voice but also meant for data transmission and video transmission. So, work focuses on DWDM technology which is designed using optisystem simulation software for Coimbatore metropolitan area. Before designing the network, Coimbatore data is surveyed and based on the survey a 36λ system is designed. The 36λ system provides a data rate of 360 Gbps which is sufficient till 2019 for particular areas. In case of increase in population, λ can

be designed and this depends on the increase in data rate. The result has been compared depends on bit error rate and quality factor and hardware configuration is done for fault detection and protection method using forward error correction. The results obtained from linear topology are better when compared to point to point topology in simulation and the same design is configured in hardware and the results as been tested.

References

- Uthayasuriyan, K., Sheela Sobana Rani, K.: Design of point to point metro DWDM network and its performance evaluation. In: International Conference on Communications and Signal Processing (ICCP), pp. 0713–0717 (2015a)
- Uthayasuriyan, K., Sheela Sobana Rani, K.: Design of metro DWDM network and its performance evaluation using linear topology. *Int. J. Appl. Eng. Res.* **10**(29) (2015b). ISSN-0973-4562
- Aloisio, A., Ameli, F., D'Amico, A., Giordano, R., Giovanetti, G., Izzo, V.: Performance analysis of a DWDM optical transmission system. *IEEE* (2010). 978-1-4244-7110-2/10
- Askarian, A., Zhai, Y., Subramaniam, S., Pointurier, Y., Brandt-Pearce, M.: Cross-layer approach to survivable DWDM network design. *Opt. Commun. Netw.* **2**(6), 319–331 (2010)
- Saleh, B.E.A., Teich, M.C.: *Fundamentals of Photonics*. Wiley, Hoboken (1991)
- Chen, R.T., Lipscomb, G.F. (eds.): *WDM and photonic switching devices for network applications*. In: Proceedings of SPIE, vol. 3949 (2000)
- Fukai, C., Nakajima, K., Zhou, J., Tajima, K., Kurokawa, K., Sankawa, I.: Optimum optical fiber design for a DRA-based DWDM transmission system. *J. Lightwave Technol.* **23**(3), 1232 (2005)
- DeCusatis, C., Maass, E., Clement, D.P., Lasky, R.C.: *Handbook of Fiber Optic data Communication*. Academic Press, San Diego (1998)
- Suzuki, H., Fujiwara, M., Iwatsuki, K.: Application of super-DWDM technologies to terrestrial terabit transmission systems. *J. Lightwave Technol.* **24**(5), 1998–2005 (2006)
- Jansen, S.L., Van Den Borne, D., Krumrich, P.M., Spalter, S., Khoe, G.D., De Waardt, H.: Long-Haul DWDM transmission systems employing optical phase conjugation. *IEEE J. Sel. Top. Quantum Electron.* **12**(4), 505–520 (2006)
- Huang, M.-F., Chen, J.(Jyehong), Yu, J., Chi, S., Chang, G.-K.: A novel dispersion-free interleaver for bidirectional DWDM transmission systems. *J. Lightwave Technol.* **25**(11), 3543–3554 (2007)
- Tonguz, O.K., Flood, F.A.: EDFA-based DWDM light wave transmission systems with end-to-end power and SNR equalization. *IEEE Trans. Commun.* **50**(8), 1282–1292 (2002)
- Lai, P.-C.: Transmission improvement of DWDM systems under VCSELs with injection-locked technique and LEAF transport. *IEEE Photonics Technol. Lett.* **17**(10), 2212–2214 (2005)
- Gamage, P.A., Nirmalathas, A., Lim, C., Bakaul, M., Novak, D., Waterhouse, R.: Efficient transmission scheme for AWG-based DWDM millimeter-wave fiber-radio systems. *IEEE Photonics Technol. Lett.* **19**(4), 206–208 (2007)



Secure Outlook View of Trustworthiness and Attacks in Cloud Computing

S. Mercy^{1(✉)}, R. Nagaraja¹, and M. Jaiganesh²

¹ Department of Information Science and Engineering,
Bangalore Institute of Technology, Bangalore, Karnataka, India
mercy.isaac.abraham@gmail.com,
prof.rnagaraja@yahoo.com

² Department of Computer Science and Engineering,
CVR College of Engineering, Hyderabad, Telangana, India
jaidevlingam@gmail.com

Abstract. Cloud computing has turned into an inexorably famous venture model where the assets are accessible on-request to the clients. It encourages in getting to the substance over the web autonomously with no reference to the fundamental facilitating framework. As of now, various kinds of trust model are led against the different cloud administrations and resources, which focus on their accessibility, administration level understandings, and execution. This paper displays a top to bottom investigation of the different sorts of the trust prediction model and attacks proposed for the cloud computing condition and groups them dependent on the Evidence based, Hardware based, Service Level Agreements (SLA) based and Secure Cloud based Trust. Furthermore, it gives a survey analysis of the vulnerabilities used in resource based attacks about the cutting edge arrangements introduced in the writing to avert, distinguish, or manage every sort of trustworthiness in the cloud computing environment.

Keywords: Cloud computing · Security · Review of trustworthiness · Attacks · Trust model

1 Introduction

Computing needs a regularly expanding number of resources to convey results for developing issue estimates in a sensible time span. In the most recent decade, while the biggest research undertakings had the option to bear the cost of costly supercomputers, different tasks were compelled to decide on less expensive assets, for example, Cheap hardware clusters, grid computing and cloud computing. “Cloud computing is a style of computing where scalable and elastic IT-enabled capabilities are delivered as a service to external customers using internet technologies” by Gartner [3]. It moves the customer application, administrations and information to a unified enormous puddle called Big Data center [11]. It upgrades adaptability and empowers server farms to be dynamic in nature. Cloud computing composes an outsider server farms known as Cloud Service Providers (CSP), for example, Amazon, Google and Salesforce.com. These administration models give the degree of administration and organization models

which gives data about the cloud that is conveyed and issued to all cloud clients. The standard sending object that is utilized in cloud computing is Virtual Machines (VM). It improves adaptability and empowers data center to be dynamic in nature. The procedures of partitioning a physical PC into a few mostly or totally separated machines are known as virtualization [6]. The benefit of utilizing virtualization is being improved by the effectiveness of server utilization and the decrease in expense of equipment, data centers and testing stage. Secure use of services in cloud computing is a critical situation. In particular, customer trustworthiness is a crucial barrier to providing users in the cloud. For instance, since users need data, device and circumference manageability, it directs them to cloud computing mistrust [10]. It is the standard information security challenge that can be solved by a lot. The cloud incorporates assets where they are exceptionally brought together and trusted. The primary objective of a data centre is to give access to a possibly huge measure of computing assets in a simple and client driven way. The assets are shared and oversaw through virtualization innovation in cloud computing condition. It utilizes hypervisor inside group condition that enables various virtual machines to share the assets allotted to them.

The customers have unapproved access to the assets (Memory, Disk space) of their neighbor hubs and these vulnerabilities thus make the stage progressively powerless against the assaults [6, 9]. In this way, the cloud clients can execute their administrations by a concentrated store called asset handler where every customer has its very own character. This character is played out various occasions remotely and it distorts the reason for Sybil attack. Thus the programmers could use different assets like processor components and furthermore perhaps use whole memory by making outrageous number of mail messages, and by embedding records in the File Transfer Protocol (FTP) zone. The proposed work contributed towards a survey of trustworthiness in cloud computing. It delivers the type of trust and which extend the trust will be calculated. It provides the current need of trust in which issues and releases the advancement towards the trusted future cloud research directions.

2 Cutting Edge of Trust Finding Methods in Cloud Computing

Inthis work, we address commonly used trust methods in cloud computing, Each methods discuss one particular way of approach for finding trust and get the proper solutions.

2.1 Earlier Evidence Based Trust

Historical conduct of the user will be used in this model to build a collection of cloud users' trusted conduct. On this grounds, it is possible to obtain the immediate confidence of trust of the user. Then, the user interaction with other cloud users can calculate the recommendation trust. Given the present historical confidence, the weighted average can be used to obtain extensive confidence [14].

Joint Risk Trust Model(JRTM) introduced to obtain trustworthiness and risk of providers and cloud users. It is purely a stochastic in nature, it delivers an uncertain

factor in cloud environment. The prediction of risk and trust in a basic level example attackers and eavedroppers. This work depends on the evidence based historic data collected by a Trust as a Service(TaaS) from cloud service provider or third party. Trust as a services is used to provide clear precision of Cloud Service Massup(CSM). The nature of risk is satisfactory for CSM explores interms of TaaS and Cloud consumer. CC also offers several parameters influencing the impacts of historical information on model outcomes based on information freshness and inclination (i.e. if it changes in adverse or positive direction). For hundreds of years, both risk and trust have been researched widely in different situations. Risk management and risk assessment specifically for IT was also a hot study [2].

The suggested technique takes into account each Software's Quality of Cloud Service (QoCS) as a Service(SaaS) and Infrastructure as a Service (IaaS) [7]. The SaaS QoCS is assessed using record registered documents using neighborhood participants who have experienced the service in the meantime, as the IaaS QoCS is assessed using proven star assets, i.e. inclination yet processing power. It is intended to distinguish between cloud suppliers to process different processing loads depending on their capacities. Tasks of Big Data are described as work where nodes represent tasks of Big Data and arrows represent the transitions between two functions. Workplace QoS is officially defined and assessed to pick the suitable cloud service to ensure these QoS. The particular methods are realted to take into account the three dimensions mentioned above: rely on the advertised QoCS of the provider, evaluations from community members and previous private experience of the customer with the cloud provider. These algorithms have been created to be lightweight and do not bring any additional strain to the customer, community members and cloud suppliers [4].

2.2 Hardware Based Trust

All cloud stage suppliers need to remotely and safely select and oversee associated gadgets; this empowers the cloud supplier to offer new administrations and send standard updates. Secure end client and gadget verification is additionally normally required, to guarantee that the supplier is cooperating with the planned gadgets and group of spectators. The key necessities of cloud stage suppliers are:

2.2.1 Registration

Cloud stage suppliers should consistently have the option to remotely oversee gadgets. To do this, the gadgets should be confided in end-focuses and they need a protected channel which enables gadget identification and provides an idea secure storage of self support assigned by cloud service providers.

2.2.2 Potential Resource Organization

End client and gadget confirmation are required crosswise over both buyer and M2M use cases, to enable the right access to stage administrations and to guarantee non-renouncement. The cloud stage supplier needs to utilize the protected administrations accessible on the gadget for this reason [5].

2.2.3 Validation

Complexities emerge with gadget enlistment when the cloud stage supplier needs to select an assortment of gadgets from heterogeneous areas (for example medicinal services, vitality, home mechanization, and so forth.) and from various makers. Dependable gadget enlistment is basic for cloud service providers crosswise over M2M and endeavor use cases[1, 8].

2.3 SLA Based Trust

In this approach the idea of Trust, Cloud units and Service Level Agreements (SLAs) alongside with their magnitude in CC context is accessible. Also, the projected SLA concept and Key Performance Indicators (KPIs) are clear. After establishing the preliminary have confidence and employing a cloud service, the cloud person desires to confirm, recalculate and consider the trust. Here Quality of Service (QoS) was monitoring and SLA verification is a vital foundation of trust management for cloud computing. SLA verification provided necessary for proposed method. Few considerable SLA constraints include Primary memory, Disk space, Bandwidth, Processing power and System software [12]. The primary memory is used for offering virtualization on the node and consequently providing higher pace to execute the assignment (cloudlet). The high primary memory guarantees availability. Disk space offers reasonable have confidence value on the node. Improving the bandwidth is better the verbal exchange between the nodes. System software need to be reliable sufficient that it would not be crashed at the run time. Processing potential capability average work load processed by means of the node.

2.4 Secure Cloud Based Trust

In this paper, they try to improve the key executives issue [13] of remote information respectability reviewing conventions by presenting biometric-based characters in customary RDIC conventions. They propose the thought of fuzzy identity-based data integrity auditing intended to streamline key the executives. In this work, at that point formalize the framework model and security model to guarantee the security called soundness of this new crude (i.e., if a cloud server can persuade a verifier that the server is putting away a document, if and just if it is really putting away that document). The novelty of method portray a solid development of fluffy character based information uprightness reviewing convention, by getting the possibility of fluffy personality based encryption[14]. The last utilizes “set cover” separation metric to gauge the separation between two personality sets. They demonstrate the security of the convention in the specific ID security model, which depends on the Computational Diffie-Hellman what's more, Discrete Logarithm suspicions.

3 Outlook View of Trustworthiness

(See Table 1).

Table 1. Classification of Trust model and their actions.

Feature	Actions
“Trust is classified into four types namely Direct trust, Recommendation trust, Historical trust and Comprehensive trust”	<ul style="list-style-type: none"> –Trust is compared with log details (Previous History) –Trust is measured using simple weighted average method –This work set average weight value for the following behavior: User authentication, Retrieval behavior, Download behavior, Upload behavior and interactive behaviour
“Trust is addressed as Joint trust and used for risk model like privacy of a cloud service and efficiency of services”	<ul style="list-style-type: none"> –Trust is monitored with help of previous performance of cloud users –Trust relation is purely launched between Cloud Consumer and Cloud Service Provider –This work distinguishes loss of performance and gain of performance based on risk assessment at Cloud consumer fondness
“Cloud resource based Trust is a multi dimensional model to provide better Quality of Cloud Service”	<ul style="list-style-type: none"> –Trust worked malicious predicted trust score from nearby nodes –Trust is measured with help of the Cloud Service Provider preferences like memory, processing cycle, data center factors, failure rate, response time and bandwidth –Trust used for three cloud service approaches like current features and repute and the past features
“Service Level Agreements (SLA)-aware trust model find the direct trust in terms of past history and performance indicators”	<ul style="list-style-type: none"> –Trust of one scenario is calculated using Quality of Service factors: response time, throughput, availability and security –Another scenario of trust is measured with the help of key performance indicators: CPU, Memory, Disk space, Bandwidth and Operating System
“The Cloud service provider reputation is calculated instead of trust with evaluation algorithm”	<ul style="list-style-type: none"> –Client justifies the nature of Cloud service provider instead of request delay, server rejection rate, feedback of cloud server and server workload –Trust should be identified from Client’s feedback, work load the data center and request rejections done by the Data center
“Device based secure multi party authentication for Session Authority Cloud(SAC)”	<ul style="list-style-type: none"> –Service Oriented Architecture (SOA) based model is developed through distributed hardware –Multi party authentication is established between the interactions among multi-cloud and Internet Of Things (IOT’s)

(continued)

Table 1. (*continued*)

Feature	Actions
	<ul style="list-style-type: none"> -This model is relevant when numerous individuals from heterogeneous security domains want to get to an assortment of administrations, under the administration of a confided in head [8]
“Trust measured interms of Weight and Correlation methods”	<ul style="list-style-type: none"> -The subjective weight is calculated using analytical hierarchy process -The dynamic recommendation trust is checked is using grey correlation methods -The dynamic direct trust updating is also done by Cloud service trust evaluation model

4 Attacks and Vulnerabilities in Cloud Computing

(See Table 2).

Table 2. Attacks and their actions

Attacks	Actions
Side channel attacks	<ul style="list-style-type: none"> -Side channel attacks are distinguished as an exceptionally complex attack in Cloud computing [1] -In situations where there exist shared equipment assets, the side channel attack misuses data acquired from the utilization of, for instance, Central Processing Unit (CPU) and abnormal state store memory instead of abusing hypothetical shortcomings like the brute force attack
VM Migration Attack	<ul style="list-style-type: none"> -This is an attack on the system during VM movement starting with one spot then onto the next. This attack is an endeavor on the portability of virtualization -Since VM images are effectively moved between physical machines through the system, undertakings continually move VMs to different spots dependent on their use

5 Conclusion

In this work reviewed, secure outlook view that favour in finding attacks to provide Cloud clients to potentially predict trustworthiness of Cloud computing. The list of trust driven factors and their native work dimensions thoroughly viewed. The most famous attacks and their actions were tabulated. Among these survey, we intended to develop trust factor is uncertainty and future work to predict the effective trust model using novel techniques.

References

1. Shahzad, A., Litchfield, A.: Virtualization technology: cross-VM cache side channel attacks make it vulnerable. In: Australasian Conference on Information Systems 2015, Adelaide, South Australia, pp. 1–14 (2015)
2. Cayirci, E., De Oliveira, A.S.: Modelling trust and risk for cloud services. *J. Cloud Comput. Adv. Syst. Appl.* **7**(14), 1–16 (2018)
3. Plummer, D.C., Bittman, T.J., Austin, T., Cearley, D.W., Smith, D.M.: Cloud computing: defining and describing an emerging phenomenon. In: Gartner Research, pp. 1–9 (2009)
4. El Kassabi, H.T., Serhani, M.A., Dssouli, R., Benatallah, B.: A multi-dimensional trust model for processing big data over competing clouds. *IEEE Access* **6**, 39989–40007 (2018)
5. Al-Aqrabi, H., Hill, R.: A scalable model for secure multiparty authentication, a distributed, parallel, and cluster computing (2019)
6. Jaiganesh, M., Kumar, A.: Fuzzy ART based User behaviour trust in cloud computing. In: Seventh International Conference on artificial Intelligence and Evolutionary Algorithms in Engineering Systems, Advances in Soft computing, vol. 324, pp 341–348 (2014)
7. Chase, J., Niyato, D., Wang, P.: A scalable approach to joint cyber insurance and security-as-a-service provisioning in cloud computing. *IEEE Trans. Depend. Secure Comput.* **16**(4), 565–579 (2019)
8. Lim, J., Yu, H., Gil, J.M.: Detecting sybil attacks in cloud computing environments based on fail-stop signature. *Symmetry* **9**, 35 (2017)
9. Karthiban, K., Smys, S.: Privacy preserving approaches in cloud computing. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC) 19 January 2018, pp. 462–467). IEEE (2018)
10. Challagidad, P.S., Reshma, V.S., Birje, M.N.: Reputation based trust model in cloud computing. *Internet Things Cloud Comput.* **5**(5–1), 5–12 (2017)
11. Fan, W., Yang, S., Pei, J.: A novel two-stage model for cloud service trustworthiness evaluation. *Exp. Syst. Appl.* **31**(2), 136–153 (2014)
12. Reese, G.: Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. O'Reilly Media Publications, Boston (2009)
13. Kumawat, S., Tomar, D.: Sla-aware trust model for cloud service deployment. *Int. J. Comput. Appl.* **90**(10) (2014)
14. Sridhar, S., Smys, S.: A survey on cloud security issues and challenges with possible measures. In: International Conference on Inventive Research in Engineering and Technology, VOL. 4 (2016)
15. Wang, Y., Wen, J., Wang, X., Tao, B., Zhou, W.: A cloud service trust evaluation model based on combining weights and gray correlation analysis. *Secur. Commun. Netw.* **2019**, 11 (2019)



Recruitment Data Analysis Using Machine Learning in R Studio

R. Devakunchari^(✉), Niketha Anand, Anusha Vedhanayaki,
and Y. J. Visishta

Department of Computer Science Engineering, SRMIST, Chennai,
Tamil Nadu, India

devakunr@srmist.edu.in, nikethaanand@gmail.com,
anusha.hari.98@gmail.com, Visishta.20@gmail.com

Abstract. Job classification is a system used to divide all jobs within a company and put them on a different regulated scale based on the overall work, salary level, skills, and commitment associated with a clear cut job. This likewise encourages organizations to look at similar jobs in various organizations inside their industry. Since the knowledge base is huge, it is difficult to physically identify the errors. Therefore, two machine learning algorithms namely Support Vector Machine and Random Forest are used to calculate the error percentage. The algorithm with the least error percentage is implemented to recruit employees. Our analysis overall shows that the random forest is more efficient than SVM.

Keywords: Support Vector Machine · Multi class classification · Random forest · R studio · Machine learning

1 Introduction

Machine learning [1, 2] is the science of making computers react immediately without being externally programmed. In the past ten years, machine learning has given us many inventions such as self-driving vehicles, efficient speech recognition, feasible web search, and an improved comprehension of the human genome. Machine Learning is inescapable today that you most likely use it consistently without knowing it. Numerous scientists think it is the most ideal approach towards human-level AI. It can be implemented in various platforms such as Mahout, Hadoop, R studio, Caffe, Veles. In this paper, R studio [3, 4] is used.

R is a programming language used for analytical computing and visuals. R Studio is usable in two versions RStudio Desktop and RStudio Server, which allows accessing RStudio using a web browser while it is functioning on a distant Linux server. R studio is a cross-platform coordinated advancement environment (IDE) for the R measurable language which causes us to do the work efficiently. This paper focuses on predicting if a person is fit for a job or not [5, 6]. Concepts such as the Random forest, multi class classification are implemented to get the error percentage [7]. And finally, tuning is performed to decide and choose the method that overall gives us the least error percentage.

2 Related Work

In the Best Multiclass SVM Method [8, 9], evidence is given that these methods are inferior to another method the one-versus-one. The evidence is strong when the training dataset is sparse. The SVM can't for the most part handle multi classification. So in the exploration on SVM improved calculation for enormous information characterization [10, 11], an algorithm is utilized to take care of these issues. This enhanced algorithm rebuilds the data feature space and advances the certainty of classification. The proposed technique is successful with examinations and the test results demonstrate that the improved algorithm accomplishes better outcomes. In the contrast of methods for multiclass support vector machines, the execution of one method is contrasted and three different techniques are dependent on binary classifications: “one-against-all”, “one-against-one,” and directed acyclic graph SVM (DAGSVM). Experiments tell that the “one-against-one” is the aptest. Results also display for large problems methods by seeing all data at once.

3 Methodology Used for Exploring Recruitment Data

In the analysis of this recruitment data, multi class classification and random forest are explained below

3.1 Multi-class Classification

In machine learning, multiclass and multinomial characterization [12, 13] is the issue of arranging occurrences. Multiclass grouping ought to never be mistaken for multi-label arrangement, where different names are to be anticipated for each occasion.

Support Vector Machine has been utilized in the implementation. The four different methods as listed below.

- Radial
- Linear
- Sigmoid
- Polynomial

Radial classification otherwise called local kernel which is equal to transforming the data into an infinite measure Hilbert space. Thus it will easily solve the nonlinear classification problem. Linear multiclass classification is a kernel function related to the parameter C, since parameter C manages the tradeoff between recurrence of mistake c and complex decision rules. Polynomial kernel otherwise called, global kernel is non-stochastic kernel approximation consisting of two parameters. Every data in set X_i has an impact on the kernel point of the value X_j , regardless of its distance from X_j . Sigmoid kernel is not as efficient compared to different kernel functions because it does not satisfy the mandatory essentials of a kernel. Finally, the best is selected based on error rate.

3.2 Random Forest

Random forest [14, 15] is a gathering learning system for grouping, relapse and various errands that work by building countless call trees at the training time and yielding the class that is the method of the classifications (order) or mean expectation (relapse) of the individual trees. In the random forest approach, an oversized range of call trees area unit created each observation is fed into each call tree. the foremost common outcome for every observation is employed because of the final output. a replacement observation is fed into all the trees and taking a majority vote for every classification model. The random Forest() function is used operate and make the tree and see it's graph. It is a very important ensemble machine learning rule that runs by making many call trees, so by connecting the result obtained by each of the trees. Call tree could be an arrangement model that executes the thought of data gain at every node. Call tree attempts to classify information points at each of the nodes and check for info increase at each of the nodes. Random forest classifies, nodes wherever info gain is most. It pursues this strategy until all the nodes area unit is tired.

4 Results

Below are the results of all the types of classification performed with the error rate obtained.

4.1 Radial

As shown in the below Fig. 1, the number of support vectors assigned is 39, the graph on the right side will also have 39 values plotted. The y-axis has age plotted from 0–60, and the x-axis has work experience plotted from 0–25. SVM-type over here is C classification, SVM Kernel is radial. The values are plotted with a different color indicating the different designations. Red represents database administrator, blue represents software engineer and green indicates production manager. The command qplot is used to generate the given graph.

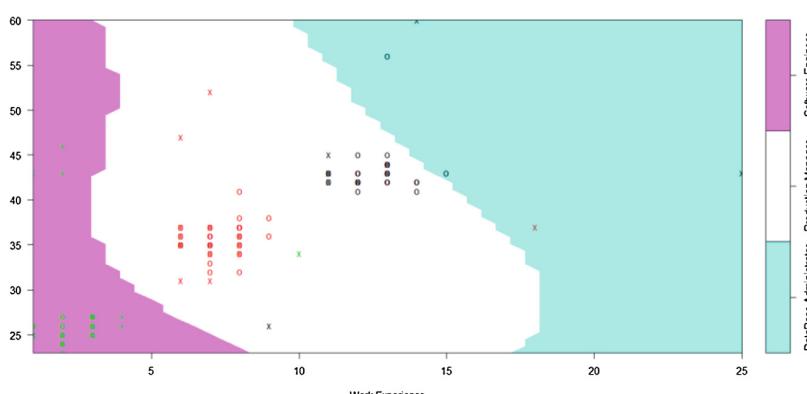


Fig. 1. Multi class classification-radial SVM classification plot

A SVM classification plot, is plotted using the plot function. A scatter plot of the input data of a SVM is fit for classification models. It alternatively draws a filled form plot of the class regions. The error obtained is around 0.05.

4.2 Linear

As shown in the below Fig. 2, a graph has been plotted and has also designed a confusion matrix using the tab function. The number of support vectors assigned is 23, the graph will also have 23 values in the form of circles plotted. In the generated matrix the actual and predicted are represented as two headings. According to the given matrix the values have to be read. In this, it is found that 50 of the 50 database administrator have been predicted properly. Whereas two have been predicted as production manager but they are actually production manager.

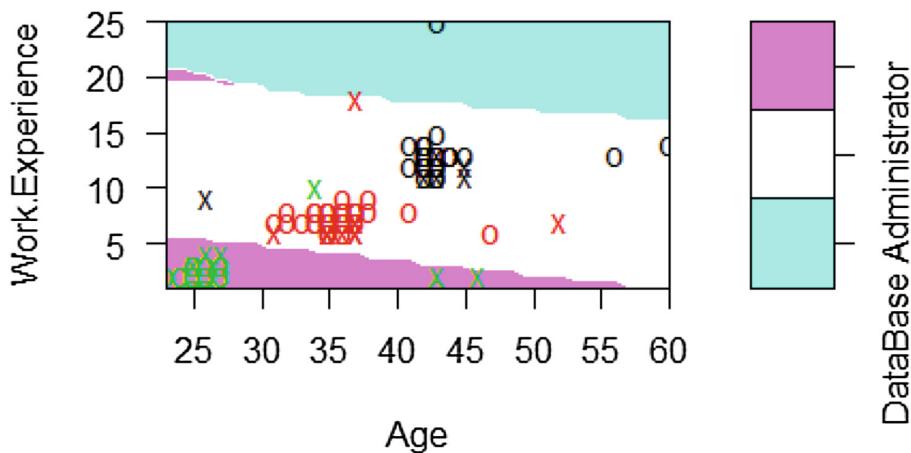


Fig. 2. Multi class classification-linear SVM classification plot

There is also a sum () function and it is used to calculate the error percentage. Over here an error of 0.0201 is got which indicates that the error percentage is around 2.01%.

4.3 Polynomial

As shown in the below Fig. 3, a graph has been plotted and has also designed. In this SVM classification plot the x-pivot is the age and y-pivot is the work experience. Each color in the graph obtained depicts a criterion.

The number of support vectors assigned is 37, the graph will also have 37 values in the form of circles plotted. The error rate is around 1.34% which is comparatively less compared to the others.

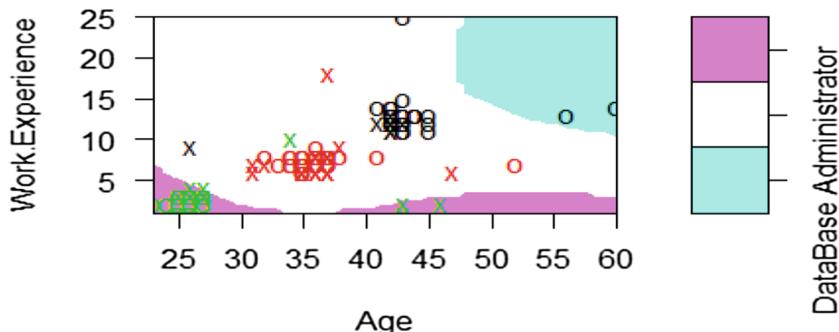


Fig. 3. Multi class classification-polynomial SVM classification plot

4.4 Sigmoid

As shown in the below Fig. 4, a graph has been plotted and has also designed. In this SVM classification plot the x-pivot is the age and y-pivot is the work experience. Each color in the graph obtained depicts a criterion.

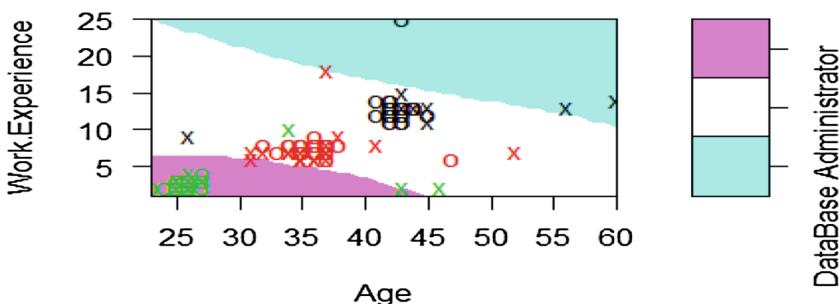


Fig. 4. Multi class classification-sigmoid SVM classification plot

The number of support vectors assigned is 42, the graph will also have 42 values in the form of circles plotted. After generating a confusion matrix, the error rate is found to be around 3% using a formula that is the addition value of the diagonals divided by the sum of all the values in the table.

4.5 Random Forest

Around 500 trees can be generated, each will have a left daughter and a right daughter. The below mentioned Fig. 5 represents a graph that has x-axis tree size and y-axis frequency It tells about the number of nodes the trees have.

There is a column known as status, this tells us about the node. If the status value is -1 it means that the given node is a terminal node, the nodes having 1 are all non terminal nodes. All the non terminal nodes will further have children. Any number can

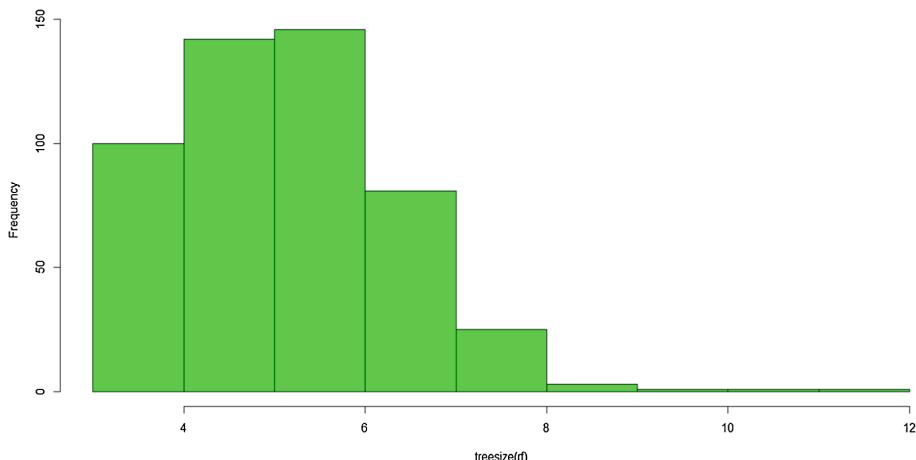


Fig. 5. Random forest classification–number of nodes for the trees

be specified and that number tree will directly be printed. Random forest has several advantages such as,

- (a) It is robust to associated indicators.
- (b) It is utilized to take care of both relapse and grouping issues.
- (c) It can deal with a huge number of information factors without variable determination.
- (d) It tends to be utilized as an element determination instrument utilizing its variable significance plot.
- (e) It deals with missing info internally.

The error rate got is 0.01 when random forest is used, which is the least compared to all other methods.

5 Conclusion and Future Work

An Employee database was used and analysis was done and several conditions were kept in mind during analysis. Initially, Multiclass classification was carried out and all 4 types were analyzed. Out of those, it was concluded that Radial has the least error rate and hence is the best model. Then Random Forest was carried out and it was found that it has a lesser error rate compared to Multiclass classification. Overall, it was concluded that Random Forest has the least error rate among the two and hence is the best model.

As future work, analyze of newer datasets can be performed, so that new policies can be framed which can help in:

Disclosure technologies can raise incident detection and enlist in public security resources sooner. Swifter incident gathering and dispatch can improve reaction times. Innovation can improve the exactness and proficiency of occurrence reaction and

detailing and the portion of insightful assets. Innovation can upgrade the productivity of occurrence examinations and help increment clearance rates. Analytic can distinguish patterns to improve operational viability and proficiency.

References

1. Langley, P.: Editorial: On Machine Learning, University of California. Springer (2001)
2. Harve, R.: Machine Learning in Recruitment & How To Do It Right. <https://harver.com/blog/machine-learning-in-recruitment/>
3. Jatain, A., Ranjan, A.: A review study on big data analysis using R studio. *Int. J. Comput. Sci. Mob. Comput.* **6**, 8–13 (2017)
4. R studio. <https://www.rstudio.com/>
5. Alghamilas, M., Alabduljabbar, R.: Predicting the suitability of IT students' skills for the recruitment in Saudi labor market. In: 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1–5, Saudi Arabia (2019)
6. Sisodia, D.S., Vishwakarma, S., Pujahari, A.: Evaluation of machine learning models for employee churn prediction. In: International Conference on Inventive Computing and Informatics (ICICI), pp. 1016–1020, Coimbatore (2017)
7. Chern, A., Liu, Q., Chao, J., et al.: Automatically detecting errors in employer industry classification using job postings. *Data Sci. Eng.* **3**, 221 (2018)
8. Duan, K., Keerthi, S.: Which is the best multiclass svm method? an empirical study. LNCS, vol. 3541, pp 278–285. Springer (2005)
9. Amudha, P., Sivakumari, S.: Big data analytics using support vector machine. In: International Conference on Soft-computing and Network Security (ICSNS) 2018, pp. 1–6. IEEE, Coimbatore (2018)
10. Dai, H.: Research on SVM improved algorithm for large data classification. In: 3rd International Conference on Big Data Analysis. IEEE (2018)
11. Hsu, C.W., Lin, C.J.: A comparison of methods for multi-class support vector machines. *IEEE Trans. Neural Netw.* **13**, 415–425 (2002)
12. Li, T., Zhang, C., Ogihara, M.: A comparative study of feature selection and multiclass classification methods for tissue classification based on gene expression. *Bioinformatic* **20**, 2429–2437 (2004)
13. Yang, Y., Liu, R., Chen, Y., Li, T., Tang, Y.: Normal cloud model-based algorithm for multi-attribute trusted cloud service selection. *IEEE Access* **6**, 37644–37652 (2018)
14. Zhu, M., Xia, J., Jin, X., Yan, M., Cai, G., Yan, J., Ning, G.: Class weights random forest algorithm for processing class imbalanced medical data. *IEEE Access* **6**, 4641–4652 (2018)
15. Díaz-Uriarte, R., Alvarez de Andrés, S.: Gene selection and classification of microarray data using random forest. *BMC Bioinf.* **7**(1), 3 (2006)



Security Enabled Smart Home Using Internet of Things

Y. Swathi¹(✉), M. B. Shanthi², Swati Kumari^{1,2}, and Priya Batni^{1,2}

¹ Department of ISE, CMR Institute of Technology, Bengaluru, India
swathi.y@cmrit.ac.in

² Department of CSE, CMR Institute of Technology, Bengaluru, India
shanthi.mb@cmrit.ac.in

Abstract. Internet of Things (IoT) is an emerging technology which connects the world with digital communication by making the devices connected to the internet to communicate with each other. It conceptualizes connecting the real-world objects remotely and monitoring them through the internet. The implication of smart technology starts from enabling us to monitor the happenings at home and take the precautions actions based on the activities remotely. Plenty of researchers have shown interest in building smart cities which we dream as our future digital world. There is ample space in developing smart solutions for automating the home. The existing solutions have a focus on monitoring and alerting the house owners in the case of suspension about any unauthorized entries in the house premises. In this paper, we have proposed a smart solution with enforces security to detect the person who enters home premises is authorized or not. It alerts the owner of the home in case of any trespass by capturing the image and providing required details. Based on the verification by the house owner, the person is either allowed to enter the house or required action to be taken by the house owner.

Keywords: IoT · Emerging · Communication · Conceptualize · Monitoring · Trespass · Suspension · Unauthorized · Automated · Verification

1 Introduction

Domotics is an emerging trend in the internet era. Globe is linked with connected intelligent devices, the human tendency has been changed to implement automated services everywhere and speedup the tasks intelligently with maintaining QoS. Homes are becoming smart by the implication of artificial intelligence in the home appliances we use in day to day life. While automating all the home-related tasks, we even need to provide security to avoid misinterpretations of automated systems and to avoid unauthenticated access to the service. Recent research works have lime lighted the importance of enabling security in automated smart homes and started developing a security solution. We in our paperwork presented a security solution to the smart home to enable the owner of the house to control the entry of a person to house premises by authenticating him and triggering the right actions.

The rest of the paper was organized as follows. Section 1 gives a brief introduction about the proposed work, in enabling security for a smart home. Section 2 highlights the current research and related approaches used in implementing home automation with enforced security. Section 3 highlights the design and implementation of the proposed approach. Section 4 discusses Experimental results. Section 5 concludes the observed results and highlights the future scope.

2 Related Work

The major intention behind IoT technology is to enable the internet with remote control ability, data sharing between the connected devices, Making and extending the connectivity and enabling all the running applications to follow a common protocol for communication over net. Using an embedded sensor in the specific device, which is always on and collecting data, all the devices would be tied to local and global networks. Many researchers have contributed to automating home appliances to make life smarter and easier. Suh and Ko [1] has implemented an intelligent home control systems based on active sensor networks. They have implemented a control system to integrate the diversified sensing information with the help of sensor network having sensors and actuators. Machado et al. [2] has implemented a routing protocol considering node energy and link quality for IoT applications. He has introduced an end to end routing solution based on cross-layer information with minimal overhead. Implemented an event-driven mechanism to improve the system performance and avoid the energy hole problem. Kodali, Jain et al. [3], has proposed smart security for home automation. They have implemented a security solution for detecting the entry of an unauthorized person to home or office and generate the alert and convey the related information to the right person for further verification and processing. Pandav et al. [4] have designed a system for enforcing security for home appliances for smart home management. Monitoring the home appliances was enabled by storing and linking the information in the cloud. Withanage et al. [5] have performed a comparative analysis of different technologies used in home automation. They have discussed the technology solutions related to X10, Z-Wave, ZigBee, INSTEON, and EnOcean and compared the pros and cons of each. Halder et al. [6] have introduced the Artificially Intelligent Home Automation System Based on Arduino as the Master Controller. They have used a low-cost solution using off the shelf components to reduce cost and open-source software to get around licensing requirements of the software. Sravanthi et al. [7] has worked on voice recognition application based home automation system with people counter. Soudari et al. [8] have implemented an interface for speech recognition for home automation based on android application. They have used GPRS technology for enabling voice recognition. User commands were used to operate different home appliances like fans and lights as per the requirement. Thus the project had an impact on conserving electrical energy by optimizing the use of it. Based on the carried out literature survey, we have tried to enhance the smart home security by extending the work done by Ravi Kishore Kodali, by alerting the building owner when there is an entry to the building by any human being. They have designed a system to generate the alert message and to send an email to the owner regarding the authorized/unauthorized

person's entry. The enhancement includes capturing the image of entry to the home premise and sending the image along with the alert message for visual analysis and to take the right action.

3 Design and Implementation

3.1 System Prototype Design

The overall design prototype is given in Fig. 1. The system uses the RENESAS microcontroller. For detecting the movement of the objects, we have made use of a PIR sensor. Door movement is controlled by the DC motor. LCD has been used for the display of the message. GSM module enables the system to send the alert to the mobile device. The following section briefs out the different Components used in the design.

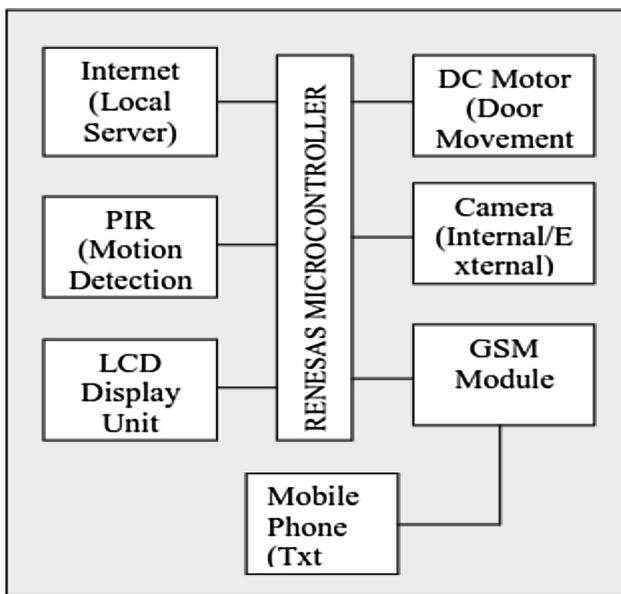


Fig. 1. System Prototype Architecture for home automation with security

3.2 RENESAS Microcontroller

RENESAS microcontroller is a very fast, low cost and highly reliable giving support to 8bit/16bit embedded applications. Figure 2 shows the design of the RENESAS microcontroller. It combines advanced low power technology, outstanding eco-friendly performance. Incorporates the latest process technology and extends support for integrating large capacity flash memory. It has a wide variety of development tools, software libraries, and user communities which made it one of the most demanding microcontrollers in automation industries.



Fig. 2. RENESAS Microcontroller

3.3 PIR Sensor

PIR sensor is a passive infrared sensor commonly used to sense the object motion in the proximity range of around 10 m. Figure 3 shows the PIR sensor component.



Fig. 3. PIR Sensor

It is made up of pyroelectric sensors which will sense the incident IR radiation and convert them to electrical signals. The PIR sensor has been used in the proposed project for detecting the human motion within the home premises.

3.4 DC Motor

These are the continuous actuators which are used to convert electrical energy into mechanical energy. They maintain a constant speed of rotation required to control higher loads. The Fig. 4 shows the pictorial representation of a DC Motor component.



Fig. 4. DC Motor

3.5 GSM Module

Figure 5 demonstrates the working of a GSM module for the secure home automation system. The figure shows the working of the prototype model enabled with GSM communication service.

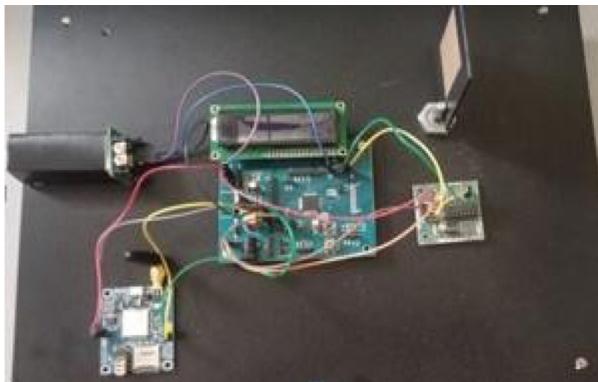


Fig. 5. GSM Module for Secure Home Automation

PIR sensor detects the movement of the object in the proximity range within home premises. PIR sensor senses the object movement and signals the micro-controller. The homeowner will receive an image captured by a camera module through an E-mail on his mobile phone along with a message about the detected object. Based on the received image the owner can decide whether to open the door or not depending upon the authenticity of the person. Moreover, if the owner finds that his building is in threat, he can send an SMS to the concerned authority of the police department to handle the situation. Thus, the homeowner can control the opening of the door from a remote location, through a mobile phone. In this project, the door gets opened or closed based on the received signals through the internet. Even though if Wi-Fi is not available we can go to 3G or 4G services to operate the system. This will help the handicapped and aged people to control their home entrance door.

4 Results

The details of the known users have been maintained in the backend database. So, whenever a person enters the home premise, the PIR sensor senses the object movement and the programmed camera becomes active and captures the image of the object. When a person with pre-recorded data enters in, the door gets opened automatically. In case if the captured object is not related to the known person's image, the image sent to the owner can be used for the further set of actions. Figure 6A and B shows the alert message received at the receiver's end. Notification alert has been generated in two different ways. Notification alert has been sent based on offline or online. An SMS has

been sent to alert the owner in the case of trespass so that even if the owner is currently offline, can receive the security alert about the intruder. The online alert includes an E-mail message to inform the owner regarding the entry of the unknown person in the user premises. Thus the paper has given focus on generating online or offline alerts to the registered owner of the house.

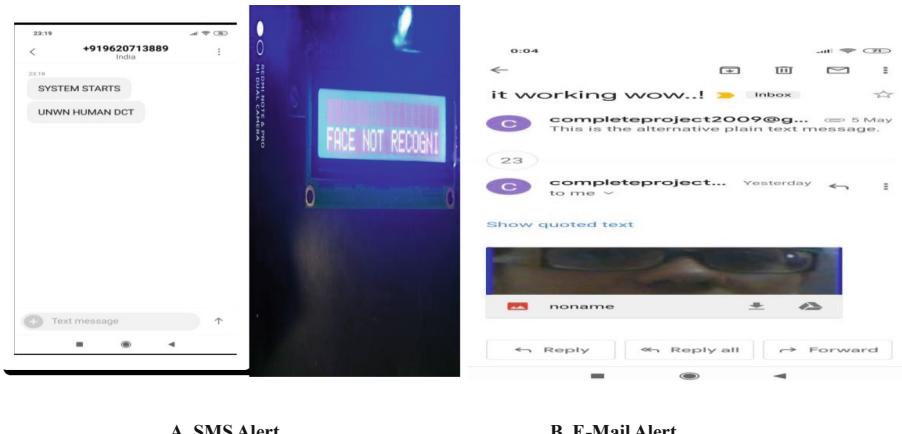


Fig. 6. Online and offline alert notification to the house owner

5 Conclusion

We have implemented an IoT enabled security module for a smart home. A security system controlled by a registered owner is installed to monitor the presence and detection of an unknown person. Automating the door of the house so that known person can enter without any manual aid. Unknown person's detection enables us to prevent crime. A digital attached copy of the person's image is sent over email so that the owner can check who has detected outside the door. By using these systems, we can create a low cost, flexible and energy-efficient smart automated homes and buildings. This model can be scaled up for higher-level security implementations like the entire commercial area, official work, and public places, etc. This system can be used for taking video surveillance of a particular area.

References

1. Suh, C., Ko, Y.-B.: Design and implementation of intelligent home control systems based on active sensor networks. *IEEE Trans. Consum. Electron.* **54**(3), 1177–1184 (2008)
2. Machado, K., Rosario, D., et al.: A routing protocol based on energy and link quality for the internet of things applications. *Sensors (Basel)* **13**(2), 1942–1964 (2013). <https://doi.org/10.3390/si30201942>

3. Kodali, R.K., Jain, V., et al.: IoT based smart security and home automation system. In: 2016 International Conference on Computing, Communication and Automation (ICCCA), 16 January 2017. IEEE Xplore (2016). <https://doi.org/10.1109/ccaa.2016.7813916>
4. Pandav, R.P., Dahatonde, S.P., et al.: Security system and home appliances control using IoT. Int. J. Adv. Res. Innov. Ideas Educ. 4(2) (2018). ISSN(O) 2395-4396
5. Ashok, R., Yuen, C., Otto, K., Withanage, C.: A comparison of the popular home automation technologies, pp. 1–11, May 2014
6. Halder, R., Sengupta, S., Ghosh, S., Kundu, D.: Artificially intelligent home automation system based on Arduino as the master controller. Int. J. Eng. Sci. (IJES) 5(2), 41–45. ISSN (e) 2319-1813 ISSN(p) 2319-1805
7. Sravanthi, G., Madhuri, G., et al.: Voice recognition application based home automation system with people counter. In: International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (2018)
8. Soundari, T., Sangeetha, S.B.: Intelligent interface based speech recognition for home automation using the android application. In: Conference: 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS). <https://doi.org/10.1109/iciiecs.2015.7192988>
9. Ambalkar, R.R., Pagrut, H.P.: A review paper on smart home using voice recognition. In: 2nd National Conference Recent Innovations in Science and Engineering (NC-RISE 17), vol. 5, no. 9, pp. 79–82. ISSN 2321-8169
10. ElShafee, A., Elkamchouchi, H.: Design and prototype implementation of SMS based home automation system, pp. 162–167, November 2012
11. Sahani, M.O.N.C.S.A.P.B.: 2015 International Conference on Circuit, Power and Computing Technologies (ICCPCT), pp. 1–6, March 2015
12. Ming Zhao, T., Chua: 8th IEEE International Conference on Automatic Face and Gesture Recognition, FG 2008, pp. 1–6, September 2008 (2008)
13. Kodali, R.K., Jain, V., Bose, S., Boppana, L.: IoT Based Smart Security and Home Automation (2016)
14. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zao, W.: A Survey on Internet of Things. IEEE Internet Things J. 4 (2017). <https://doi.org/10.1109/jiot.2017.2683200>
15. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Advances in Cryptology. Lecture Notes in Computer Science, vol. 196, pp. 47–53. Springer (1984)



Review of Software Defined Networking: Applications, Challenges and Advantages

Upendra Singh^{1(✉)}, Vikas Vankhede², Shyam Maheshwari²,
Devesh Kumar², and Narendra Solanki²

¹ Shri Govindram Seksaria Institute of Technology and Science,
Indore, Madhya Pradesh, India
upendrasingh49@gmail.com

² Institute of Engineering and Technology, DAVV,
Indore, Madhya Pradesh, India
vikasv3887@gmail.com, shyamrjit@gmail.com,
devesh2222@gmail.com, nksolanki273@gmail.com

Abstract. In the modern era of the internet, the network facilitates the exchange of information which makes communication simple and faster. Due to change in an environment of the network, traditional IP suffers from some issues such as its management in a dynamic environment is not easy, complexity increases, can't tolerate fault, workload balance and not easily adapted. So, to overcome these problems of the network, the concept of the programmed network came into existence. Software-Defined Network (SDN) is a programmed network which is proposed as a solution to overcome the problems that traditional networking suffers. It uses a software application to make network programmed for network management and to improve its efficiency in terms of performance. This paper consists of a systematic review of software-defined networking (SDN), advantages and detailed survey of its applications in various fields like cloud-based services, security services, etc. Although SDN overcomes the issues that traditional IP faces but it faces few challenges related to reliability, security, and management. It presents a brief of past research that has been done in the field of SDN and the scope of SDN in the future.

Keywords: Software Defined Networking · Software defined environment · Programming languages · Programmed network

1 Introduction

In the modern era of the internet, communication at worldwide becomes easy due to connected nodes which form a network, this network can be wired or wireless. In a dynamic environment, traditional IP suffers from the problem of complexity and management issue. [1] It has been seen that in the case of traditional network forwarding policy matters. So, once it is decided then to make changes, there is a need to change the configuration of devices which restrict the network operator and makes configuration difficult. Whenever someone wants to expand their network in responding to change in network traffic, due to an increasing rate of cellphones it

becomes tough to respond to faults, changes and loads. In the current scenario, applications require the network to be fast, manageable in case of a large amount of traffic and efficient in terms of time.

To get rid [2] of the problem occurs due to traditional network a new approach has been came into existence that is, Software-defined networking abbreviated as SDN. It is a network management approach used to improve the performance of the network that facilitates efficient, improved and programmatically configuration of the network. Using SDN will open new opportunities for innovation and applications like power management by the switch during a change in load on the network and home networking. Although SDN facilitates easy deployment and low maintenance cost it faces some challenges also like, development regarding, security issues, abstraction and maintenance issues. It is widely used in area where high performance needed, cloud based applications, intelligent network needed as well as security related fields.

In this paper, we are going to discuss software-defined networking (SDN), its applications in different fields, challenges it faces and advantages of using SDN over traditional IP network. A comparative study has also done to explain why SDN is suitable not traditional networking. Along with detail study of SDN and its architecture which explain it's working. Future scope of this research is also presented.

2 Related Work

Jammal et al. [1] have done research on problems like tracking of frequent users that current network is facing nowadays. As a result two emerging techniques, Software defined networking (SDN) and Network Function Virtualization (NFV) is useful. These can affect the changes in cost estimation and quick response. They found that SDN support NaaS which is a internet model and acts as a link between cloud computing and Software Defined Networking. This paper consist benefits of using SDN in an environment where traffic is more, challenges SDN faces and solution for these challenges. These can be related to security, flexibility, cost estimation etc.

Sezer et al. [2] presented a discussion on Software Defined Networking and its requirement. Their main focus is to achieve a successful carrier grade with Software Defined Networking. In their discussion there main focus is on challenges which SDN suffers like flexibility, security, scalability and centralized control. They have presented a vision of distributed network elements physically as well as virtually. SDN is perfect for the contribution in this kind of communication. In future SDN will be proved as evolutionary step in networking.

Sood et al. [3] work on the integration of Software Defined Networking and Internet of Thing where IoT has been used for simplification of wireless network controls. So, integration of SDN (Software Defined Network) and IoT (Internet of Things) might be beneficial in terms of efficiency as it can provide simpler, easier and strain less network. This paper draws attention of researchers towards challenges like

security and scalability that integration of SDN and IoT faces. They concluded that SDN becomes a preference for network management as there is a scope in SDN for researchers also.

Mousa et al. [4] focused on the open research challenges in new technology like SDN and introduced the concepts and applications of Software Defined Networking. They have done a comparative study of SDN and traditional network on the basis of management, security and availability. Also, they have conducted a survey of various applications which are utilizing the benefits of Software Defined Networking in domains like, Hybrid network control, Traffic Engineering, Data Center networking, wireless networks & network security applications. This study will be helpful for professional as well as for students who wants to do something beneficial in this field.

Rana et al. [5] found that using traditional method for configuration of switch and router may generate error and not fully utilize the capability of hardware. So, they have presented a summarize research on Software Defined Network (SDN). It consist basic model and software used to build a network using SDN along with software tools, challenges and issues.

Dorsch et al. [6] presented a network control approach which is based on Software Defined Networking (SDN) and have dynamic and flexible by nature. It is beneficial for distributed and transmitted power grid to fulfill its requirement. For this a testbed is introduced which helps in evaluation of multiple failure like link disturbance and congestion by fast recovery and setting priority of solutions. As a result it has been observed that it increases reliability on communication which helps to handle complex failures. On the basis of these results they demonstrate challenges and derive future benefits.

Dorsch et al. [7] proposed an approach which is economical beneficial and works with the integration of Software Defined Network (SDN) to smart grid communication infrastructure. For cost reduction slicing facilitates sharing of infrastructure in between critical power system and end consumer broadband traffic. Also they have perform a comparative study of dedicated infrastructure and grid operator on the basis of installation and operation.

Mishra et al. [8] discussed about challenges, research issues and opportunities of Software Defined Network (SDN) and give an idea to which helps to select best SDN controller among NOX, POX, Ryu, Floodlight, and Open Daylight etc. on the basis of less complexity of controller, more scalable and supports maximum resource utilization. For making decision of best controller they have done a survey on Software Defined Network (SDN), protocol (OpenFlow) and research challenge.

Xia et al. [9] found that Software Defined Network (SDN) has two features, including data plane decoupling of control plane and provide programmability for network application development. They presented a survey paper which includes overall study of SDN (includes benefits, architecture, implementation) and suggested some open research challenges.

Astuto et al. [10] discussed about programmable networks like, Software Defined Network (SDN), its architecture and the OpenFlow standard. Also they have discussed on current alternatives for implementation and testing of protocols and services.

Jarraya et al. [11] presented a survey paper which is divided into different sections. In these sections it consist detailed survey of Software Defined Network (SDN), architecture and components of SDN. Taxonomies related to SDN and proposed a taxonomy that helps to classified related research and provides a proper direction to the research. They presented a comparative study of existing research on field of programmable network like, SDN.

Feamster et al. [12] observed that every research is based on the present of Software Defined Networking (SDN) in detail. So, they presented a study which says a lot about SDN, it's like a road to SDN. It includes past, present and future of SDN.

Hakiri et al. [13] observed that for multi-cast services is an issue in traditional IP network which needs to be solve. So, they presented a detailed survey of SDN which includes in-depth study of its requirement, existing technologies and major challenges of SDN.

Nadeau et al. [14] have written a book on software defined network. It gives a detail guidance of Software Defined Network (SDN) including architecture, controllers, application, challenges, possible solution etc.

Ramesh et al. [15] proposed an approach known as software-based heuristic clustered (SBHC) technique. It is especially designed to improve the performance of mobile ad-hoc network (MANET) in terms of QoS. It works in three stages namely, clustering formation, software-based clustering heuristic clustered routing protocol (Table 1).

Summary

During survey it has been observed that traditional approach is good but not capable to deal with dynamic environment of the network. Software Defined Network (SDN) is a programmable network which is very ancient by concept but its implementation and research is done in recent years. It has been observed that recent research has cover wide area network but challenges like reliability, security, adaptability, etc. still a concern which needs proper solution for future enhancement. In future integration of SDN with IoT also has a scope and efficiency can be improved by doing certain experiments. Although research of SDN has cover half way but its long way to cover in the field of research and implementation.

Table 1. Comparison of related work

	Paper	Year	Authors	Proposed approach	Future work
1.	Software defined Networking: State of art and research challenges	2014	Manar Jammal, Taranpreet Singh, Adballah Shami, Rasool Asal, Yiming Li	They found that SDN support NaaS which is a internet model and acts as a link between cloud computing and Software Defined Networking. This paper consist benefits of using SDN in an environment where traffic is more, challenges SDN faces and solution for these challenges	This research has future benefits for other researchers as well
2.	Are We Ready for SDN? Implementation Challenges for Software-Defined Network	2013	Sakin Sezer, Sandra Scott-Hayward, Pushpinder Kaur Chouhan, Barbara Fraser, David Lake, Jim Finnegan, Niel Viljoen, Marc Miller, Navneet Rao	Their main focus is to achieve a successful carrier grade with Software Defined Networking. Also, it includes discussion on challenges which SDN suffers	This research is helpful for researchers in future who wish to work for challenges of SDN
3.	Software Defined Wireless Networking Opportunities and Challenges for Internet of Things: A Review	2015	Keshav Sood, Shui Yu, Yong Xiang	Proposed an integrated approach of IoT and SDN which provides simple, easier and strain less network	In future this research will help to find scope of IoT and SDN integration
4.	Software Defined Networking Concepts and Challenges	2016	Mohammad Mousa, Ayman Bahaa-Eldin, Mohamed Sobh	They have conducted a survey of various applications which are utilizing the benefits of Software Defined Networking in domains like, Hybrid network control, Traffic Engineering, Data Center networking, wireless networks & network security applications	This study will be helpful for professional as well as for students who wants to do something beneficial in this field

(continued)

Table 1. (*continued*)

	Paper	Year	Authors	Proposed approach	Future work
5.	Software Defined Networking (SDN) Challenges, issues and Solution	2019	Deepak Singh Rana, Shiv Ashish Dhondiyal, Sushil Kumar Chamoli	They have presented a summarize research on Software Defined Network (SDN). It consist basic model and software used to build a network using SDN along with software tools, challenges and issues	This study is helpful for future researchers
6.	Software-Defined Networking for Smart Grid Communications: Applications, Challenges and Advantages	2014	Nils Dorsch, Fabian Kurtz, Hanno Georg, Christian Hägerling, Christian Wietfeld	They presented a network control approach which is dynamic and flexible based on Software Defined Networking (SDN). It is especially designed to fulfill the requirement of distributed and transmitted power grid	This paper is helpful for future researchers who want to work on power grid
7.	On the economic benefits of software-defined networking and network slicing for smart grid communications	2018	Nils Dorsch, Fabian Kurtz, Christian Wietfeld	Proposed an approach which is economical beneficial and works with the integration of Software Defined Network (SDN) to smart grid communication infrastructure	In future they aim to add emerging 5G radio access technologies to the evaluation
8.	Software Defined Networking: Research Issues, Challenges and Opportunities	2017	Shailendra Mishra, Mohammed Abdul Rahman AlShehri	Discussed about challenges, research issues and opportunities of Software Defined Network (SDN) and gives idea to select best SDN controller among NOX, POX, Ryu, Floodlight, and Open Daylight etc.	It is helpful in future research to decide which controller is best for implementation

(continued)

Table 1. (*continued*)

	Paper	Year	Authors	Proposed approach	Future work
9.	A Survey on Software-Defined Networking	2015	Wenfeng Xia, Yonggang Wen, Dusit Niyato	Presented a survey paper which includes study of SDN, its benefits, three layer architecture, implementation and at last suggested some open research challenges	This paper is useful for future researchers who want to works with decoupling feature of SDN
10.	A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks	2013	Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, Thierry Turletti	Discussed about programmable networks and especially emphasis on Software Defined Network (SDN), its architecture and the OpenFlow standard	This paper is useful for future researchers who want to works with SDN
11.	A Survey and a Layered Taxonomy of Software-Defined Networking	2014	Yosr Jarraya, Taous Madi, Mourad Debbabi	Proposed a taxonomy that classified related research and gives direction to the research. They presented a comparative study of existing research	They have investigated some of the open issues that have been poorly addressed by the literature and thus need to be addressed by future research efforts
12.	The Road to SDN: An Intellectual History of Programmable Networks	2014	Nick Feamster, Jennifer Rexford, Ellen Zegura	Presented a study which says a lot about SDN, it's like a road to SDN. From its beginning to its future and area where it is required	This research is helpful for researcher in future
13.	Software-defined Networking: Challenges and Research Opportunities for Future Internet	2014	Akram Hakiri, Aniruddha Gokhale, Pascal Berthou, Douglas C. Schmidt, Gayraud Thierry	They presented a detailed survey of SDN which includes in-depth study of its requirement, technologies and challenges of SDN	There research is useful for those researchers who want to work on challenges of SDN

(continued)

Table 1. (continued)

	Paper	Year	Authors	Proposed approach	Future work
14.	Software Defined Networks	2013	Thomas D. Nadeau, Ken Gray	It gives a detail guidance of Software Defined Network (SDN) including architecture, controllers, application, challenges, possible solution etc.	For future researchers it will be a milestone
15.	A software-based heuristic clustered (sbhc) architecture for the performance improvement in manet	2017	Ramesh S, Smys S.	An approach known as software-based heuristic clustered (SBHC) technique. It is especially designed to improve the performance of mobile ad-hoc network (MANET) in terms of QoS	For researcher it provides a direction for SDN in MANET

3 Detailed Study

This section includes the brief of SDN architecture and how openflow protocol helps in implementation, application, challenges and advantages.

3.1 Architecture and Working

Software Defined Network (SDN) architecture shows how combination of software-based technologies built a networking and computing system. SDN architecture mainly consist of three layers namely, application layer, control layer and infrastructure layer and two interfaces.

Three layers bottom to-up approach:

- **Infrastructure Layer:** It is a physical layer which supports virtualization with the help of control layer. To forward network traffic switches and routers), it uses network form by various networking equipment.
- **Control Layer:** It is known as land of control panel where various types of SDN controller resides and control network infrastructure. Every network vendor who is working in this area will present their products for controller and framework. This layer consist of business logic which helps to get and maintain network information, states information, statics information and many more.
- **Application Layer:** It is an open area which is used to develop application related to automation, configuration, management, monitoring, troubleshooting, policies

and securities. These applications help to provide end to end solutions for real world enterprise and data center networks (Fig. 1).

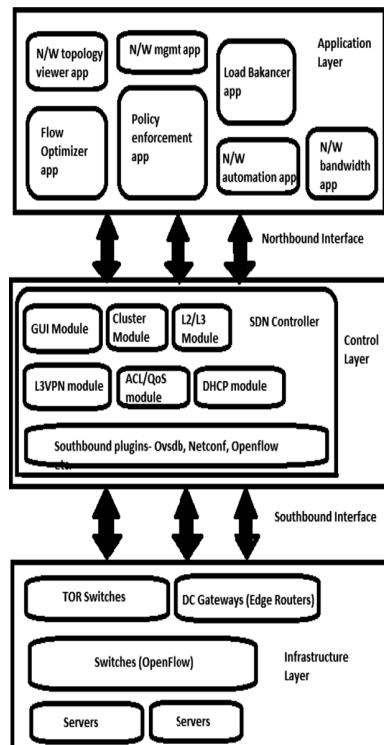


Fig. 1. Architecture of SDN

In between these 3 layers interfaces are used:

- **Southbound Interface:** It establishes communication with the lower layer that is, Infrastructure layer. It uses certain protocols known as southbound protocols like OpenFlow, Netconf, etc.
- **Northbound Interface:** It establishes communication with the upper layer that is, Application layer. It would be in general realized through REST APIs of Software Defined Network (SDN) controllers.

Working:

SDN is a combination of several technologies which includes virtualization and automation. Its main focus is on the separation of network control plane from data plane. Control plane mainly controls the flow of data packets while data plane is responsible for movement of packets from source to destination. It uses switch as data plane device which gives information about traffic it handles. SDN uses two types of operation mode known as adaptive or dynamic; it is useful in case when packet does

not have a specific route so request will be send to controller. But in case of adaptive routing, route request issues through network topology based routers and algorithms.

On the top of physical layer, there exists a logically separate network known as virtual overlay. This overlay is used to abstract the network and its traffic. This setup is useful for service providers and operators working over cloud environment.

3.2 Advantages

Over traditional networking SDN returns best results because of its advantages and services it facilitate. Some advantages of SDN are:

1. **Budget Friendly** - It minimizes overall operating cost of the network which ultimately results in administrative savings.
2. **Reliability** - It controls the traffic which improves quality of services (QoS). SDN improves network responsiveness which ensures reliability of the network.
3. **Centralized Network** - Software Defined Networking provides a centralized view of the network which helps to make management easier and improves reliability of the network.
4. **Reduce Infrastructure** - On using Software Defined Networking, SDN controller helps to optimize hardware because hardware can be repurposed using instructions from the SDN controller.

Other than these advantages SDN provides other advantages also like, traffic programmability, network automation, security, quick response, cloud abstraction, management, etc.

3.3 Applications

Due to its advantages and reliability it can be used in several fields. We are going to discuss five major fields where it is best suited:

1. **Security Services:** When NFV function is incorporates into SDN platform then a secure system is obtained which can be useful for applications where security is major concern and needs to protect system from different types of attacks.
2. **Intelligent network:** Applications which are having heavy network issue and heterogeneous network architecture use SDN for handling heavy data traffic. Applications which need network intelligence and monitoring prefer SDN rather than traditional network.
3. **Cloud Based Application:** Cloud vendors provide space to store and work with compliance-bound workload and they need to manage traffic segment as well. So, for such kind of cloud based application SDN architecture is beneficial.
4. **High-Performance Applications:** In recent years, use of virtualization concept is increases as it deliver high level apps like, CAD, engineering and graphics design software. So, to secure confidential data and to provide quality of services SDN architecture is helpful as it provides high-performance and supports rich applications.

5. **Distributed Applications:** One of the advantages of SDN is agility which is helpful to integrate distributed location and entire organization. SDN is actually a form of network virtualization and it facilitates integration like powerful APIs with cloud provider, etc.

3.4 Challenges

Even after so many advantages SDN have, there is half way remain to cover by facing challenges which somehow affects the efficiency of SDN. Few of them are:

1. **Challenges Regarding Deployment:** Heterogeneity in network devices is still a major concern that affects scalability of apps and controller.
2. **Security Issue:** Although SDN is more secure than traditional network but in a dynamic environment where at every moment types of attacks and their modes changes security becomes a major concern.
3. **Speed:** SDN controller is beneficial in many fields but speed of controller is an issue. As controller is much slower than switches while they process packets.
4. **Abstraction Challenge:** In the dynamic environment of network replacement of old rules with the new rules and to maintain consistency in network is a challenge.

4 Conclusion and Future Work

In the modern era of the internet, the network facilitates the exchange of information which makes communication simple and faster. Due to change in an environment of the network, traditional IP suffers from some issues such as its management in a dynamic environment is not easy, complexity increases, can't tolerate fault, workload balance and not easily adapted. So, to overcome these problems of the network, the concept of the programmed network came into existence. Software-Defined Network (SDN) is a programmed network which is proposed as a solution to overcome the problems that traditional networking suffers. It uses a software application to make network programmed for network management and to improve its efficiency in terms of performance. This paper consists of a systematic review of software-defined networking (SDN), advantages and detailed survey of its applications in various fields like cloud-based services, security services, etc. Although SDN faces few challenges related to development, abstraction and security in dynamic environment of the network which needs to be resolve in future.

This study will be helpful for researchers in future who want work in the field of programmed network that is, Software Defined Network (SDN). To resolve its issues at certain level and for improvement of the efficiency in terms of performance.

References

1. Jammal, M., Singh, T., Shami, A., Asal, R., Li, Y.: Software defined networking: state of art and research challenges. *Comput. Netw.* **72**, 1–25 (2014)
2. Sezer, S., Scott-Hayward, S., Chouhan, P.K., Fraser, B., Lake, D., Finnegan, J., Viljoen, N., Miller, M., Rao, N.: Are we ready for SDN? Implementation challenges for software-defined network. *IEEE Commun. Mag.* **51**, 1–8 (2013)
3. Sood, K., Yu, S., Xiang, Y.: Software defined wireless networking opportunities and challenges for internet of things: a review. *IEEE Internet Things J.* **3**, 1–12 (2015)
4. Mousa, M., Bahaa-Eldin, A., Sobh, M.: Software defined networking concepts and challenges. In: 11th International Conference on Computer Engineering and Systems (ICCES), pp. 1–13 (2016)
5. Rana, D.S., Dhondiyal, S.A., Chamoli, S.K.: Software defined networking (SDN) challenges, issues and solution. *Int. J. Comput. Sci. Eng.* **7**, 1–7 (2019)
6. Dorsch, N., Kurtz, F., Georg, H., Hägerling, C., Wietfeld, C.: Software-Defined networking for smart grid communications: applications, challenges and advantages. In: IEEE International Conference on Smart Grid Communications, pp. 1–6 (2014)
7. Dorsch, N., Kurtz, F., Wietfeld, C.: On the economic benefits of software-defined networking and network slicing for smart grid communications. *NETNOMICS: Econ. Res. Electron. Netw.* **19**, 1–30 (2018)
8. Mishra, S., AlShehri, M.A.R.: Software defined networking: research issues, challenges and opportunities. *Indian J. Sci. Technol.* **10**(29), 1–9 (2017)
9. Xia, W., Wen, Y., Niyato, D.: A survey on software-defined networking. *IEEE Commun. Surv. Tutor.* **17**, 1–25 (2015)
10. Nunes, B.A.A., Mendonca, M., Nguyen, X.-N., Obraczka, K., Turletti, T.: A survey of software-defined networking: past, present, and future of programmable network. *IEEE Commun. Surv. Tutor.* **16**, 1–18 (2013)
11. Jarraya, Y., Madi, T., Debbabi, M.: A survey and a layered taxonomy of software-defined networking. *IEEE Commun. Surv. Tutor.* **16**(4), 1–26 (2014)
12. Feamster, N., Rexford, J., Zegura, E.: The road to SDN: an intellectual history of programmable networks. *ACM SIGCOMM Comput. Commun.* **44**, 87–98 (2014)
13. Hakiri, A., Gokhale, A., Berthou, P., Schmidt, D.C., Thierry, G.: Software-defined networking: challenges and research opportunities for future internet. *Comput. Netw.* **75**, 1–31 (2014)
14. Nadeau, T.D., Gray, K.: Software Defined Networks, pp. 1–384 (2013)
15. Ramesh, S., Smys, S.: A software-based heuristic clustered (SBHC) architecture for the performance improvement in MANET. *Wirel. Pers. Commun.* **97**, 6343–6355 (2017)



Trust Based Model for Mobile Ad-Hoc Network in Internet of Things

Upendra Singh^{1(✉)}, Mukul Shukla¹, Ashish Kumar Jain²,
Mohan Patsariya³, Ravikant Itare⁵, and Sakshi Yadav⁴

¹ Shri Govindram Seksaria Institute of Technology and Science, Indore, India
upendrasingh49@gmail.com, mukulrshukla@gmail.com

² Institute of Engineering and Technology, DAVV, Indore, India
ashishjainji@gmail.com

³ BSF Polytechnic CSMT, Tekanpur, India
mohan.patsariya@gmail.com

⁴ Techbeanssolution, Indore, Madhya Pradesh, India
sakshiyad06@gmail.com

⁵ TCS, Indore, India
ravikantjecll1@gmail.com

Abstract. Internet of things (IoT) is the internet connectivity of heterogeneous network with physical devices. The main idea of IoT is to establish communication of smart devices with global communication. These wireless networks can be wireless sensor network (WSN), Wi-Fi and mobile ad-hoc network (MANET). To make IoT a reality for smart and user-friendly environment as well as economical, it needs compatibility of IoT with wireless sensor network (WSN) and mobile ad-hoc network (MANET). This MANET is an infrastructure less network that provides dynamic environment to the nodes that makes easy deployment and less configuration of the network. During incorporation of wireless networks with physical devices improves the performance of the system in terms of efficiency, reliability and security. This combination of IoT with MANET will be beneficial for the development of predictive model. This paper proposed a trust-based model for IoT and MANET which calculates trust value for a node by combining both direct and indirect trust opinion. For combining recommended trust evidences, ARMA/GARCH theory has been used which is helpful for the prediction of trust value for each node in multi-step. To increase the security and reliability of the proposed model a protocol is also designed which ensures end-to-end delivery through trusted nodes. Result shows that proposed approach improves the value of throughput and packet delivery ratio while it reduces the end-to-end delay. As compare to existing approach PDR value increases by 7%, End-to-end delay decreases by 20% and throughput increases by 7%. Also it has been observed that proposed approach improves efficiency and security.

Keywords: Internet of things · Mobile ad-hoc network · ARMA theory · GARCH theory · Trust value

1 Introduction

Internet of things (IoT) is the future of technology development which includes internet connectivity of heterogeneous network with physical devices. This heterogeneous network can be of home appliances, vehicles and other objects [1]. The main idea of IoT is to establish communication of smart devices with global communication. It provides various business opportunities, used in buildings (like home, school, and offices), utility network (gas, electricity, and water), transportation network and transportation vehicles, information technology etc. Incorporation of wireless networks with physical devices improves efficiency, reliability and security.

Mobile ad-hoc network (MANET) is a wireless network in which random nodes as cellphones are connected to each other and helpful in transferring data in form of packets from one node to another. It is infrastructure less network and provides dynamic environment to the nodes [2]. Communication between nodes takes place through radio waves that is nodes which are in radio range can communicate with each other directly but those nodes which are not in radio range communicate through intermediate nodes. That means nodes acts as a router while communicating and transferring data packets from source to destination. MANET used in different fields like battlefields, law enforcement, conferences etc. Although security is a main concern in MANET as it does not have any predefine security measures so, it uses certain protocols to ensure security from different types (data and control) of attacks.

IoT-MANET suffers from problem of uncertain nodes which needs to be solved for better results. In this paper we have proposed a trust management scheme in which IoT and MANET combine together to design a trust based predictive model. To ensure security of the model, cryptography and trust decision framework has been used. It works for direct as well as indirect trust opinion. For final trust, a mathematical prediction model of ARMA/GARCH theory used to combine various recommendations. It has been found that proposed model is light weighted, flexible, reliable and able to manage trust in IoT-MANET.

2 Related Work

Bruzgiene et al. [1] research focused on energy consumption and reliability of IoT-MANET network. Also for IoT they have proposed routing solutions by using MANET protocols and WSN routing protocols. For experiment, they have used clustering method so that each node in a network organized into hierarchical structures.

Djedjig et al. [2] observed the problem of selfish node in Routing Protocol for Low-Power and Lossy network which is a standardized protocol of IoT. To get rid of it, proposed approach strength the RPL by adding trustworthiness metric. It helps to decide whether or not to trust a node.

Rath et al. [3] presented a study of security and safety issues related to the combination of IoT and MANET technology along with analytical study of insolent configurations. In future this analysis will helpful for researchers in their further research related to security issues arises due to handshaking of IoT and MANET.

Josang et al. [4] presented a survey of existing and proposed systems available for internet transaction measures like, trust and reputation. Analyze the current trends and developments which will helpful in future in different practical and commercial applications.

Virendra et al. [5] proposed security architecture for MANET (Mobile ad-hoc network) which is trust based. It works in two folds: to use trust to establish keys and to use trust as a metrics to establish security infrastructure. Although for the grouping of nodes they have introduced the concept of PLDs (Physical Logical Domains) which is self-organized and based on trust.

Liu et al. [6] presented a study of different routing protocols and describe AODV in detail. Also they proposed an optimized protocol B-AODV which is based on problem of finding route and repair of AODV. As a comparative study of AODV and B-AODV, it has been observed that B-AODV is better than AODV on the basis of parameters like, control packets, ratio of packets and end-to-end delay.

Jain et al. [7] proposed a mechanism which uses trust metrics which is derived from various methods to improve security aspects. It requires minimum modification with existing on demand routing protocol. Like every approach they utilize node trust but additionally they utilize link trust also. Simulation results show that efficiency increases up to certain level.

Ghosh et al. [8] proposed a scheme which allocates secure IP addresses to authorized nodes of MANET. It is known as low-overhead identity-based distributed dynamic address configuration scheme which improves security as well as takes care of design challenges like overhead problem.

Velloso et al. [9] proposed model which uses recommendation exchange protocol (REP). In MANET this will built trust relationship among nodes and allows nodes to exchange recommendation about their neighbors. It works for nodes within radio range and improves performance by reducing number of messages. Relationship maturity is the key concept of this model. Simulation results show that efficiency increases.

Chatterjee et al. [10] have done a research on internal compromised nodes which are threat in network. On the basis of their research, they proposed a clustering protocol which ensures secure data delivery. The proposed trust model uses self and recommendation evidences for computation of trust of a node. It is flexible and light-weighted. To find most qualified trustworthy node, it uses voting scheme using parallel multiple signature. Simulation results shows that in terms of throughput and packet delivery ratio protocol outperforms the popular ECS, CBRP and CBTRP.

El Defrawyet al. [11] proposed an anonymous MANET routing protocol that is PRISM which is location based and on demand protocol. It helps to achieves security and privacy against both insider and outsider threats. Results shows that PRISM is better as compare to other techniques in terms of privacy.

Zhang et al. [12] presented an analysis which shows relationship of trust metrics and trust based routing protocols by focusing on identification of basic algebraic properties. This framework helps to model the interaction between different trusts based routing protocol.

Jain et al. [13] focused on integrated attacks known as combination of attacks MANET suffers. So, as a solution they have presented a trust based routing approach and for experiment three different scenarios of integrated attacks have been taken. Results show improvement in performance of the network.

Singh et al. [14] proposed work focused on to reduce the effect of black hole, worm hole and collaborative black hole attacks using trust value which lies in between 0 to 1 where value greater than 0.5 shows reliable node otherwise block the node. Results show that performance of TSAODV improves as compare to AODV.

Parihar et al. [15] focused on security issue occurs due to infrastructure less network of MANET results into false entry of misbehaving node. They have taken Support Vector Machine for the experiment which classified nodes as normal or malicious. Results show a satisfactory improvement in performance.

Anguraj et al. [16] found tele health application that is, Body Area Network (BAN) beneficial for the user. Their research focused on security aspects of the BAN as BAN suffers from malicious attacks. BAN-Trust scheme uses trust value calculation on the basis of which they detect attack and affected node. Precision, Recall, Throughput, PDR and end-to-end delay are evaluation parameters used to check improvement in performance of the system.

Panda et al. [17] focused on intrusion detection by using sequential information bottleneck (sIB) clustering algorithm. For experiment dataset of KDDCup1999 has been used. A comparison has been done in between existing methods and proposed method and it has been observed that our approach is efficient in terms of detection accuracy and returns low false positive rates.

Sharma et al. [18] focused on active attacks through which MANET suffers. As a solution to this problem SAODV used with hybrid cryptography techniques (DEA, RSA algorithm) which returns effective values of parameters like, energy, PDR and throughput. For its implementation they have used NS2 simulator.

Saurabh et al. [19] found that due to low configuration and quick deployment, MANET can be used in emergency situations like disasters and military operation but security is the main issue with it. So, they have proposed an approach which uses AODV with clustering and ensures security. Even evaluation parameters like PDR, energy and end-to-end delay returns effective results.

Chouhan et al. [20] proposed a technique of dynamic wormhole detection and prevention which is based on hybrid model and uses location, neighbor node and hop count. It has lower overhead and minimum battery consumption which ultimately results into longer survival of the network and minimum respond time.

3 Proposed Approach

This section covers the detailed study of proposed approach. It consist two parts, one is trust model and second is trust generation. They have used clustering framework for the purpose of clustering and cluster-head election. For the purpose of trust calculation certain network parameters are needed, like for direct trust evidence in a time period

node A monitors traffic of neighbor nodes of node B. To ensure reliable data delivery certain parameters are taken into consideration like, numbers of packets deliver properly, packets dropped and packets falsely injected. It categorizes nodes on the basis of good and bad behavior of nodes.

A. *Trust Model*

Figure 1 shows the trust model. It consists of five phases from trust calculation to trust propagation then establish possible routes from source node to destination node which ultimately ensures end-to-end packet delivery and node availability. The trust model is evidence based so it changes frequently. Therefore, a trade-off is required between trust revocation and trust initialization. It is application-specific and depends upon the environment.

1. Trust Revocation

It is the first phase from which cluster-head initiates trust calculation for every member of the cluster. In IoT-MANET nodes calculation at fixed interval and singleton trust generation is not possible due to randomness in nodes that is node mobility.

2. Trust Generation

It is the second phase in which evaluation of the value of trust for every member of cluster takes place. This phase is performed in two phases namely, direct trust calculation and resultant trust generation. After trust calculation node will be categorized.

3. Categorization of nodes

In MANET packet dropped due to several reasons like link failures, contentions, and interference and malicious. But in our scenario we have categorized node as good or bad on the basis of their behavior using threshold value. Node which drops the packet on regular basis consider as “bad node”.

- A node considers as good if value of resultant trust is greater than or equals to maximum threshold value.
- A node considers as bad if value of resultant is less than or equals to minimum threshold value.
- A node is consider as uncertain if value of resultant lies in between minimum to maximum threshold value.

4. Trust Propagation

In this phase, cluster-head propagates values of finalized trust-value of each member node to other cluster members.

5. Routing

Route creating between source and destination works in three phases that is, neighbor discovery, route discovery and route maintenance.

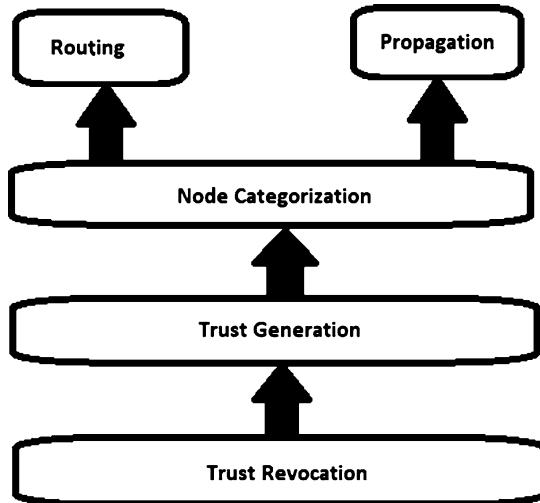


Fig. 1. Trust Model for Routing and Propagation on Mobile Ad-Hoc Network

B. Trust Generation

Trust generation carried out in two steps: direct trust calculation and resultant calculation.

- **Direct trust calculation**

Direct trust calculation works in three phases namely, trust initiation, evidence collection and trust aggregation. In trust initiation, cluster-head plays an important part in the bootstrapping the IoT-MANET and initialization of trust calculation. Then they collect the evidences of Good and Bad in second phase that is, evidence collection. In third phase of trust calculation, trust aggregation takes place in which every member of cluster and cluster-head itself collects and stores data for all good and bad events. For calculation of direct trust value β probability function has been used. It is mathematical representation of combination of feedback and reputation ratings.

Working

Suppose we are having two nodes, namely X and Y where node X collects information of good and bad behavior of node Y. Here, α represent good behavior while β represents bad behavior. B distribution function helps to predict posterior probabilities of trust value. The β distribution can be expressed using the Γ function as,

$$f(p|\alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) + \Gamma(\beta)} p^{(\alpha-1)} (1-p)^{(\beta-1)}$$

Where, p lies between 0 to 1 and value of α, β should be greater than 0.

There is a restriction that if $\alpha < 1$ than probability variable $p \neq 0$.

If $\beta < 1$ than $p \neq 1$.

Although it is an uncertain probability and $E(p)$ is the expected probability which is more likely to relative frequency of outcome.

Direct trust of node can be calculated as:

$$E(p) = \alpha / (\alpha + \beta)$$

Initially direct trust value of each node is set to 0.5 as for review there is no recorded observation or evidence of a node available. Set $\alpha = \beta=1$ which makes value of expectation and direct trust equals to 0.5.

- **Resultant trust Calculation**

It works in three phases namely, neighbor management, trust information collection and trust aggregation. In first phase, each member of the cluster maintains a list of neighbor nodes by sending Hello message to them. These neighbor helps in recommendation which is collected by cluster-head in second phase that is, trust information collection. For the calculation of final trust value of resultant cluster-head executes ARMA(1, 1)/GARCH(1, 1) when it receives recommendation of trust evidences from the cluster members.

Using ARMA(1,1) resultant trust can be calculated as,

$$X_t = \varepsilon_t + \sum_{i=1}^p \varphi_i X_{t-i} + \sum_{i=1}^p \theta_i X_{t-i}$$

To estimate ε_t (which is independent of s and s is set of independent trust evidence collected from common neighbors and self-evidences). Likelihood function for the ARMA(1,1) model is computed by,

$$\begin{aligned} L(\varphi_1 \theta_1, \sigma_\varepsilon^2) &= \prod_{t=2}^T \frac{1}{\sqrt{2\pi}\sigma_\varepsilon} \\ &\times \exp \left\{ -\frac{(y_t - c - \varphi_1 y_{t-1} - \theta_1 \varepsilon_{t-1}^*)^2}{2\sigma_\varepsilon^2} \right\} \end{aligned}$$

Log likelihood function is,

$$\begin{aligned} l(\varphi_1 \theta_1, \sigma_\varepsilon^2) &= -(T-1) \log \sigma_\varepsilon - \frac{1}{2\sigma_\varepsilon^2} \\ &\times \sum_{t=2}^T (y_t - c - \varphi_1 y_{t-1} - \theta_1 \varepsilon_{t-1}^*)^2 \end{aligned}$$

The GARCH(1,1) model is expressed as,

$$\sigma_t^2 = k + G_1 \sigma_{t-1}^2 + A \varepsilon_{t-1}^2$$

Where, $\sigma_t^2 \varepsilon_t$ is taken from the ARMA(1,1) model and it is assumed that it has conditional variance ε_t^2 .

$$L(k, G^1, A_1) = \prod_{l=2}^1 \frac{1}{\sqrt{2\pi\varepsilon_t}} \exp \left\{ -\frac{\varepsilon_t^2}{2\sigma_{\varepsilon_t}^2} \right\}$$

The log likelihood function, neglecting the constant term, can be written as

$$l(k, G^1, A_1) = \frac{1}{2} \sum_{t=2}^T \left\{ \log \sigma_t^2 + \frac{\varepsilon_t^2}{\sigma_t^2} \right\}$$

By using ARMA/GARCH model, cluster head can predict multi-step value of trust series, results into increasing likelihood of good nodes and reduce trust revocation. It has been seen that it provides flexibility in terms of energy.

4 Simulation

Proposed approach is implemented using NS-2 Simulator. During simulation, as MAC layer protocol IEEE 802.11 standard has been used. Where transmission ranges is set to be 250 m. In network nodes travel within the speed range from 0 to 5 m/s and pause time set to 5 s. As the result of node randomness, cluster get partitions very frequently. Information transferred in form of packets of size 512 bytes. Simulation has been performed for 500 s with a 21-node cluster over a network area of 450 m × 450 m because proposed trust protocol is based on 1-hop cluster. Although it has been observed that it is tough to identify the reason of packet drop that's why we have consider a node as bad node on the basis of trust value. Table represent the simulation parameters and their respective values (Table 1):

Table 1. Simulation parameters

Simulation parameter	Assigned value
Application Agent	CBR
Addressing Scheme	IDDIP
Packet Size	512 bytes
Transport Agent	UDP
Routing Protocol	AODV
Network Area	450*450
Mobility	0–5 m/s
No. of nodes	21
Malicious nodes	5
Mobility Model	Random way point
Pause Time	5 s
Simulation Time	500 s

5 Result

This section includes results which we have been observed during experiment. Evaluation parameters are packet delivery ratio, end to end delay, throughput, energy. A comparative studied has been done for proposed approach.

- a. **Packet Delivery Ratio:** It is the ratio of delivered packets to the destination to generated packets by source. It has been observed that, in AODV and MTAODV, packet delivery ratio increases as the number of nodes increases but in case of BAODV it returns poor results (Fig. 2).

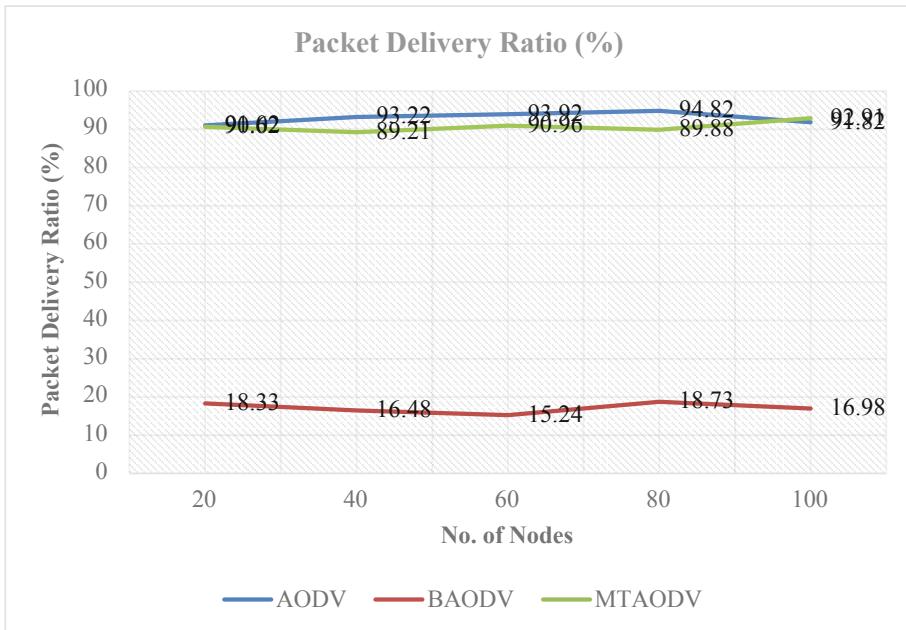
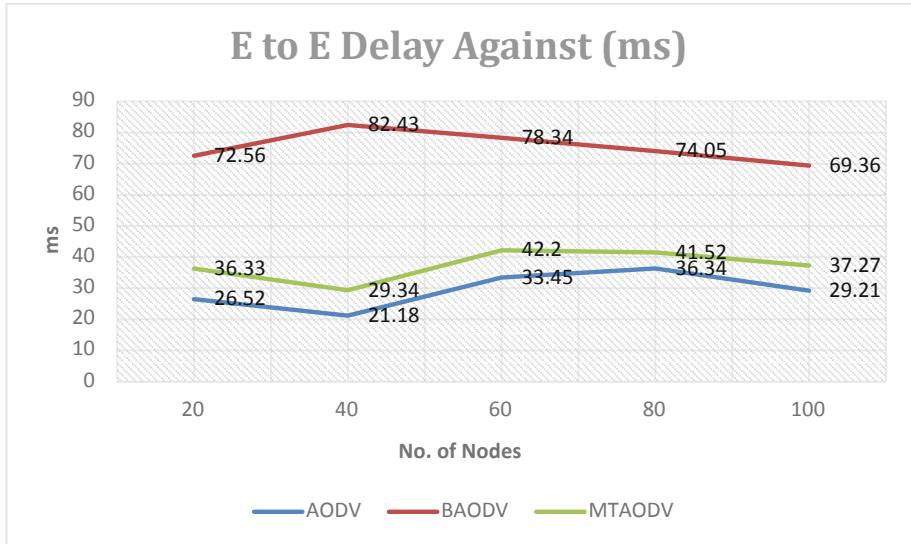
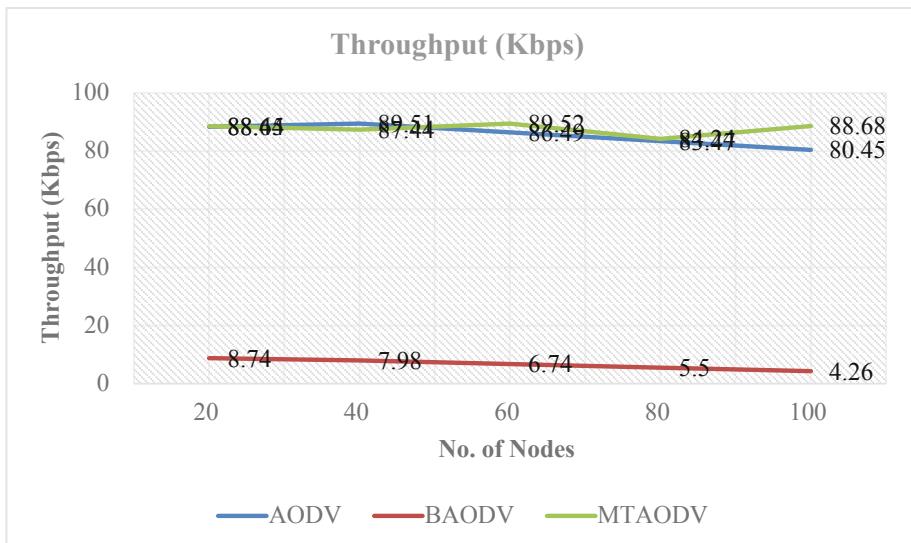


Fig. 2. Packet Delivery Ratio

- b. **End-to-end Delay:** It is the time taken by a packet to cover the distance between source to destination. It has been observed that, MTAODV returns efficient results even in case of number of nodes increases. But, in BAODV this delay increases as the number of nodes increases (Fig. 3).

**Fig. 3.** End-to-End Delay

- c. **Throughput:** Throughput is the successfully received packets in unit time. As a result it has been observed that, for AODV and MTAODV value of throughput is good although it reduces as the number of nodes increases. While in case of BAODV, it returns poor results (Fig. 4).

**Fig. 4.** Throughput

d. **Energy:** This parameter shows the effect of nodes on the energy consumption (Fig. 5).

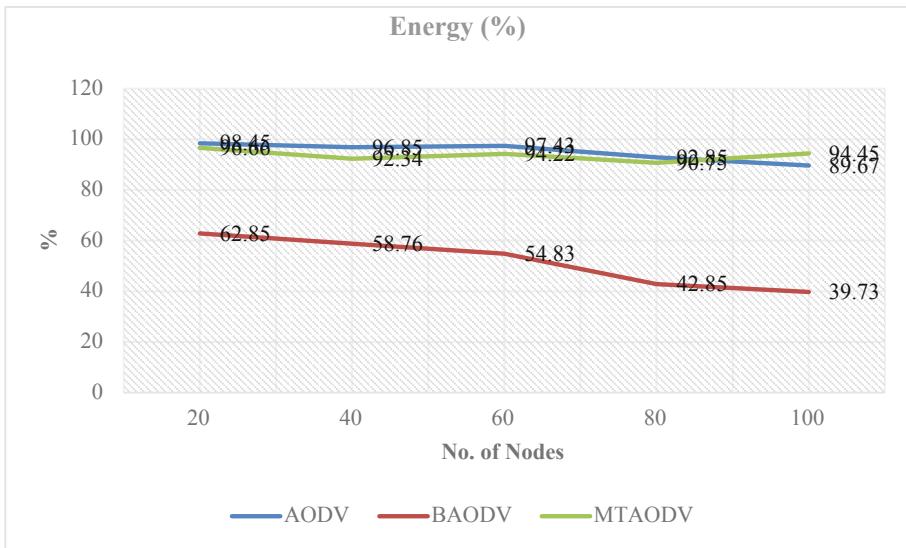


Fig. 5. Energy

Comparison

On comparing our proposed approach with existing approach, it has been observed that:

- Packet delivery ratio increases by 7% approximately as in case of existing approach its value is 82.74% while in proposed approach it returns 89.98%.
- End-to-end delay decreases by 20% approximately from 31.42% in existing work to 11.23% in proposed approach.
- Throughput increases by 7% which is satisfactory.
- Other these parameters energy values improves the performance of the network.

6 Conclusions

Internet of things (IoT) is the internet connectivity of heterogeneous network with physical devices. These wireless networks can be wireless sensor network (WSN), Wi-Fi and mobile ad-hoc network (MANET). To make IoT technology economical as well as user-friendly, it needs compatibility of IoT with wireless sensor network (WSN) and mobile ad-hoc network (MANET). This combination of IoT with MANET will be beneficial for the development of predictive model. In this paper they have proposed a trust-based model for IoT and MANET which calculates trust value for a node by

combining both direct and indirect trust opinion. For combining recommended trust evidences, ARMA/GARCH theory has been used which is helpful for the prediction of trust value for each node in multi-step. As result we observed that, proposed approach increases the packet delivery ratio, throughput and reduces end-to-end delay. As compare to existing approach PDR value increases by 7%, End-to-end delay decreases by 20% and throughput increases by 7%.

In the future, this study is beneficial for researchers who want to work in IoT field to make its implementation possible as well as integration of IoT-MANET after improving security aspects.

References

1. Bruzgiene, R., Narbutaite, L., Adomkus, T.: MANET network in internet of things system, pp. 1–27 (2017)
2. Djedjig, N., Tandjaoui, D., Medjek, F.: Trust-based RPL for the Internet of Things. In: 20th IEEE Symposium on Computers and Communication (ISCC), pp. 1–6 (2015)
3. Rath, M., Panigrahi, C.R.: Prioritization of security measures at the junction of MANET and IoT. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies, pp. 1–5 (2016)
4. Josang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. *Decis. Support Syst.* **43**(2), 618–644 (2007)
5. Virendra, M., Jadliwala, M., Chandrasekaran, M., Upadhyaya, S.: Quantifying trust in mobile ad-hoc networks. In: KIMAS 2005, 18–21 April 2005, pp. 1–6 (2005)
6. Liu, S., Yang, Y., Wang, W.: Research of AODV routing protocol for ad hoc networks. In: 2013 AASRI Conference on Parallel and Distributed Computing and Systems Research of AODV Routing Protocol for Ad Hoc Networks, pp. 1–11 (2013)
7. Jain, S., Baras, J.S.: Distributed trust based routing in mobile ad-hoc networks. In: 2013 IEEE Military Communications Conference, pp. 1–7 (2013)
8. Ghosh, U., Datta, R.: A secure addressing scheme for large-scale managed network. *IEEE Trans. Netw. Serv. Manag.* **12**, 1–14 (2015)
9. Velloso, P.B., Laufer, R.P., Cunha, D.D.O.O., Duarte, O.C.M.B., Pujolle, G.: Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Trans. Netw. Serv. Manag.* **7**(3), 1–14 (2010)
10. Chatterjee, P., Ghosh, U., Sengupta, I., Ghosh, S.K.: A trust enhanced secure clustering framework for wireless ad hoc networks, pp. 1–16. Springer, New York (2014)
11. El Defrawy, K., Tsudik, G.: Privacy-preserving location-based on-demand routing in MANETs. *IEEE J. Sel. Areas Commun.* **29**(10), 1–9 (2011)
12. Zhang, C., Zhu, X., Song, Y., Fang, Y.: A formal study of trust-based routing in wireless ad hoc networks. In: 2010 Proceedings IEEE INFOCOM, pp. 1–9 (2010)
13. Jain, A.K., Tokekar, V., Singh, U.: Detection and avoidance of integrated attacks on MANET using trusted hyperbolic AODV routing protocol. *J. Mob. Comput. Commun. Mob. Netw.* **3**, 21–34 (2016)
14. Singh, U., Samvatsar, M., Sharma, A., Jain, A.K.: Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol. In: Symposium on Colossal Data Analysis and Networking (CDAN), pp. 1–6 (2016)

15. Parihar, R., Jain, A., Singh, U.: Support vector machine through detecting packet dropping misbehaving nodes in MANET. In: International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, pp. 481–486 (2017)
16. Anguraj, D.K., Smys, S.: Trust-based intrusion detection and clustering approach for wireless body area networks. *Wirel. Pers. Commun.* **104**, 1–20 (2019)
17. Panda, M., Patra, M.R.: A novel classification via clustering method for anomaly based network intrusion detection system. *Int. J. Recent Trends Eng.* **2**(1), 1–7 (2009)
18. Sharma, A., Bhuriya, D., Singh, U.: Secure data transmission on MANET by hybrid cryptography technique. In: 2015 International Conference on IEEE Computer, Communication and Control (IC4), 10–12 September 2015, pp. 1–6 (2015)
19. Saurabh, V.K., Sharma, R., Itare, R., Singh, U.: Cluster based technique for detection and prevention of black-hole attack in MANETs. In: 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), pp. 489–494 (2017)
20. Chouhan, A.S., Sharma, V., Singh, U., Sharma, R.: A modified AODV protocol to detect and prevent the wormhole using hybrid technique. In: 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), pp. 621–625 (2017)



Offset Generator for Offset Quadrature Phase Shift Keying Modulation

Alphyn Stanley^(✉) and R. K. Sharma

School of VLSI Design and Embedded Systems,
National Institute of Technology Kurukshetra, Kurukshetra, India
alpstansley@gmail.com

Abstract. The key concept of this paper is development of an Offset generator architecture for Offset Quadrature Phase Shift Keying (OQPSK). Offset generator designed is embedded into QPSK and generates OQPSK modulation. The symbol pattern which the offset generator generates is such that there is only a maximum phase shift of $\pm 90^\circ$ between the consecutive symbols, unlike the QPSK which have $\pm 180^\circ$ maximum phase shift between the transmissions of symbol. The offset generator is designed so that it has a minimal combinational logic. The major focus of this paper is regarding the design and working of the offset generator, and OQPSK modulation. The offset generator which takes the symbol to be transmitted as input will generate an intermediate symbol when the phase of the consecutive symbols varies $\pm 180^\circ$ in constellation. The intermediate symbol differs only in $\pm 90^\circ$ with the previous symbol. After the generation of the intermediate symbol, offset generator gives out the next original symbol to be transmitted. This follows the exact OQPSK technology while it doesn't follow the conventional generation method of OQPSK modulation which provides an offset between the even and odd bit patterns of the symbols to be transmitted. The architecture is modelled using Verilog HDL and the functionality is validated from the simulation result.

Keywords: Offset Quadrature Phase Shift Keying · VLSI architecture · OQPSK · OQPSK modulator · Direct Digital Synthesizer · Conventional OQPSK methodology · Offset generator

1 Introduction

Modulators are the main part of any communication system which enables the secure and long distance communication, which is possible today. The objective of this paper is to develop a simple hardware for the Offset Quadrature Phase Shift Keying. Over the preceding years, big adaptation from techniques of analog and angle modulation transpired to the latest techniques of digital modulation [7]. Digital transmission evolved into the backbone of Satellite/Wireless/Cellular transmissions [9]. With the advent of hardware modelling in these areas, there can be a solution in developing modulators in a single chip. Direct Digital Synthesizer (DDS) are used to generate the carrier waves for the modulation [3]. The major factor of motivation for this area is the implementation of various circuits in digital domain using the Verilog code for

describing the corresponding hardware. By modelling these circuits in Verilog and as the IC technologies have improved, the future of digital modulators can be seen in a single chip.

This research work implements an offset generator for OQPSK. In conventional technique of OQPSK, the modulator splits up the symbols into odd and even bit patterns, and provides an offset delay between them [2]. This will cause no phase change more than $\pm 90^\circ$. There is a requirement of multiplier in case of conventional modulator of interest. The significance of the implemented Offset QPSK modulator is that it avoids the complex design and multipliers. The design of the offset generator is such that it can be embedded onto a current QPSK generator and will produce an Offset QPSK.

Many research works related to modelling modulators and demodulators are there over the past years. In recent years, there were simpler modelled fundamental modulators which are widely used in techniques of digital modulation such as BASK, BFSK, BPSK and QPSK [1]. The efforts of authors in [1] discuss about the idea of the sinusoidal wave generation (carrier wave) which is fundamentally based on signal sampling and quantization. In [2] VLSI architecture for high speed MPSK-modems presented architectures for BPSK, 8PSK, and 16PSK based on direct digital synthesizer (DDS). In contrast to conventional modulators, the proposed work was having no multipliers and hence they are fast & area efficient [2]. The aspiration of Vannka and Halonen in [3] was to determine DDS as a potential applications in radio communication system [3]. Research work [4] which uses, for BPSK/QPSK modulation, data stored inside a memory block to produce a symbol according to the given input data. In this also, a DDS is used for cosine and sine wave generation which is accounted as the carrier signal with the data signal to produce QPSK/BPSK output signal. In [5] authors have tried to implement the “BASK”, BFSK”, “BPSK” using encoding scheme. Binary data input is fed into an encoding scheme which is being encoded to equal number of bits [5]. [6] discusses the implementation of the offset QPSK using four different DDS systems. Each of the DDS generates 0, 90, 180 and 270 degree respectively for the carriers [6]. This architecture has the limitation when it comes to implementing more number of DDS in it since power consumption will be more. OQPSK is generated and transmitted using an optimized architecture when compared to the conventional methodology in [8]. [10–12] are some of the old publications which explains the basics of the offset QPSK and MSK. They also gives some of the disadvantages of QPSK when compared with OQPSK [15]. There are have been MATLAB/SIMULINK environment for different modulation techniques [13]. CORDIC [14] algorithm has also been used for QPSK but it increases the complexity.

2 Architecture of Offset Generator and OQPSK Modulator

2.1 Offset Generator

When it comes to modulators constellation comes in to picture first which determines in what way the incoming symbol would modify the carrier signal. Figure 1 represents the constellation diagram for which the proposed OQPSK is implemented. The QPSK for

this constellation will generate 45° , 135° , 225° , 315° when symbols are 00, 01, 10, 11 respectively. For conventional QPSK it is expected that a maximum delay of $\pm 180^\circ$ is expected. This happens when symbols 00, 10 or 01, 11 comes consecutively.

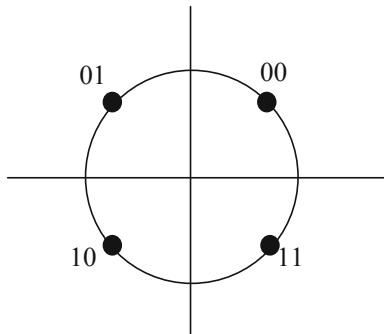


Fig. 1. Constellation diagram

The offset generator is shown in figures Figs. 2 and 3. This combinational logic of offset generator reduces the maximum phase shift of $\pm 180^\circ$ that can occur in the conventional QPSK to $\pm 90^\circ$ which converges to the concept of Offset QPSK.

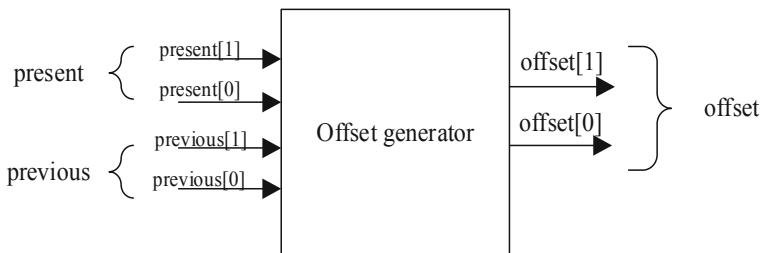


Fig. 2. Proposed offset generator architectural

The offset generator architecture has present and previous input bits that implies the incoming symbols to the conventional QPSK. This architecture, when it receives symbols that differ in $\pm 180^\circ$ will not allow the transmission of the second symbol for the first half of symbol transmission. During this period it will produce an intermediate symbol which is fed in to the QPSK and has only $\pm 90^\circ$ phase shift with the previous symbol. For next half of symbol transmission it transmits the actual symbol. The output “offset” drives the QPSK modulator.

The simple combo logic of offset generator represented in figure Fig. 3. The symbol bits previous and present are fed into XOR gate. “Offset [1]” is same as “Present [1]”.

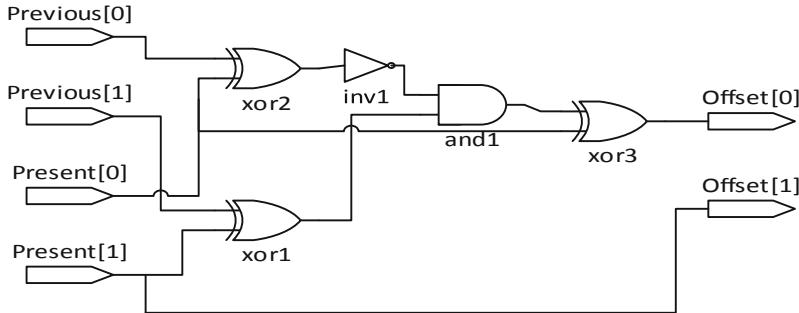


Fig. 3. Gate level view of offset generator

The working of the offset generator can be explained with an example. Consider 01 symbol is followed by 11 which is differing in 180° phase. During the transmission of first symbol “01” both Previous [1:0] and Present [1:0] will be loaded with the same symbol. Since Offset [1] is same as Present [1], it will be “0” (Most significant bit). For the symbol 01 output of xor1 and xor2 will be 0. Output of and 1 will be “0”. So, finally Offset [0] which is driven by output of xor 3 will have “1” since it has “1” as one of the input from Present [0] and “0” as the other input from output of and 1. Now for the first symbol it Offset [1:0] has “01” symbol at output. For the next transmission symbol to be transmitted is “11”, previous bit is 01 and present bit is 11. Now output of xor 1 will be 1 and output of xor 2 will be 0. The AND gate and 1 has output 1. Finally, the offset bits will have “10”. This symbol which differs only in 90° phase with the previous symbol 01, is transmitted for the first half of symbol transmission. For next half of symbol transmission, the previous bits will now loaded with “11”. This will give “11” at output of the offset generator.

2.2 Implementation of Offset Generator in QPSK Modulator to Generate Offset Qpsk

This implementation of Offset generator is on a QPSK modulator from [2]. Figure 4 depicts the complete architecture of the OQPSK modulator. The implementation is different from the conventional OQPSK, where the odd and even bits are introduced with a delay. The architecture uses a 7 bit counter which is the clock generator for other blocks as well as contributes to the input of the ROM address. The technology used is to generate a carrier wave using ROM, the Direct Digital Synthesizer (DDS) [3]. The digitized sample points of the sinusoidal carrier till $\pi/2$ are saved, in 8 bits digital format, in the 16x8 ROM. The generated clocks for the blocks in Fig. 4 is such that the offset bits are captured properly by the register. The 1's compliment (1'sC) and 2's compliment (2'sC) blocks along with 6 bit output of adder are used to alter the normal sinusoidal generation at output of ROM to a modulated signal [2].

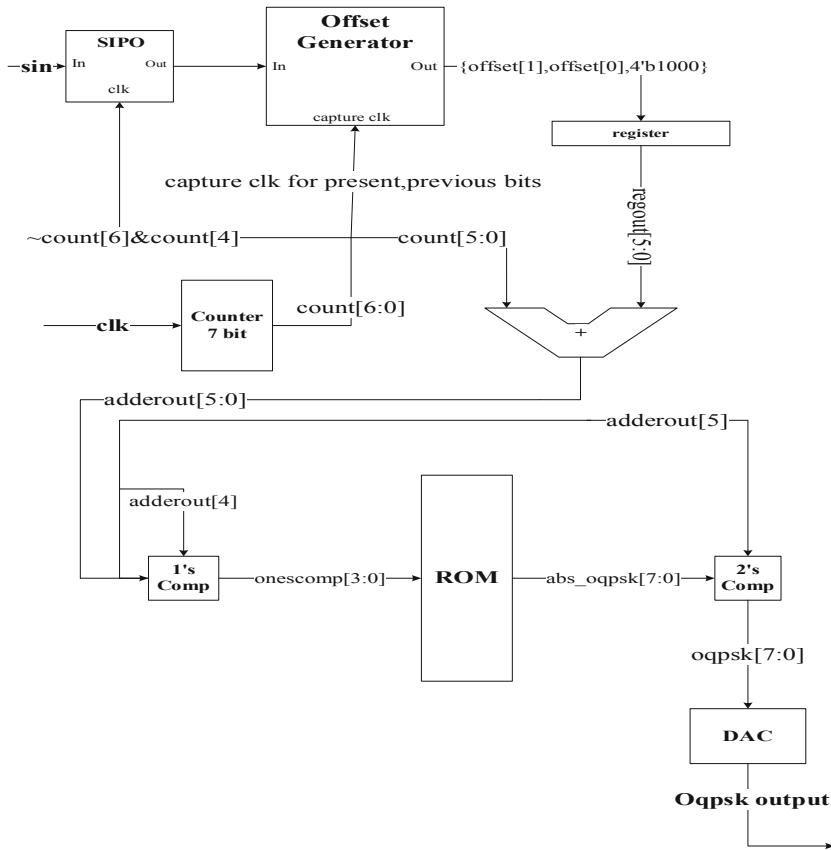


Fig. 4. Architecture of implemented OQPSK

The ROM locations indicates the value of sinusoidal signal at particular phase. There are 16 locations corresponding to the range 0° to 90° phases. The 8th location of ROM indicates 45° phase of sinusoidal signal. The 1'sC and 2'sC serve the purpose of completing the sinusoidal wave from 16 samples. When the 2nd MSB of the 6 bit adder output is '1', the 1'sC value of 'adderout [3:0]' is given as ROM address input which outputs the sinusoidal wave such that it is continuing form 90° . For example, if adderout [5:0] is 001111 which points to ROM location corresponding to 90° phase of signal. Now during the next cycle the value becomes '010000' which enables the 1'sC and outputs 1'sC of 0000 (adderout [3:0]); i.e., '1111', which in turn again points to 90° phase value. When adderout [5:0] increments to next value '010001', ROM's address input now will be '1110' which points to value lesser than 90° phase of the sinusoidal signal (approx.. $\sin(84.375^\circ)$). When the MSB of the 6 bit adder is '1', it gives out 2'sC of the value which completes the sinusoidal carrier for negative value range.

3 Results

The working of OQPSK modulator is explained based on an example. Consider input symbols 00, 10, 00 which shows a 180° phase shift between the symbols.

When first symbol ‘00’ is input through ‘sin’, the offset generator will give out ‘00’ as explained earlier. This is combined with ‘1000’ to form ‘001000’, which is captured by the register and adder adds it with the 6 bit counter value. The output of adder given to the combination of ROM, 1’sC and 2’sC produces sinusoidal signal starting at 45°. When the next symbol ‘10’ enters, which differs in 180° phase with ‘00’, Offset generator will give out ‘11’ during first half of symbol transmission. From count [5:0] value starting from zero, the output of adder will be ‘111000’ which will feed 1’sC as well as 2’sC with ‘1’. So, output of 2’sC will be giving a value corresponding to sin (315°), since “ $-\sin(45^\circ) = \sin(315^\circ)$ ”. Thus carrier signal corresponding to ‘11’ produced is of phase 315°. For the next half of symbol transmission, offset generator outputs ‘10’ for which the output will correspond to 225° phase of carrier. The OQPSK output waveform for the architecture is shown in Fig. 7 for same set of input symbols.

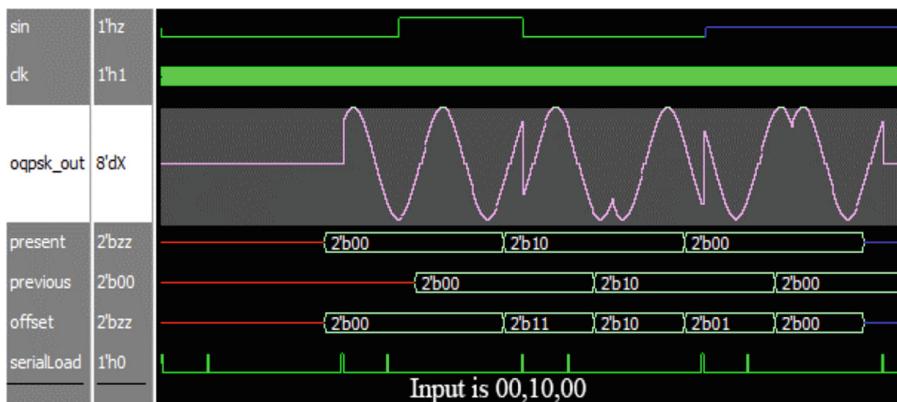


Fig. 5. OQPSK modulation waveform for input symbols 00, 10, 11

4 Conclusion

The key concept of this research of developing an architecture for Offset Quadrature Phase Shift Keying (OQPSK) implies the scopes of architecture with respect to the usage and integrity of the architecture with other systems. Minimal combinational logic used for the Offset generator ensures the integrity of the same with a “QPSK modulator”. We have tried to implement the offset generator with minimal combinational logic. The authors have attempted to design the offset generator as an add-on to the QPSK modulator such that OQPSK is generated and is different from the conventional

OQPSK modulators. OQPSK using offset generator type technology is not present to the best of our knowledge at the time of this design. The proposed design was implemented using Verilog HDL and simulated using Model Sim PE Student Edition 10.4a.

Acknowledgements. The authors are thankful to School of VLSI Design and Embedded Systems of National Institute of Technology Kurukshetra, India, for the technical requirements of this work.

References

- Sharma, S.A., et al.: VERILOG based simulation of ASK, FSK, PSK, QPSK digital modulation techniques. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). IEEE (2017)
- Mamidala, C., Dhar, A.S.: High-performance VLSI architectures for M-PSK modems. *IET Circ. Devices Syst.* **11**(2), 166–172 (2017)
- Vankka, J., Halonen, K.A.: Direct digital synthesizers: theory, design and applications, vol. 614. Springer (2013)
- Patel, M., Desai, N., Soni, B., Purani, A.: Design of BPSK/QPSK modulator using verilog HDL and matlab. *Communications on Applied Electronics (CAE) – Foundation of Computer Science FCS*, vol. 2, p. 3, New York, USA (2015). ISSN 2394-4714
- Sushmaja, K., Noorbasha, F.: Implementation of binary shift keying techniques. *Int. J. Eng. Trends Technol. (IJETT)*, **4**(6) (2013)
- Li, F., Ke, X., Li, Q.: Design and implement of OQPSK modulator based on FPGA. In: 2007 8th International Conference on Electronic Measurement and Instruments. IEEE (2007)
- Aaron, M.: Digital communications—the silent (R) evolution? *IEEE Commun. Mag.* **17**(1), 16–26 (1979)
- Muthalagu, R., Sudheer, R., Ibrahim, S.: FPGA implementation of optimized QPSK and OQPSK using VHDL. *J. Commun.* **13**(4) (2018)
- Haykin, S.: Digital Communications. Wiley, New York (1988)
- Rhodes, S.A.: Effect of noisy phase reference on coherent detection of offset-QPSK signals. *IEEE Trans. Commun.* **22**(8), 1046–1054 (1974)
- Gronemeyer, S., McBride, A.: MSK and offset QPSK modulation. *IEEE Trans. Commun.* **24**(8), 809–820 (1976)
- Moraes, D., Feher, K.: Bandwidth efficiency and probability of error performance of MSK and offset QPSK systems. *IEEE Trans. Commun.* **27**(12), 1794–1801 (1979)
- Quadri, F., Tete, A.D.: FPGA implementation of digital modulation techniques. In: 2013 International Conference on Communication and Signal Processing. IEEE (2013)
- Brahmachari, A., Paily, R.P.: Low power 2.4 GHz RF transmitter for satellite subsystem using CORDIC based frequency translator. In: 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN). IEEE (2012)
- Chen, H.-H.: Waveform shaping techniques for bandwidth-efficient digital modulations. In: *Wireless Communications Systems and Networks*, pp. 559–612. Springer, Boston (2004)



Quantitative Analysis of Radio Frequency Spectrum Occupancy for Cognitive Radio Network Deployment

Sheetal Borde¹(✉), Kalyani Joshi², and Rajendrakumar Patil¹

¹ College of Engineering, Pune, India

sdbpune@gmail.com, rap.extc@coep.ac.in

² PES's Modern College of Engineering, Pune, India

krjpune@gmail.com

Abstract. The increasing demand of wireless applications has increased need for Radio Frequency (RF) spectrum. But the fixed spectrum allocation policy has created a spectrum scarcity issue. In this scenario, cognitive radio is emerging as a promising solution for the effective utilization of the RF spectrum. The spectrum occupancy measurements are one of the preliminary requirements for the exploitation of cognitive radio technology in any geographical location. In this paper, the experimental results for a real time analysis of spectrum utilization of the RF band from 50 MHz to 1930 MHz in Pune city (Maharashtra, India) are discussed and a simple demonstration for utilization of the white space is also presented. Real time measurements are taken using Wideband Spectrum Sensing (WSS) algorithm with the help of Universal Software Radio Peripheral hardware. The results clearly indicate the presence of spectrum white spaces enabling the future scope for cognitive radio network deployment.

Keywords: Cognitive radio · NI-USRP 2920 · Spectrum occupancy · Spectrum sensing · Wideband spectrum sensing

1 Introduction

The usage of wireless communication has expanded rapidly due to the need of mobility and convenience. The increasing demands for frequency channels made the current allocation methods unfeasible. Besides the wide sharing of spectrums, it was also found that most of the allocated spectrums are not fully utilized by primary users (PU). This leads to the creation of white spaces. When a band of frequencies is assigned to a PU but at a particular time and specific geographical location, the band is not being utilized by that user then it is called as White Space.

Cognitive Radio (CR) is a special type of wireless communication in which a transceiver can wisely detect the free communication channels and allocate them to secondary users. The available radio-frequency (RF) spectrum is utilized in such a way so that minimum interference is caused to the primary users. Thus CR technology can prove to be effective to address the problem of spectrum scarcity. The cognitive cycle is a continuous process and it involves different stages as shown in Fig. 1.

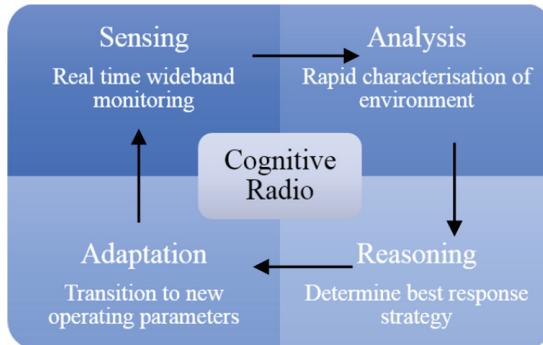


Fig. 1. Stages in a cognitive cycle

The cognitive radio receiver is supposed to do continuous sensing and monitoring of the wideband spectrum in order to find out spectrum white spaces. After sensing, the receiver should do analysis of the characteristics of the environment. Based on the analysis, the best response strategy is decided and then the receiver adapts to the new operating parameters [3].

Though, spectrum scarcity is becoming a big problem for upcoming wireless applications, there is actually no scarcity of the spectrum. Just because of static spectrum allocation policies of the government, this scene has been created.

Considering the importance of spectrum occupancy measurements, this paper aims to give a quantitative measurement of spectrum occupancy in the frequency bands ranging from 50 MHz to 1930 MHz in the crowded urban part of Pune city (Maharashtra, India). The experimental set up uses a Software Defined Radio (SDR) platform from National Instruments which can be programmed using LabVIEW software. All measurements are carried out in an indoor lab environment during busy hours with varying noise conditions. As a large band of spectrum is to be scanned, a simple wideband spectrum sensing algorithm is used here. The main contribution of the paper is the estimation of percentage spectrum occupancy of the frequency bands assigned for various applications for exploring the possibility of cognitive radio network deployment.

2 Spectrum Occupancy Measurement Survey and Process

Many campaigns were conducted worldwide in past few years to find out the actual utilization of the spectrum. A first this kind of spectrum measurement campaign was conducted in USA by National Telecommunication and Information and Administration (NTIA) in 1998 [17]. The main motivation of the activity was to measure the spectrum utilization in different parts of the USA. The results varied geographically and most of the licensed spectrum was found vacant most of the time. The next large scale spectrum occupancy measurement was done by McHenry et al. in year 2006. The motivation was to find out actual utilization of the spectrum in crowded urban

environments. The average spectrum utilization in Chicago was found to be only 17.4% during this campaign [12].

Similar measurement were also carried out at different places in the world namely, Spain, Germany, New Zealand, Singapore, Malaysia etc. by different research groups. The results indicated that overall utilization of the spectrum is very low and there is a lot of scope for cognitive radio technology in the future to solve the problem of spectrum scarcity [16]. Matinmikko et al. [11] presented a directional and cooperative spectrum occupancy measurements in the 2.4 GHz ISM band where several systems coexist and share the same spectrum using low transmission power levels. The main aim of the paper was to actually demonstrate a directional and cooperative spectrum occupancy measurement approaches so as to show the influence of the spatial dimension on the actual spectrum use.

Considering the importance of spectrum scarcity problem, few spectrum measurement activities were also conducted in different parts of India in order to find out spectrum utilization. Patil et al. in year 2011 conducted measurement campaign for the frequency band from 700 MHz to 2700 MHz in the central part of the Mumbai (Maharashtra, India) which has reported very low spectrum usage. A quantitative analysis of the 470–590 MHz UHF TV band was performed to estimate the available TV white space India. The results were very astonishing which have shown that almost 100% of the TV band (all 15 TV channels) are free in 36.43% of the areas of the four zones in India [13].

A similar spectrum measurement activity in the Kochi city (Kerala, India) and Jaipur city (Rajasthan, India) by different research groups have shown a prominent presence of spectrum white spaces in the frequency bands ranging from 50 MHz to 4400 MHz specially in the VHF/UHF, GSM and ISM bands [1, 9].

The spectrum occupancy measurement process mainly has three main steps- collection of raw data from USRP, setting appropriate threshold and calculation of average duty cycle for each frequency band. The received signal power is called as raw data inputs. For setting appropriate threshold for each band, first of all average noise floor is estimated and then threshold is set 10 dB above the noise floor in order to avoid false alarming as per the ITU recommendations [8]. It is also confirmed during a measurement campaign in New Zealand that with a noise margin of 10 dB above the noise floor, the false alarm rate is only 0.0005% [10]. The decision threshold for different bands given in the previous research paper were also useful for finalizing the values [16].

The Duty cycle or the average calculated occupancy indicates that for what portion of time the signal is present during a sampling period of scanning of a band. The duty cycle is defined as the percentage of time a frequency band or channel is occupied over the given period of observation

$$\text{Duty Cycle} = \frac{\text{Occupation Period of Signal}}{\text{Total Period of Observation}} \times 100\%$$

When the channel power is measured in the time slots,

$$\text{Duty Cycle} = xT/y$$

Where x is the number of time slots T where the received signal level is greater than the decision threshold and y is the total time slots.

Alternatively, Co-operative spectrum sensing (CCS) techniques can also be used to estimate the spectrum occupancy. Each CR node can sense a small sub band in a parallel and then their decisions can be combined to decide the presence of white spaces in the spectrum. But the implementation complexity and increased communication overheads are the main limitations of CCS because of which it is not considered in practical scenarios [6, 19].

3 Wideband Spectrum Sensing Algorithm

In one single scan, a wideband spectrum sensing technique is able to sense a band of spectrum that is usually greater than the coherence bandwidth of the channel. Wideband spectrum sensing senses multiple frequency bands rather than considering one band at a time. An effective spectrum sensing technique is one which accurately senses the desired band of frequency to find out white spaces without interfering the licensed primary user. Wideband spectrum sensing technique actually can improve the throughput of the CRNs by sensing multiple bands simultaneously and thus reducing the overall sensing duration [4, 7, 20].

There are many wideband spectrum sensing techniques suggested in the earlier research papers which can be broadly categorized as Nyquist based techniques and Sub-Nyquist based techniques as the later one do not follow the Nyquist rate for sampling. Though it is true that, traditional Analog to Digital convertor (ADC) based WSS technique which follows Nyquist rate, requires a high sampling rate, they give more accurate results. The compressive sensing technique which operates below Nyquist rate is simple to implement but accuracy is not guaranteed. This is because the main limitation of the compressive sensing is the requirement of sparsity of the received power spectrum which is very difficult to obtain in the practical scenario [18]. Thus, there is a need of a simple wideband spectrum sensing technique which can overcome this limitation.

In this paper, for spectrum occupancy measurement, a simple Wideband Spectrum Sensing (WSS) algorithm is proposed. The flowchart of the algorithm is as shown in Fig. 2. The basic idea is to scan the spectrum in the given frequency limits, calculate the energy of the received signal for each frequency value and plot a power spectrum. Then estimate the noise floor and set the decision threshold 10 dB above the noise floor in order to avoid the false alarms. For each band, compare the received signal with the threshold, calculate the duty cycle and the percentage occupancy of the band. This is a Nyquist based WSS technique in which sampling rate as high as 1 MHz or greater than that is used.

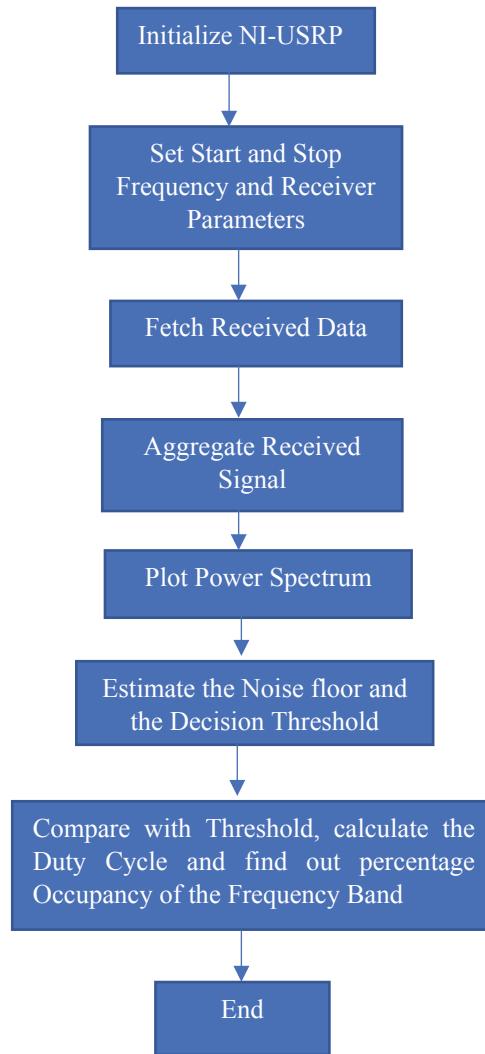


Fig. 2. Flowchart of wideband spectrum sensing algorithm

4 Results and Discussions

Wideband Spectrum Sensing of the RF Spectrum was successfully performed by NI-USRP 2920 and NI-LabVIEW [2, 5, 15]. The power spectrum of all the bands in the RF range from 87 MHz to 1930 MHz were obtained. As per the National Frequency Allocation Plan 2018 of the Wireless Planning & Coordination Wing (WPCW) of Indian Government, various bands in this range are allocated for different applications. The band allocation by WPCW is mentioned in the Table 1 [14].

The Figs. 4, 5 and 6 show some of the results of real time spectrum sensing of three different bands obtained using wideband spectrum sensing algorithm. Figure 3 shows results for GSM 900 band (both uplink and downlink). As can be seen from the power spectrum, the GSM uplink band (890 MHz to 915 MHz) is more utilized than the downlink band (935 MHz to 960 MHz). This may be because the sensing activity is done in the vicinity of a base station so that signals transmitted by the base station antenna in the downlink band are traced in the scan.

But, as all the mobile stations can not be in the vicinity of the USRP, only few signals transmitted by the mobile station on the uplink band can be captured. On an average, only 51 MHz band is utilized out of total 155 MHz allocated spectrum which results in only 32.9% spectrum utilization. Figure 4 displays the power spectrum for GSM 1800 band. In this also more utilization of downlink band as compared to uplink band is observed for the same reasons as stated above. The spectrum utilization is found to be only 20.22%. There is almost white spectrum observed in the 159.75 MHz to 173 MHz band as shown in Fig. 5. As stated in Table 1, this band is allocated for Satellite communication, aeronautical navigation, outdoor broadcast vans and no activity was detected in the band for the given time and geographical location. Table 1 enlists the band allocation and percentage occupancy of other frequency bands used for different application obtained using wideband spectrum sensing algorithm. Figure 6 shows the presence of five FM channels broadcasted in Pune region specifically at frequencies of 91.1 MHz, 93.4 MHz, 94.3 MHz, 95 MHz and 98.3 MHz, respectively. There is one more FM channel at 101 MHz which is not displayed as it is out of range of the graph.

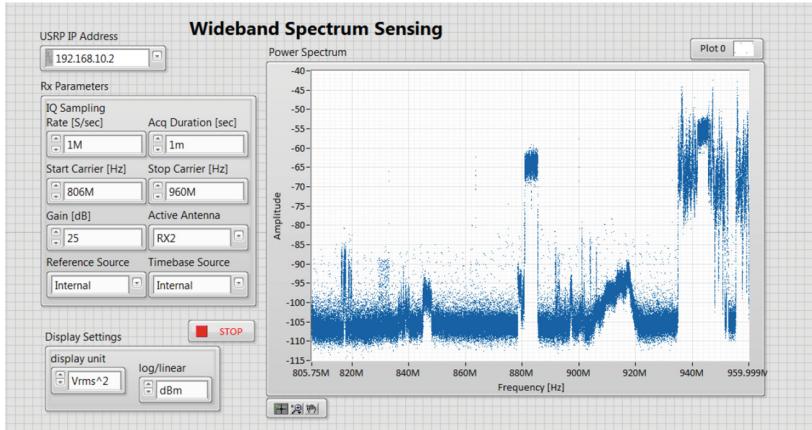


Fig. 3. Real-time frequency spectrum from 805 MHz to 960 MHz (900 MHz GSM Band).

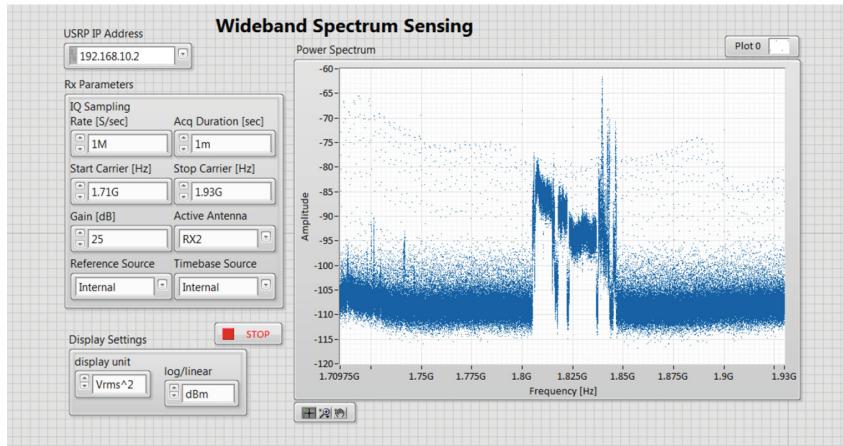


Fig. 4. Real-time frequency spectrum from 1.7 GHz to 1.93 GHz (1800 MHz GSM Band).

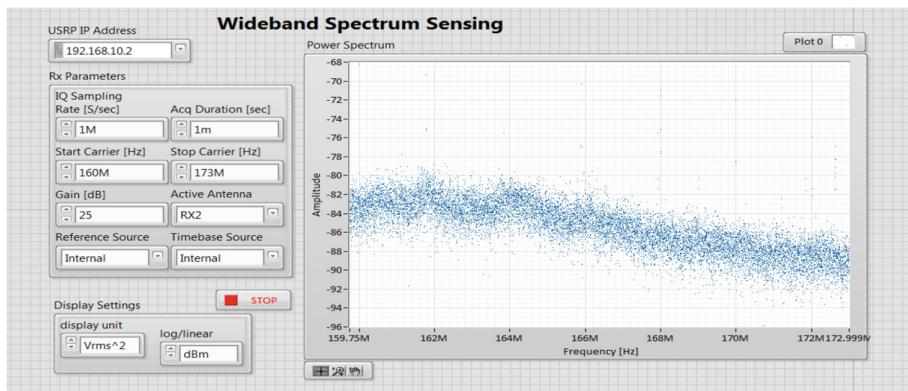


Fig. 5. Real-time frequency spectrum from 159.75 MHz to 173 MHz

5 Utilization of White Spaces

The analysis of FM band in Pune shows that, a major portion of FM band is unutilized. There are only six active FM channels in Pune region in the total allocated band of 87 MHz to 108 MHz. The percentage occupation of FM band was found to be only 24.3%. The unutilized band can be used for affordable backhaul communication. Advantage of FM band is that it has long range for data communication up to several kilometres and can pass through walls because of its high wavelength. To demonstrate how the spectrum white spaces can be utilised, one unutilised band in FM spectrum is

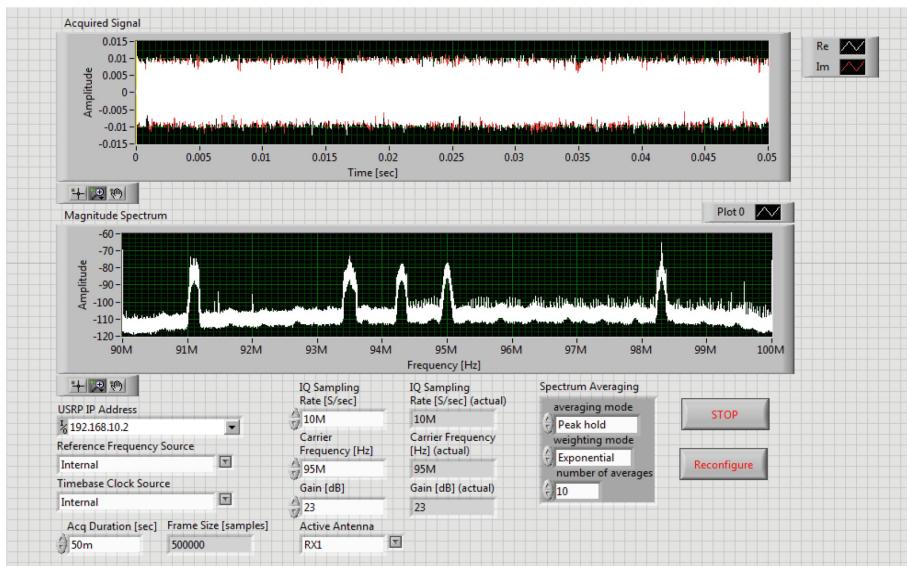


Fig. 6. Real-time frequency spectrum of FM band showing presence of five FM channels in Pune region

Table 1. Frequency band allocation and occupancy

Band	Services	Occupied spectrum (%)
50–87.5 MHz	Marine and aeronautical navigation, short and medium wave radio, amateur radio	10.28%
87.5–108 MHz	FM radio broadcasts	24.3%
159.75–173 MHz	Satellite communication, aeronautical navigation, outdoor broadcast vans	0%
174–187.5 MHz	Radio astronomy services	8.9%
230–450 MHz	Satellite communication, aeronautical navigation	4.09%
450–585 MHz	Public Protection and Disaster Relief (PPDR) applications	5.18%
585–806 MHz	Digital Broadcasting services	14.02%
805–960 MHz	GSM 900 Band	32.9%
960–1710 MHz	Aeronautical and space communication	0%
1710–1930 MHz	GSM 1800 Band	20.2%

chosen for experimentation purpose. NI-USRP is programmed as a FM transmitter as shown in Fig. 7. An audio file as shown in Fig. 8 is transmitted on one of the unused FM band. At the same time, 2–3 FM receivers were kept in the vicinity of the USRP and tuned to the same FM band. It was observed that the transmitted audio file of 2.5 s was successfully received on all the nearby FM receivers.

This indicates that the spectrum white spaces can be used in enormous ways to satisfy short distance wireless applications and thus can help to address the problem of spectrum scarcity.

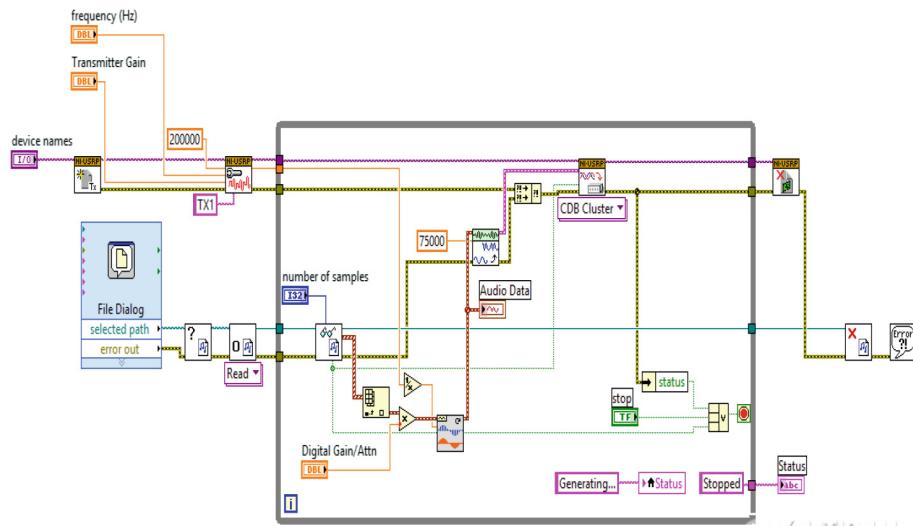


Fig. 7. LabVIEW block diagram of USRP as a FM transmitter

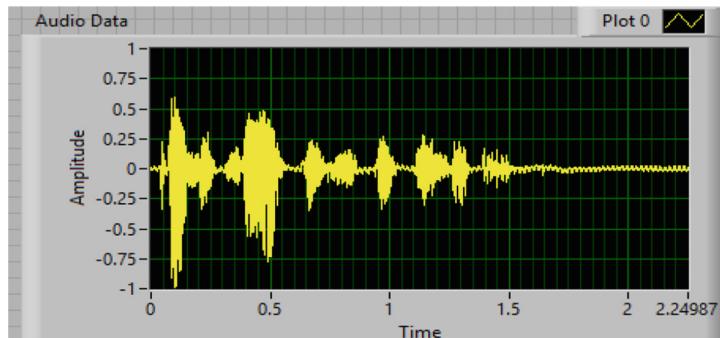


Fig. 8. Audio file transmitted using USRP

6 Conclusion

For cognitive radio network deployment, it is necessary to exploit the presence of white space in the RF band. The work presented in this paper illustrates the spectrum occupancy in RF band licensed for various applications. As can be seen from the results, there are many white spaces available in each of the band. Wideband Spectrum Sensing algorithm can be used for the analysis of a large frequency spectrum and

provides basic idea about the presence of a primary user. The NI-USRP and NI-LabVIEW were used for analysis of the RF Spectrum. The RF spectrum (87 MHz–1930 MHz) was scanned during particular sessions. The presented work in this paper concluded that the spectrum utilization of the RF Spectrum as a whole in the Pune central part is not efficient at all times and the spectrum can be utilized for cognitive radio network deployment when it's unoccupied. A demonstration of transmission of FM signal on unused FM band illustrates the same fact.

References

1. Agarwal, A., Sengar, A.S., Gangopadhyay, R., Debnath, S.: A real time measurement based spectrum occupancy investigation in north-western India for Cognitive Radio applications. In: Proceedings of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, pp. 2035–2039 (2016)
2. A Hands-on Introduction to Software Defined Radio with NI USRP and NI LabVIEW. https://lumen.ni.com/nicif/US/GB_EKITNIUSRPLV/content.xhtml
3. Akyildiz, I.F., Lee, W.-Y., Vuran, M.C., Mohanty, S.: NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Comput. Netw.* **50**(13), 2127–2159 (2006)
4. Chen, D., Yang, J., Wu, J., Tang, H., Huang, M.: Spectrum occupancy analysis based on radio monitoring network. In: Proceedings of the 1st IEEE International Conference on Communications in China (ICCC), Beijing, pp. 739–744 (2012)
5. Getting Started Guide NI USRP-2920. www.ni.com/pdf/manuals/376358a.pdf
6. De, C.K., Kundu, S.: Adaptive decode-and-forward protocol-based cooperative spectrum sensing in cognitive radio. *Int. J. Commun. Netw. Distrib. Syst.* **14**(2), 117–133 (2015)
7. Hoseini, P.P., Beaulieu, N.C.: An optimal algorithm for wideband spectrum sensing in cognitive radio systems. In: Proceedings of the IEEE International Conference on Communications, Cape Town, South Africa, pp. 1–6 (2010)
8. HANDBOOK Spectrum Monitoring. International Telecommunication Union (ITU), Radiocommunication Bureau (2011). <https://www.itu.int/pub/R-HDB-23-2011>
9. Jacob, J., Jose, B.R.: Spectrum occupancy measurement and analysis in Kochi-India from a cognitive radio perspective. In: Sixth International Symposium on Embedded Computing and System Design (ISED), Patna, India, pp. 328–333 (2016)
10. Lee, B.M., Song, H., Lee, J.S.: Implementation of a regional spectrum sensing based cognitive radio system for digital TV white space. *IETE Tech. Rev.* **35**(6), 590–598 (2018)
11. Matinmikko, M., Mustonen, M., Höyhtyä, M., Rauma, T., Sarvanko, H., Mämmelä, A.: Directional and cooperative spectrum occupancy measurements in the 2.4 GHz ISM band. *Int. J. Autonom. Adapt. Commun. Syst.* **7**(4), 339 (2014)
12. McHenry, M.A., Tenhula, P.A., McCloskey, D., Roberson, D.A., Hood, C.S.: Chicago spectrum occupancy measurements & analysis and a long-term studies proposal. In: Proceedings of the Workshop on Technology and Policy for Accessing Spectrum (TAPAS), Boston, USA (2006)
13. Naik, G., Singhal, S., Kumar, A., Karandikar, A.: Quantitative assessment of TV white space in India. In: Proceedings of the Twentieth National Conference on Communications (NCC), Kanpur, India, pp. 1–6 (2014)
14. National Frequency Allocation Plan, October 2018. <http://wpc.dot.gov.in/WriteReadData/userfiles/NFAP%202018.pdf>
15. NI USRP 2920 manual. <https://www.ni.com/en-us/support/model.usrp-2920>

16. Patil, K., Skouby, K., Chandra, A., Prasad., R.: Spectrum occupancy statistics in the context of cognitive radio. In: Proceedings of the 14th International Symposium on Wireless Personal Multimedia Communications (WPMC), Brest, France, pp. 1–5 (2011)
17. Sanders, F.H.: Broadband spectrum surveys in Denver, CO, San Diego, CA, and Los Angeles, CA: methodology, analysis, and comparative results. In: 1998 Proceedings of IEEE Symposium on Electromagnetic Compatibility (1998)
18. Shaban, M.: Sub-Nyquist spectrum sensing for wideband cognitive radios: a survey. *Int. J. Wirel. Mob. Comput.* **12**(2), 107–116 (2017)
19. Shukla, S., Srivastava, N.: An overview on cooperative spectrum sensing in cognitive radios. *Int. J. Wirel. Mob. Comput.* **11**(4), 267 (2016)
20. Sun, H., Nallanathan, A., Wang, C., Chen, Y.: Wideband spectrum sensing for cognitive radio networks: a survey. *IEEE Wirel. Commun.* **20**(2), 74–82 (2013)



Multiprocessor Systems Design: Reliability Analysis of Multistage Interconnection Network

Amit Prakash^{1(✉)} and Dilip Kumar Yadav²

¹ Department of Electronics and Communication Engineering, NIT Jamshedpur,
Jamshedpur, Jharkhand, India

amitprakash.ece@nitjsr.ac.in

² Department of Computer Applications, NIT Jamshedpur, Jamshedpur,
Jharkhand, India
dkyadav.ca@nitjsr.ac.in

Abstract. The recent research in computing methodologies and the demand for high-speed computational resources are growing at an unprecedented rate. The communication performance is a crucial factor, influencing the performance of supercomputers, which forms the elemental parallel architecture of high-performance computer systems. The multistage interconnection network is a communication channel in the multiprocessor systems, which is primarily used to interconnect a number of processing elements and memory components that remains as an adequate substitute for the crossbar switches used earlier.

In this paper, Terminal reliability between the source-destination node pair of multistage interconnection network is evaluated to access the probability of successful transmission. Terminal reliability is evaluated for multistage interconnection network with an assumption that the fault occurs independently, links of the network are reliable, switches are either working or failed, and routing through alternative paths using path sets method based on the reliability block diagram.

Performance of these multistage interconnection networks are evaluated based on Terminal reliability, fault-tolerance, and hardware cost.

Keywords: Terminal reliability · Reliability block diagram · Fault-tolerance · Switching element

1 Introduction

The growth of high performance, low hardware, and fault-tolerant multistage interconnection network (MIN) is the necessity for powerful multiprocessor system to achieve the technological advancement in parallel computing. Crossbars used earlier had high cost, maintainability with low performance, the MINs were developed as substitution [1, 2].

The design of MIN, comprise of fault-tolerant ability, alternative paths, hardware cost, self routing and re-routing behaviour, which provides strong re-readability under

any switch failures [3]. Multiple switch component failures of MIN must be tolerated, *i.e.* if processing element (PE) fails, the residual PEs can communicate without any interruption and reliability should be higher to determine the performance of the network [4].

Fault-tolerance and reliability of MINs, count on disjoint and redundant paths, *i.e.* more disjoint paths improves the performance and reliability [5]. It provides multiple paths for source-destination pair *i.e.* alternate paths can be used [6].

Shuffle-exchange, baseline, omega, cube possess single path interconnection for each source-destination node pair. The disadvantage of these models are that if any switch/link fails it results in loss of transmission [7].

In crash/failure of switch/link, disjoint path predicts the node failures required to trigger the network failure. Therefore for n disjoint paths, at least n number of disjoint paths for any node pairs will have the information to tolerate minimum number of switch failures.

Shuffle Exchange Network (SEN+ and SEN+2) was introduced by increasing a significant number of stages, but they possess low Terminal reliability (TR) due to increase in components and complexity. The significant advantages of terminal reliability are the shorter formula, less storage, much less computing time, and the ability to process a wider variety of large and complex networks [8, 9].

In this paper, path sets method based on Reliability block diagram (RBD) and the Sum of disjoint products-multiple variable inversion technique (SDP-MVI) is used for evaluating the TR with assumptions, that the fault occurs independently, links are reliable, switches are either working or failed [10]. The technique to evaluate the reliability of a systems based on minimal path sets, the path sets enumeration technique produces path sets in lexicographic increasing order of cardinality, which obtains sum of disjoint products (SDP) reliability expressions in compact form [11].

The paper is structured as follows: Sect. 1 states the introduction and motivation for the need of MINs, in Sect. 2 the Terminal reliability has been estimated for MINs, Sect. 3 presents performance analysis and comparison summary of MINs. Section 4 concludes the paper, followed by the references.

2 Terminal Reliability Estimation of Various Multistage Interconnection Network having Single Fault-Tolerant

2.1 SEN

Single path and single switch/link failure network, with each stage having $N/2$ switching elements (SE) which are either operating/non-operating states [12] of size 2×2 , and network complexity of $((N/2) * \log_2 N)$ [1, 7, 10] the model is shown in Fig. 1 with the RBD [13] presented in Fig. 2.

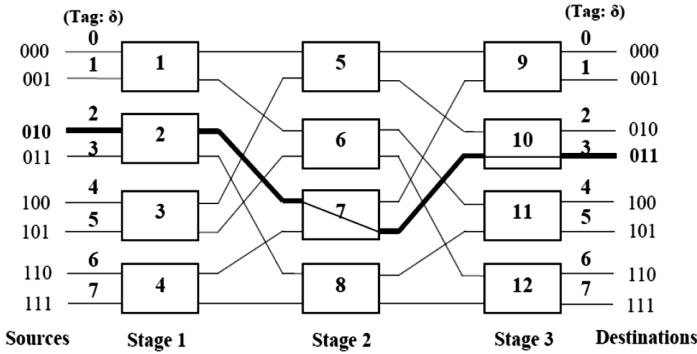


Fig. 1. SEN: TR paths from S_2 ($\delta = 2,3$) to D_{10} ($\delta = 2,3$)

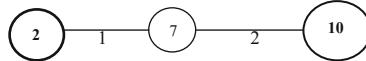


Fig. 2. RBD of SEN (S_2 - D_{10})

Reliability expression for SEN: $R = p_2 p_7 p_{10}$

Here, ' p_i ' is the reliability of i^{th} SE and by assuming identical SEs, with reliability $p_i = r$,

$$\text{TR (SEN)} = r^3$$

Node Pairs (2, 3; $\delta = 1$) or (010,011): {2-7-10}

For Tag Values (0, 1, 2, 3, 4, 5, 6, 7): TR of SEN at SE reliability (0.5, 0.6, 0.7, 0.8, 0.9, 0.91, 0.92, 0.93, 0.94, 0.95, 0.96, 0.97, 0.98, and 0.99) is same. The values depicts the percent of reliability of a network.

2.2 SEN+

Stage of $N \times N$ size is added having $N/2$ SEs of 2×2 . It has $(\log_2 N + 1)$ stage, network complexity is $((N/2) * ((\log_2 N) + 1))$ [1, 14] for the model shown in Fig. 3 with the RBD presented in Fig. 4.

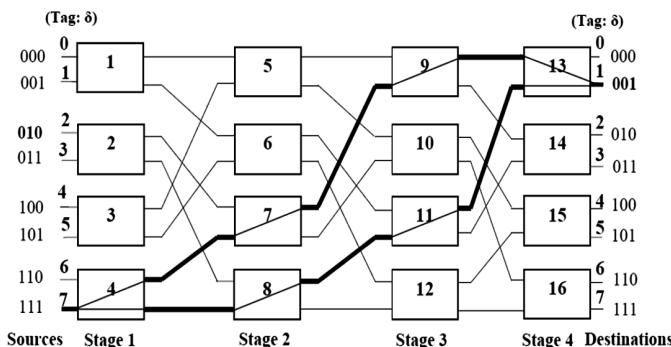


Fig. 3. SEN+: TRpaths from S_4 ($\delta = 6,7$) to D_{13} ($\delta = 0,1$)

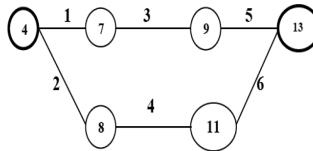


Fig. 4. RBD of SEN+ for S₄-D₁₃

Reliability expression for SEN+: $R = p_4 p_7 p_9 p_{13} + p_4 p_8 p_{11} p_{13} (1 - p_7 p_9)$
 $TR(SEN+) = r^4 (2 - r^2)$

Node pairs (6, 7; $\delta = 1$) or (111,001): {4-7-9-13}, {4-8-11-13}

For Tag Values: TR of SEN+ at SE reliability (0.5, 0.6, 0.7, 0.8, 0.9, 0.91, 0.92, 0.93, 0.94, 0.95, 0.96, 0.97, 0.98, and 0.99) is same.

2.3 SEN+2

N/2 SEs per stage having complexity of $((N/2) * ((\log_2 N) + 2))$ [1, 10, 15] for the model shown in Fig. 5 with the RBD presented in Fig. 6.

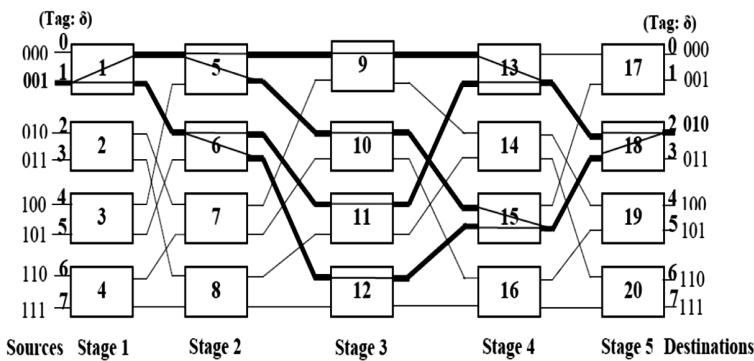


Fig. 5. SEN + 2: TRpaths from S₁($\delta=0,1$) to D₁₈ ($\delta = 2,3$)

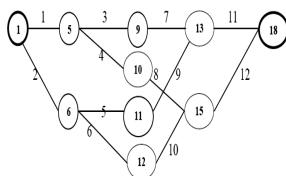


Fig. 6. RBD of SEN + 2 for S₁-D₁₈

Reliability expression for SEN+2: $R = p_1 p_5 p_9 p_{13} p_{18} + p_1 p_5 p_{10} p_{15} p_{18} (1 - p_9 p_{13}) + p_1 p_6 p_{11} p_{13} p_{18} (1 - p_5) + p_1 p_5 p_6 p_{11} p_{13} p_{18} (1 - p_{10} p_{15}) (1 - p_9) + p_1 p_6 p_{12} p_{15} p_{18} (1 - p_5) (1 - p_{11} p_{13}) + p_1 p_5 p_6 p_{12} p_{15} p_{18} (1 - p_{10}) (1 - p_{13}) + p_1 p_5 p_6 p_{12} p_{13} p_{15} p_{18} (1 - p_9) (1 - p_{10}) (1 - p_{11})$

$$TR(SEN+2) = r^5 (4 - r^5 + 4r^4 - 2r^3 - 4r^2)$$

Node Pairs (1, 2; $\delta = 1$) or (001,010): {1-5-9-13-18}, {1-5-10-15-18}, {1-6-11-13-18}, {1-6-12-15-18}

For Tag Values: TR of SEN+2 at SE reliability (0.5, 0.6, 0.7, 0.8, 0.9, 0.91, 0.92, 0.93, 0.94, 0.95, 0.96, 0.97, 0.98, and 0.99) is same.

3 Performance Analysis

Performance analysis of multistage interconnection network is a very critical issue in parallel processing systems. Different indices like TR, fault-tolerance, hardware cost the performance of MIN is characterized.

3.1 Terminal Reliability Comparison

Evaluation of MINs, the terminal reliability for all source to destination node pairs is presented in Table 1 and Fig. 7.

Table 1. TR evaluation of MINs at SE reliability value (0.5, 0.6, 0.7, 0.8, 0.9, 0.91, 0.92, 0.93, 0.94, 0.95, 0.96, 0.97, 0.98, and 0.99) for $N = 8$

Model	Switching Element Reliability													
	0.50	0.60	0.70	0.80	0.90	0.91	0.92	0.93	0.94	0.95	0.96	0.97	0.98	0.99
Terminal Reliability														
SEN [1], [10]	0.12500	0.21600	0.34300	0.51200	0.72900	0.75357	0.77869	0.80436	0.83058	0.85738	0.88474	0.91267	0.94119	0.970299
SEN+ [1], [14]	0.10938	0.21254	0.36255	0.55706	0.78076	0.80363	0.82643	0.84911	0.87163	0.89392	0.91594	0.93761	0.95889	0.979712
SEN+2 [10], [15]	0.08496	0.18481	0.33956	0.54484	0.78884	0.81088	0.83276	0.85445	0.87593	0.89719	0.91823	0.93902	0.95957	0.979896

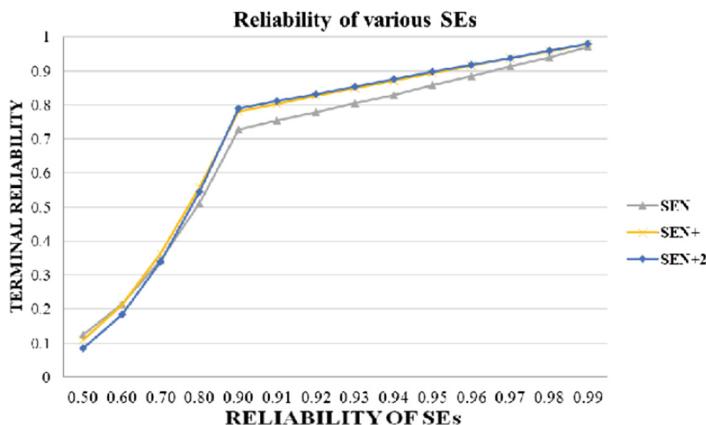


Fig. 7. TR evaluation of MINs

3.2 Hardware Cost

It is calculated by switch and link connection to MIN model, *i.e.* product of *Input*, *Output* and *Switches* [10]. MINs comparisons based on hardware cost is illustrated in Table 2.

Table 2. Cost of MINs for $N = 8$, *i.e.* size of the network

STAGES	SEN	SEN+	SEN + 2
1	$2 \times 2 \times 4$	$2 \times 2 \times 4$	$2 \times 2 \times 4$
2	$2 \times 2 \times 4$	$2 \times 2 \times 4$	$2 \times 2 \times 4$
3	$2 \times 2 \times 4$	$2 \times 2 \times 4$	$2 \times 2 \times 4$
4	—	$2 \times 2 \times 4$	$2 \times 2 \times 4$
5	—	—	$2 \times 2 \times 4$
Cost	48	64	80
No. of SEs	12	16	20

3.3 Comparison Summary of MINs

In Table 3 for ease of understanding, the various features of MINs is given below.

Table 3. Comparison summary of MINs

Sl. No.	Parameters	SEN	SEN+	SEN + 2
1.	No. of stage ($N = 2^n$)	$\log_2 N$	$\log_2 N + 1$	$\log_2 N + 2$
2.	Switches	$N/2$ ($\log_2 N$)	$(N/2)$ ($\log_2 N + 2$)	$(N/2) (\log_2 N + 1)$
3.	Size of switches	2×2	2×2	2×2
4.	8×8 size	3 stage 12 SE 32 Link	4 stage 16 SE 40 Link	5 stage 20 SE 48 Link
5.	Fault-tolerance	No	Yes	Yes
6.	Fault-tolerance path	—	Disjoint	Disjoint
7.	Disjoint path	0	2	2
8.	MUX/DMUX	—	—	—
9.	Hardware	48	64	80
10.	Terminal Reliability	r^3	$r^4(2 - r^2)$	$r^2[1 - (1 - (r^2(1 - (1 - r)^2)))^2]$

4 Conclusion

Terminal reliability of MINs is evaluated for different tag values and validated. In any switch/link failure state, the MIN design provides full access and dynamic re-routing property. The performance analysis based on various parameters signifies these networks are fault-tolerant, cost-effective, re-routable, and ideal for multiprocessor interconnection network.

Further, for switching element reliability values 0.5 to 0.9 the TR increases exponentially and than linearly for 0.9 to 0.99. However, the cost of SEN+2 model is high than that of other existing models, the additional paths does not increase the TR of the network rather the complexity leads to network failure.

Researchers should attempt for new MIN designs and techniques to compute the reliability for complex parallel systems. The validation results are satisfactory for all switching component reliability values. It is concluded that for better terminal reliability, the switching component reliability should be high.

References

1. Rajkumar, S., Goyal, N.K.: Multistage interconnection networks reliability analysis. *J. Supercomput.* **72**, 2310–2350 (2016)
2. James, T.B., Trivedi, K.S.: Reliability analysis of interconnection networks using hierarchical composition. *IEEE Trans. Reliab.* **38**(1), 111–120 (1989)
3. Abd-El-Barr, M.: Design and Analysis of Reliable and Fault-Tolerant Computer Systems. Imperial College Press, London (2007)
4. Gunawan, I.: Fundamentals of Reliability Engineering. Wiley (2014)
5. Rajkumar, S., Goyal, N.K.: Fault-tolerant interconnection network design. *IETE Tech. Rev.* **33**, 396–404 (2016)
6. Bansal, P.K., Singh, K., Joshi, R.C.: QuadTree: a cost-effective fault-tolerant multistage interconnection network. In: INFOCOM. IEEE (1992)
7. Gunawan, I.: Reliability analysis of shuffle-exchange network systems. *Reliab. Engg. Syst. Saf.* **93**(2), 271–276 (2008)
8. Locks, M.O.: Recent developments in computing of system-reliability. *IEEE Trans. Reliab.* **R-34**(5), 425–436 (1985)
9. Chaturvedi, S.K.: Measures and Evaluation. Scrivener Publishing LLC/Wiley, Beverly/Hoboken (2016)
10. Prakash, A., Yadav, D.K.: Design and reliability analysis of fault-tolerant shuffle exchange gamma logical neighborhood interconnection network. *J. Supercomput.* 1–18 (2019). <https://doi.org/10.1007/s11227-019-02929-z>
11. Chaturvedi, S.K., Misra, K.B.: An efficient multi-variable inversion algorithm for reliability evaluation of complex systems using path sets. *Int. J. Reliab. Qual. Saf. Eng.* **9**(3), 237–259 (2002)
12. Gunawan, I.: Redundant paths and reliability bounds in gamma networks. *Appl. Math. Model.* **32**, 588–594 (2008)
13. Bistouni, F., Jahanshahi, M.: Analyzing the reliability of shuffle-exchange networks using reliability block diagrams. *Reliab. Eng. Syst. Saf.* **132**, 97–106 (2014)
14. Blake, J.T., Trivedi, K.S.: Multistage interconnection network reliability. *IEEE Trans. Comput.* **38**(11), 1600–1604 (1989)
15. Farid, N.F., Gunawan, I.: Terminal reliability improvement of shuffle-exchange network systems. *Int. J. Reliab. Qual. Saf. Eng.* **12**(1), 51–60 (2005)



An Approximative Study of Database Partitioning with Respect to Popular Social Networking Websites and Applications

S. V. G. Sridevi^(✉) and Yogesh Kumar Sharma

Shri Jagdishprasad Jhabarmal Tibrewala University, Churela, India
devisayana@gmail.com, dr.sharmayogeshkumar@gmail.com

Abstract. The users of social networking applications and websites are the prime producers of huge amounts of data that the world is witnessing today. With these growing databases, all the social networking websites and applications are looking for an easy, secure and efficient maintenance of the database. As the size of both the database and the network grow, the entire database cannot be kept in a single node/single location. So the need arises for distributing the database over a network by dividing the database into portions called partitions. The partitions may be replicated at multiple nodes depending on the needed degree of availability. At the same time a single partition may further be split across a collection of nodes depending on how much data is need at a node. In this article, we have highlighted what is database partitioning, what is its need. This article also highlights some of the popular social networking websites and applications that are using a numerous database depending on the features they are providing. During our study, we have studied upon some of the data bases used by the example websites considered and what type of partitioning scheme might have been used. This article discusses some key features of database partitioning schemes of Facebook, twitter, amazon, WhatsApp and Instagram.

Keywords: Data base partitioning · Types of partitioning · Need for partitioning · Social networking websites

1 What Is Database Partitioning???

A **database partition** is a division of a logical database or its constituent data elements into distinct and/or independent portions. Database partitioning is normally done for the following reasons:

- (a) **Manageability**- the ability to deal with the retrieval and manipulations on a small data set becomes easier and faster than that of a large, single/un-partitioned database.
- (b) **Performance**- can be studied in terms of either the speed of execution of application programs or the amount of storage occupied.

- (c) **Availability reasons**- data should be available at a needed level of performance in situations ranging from normal performance indicator through disastrous performance indicators.
- (d) **Load balancing**- this feature aims to optimize resource utilization, maximizing the throughput, minimize the response time, and avoid overloading any single resource.

To summarize, data **Partitioning** is the process of logically and/or physically dividing data into segments that can be more easily maintained and/or accessed. It helps in making the data highly available and optimum utilization of the available resources.

A database table partitioning can be done in two possible ways –

- (i) **Single-level partitioning** (ii) **Composite level partitioning**.
- (i) The **single-level** partitioning uses only any one of the methods of data distribution like range or hash or list in one or more columns constituting the partitioning key.
- (ii) The **composite partitioning** is generally a combination of two data partitioning methods. First, a table is partitioned using one of the data distribution methods, and then each partition is further divided into sub partitions using a second data distribution method. Partitions obtained through a composite partitioned table are generally metadata, and they will not represent the actual data storage.

2 Why Database Is to Be Partitioned???

Partitioning is generally opted in the following scenarios:

- (i) When the table size is more than 2 GB
- (ii) When the tables contain historical data
- (iii) The contents of a table need to be distributed across various types of storage devices.

Partitioning is a tool for building multi-terabyte systems which work under extremely high availability requirements. It is time efficient because the maintenance and recovery operations on a particular failed partition can be carried out while other partitions are available to users, thereby improving the availability of the data and in turn improving the performance and durability degree.

3 What Are the Major Advantages???

- (i) The major advantage of Partitioned database objects is that they provide partition independence. The user of the database is unaware or need not know about the partitioning.

- (ii) Adding new data into a single partition is very easy and can be done very efficiently.
- (iii) Modifying an existing data of one partition is much more efficient and desired than modifying the entire table.
- (iv) Removing data from the partitioned table using drop or truncate can be done very efficiently.
- (v) Loading and exchanging of partitions becomes easy during retrieval/manipulation operations by application programs.
- (vi) Backup and recovery operations on a single partition can be carried out independent of the other partitions of the table.
- (vii) Partitioning of database tables can reduce scheduled downtime which in turn improves performance.

4 Various Types of Partitioning Schemes

The choice of a partitioning scheme depends on various factors like size of the database, possible usage/user requirements, the type of storage devices available and so on. As per **Oracle docs**, the following types of partitioning schemes are generally used [3–5, 8, 12, 14, 18].

(i) RANGE Partitioning

A table that is partitioned by this scheme is partitioned in such a way that each partition contains rows that satisfy a given range expression. Ranges should always be continuous and non-overlapping. The ranges are always defined using the **VALUES LESS THAN** operator.

For example, the following SQL statement shows creation of table *employees* and four partitions namely *p0*, *p1*, *p2* and *p3* defined on it (Fig. 1).

```
CREATE TABLE employees (
    id INT NOT NULL,
    fname VARCHAR(30),
    lname VARCHAR(30),
    job_code INT NOT NULL,
    store_id INT NOT NULL
) PARTITION BY RANGE (store_id)
(
    PARTITION p0 VALUES LESS THAN (6),
    PARTITION p1 VALUES LESS THAN (11),
    PARTITION p2 VALUES LESS THAN (16),
    PARTITION p3 VALUES LESS THAN (21)
);
```

Fig. 1. Range partitioning

(ii) LIST Partitioning

This scheme is almost similar to range partitioning. In this scheme, just like range partitioning, each partition must be defined explicitly. The important difference between the above two types of partitioning schemes is that, *in list partitioning, each partition is defined and selected depending on a column value belonging to one of a set of value lists, instead of a set of continuous values*. This is done by using **PARTITION BY LIST (expr)**.

Where *expr* is the value of a column or an expression involving a column value and returning an integer value, and then defining each partition by means of a **VALUES IN (value_list)**, where *value_list* is a list of integers separated by commas (Fig. 2).

```
CREATE TABLE employees (
    id INT NOT NULL,
    fname VARCHAR(30),
    lname VARCHAR(30),
    job_code INT,
    store_id INT
)
PARTITION BY LIST(store_id)
(
    PARTITION pNorth VALUES IN (3,5,6,9,17),
    PARTITION pEast VALUES IN (1,2,10,11,19,20),
    PARTITION pWest VALUES IN (4,12,13,14,18),
    PARTITION pCentral VALUES IN (7,8,15,16)
);
```

Fig. 2. List partitioning

The above SQL statement shows creation of table *employees* and four partitions *pNorth*, *pEast*, *pWest* and *pCentral* defined on it.

(iii) Hash Partitioning

Partitioning by this scheme is used primarily to make sure that the data is evenly distributed among the partitions. The number of partitions must be predetermined.

To partition a table using HASH partitioning, we should append the **PARTITION BY HASH (expr)** clause, to the create table statement where *expr* is an expression that returns an integer (Fig. 3).

The above statement results in 4 partitions. If the number of partitions is not mentioned in the statement, then by default it is taken to be 1.

(iv) Key Partitioning

This partitioning scheme is similar to partitioning by hash, and the difference being that the hash partitioning scheme takes a user-defined expression (Fig. 4).

```

CREATE TABLE employees(
    id INT NOT NULL,
    fname VARCHAR(30),
    lname VARCHAR(30),
    job_code INT,
    store_id INT
)
PARTITION BY HASH(store_id);
PARTITIONS 4;

```

Fig. 3. Hash partitioning

```

CREATE TABLE employees(
    id INT NOT NULL PRIMARY KEY,
    fname VARCHAR(30),
    lname VARCHAR(30),
)
PARTITION BY KEY
PARTITIONS 2;

```

Fig. 4. Key partitioning

The above statement automatically takes the key item specified. If no key item is specified, then it will look for a UNIQUE item. If no key and no unique item is specified, then the statement to create partitions would become *invalid*.

(v) *Composite Partitioning*

This is also known as Sub Partitioning. This scheme consists of a combination of partitions. First a partitioning scheme is used and in turn, another technique is used to sub-partition each partition (Fig. 5).

The table *ts* in the above statement has 3 Range partitions. They are again partitioned into 2 sub partitions leading to a total of $3 \times 2 = 6$ partitions.

```
CREATE TABLE ts(id INT, purchased DATE)
PARTITION BY RANGE(YEAR(purchased))
SUB PARTITION BY HASH(TO_DAYS(purchased))
SUBPARTITIONS 2(
PARTITION p0 VALUES LESS THAN(1990),
PARTITION p1 VALUES LESS THAN(2000),
PARTITION p2 VALUES LESS THAN MAXVALUE);
```

Fig. 5. Composite partitioning

5 Partitioning the Data on Social Networking Websites/Applications – Some Examples

A social networking service is an online platform which people use to share similar personal or career interests, activities, backgrounds or real-life connections. Using these services, people are building their social networks which allow them to be in touch with their peers, friends, family, relations or associations irrespective of their geographical location differences. The social network is distributed across various computer networks. With almost all people onto social networking sites, and with heavily growing data, the social networking sites definitely are going for distributed databases and obviously for data base partitioning.

In this article, the following social networking services/applications have been considered to give an approximation of what is the structure of the database and what type of partitioning schemes would have been used [9–11, 13].

1. Facebook

Facebook started in 2004 as a people community builder so that communication becomes much easier. Its hit is so massive that undoubtedly, truly and very quickly the world turned into a “Global village”. Facebook products are used by people to be in almost continuous touch with their kith and kin, peers, also to know what is happening in the world and to share their thoughts and so on. Today it is considered one of the Big Four technology companies along with Amazon, Apple, and Google [2, 16].

Apache Cassandra is a distributed database. It is a type of NoSQL database with the following desirable features:

- Distributed
- Uses column-store
- Open source
- Highly scalable
- High-performance
- Can handle large amounts of data across various commodity servers
- Highly available with no single point of failure

Cassandra [1] is a distributed storage system that is used by Facebook, which uses consistent hashing of user IDs for better performance with incremental and dynamic data.

If a table has a composite partition key, then multiple columns are used as a partition key in Cassandra. To facilitate easy retrieval, the columns selected for partitioning form logical sets inside the partitions. In contrary to a simple partition key, using two or more columns, a composite partition key identifies where the data should reside. Usage of more columns to make up the partition key, divides the data into buckets or chunks. This results in smaller chunks of data groups. This method proves to be effective if a cluster in Cassandra experiences hotspots or there is congestion in writing data repeatedly to one node because of a heavily writing partition. Often, for time series data, Cassandra is used and hotspotting can prove to be a real issue. One solution is to Divide the incoming data into data chunks or buckets based on the time stamp values, *year: month: day: hour*. Using four columns to route to a partition can decrease hotspots.

2. Twitter

Majority of online social networking sites generally use hash-based horizontal partitioning of data because it is a very simple technique. It uses a row of a table as the base unit of partitioning. With nearly 180 million users, Twitter, a micro-blogging social network developed by Gizzard [Kallen 2006] uses range partitioning scheme for its database.

3. Amazon Dynamo

DynamoDB supports same data model as Dynamo, with a different implementation scheme. Dynamo is a distributed data store which provides high availability. It uses the key-value structure for the storage system. Dynamo has properties of both databases and distributed hash tables (DHTs).

Amazon uses this DynamoDB [de Candia 2007] for storage and retrieval of shopping carts on its online shopping site. While doing operations on the cart, it uses an updated and consistent hashing scheme which resolves the issues of non-uniform load distribution.

4. WhatsApp

It is an instant messaging application. Its major advantage is the support for cross-platform. It allows all Smartphone users to exchange multimedia messages for free of cost. The data being exchanged can be text, image, video and/or audio. WhatsApp is especially popular with end users who have limited text messaging. In addition to basic messaging, WhatsApp provides group chat, individual or group calling and location sharing options [17].

WhatsApp relied on Mnesia only as database (for non media content). The Mnesia tables had to be partitioned to hold all data. WhatsApp contributed to some optimizations and improvements of the Erlang code base related to handling the Mnesia database. For various kinds of features, the site depends on various software options.

5. Instagram

Instagram mainly uses two backend database systems: PostgreSQL and Cassandra. PostgreSQL has built-in support for Range **Partitioning**. The table is **partitioned** into various “ranges” defined by a key column or a set of columns. The key or columns used for partitioning should be selected with no overlap between the ranges of values assigned to different **partitions**.

6 Conclusion

The concepts of database are not new and so as the concepts of database partitioning. The choice of database and its partitioning scheme always depends on

- (a) how we want to maintain our application/website
- (b) the performance expectations
- (c) the capacity of the server to tolerate the load
- (d) the amount of storage being offered to the users

And the list goes on endlessly.

This article highlights what exactly we mean by database partitioning, what is the need for partitioning the large databases. It also highlights on the partitioning schemes of various very well known social networking websites and/or applications.

- It illustrates Facebook’s usage of Cassandra with consistent hashing of user IDs for better performance with incremental and dynamic data.
- It also highlights that Twitter, the popular micro-blogging application uses range partitioning.
- Amazon uses DynamoDB for storage and retrieval of shopping carts on its online shopping site. While doing operations on the cart, it uses an updated and consistent hashing scheme. WhatsApp and Instagram, are using these concepts in order to store and maintain their huge datasets.
- WhatsApp relied on Mnesia only as database (for non media content). It focuses on the software options the site depends on for various kinds of features.
- Finally, this article highlights that Instagram uses range partitioning without overlapping between partitions.

These are only some of the applications that highlight database partitioning, need of it, advantages of it.

References

1. Cassandra. (n.d.). <https://academy.datastax.com/>
2. Bouchard, J.-L.: Mark Zuckerberg’s full commencement address at Harvard, the school he left to start Facebook, 26 May 2017. <https://qz.com/992048/mark-zuckerbergs-harvard-speech-a-full-transcript-of-the-facebook-ceos-commencement-address/>
3. Navathe, S., Ceri, S., Wiederhold, G., Dou, J.: Vertical partitioning algorithms for database design. ACM Trans. Database Syst. (TODS) 9(4), 680–710 (1984)

4. Fowler, A.: Nosql data partitioning, January 2015. <https://www.dummies.com/programming/big-data/handling-partitions-in-nosql/>
5. Partitioning methods (n.d.). <https://www.oracle.com/technetwork/database/options/partitioning/overview/index.html>
6. Google's NoSQL BIG DATA database service. Cloud Bigtable documentation. <https://cloud.google.com/bigtable/docs>
7. Cesarini, F., Vinoski, S.: Designing for Scalability with Erlang/OTP: Implement Robust, Fault-Tolerant Systems, 1st edn., pp. 405–422. O'Reilly (2016). Chapter 15 Scaling out
8. Partitioning types (n.d.). https://docs.oracle.com/cd/E17952_01/mysql-5.1-en/partitioning-types.html
9. Thomas, S.: (Guest Post): database design practices in various social media sites (n.d.). <https://www.pixelproductionsinc.com/11-database-design-practices-for-social-media-sites/>
10. Aarepu, L., Prasad, B.M.G., Sharma, Y.K.: A review on data mining and bigdata. Int. J. Comput. Eng. Technol. (IJCET) **10**(1), 117–123 (2019)
11. Rivas, T.: Ranking the big four tech stocks: Google is No. 1, Apple comes in last, 22 August 2017. <https://www.barrons.com/articles/ranking-the-big-four-internet-stocks-google-is-no-1-apple-comes-in-last-1503412102>
12. Partitioning the database, 6 June 2019. www.wikipedia.com
13. Wakita, K., Tsurumi, T.: Finding community structure in mega-scale social networks. In: Proceedings of the 16th International Conference on World Wide Web, WWW 2007. ACM, New York (2007)
14. Sharma, Y.K., Sharif, G.M.: Framework for privacy preserving classification in data mining. J. Emerg. Technol. Innov. Res. **5**(9), 178–183 (2018)
15. Lu, Z., Zhu, Y., Li, W., Wu, W., Cheng, X.: Influence-based community partition for social networks. Comput. Soc. Netw. (2014). <https://computationsocialnetworks.springeropen.com/articles/10.1186/s40649-014-0001-4>
16. Markova, V., Shopov, V.: Graph partitioning methods in social network analysis (2016). https://www.researchgate.net/publication/321797991_GRAPH_PARTITIONING_METHODS_IN_SOCIAL_NETWORK_ANALYSIS
17. Rouse, M.: Definition of WhatsApp (n.d.). <https://searchmobilecomputing.techtarget.com/definition/WhatsApp>
18. Sharma, D.Y.K., Kumar, S.: Designing hybrid data mining technique for efficient industrial engineering domain. J. Comput. Inf. Syst. **15**(3), 128–136 (2019)



A Novel Approach for Gigantic Data Examination Utilizing the Apache Spark and Significant Learning

Anilkumar V. Brahmane^(✉) and B. Chaitanya Krishna

Department of CSE, KLEF Deemed to be University, Vijaywada, A.P., India
vb_anil@yahoo.co.in

Abstract. With the spreading certainty of Gigantic Data, particular prompts and advancements are made in this area of Gigantic Data and systems, for example, the Apache Hadoop as well as the Apache Spark are very much widely used and spread in industry and a part of balance over the previous decades and have wrapped up gigantically phenomenal, particularly in affiliations. It is finding the opportunity to be interminably clear that profitable tremendous data evaluation is fundamental to perception artificial experiences issues. All things considered, a diversified-calculation repository executed inside the Apache Spark structure, it is MLLib. Disregarding the way that this library reinforces different AI figurings, there's still expansion to utilize the Spark course of action ably for out and out time-genuine also, computationally absurd methods like essential acquisition of knowledge. We are trying to put forward an effective structure which consolidations the separative assessment cutoff purposes of the Apache Spark and the pushed AI plan for a fundamental multilayer perceptron (MLP), utilizing pervasive thought of cascade learning. We lead observational evaluation of our structure on two veritable famous datasets. The outcomes around are attracting and show our proposed structure, accordingly sketching out that it is an alter over routine goliath data evaluation strategies that utilization either Spark or Significant learning as individual parts.

Keywords: Deep learning · Apache Spark · Big data

1 Introduction

1.1 Outline

Accompanied by the aggregate of information making at an augmented measure, it is chief to make gadgets that can deal with that information and expel respect from it. Each affiliation or association, be it inside the restorative administrations, assembling, vehicle or PC program industry, should oversee and stall the broad information volumes that it produces. This thusly prompts speedier and increasingly gainful tasks. The creating should regulate logically gigantic information accumulations has headed to important interested in making such huge data gadgets. Explore is being directed inside the zones of Huge Information Framework, for example, (1) cloud registering stages, (2) vitality productive applications and processing, (3) system program frameworks,

(4) present day current programming modules, Enormous Information Administration (look and mining, algorithmic structure, data verifying, coordination and cleaning, computational demonstrating, graph mining, scattered and shared look and so forth), Enormous Information Look and Mining (social sort out assessment and mining, web look, semantic based data mining and so forth), Enormous Information Security (tall execution cryptography, security perils to colossal data, sociological points of view of tremendous data security and so forth) and various other related regions. This constantly creating solicitation has headed to the improvement of a couple of gigantic data investigation mechanical assemblies inside the business.

Among the primary recognizable defiant that satisfy this undertaking is Hadoop, an open source orchestrate that gives surprising information association blueprints. Its central use is to stimulate the dealing with of remarkably clearing datasets in a scattered processing condition using segments like the Hadoop Ecosystems elements. The paper regardless, looks at a progressively fit and enthusiastic gadget, The Apache Spark, which was masterminded for functioning related to Hadoop in coordinate to address a portion of its confinements.

1.2 Difficulties

The fundamental reason of The Apache Spark advantageously oversee the facts and statics for a more general tremendousness. Utilizing the worked in repositories independently, living frameworks created the Apache Spark to examination of Colossal Facts and Stastistics. Be that since it might, there's still degree for exploring unused models that yield comes for the most part with progressively fundamental correctnesses anyway as of not long ago utilizing the Apache Spark system to standing operationally possible.

The main explanation solicitation: (1) How to remove most amazing data from the past features inside the dataset to neglect immaculate exactness? (2) How to sensibly address the issue plainly inconsistency that is show up in beast scale authentic world datasets? (3) How to interface the a concise range later advances made inside the field of Fake Experiences in any case as of not long ago using Spark s computational control?

1.3 Answering Difficulties

To discourse the inconveniences said over, the article shows the structure that handles a control clearly learning underneath the support of the Apache Spark system. Utilizing the available system, information grabbed through major getting sorted out is used to wire respect to the past features of the information being broke down. This pushed ahead data is plainly strengthened into a moment learning plan. The surrender of this two-advance learning handle likely could be a demonstrate that is basically more ideal than typical single sort out AI models. Help, the resultant demonstrate what's progressively keeps an eye on the course enormity issue.

1.4 Applications

1. **Healthcare** - Examination of point by point enormous scale hardware readings inside the condition of the two works and pictures. Inconceivable learning calculations will achieve dominating social protection figures and suggestions.
2. **Instruction** - Examination the execution of understudies, educators.
3. **Mechanical Division** - Instruments central purposes of intrigued, for instance, information annals for gigantic industries can be surveyed utilizing this system.
4. **Information Technology Industry** - Moving forward current structures from superseding, fusing labouring task with gigantic facts depends phony bits of learning shapes.

1.5 Layout of the Paper

The everything considered structure showed up in this paper focuses to manage the formally decided troubles. The paper is bound as takes after: Range II can be an audit of the making that is accessible inside the degrees underneath thought and a brief timeframe later incites inside the comparable. Region III gives a speedy clarification of the proposed technique and the considering behind it. Part IV could be a point by point consider of the tests, diversions. Last part offer closures that take a gander at together with the degree and potential results.

2 The Associated Efforts

The making consider relating to this paper has been showed up in following four segments.

2.1 Efforts Associated with the Apache Spark

Structure as well as the usefulness of the Apache Spark help to perform the operations with appeared framework from producers [1]. It grants concise graph concerning organizing plot, this joins Resilient Distributed Data Sets (RDD), concurrent figuring, and so on. It additionally demonstrates a couple of utilization inside the earth. [2] presents Apache Flashes AI repository, MLlib. This associations inside distinctive also contrasting areas setting up the MLlib library. The work obliterated [3] assesses Shines fundamental system by running a test ML occasion on it. The producers give off an impression of being done comes around dependent on their appraisals that segment Shimmers tendencies. The producers of [4] show up a nearby use of Spark by investigating twitter information using Shimmers structure.

2.2 Efforts Associated with Attribute Group, Facts Finagle

Course variance issue might be key connect enchanted inside AI society which is tended to article. Makers of [6] show up analysis specific devices, methods which utilized for getting a handle on the clumsiness issue. A broad evaluation of specific

systems concentrated on towards understanding the issue has been appeared in [7]. [10] presents a state-of-the-craftsmanship technique to the trademark tongue managing issue of patching up locale, utilizing unequivocal list of capabilities improvement. Producers of [11] additionally show up a broad design illustrating express join progress and control for concealing run the show learning tallies.

2.3 Work Related to Deep Learning Using MLPs

Essential getting the hang of using differing layer perceptrons has been snappy grabbing centrality inside the caused encounters to sort out, especially when overseeing gigantic information. The producers of [12] present information social event utilizing Multilayer Perceptrons. [13] dispense occasion epic plate highlights the central focuses advanced by MLPs when managing with clearing datasets rather than little or expectedly evaluated ones. Another occasion of the use of MLPs in depiction issues is appeared in [14]. Thusly of reasoning used a pleasant in a general sense based incitation work.

2.4 Efforts Associated with Cataract Acquisition of Knowledge

Twice system displayed in article, to be express assessment utilizing the Apache Spark, Multilayer Perceptron, associated by assemblies of falling. Falling, Cataract Acquisition of Knowledge regularly utilized conditions. Characteristic Lingo Taking idea of, Computer Vision, and so on and has exhibited to be astoundingly sensible. [16] proposed a period competent two-mastermind fell classifier for the hankering for purchase sessions and gotten things inside.

Having pondered the current making, we point to address the starting at now said challenges through the system delineated in this paper. Inside the taking after piece, we exhibit a down to business ponder the proposed structure and the strategies took an interest in it.

3 The Suggested Technique

Here we delineate structure mentioned in article. Technique joins advantages utilizing goliath information planning structure namely the Apache Spark close to focal motivations behind giant acquisition of knowledge clearing facts after utilizing a methodology known Cataract Acquisition of Knowledge.

3.1 Cataract

Routine regulated AI checks, singular models are organized their individual undertakings. This has been a basically advantageous strategy at anything point the checked information for the activity waiting be done is available. In show detest toward of reality that, in conditions where there's an expect of worthy named data appearing differently in relation to the utilization case, the normal estimations achieve beguiling models.

Falling awards for the use of ‘information’ grabbed from a starting at now masterminded appear to another show, in order to make progress the execution on the job that needs to be done. This model-to-data exchange is used as an extra join for the as a rule show, accordingly giving extra related data.

3.2 The Proposed System Framework

The structure depicted in this paper is rotated around dealing with genuine epic data issues utilizing huge data assessment systems and fake bits of learning. To manage such issues is attempting a direct result of presence checks.

The paper proposed work joins the thoughts of enormous information evaluation, AI, colossal learning and falling. The center crucial structure showed up in this piece shapes the focal point of our examine and tests.

The substance of this structure lies in utilizing falling between the authoritatively decided conditions of enormous data assessment and colossal learning. These shapes are clarified taking after.

- (1) Colossal Data Examination Utilizing Spark: The diverse AI figurings on Spark have been considered in significance with reference to tremendous information. For the reason of this get some information about, we utilize the MLlib library of Spark to acknowledge Calculated Relapse, Choice Trees and Sporadic Forest descend into sin estimations. In this sort out, the pre-arranged dataset is experienced these calculations to make a fall away from the confidence make the feeling that displays the probability of each datum point having a put to a twofold exercise. This create may be a twofold learning mastermind.
- (2) Significant Learning: This sort out is the summit of our structure.

The Proposed system framework is detailed in Fig. 1.

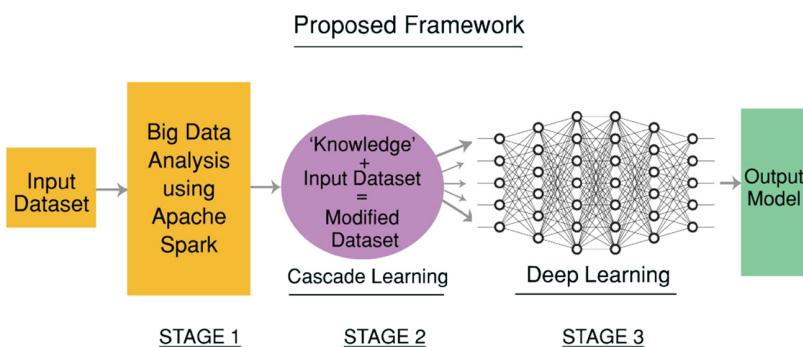


Fig. 1. Overview of proposed system.

3.3 Thinking Behind Choice of Approach

The structure we have reviewed inside the prior fragment might be a novel philosophy for understanding routine AI issues. It considers all points of view of a standard AI while pushing ahead accuracy and speed of the arrangement. The significant purposes for picking this system are advance inspected.

1. **Overhauled Highlight Group:** Pleasant facts gotten structure two makes progress present join group showed up in any issue. It supports the accuracy of any show where this data is used from a little while later on. This consolidate duplicates somewhat the ground truth of this information, along these lines moving the odds of tall exactness when the fundamental learning show is made and related on it. In this way, our structure can move the current combine set to far away better;a much better;a higher;a stronger;an improved”>a more grounded state.
2. **Operational Schedule Thought:** Managing twice coat technique utilizing twice basic acquisition of knowledge prototype at the same time might be an alarming and time-depleting task. Displacing a sort out with an a lot speedier enormous information assessment structure, for example, the Apache Spark or Apache Hadoop decreases schedule multifaceted nature.

4 Implementation of the System

The proposed system implementation is shown in following Fig. 1. The implementation requires following configuration;

- GNU – Linux OS, High capability processing power, RAM of 16 GB

The execution of the framework led and tried on following;

4.1 Assignment 1 - Classification Based on “Case-Status”

The informational index causes a course cumbersomeness issue (Lesson 1: 2.6 Million, Course 0: 180 K). Consequently, some time starting late applying the proposed show, the course disparity issue is edified by carelessly under-testing the more unmistakable course (For this circumstance, Course 1). This decreased dataset is utilized for portrayal undertaking utilizing our show (Figs. 2 and 3).

Results are showed.

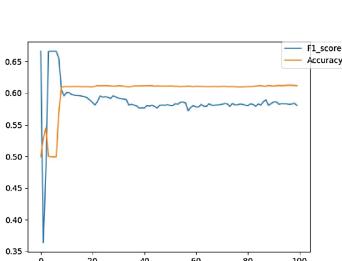


Fig. 2. F_1 and Correctness for Job

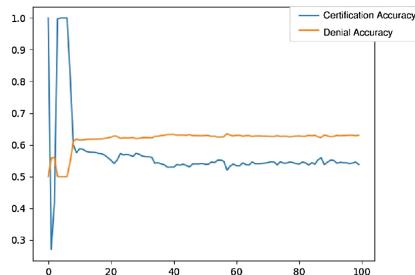


Fig. 3. Corroboration and contradiction correctness for Job_1

4.2 Errand 3 - Recommendation Based on Prevailing-Wage

The reason for this assignment is to propose the perfect stipend run, inside which the up-and-comer found the opportunity to deal with his/her coalition pay with the business. Since it were the ensured up-and-comers are considered in this show. The greater bit of steps look like Assignment 2, the improvements made inside the show for this undertaking are referenced underneath.

Precision, F1 Score and Person Lesson correctnesses are showed up in Table 1. A hypothetical of the man-made thinking defiant utilized in this undertaking is shown in Table 2. Eventually, we look at the endeavors keep running on dataset 2 or the Arrhythmia Dataset (Fig. 4):

Table 1. Presentation measurements (F_1 Result, Correctness) for diverse errand build prototypes.

	Later phase 1		Later phase 2	
	F_1_ score	Correctness	F_1_ score	Correctness
Job _1	0.4568	0.5005	0.4701	0.5005
Job _2	0.6150	0.6248	0.6241	0.6330
Job _3	0.3800	0.4067	0.4002	0.4100
Job _4	0.5640	0.5010	0.5785	0.5204

Table 2. Study AI prototype utilized in phase_1, profound queasy system utilized phase_ 3.

	Phase 1 classifier	Phase 2 deep learning layers
Job_1	Logistic regression	[1012,529,118,1]
Job_2	Naive Bayes	[1119,256,32,2]
Job_3	Naive Bayes	[1319,216,32,2]
Job_4	Logistic regression	[171,53,47,1]

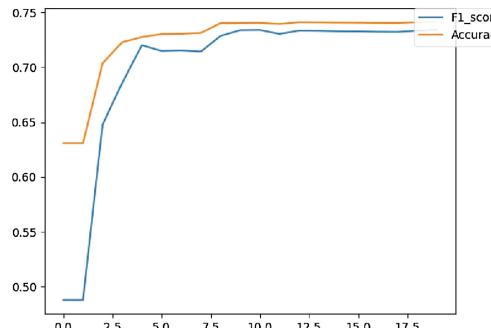


Fig. 4. F_1 and Correctness for Job_2

4.3 Errand 4: Classification of Cardiac Arrhythmia

The issue may be a parallel get-together issue which sees whether an understanding has arrhythmia or not, given his/her characteristics. Coming up another is executed for this errand:

1. All 279 traits are utilized for what it's worth. These properties are as numerical attributes, from this time forward all of the characteristics are utilized for different system.
2. The Vector Assembler is used to interface all the 279 properties into a solitary vector. This vector property is set underneath Highlights inside the information structure.
3. The dataset contained 16 stand-out sorts of arrhythmia.
4. Separated from the advancements referenced over, Arrange 1 and Arrange 2 of the show utilized could be an equivalent one utilized in Assignment 1.

5 Conclusion

Article demonstrated effective structure analysister colossal facts. Suggested structure joined twice by and large noticeable resistant, in unequivocal the Apache Spark Profound acquisition of knowledge, underneath support specific formation. Relationship connecting gadgets set up utilizing a ternary expertise known Course acquisition of knowledge. Ternary level blend empowered arrange enormous information assessment with higher accuracy from another purpose of see. By using these outstandingly acclaimed individual defiant in clarity with each other, we had the choice to get a demonstrate that is set up for driving giant scale enormous information assessment tries inside brief time spans, accompanied minor operational intricacy, basically major precision. Display outside construction which empowered for exhibit completely AI undertakings, for delineation, game-plan and recommendation, effectively. Our assessments on two true blue famous, recognised facts corroborate instances made progress precision changed AI blueprints, and along these lines refreshed the centrality of the proposed methodology.

References

1. Zaharia, M., Chowdhury, M., Franklin, M.J., Shenker, S., Stoica, I.: Spark: cluster computing with working sets. In: Meng, X., Bradley, J., Yavuz, B., Sparks, E., Venkataraman, S., Liu, D. (eds.) HotCloud, vol. 10, no. 10, p. 95 (2010)
2. Freeman, D.T., Amde, M., Owen, S., et al.: Mllib: machine learning in apache spark. *J. Mach. Learn. Res.* **17**(34), 1–7 (2016)
3. Fu, J., Sun, J., Wang, K.: Spark-a big data processing platform for machine learning. In: 2016 International Conference on Industrial Informatics-Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICTI), pp. 48–51. IEEE (2016)
4. Nair, L.R., Shetty, S.D.: Streaming twitter data analysis using spark for effective job search. *J. Theor. Appl. Inf. Technol.* **80**(2), 349 (2015)
5. Nodarakis, N., Sioutas, S., Tsakalidis, A.K., Tzimas, G.: Large scale sentiment analysis on Twitter with spark. In: EDBT/ICDT Workshops, pp. 1–8 (2016)
6. Kotsiantis, S., Kanellopoulos, D., Pintelas, P., et al.: Handling imbalanced datasets: a review. *GESTS Int. Trans. Comput. Sci. Eng.* **30**(1), 25–36 (2006)
7. Sonak, A., Patankar, R., Pise, N.: A new approach for handling imbalanced dataset using ann and genetic algorithm. In: 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 1987–1990. IEEE (2016)
8. Guyon, I., Elisseeff, A.: An introduction to variable and feature selection. *J. Mach. Learn. Res.* **3**(Mar), 1157–1182 (2003)
9. Popescu, M.C., Sasu, L.M.: Feature extraction, feature selection and machine learning for image classification: a case study. In: 2014 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM), pp. 968–973. IEEE (2014)
10. Dey, K., Shrivastava, R., Kaushik, S.: A paraphrase and semantic similarity detection system for user generated short-text content on microblogs. In: COLING, pp. 2880–2890 (2016)
11. Lavrač, N., Fürnkranz, J., Gamberger, D.: Explicit feature construction and manipulation for covering rule learning algorithms. In: Advances in Machine Learning I, pp. 121–146. Springer (2010)
12. Silva, L.M., de Sa, J.M., Alexandre, L.A.: Data classification with multilayer perceptrons using a generalized error function. *Neural Netw.* **21**(9), 1302–1310 (2008)
13. Sharma, C.: Big data analytics using neural networks (2014)
14. Hu, Y.-C.: Pattern classification by multi-layer perceptron using fuzzy integral-based activation function. *Appl. Soft Comput.* **10**(3), 813–819 (2010)
15. Pal, S.K., Mitra, S.: Multilayer perceptron, fuzzy sets, and classification. *IEEE Trans. Neural Networks* **3**(5), 683–697 (1992)
16. Sarwar, S.M., Hasan, M., Ignatov, D.I.: Two-stage cascaded classifier for purchase prediction. arXiv preprint [arXiv:1508.03856](https://arxiv.org/abs/1508.03856) (2015)
17. Simonovsky, M., Komodakis, N.: Onionnet: sharing features in cascaded deep classifiers. arXiv preprint [arXiv:1608.02728](https://arxiv.org/abs/1608.02728) (2016)
18. Christ, P.F., Elshaer, M.E.A., Ettlinger, F., Tatavarty, S., Bickel, M., Bilic, M.R., Armbruster, M., Hofmann, F., DAnastasi, M., et al.: Automatic liver and lesion segmentation in ct using cascaded fully convolutional neural networks and 3d conditional random fields. In: International Conference on Medical Image Computing and Computer-Assisted Intervention, pp. 415–423. Springer (2016)
19. Long, J., Shelhamer, E., Darrell, T.: Fully convolutional networks for semantic segmentation. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 3431–3440 (2015)



Multiple Linear Regression Analysis of Factors Affecting the Consumption

Jesús Silva^{1(✉)}, Omar Bonerge Pineda Lezama², and Darwin Solano³

¹ Universidad Peruana de Ciencias Aplicadas, Lima, Peru
jesussilvaUPC@gmail.com

² Universidad Tecnológica Centroamericana (UNITEC),
San Pedro Sula, Honduras
omarpineda@unitec.edu

³ Universidad de la Costa, St. 58 #66, Barranquilla, Atlántico, Colombia
dsolanol@cuc.edu.co

Abstract. Econometrics provides the researchers with methods, theoretical basements, and procedures that allow the formulation and estimation of economic models that explain the study variable during a reference time period, as well as making predictions about the behavior of the studied reality based on the explanatory variables. The entire process, analyzed from econometrics after having formulated and estimated the model, leads to a very important phase: the statistical validation, which helps the researcher to ensure that the model satisfactorily passes a series of tests. These tests will allow the use of the model not just to explain the behavior of the independent variable under study, but to make predictions based on scenarios of occurrence based on those explanatory variables included in the model, offering a theoretical-practical support to formulate policies related to the studied phenomenon. This research aims to generate the first elements to know the private consumption behavior in India in the period from 2012 to 2018.

Keywords: Private consumption · Analysis · Influence · Correlation

1 Introduction

The model applied in this study is the Multiple Regression, which considers certain assumptions that are corroborated by means of analysis with Chi-squared test, Durbin Watson, and Heteroskedasticity, obtaining conclusions related to the variables that explain the significance of each for the model [1–3].

The present research seeks to describe the variables that explain the behavior of the domestic consumption of goods and services in the period from 2012 to 2018. Knowing the variables that affect the consumption and its incidence will allow to measure the impact over the selected time period, offering a reference to the variations that were generated in the domestic consumption [4–6].

The knowledge of the variables affecting the domestic consumption becomes relevant in microeconomic terms, either for companies, businesses in general, and could serve as input for generating policies to impact in the future plans and decision-making

processes. In macroeconomic terms, this topic is relevant for decision-making processes on economy, government policies, and tax issues [7–9].

For the above mentioned, this study is carried out on the basis of official data published by the Central Bank of Colombia, which could also serve as a basis for future researches to extend knowledge on the domestic consumption behavior [10–12].

As a general objective, the study aims to recognize the factors that explain the behavior of private consumption in Colombia during the mentioned period. The specific objectives are: identify the correlation between the selected variables; generate an econometric model to explain the behavior of private consumption; and learn about the incidence of each variable over the consumption.

2 Method

The linear regression forecasting model was applied, allowing to find the expected value of a random variable a when b takes a specific value. The application of this method implies an assumption of linearity when the demand presents an increasing or decreasing behavior [13, 14].

2.1 Explanation of the Analyzed Variables

2.1.1 Dependent Variables

Private consumption: Private consumption refers to the spending incurred by family units, private companies, and private non-profit institutions with residence in a country. Purchases of land and buildings for housing are excluded from this calculation since they refer to a form of investment (real estate) [15].

2.1.2 Independent Variables

CPI: The Consumer Price Index (CPI) is an economic indicator in which the prices of a specific set of goods and services (known as “family basket”) that a number of consumers regularly purchase are determined on the basis of continuous surveys on family budgets (also called “survey of household spending”) and the variation with respect to the price of each product compared to a previous sample. It measures the changes in prices of a family basket of consumer goods and services purchased by households. It is a percentage that can be positive (indicating an increase in prices) or negative (reflecting a fall in prices) [16].

Nominal Wage Rate: Nominal wage is the amount of money received by wage-earners as remuneration for their work. The nominal wage of workers can increase without an increase in their well-being, that is to say that prices of goods and services can rise more or in the same proportion than nominal wages.

Private sector credit: The domestic credit to the private sector refers to financial resources granted to the privately-owned companies through loans, purchase of values which do not constitute a share of capital, and trade credits and other accounts receivable, which create a right of reimbursement [17].

Default rate: It is defined as the ratio between the value of the doubtful loans and the value of the portfolio of total credits [16].

3 Results

3.1 Formation of Variables

For the purposes of this study, the data collected from the years 2012 to 2018 was obtained from official reports of the Central Bank of Colombia for the analysis of variables of an econometric model to explain the factors that affect the variation of commercial consumption in Colombia.

A model was adjusted considering the total of variables selected with the aim of knowing the findings and interpret the significance that each variable would contribute (see Tables 1 and 2).

Table 1. Regression with all variables

	Coefficients
Interception	-11450304994
IPC	13850949.01
Nominal wage index	-8298.758452
Default	-25769393489
Private sector credit	545.3611706

Table 2. Correlation between variables

	Private consumption	CPI	Wage Index	Default	Private sector credit
Private consumption	1				
CPI	0.98546258	1			
Nominal wage index	0.98536214	0.99658745	1		
Default	-0.74538966	-0.80126354	-0.8024369	1	
Private sector credit	0.95368752	0.91239865	0.89632147	-0.5523669	1

It can be observed that the variables explain a 99% of consumption and the significance of the model is good, however, some variables do not contribute to the model and when its significance shows zero it is very high. These are:

- The nominal wage rate: it may be due to its high relation with the CPI. Another point that highlights is that when working with this variable, it does not affect the analysis of private consumption and it can be assumed that people with a minimum income must go into debt to purchase the goods and services in the market.
- The default: it may be due to the fact that it is an indicator taken into account in the analysis for granting credits.

Due to the above, it excludes irrelevant variables and a new model with variables that will provide greater significance to the analysis is proposed.

3.2 Selected Variables

The model runs again using just the selected variables, obtaining the following (see Eq. 1).

$$Y = -21388575858, 154 + 14253987, 254x_1 + 547, 98x_2 \quad (1)$$

Where:

x_1 = CPI

X_2 = Private sector credit

In this model, where variables of CPI and credit to the private sector are used, it can be observed that:

- The dependent variables explain 99% of private consumption in Colombia.
- The significance of the model is very good, showing a critical value or P value that is practically 0 (zero).
- The value of the intercept of $-21388575858, 154$, indicates the private consumption when the CPI and the credit are 0 (zero). The interception is located in the axis - Y
- For each unit of change in the CPI, the private consumption will vary in direct relation to $14253987, 254$ units.
- For each unit of change in the credit, private consumption will vary in direct relation to 547.98 units.

3.3 Chi-Squared Test

The calculated Chi-squared is less than the critical Chi-squared, therefore, the model does not present Heteroskedasticity, that is, the average of the variables is close to the average of the population (see Table 3).

Table 3. Chi-squared test

		Freedom degrees
# variables	5	4
Level of significance	0.05	
n	17	
R ²	0.25487	
Calculated Chi-squared	4.32546	
Critical Chi-Squared	9.4578	
Decision Tree		
Calculated Chi-squared	Greater than 4.32546	Critical Chi-Squared 9.4578

There is no Heteroskedasticity

3.4 Proof of Auto-correlation Between Variables

Durbin Watson test is applied, obtaining the results shown in Table 4.

Table 4. Durbin Watson test (DW)

Rule	
H ₀	There is no correlation
H ₁	There is correlation
DW	2.214587
Positive autocorrelation	

4 Conclusions

In the analysis on the variables that affect the private consumption in Colombia was applied on collected reports from government data in order to identify the variables that influence the domestic private consumption. In this context, official data was collected on variables such as: CPI (Consumer Price Index), nominal wage rate, loan default, credit to the private sector during the period from 2012 to 2018.

In order to achieve the objectives outlined in the present paper, the regression analysis tool was applied for obtaining the correlations between the independent and the dependent variables. The applied statistical method was based on the Ordinary Least Squares (OLS) regression, complying with all its assumptions to obtain an optimal model. Regressions were performed for selecting the variables that explain the private consumption. The carried-out regressions allowed to achieve an equation that meets the OLS assumptions, thus obtaining coefficients that explain the behavior of private consumption.

The variables that best explain the behavior of private consumption are the CPI and Credit, whose model shows a R² 0.9959 and R² adjusted of 0.9953, which shows that

the CPI and credits have a 99% correlation with private consumption. The ANOVA analysis data showed consistency in obtaining the variables with a confidence of 95%. The *t* student, heteroskedasticity tests, and the absence of correlation between variables allow to obtain the status of variables MELI5. The equation components show a negative intercept, indicating that, in terms of consumption, economic agents mostly purchase consumer goods with credits.

The coefficient of the CPI is positive, indicating that consumption also increases with an increase in this variable. As this variable (CPI) shows, the level of price and the theory of demand refers that with a price increase, the consumption decreases, and the composition of the sign of coefficient does not show such a result. However, the negative sign of the autonomous consumption and the sign of the Credits could explain how consumers are faced with the increase in the price in order to maintain or increase their acquisition level of consumer goods [17, 18].

The variable of credits is the second variable in the equation, where the coefficient shows positive sign, indicating that the possibility of credits in the short term increases as the incomes of people through credits increase. This can be supported by the theory of consumer in the explanation of the budget line. Although, the price of the credits could also affect the demand, this issue is not related to the study and can be approached in another research.

Therefore, the linear regression applied on the collected data shows that private consumption has a correlation between CPI and credits, whose correlations are positive, but the intercept of the equation is negative. This result indicates that the autonomous consumption is not possible and the sustainability is feasible in the case of a shock in the market. Another point to note is that, according to the analyzed data, loans are important for consistency in the level of consumption and help people to finance the price increases.

References

1. Rahman, M.A., Islam, M.Z.: A hybrid clustering technique combining a novel genetic algorithm with K-means. *Knowl.-Based Syst.* **71**, 345–365 (2014). <https://doi.org/10.1016/j.knosys.2014.08.011>
2. Ramadas, M., Abraham, A., Kumar, S.: FSDE-forced strategy differential evolution used for data clustering. *J. King Saud Univ. - Comput. Inf. Sci.* (2016). <https://doi.org/10.1016/j.jksuci.2016.12.005>
3. Vásquez, C., Torres, M., Viloria, A.: Public policies in science and technology in Latin American countries with universities in the top 100 of web ranking. *J. Eng. Appl. Sci.* **12** (11), 2963–2965 (2017)
4. Torres-Samuel, M., Vásquez, C., Viloria, A., Borrero, T.C., Varela, N., Cabrera, D., Gaitán-Angulo, M., Lis-Gutiérrez, J.P.: Efficiency analysis of the visibility of Latin American Universities and their impact on the ranking web. In: Tan, Y., Shi, Y., Tang, Q. (eds.) *Data Mining and Big Data, DMBD 2018. Lecture Notes in Computer Science*, vol. 10943. Springer, Cham (2018)
5. Bandyopadhyay, S., Maulik, U.: Genetic clustering for automatic evolution of clusters and application to image classification. *Pattern Recognit.* **35**, 1197–1208 (2002)

6. Tam, H., Ng, S., Lui, A.K., Leung, M.: Improved activation schema on automatic clustering using differential evolution algorithm. *IEEE Congr. Evol. Comput.* 1749–1756 (2017). <https://doi.org/10.1109/CEC.2017.7969513>
7. Duque Oliva, E., Finch Chaparro, C.: Measuring the perception of service quality education by students AAUCTU Duitama. *Free Criterion Mag.* **10**(16) (2012)
8. Wickramarachchi, D., Robertson, B., Reale, M., Price, C., Brown, J.: HH CART: an oblique decision tree. *Comput. Stat. Data Anal.* **96**, 12–23 (2016)
9. Hong, S., Yang, D., Park, B., et al.: An efficient intra-mode decision method for HEVC. *SIViP* **10**(6), 1–9 (2016)
10. Kavzoglu, T., Sahin, E.K., Colkesen, I.: An assessment of multivariate and bivariate approaches in landslide susceptibility mapping: a case study of Duzkoy district. *Nat. Hazards* **76**, 471–496 (2015)
11. Lei, J., Sun, Z., Gu, Z., Zhu, T., Ling, N., Wu, F.: Simplified search algorithm for explicit wedgelet signalization mode in 3D-HEVC. In: 2017 IEEE International Conference on Multimedia and Expo (ICME), Hong Kong, pp. 805–810 (2017)
12. Zhao, J., Zhao, X., Zhang, W., et al.: An efficient depth modeling mode decision algorithm for 3D-HEVC depth map coding. *Optik Int. J. Light Electr. Opt.* **127**(24), 12048–12055 (2016)
13. Núñez, J.: Universidad, conocimiento, innovación y desarrollo local. Ed. Félix Varela, La Habana (2014)
14. Arzola, C., Sanso, M.: Knowledge Management Program for Local Development (2015)
15. Valle Cuéllar, D.Y.: Evaluación y diseño de estrategias para el logro del Desarrollo Sostenible en el Centro Histórico Urbano de Cienfuegos (2011)
16. Reguant-Álvarez, M., y Otros.: El método Delphi. Recuperado de (2016). <http://revistes.ub.edu/index.php/REIRE/article/download/reire2016.9.1916/18093>
17. Varela, N., Fernandez, D., Pineda, O., Viloria, A.: Selection of the best regression model to explain the variables that influence labor accident case electrical company. *J. Eng. Appl. Sci.* **12**, 2956–2962 (2017)
18. Izquierdo, N.V., Lezama, O.B.P., Dorta, R.G., Viloria, A., Deras, I., Hernández-Fernández, L.: Fuzzy logic applied to the performance evaluation. Honduran coffee sector case. In: Tan, Y., Shi, Y., Tang, Q. (eds.) *Advances in Swarm Intelligence, ICSI 2018. Lecture Notes in Computer Science*, vol. 10942. Springer, Cham (2018)



Collaborative Spaces in Virtual Environments: Socio-Cultural Support for the University Beginning Teacher

Jesús Silva^{1(✉)}, Juliana Ferrer², Mercedes Gaitán³,
and Jenny Paola Lis⁴

¹ Universidad Peruana de Ciencias Aplicadas, Lima, Peru
jesussilvaupc@gmail.com

² Universidad San Pablo-CUE, Madrid, Spain
Julianaferre55@yahoo.es

³ Corporación Universitaria Empresarial de Salamanca, Barranquilla, Colombia
m_gaitan689@cues.edu.co

⁴ Universidad Corporación del Meta (UNIMETA), Villavicencio, Colombia
Jenny.lis@unimeta.edu.co

Abstract. At present, the integration of educational social networks are acquiring a fundamental role, the use of portable digital tools to support the teaching and learning processes that allow improving the processes of Teaching-Learning (E-A) in the university environment, it is important to highlight in the same way the concept of leadership that was developed in the beginning in the organizational environment to stimulate the workers in the achievement of the established goals, which through time gender that this term was used in other areas such as sports, management and politics. Recently, in the field of education, efforts have been made to develop leadership in a pedagogical, distributed, and transformational manner in the management and teaching teams of institutions in order to improve learning outcomes. The academic community is influenced by an environment of intellectual, social, cultural, and technological development, which converts the beginning teacher into an active agent who must deal with a global reality of uncertain changes. In this context, the collaborative virtual learning environments are assumed as the optimum scenario to board the training and development of the future trainers at university level, generating a critical and reflexive attitude for their formation in the teaching/learning process. The motivation of this paper arises from these reflections with the purpose of analyzing the collaborative spaces in virtual environments as socio-cultural support for university beginning teachers. Based on a qualitative research with a documentary phase, a theoretical comparison was developed to generate analysis categories which allowed to perform a depth interview addressed to teachers from different countries of Latin America and the Caribbean involved in this training. Concerns and expectations emerged within the formative phase of the beginning teachers, characterized by the pursuit of learning processes that do not exist in their training plan to connect them to a virtual and collaborative reality. The paper invites to reflect on the importance of this issue to build a favorable scenario for future generations.

Keywords: Collaborative learning · Beginning teacher · Teacher work · Virtual learning

1 Introduction

The emergence of a new world order with the appearance of global spaces has generated uncountable changes, asymmetries, and profound gaps that have brought unprecedented demands from social agents that take part in this global world. This new reality is evident at all levels of the education system [1–5]. So, the technological revolution and its relationship with the global learning environment urges the adoption of a new teaching approach in which the collaborative actions can be articulated. Such teaching/learning environment presents evaluative traits for collaboration, such as interactivity, universality, synchronicity and use of language as part of the teacher-student, student-student, and teacher-teacher interrelationships [6–8].

In this way, collaborative learning in virtual spaces arises and recognizes a new socio-cultural context of agents in virtual collaborative activities engaged in teaching-learning tasks that lead to a proposal for a reflection which, at the same time, confronts the individualistic approach and promotes a model that differentiates the group activities regarding to cooperative and collaborative experiences, and pointing to the deepening of knowledge and a change of attitude on the part of those social actors, thus generating the necessary synergy to enhance creativity and inquiry of ideas [9–11].

For all the above, it is important to actively involve the novel teachers as facilitators in the teaching/learning process in this socio-cultural scheme and make them become active agents of change to respond to the demands of a global world. This task requires creativity and commitment in the assumed didactics, but also responsibility for transmitting the proper use of language in terms of rigor and management of a technical vocabulary operated by the socio-cultural reality [6, 12–15].

The motivation of this paper arises from this reflection as a result of a non-experimental analytical-descriptive qualitative research, product of the follow-up during several years of the initiation process of beginning teachers at the university context [16–19]. The search and collection of information was carried out to gather useful experiences for contextualizing the subject, thus developing a categorization that led to the generation of a depth interview instrument which results allowed the generation of knowledge about the study subject.

2 Theoretical Review

In this section, there is a theoretical comparison of different authors who deepen the analysis categories.

2.1 The Beginning Teacher in the University Space Reality

Within the study of educational organizations and especially the universities, a vision intimately linked to a heteronomous context is outlined to understand the institution in interaction with the environment, the expectations of the society and, at the same time, to manage the values that must be assumed as part of the socio-cultural context.

Historically, the vision of society about the university teacher has changed over time. Its concept has experienced an advance toward secularization and material

development leading to a professional who integrates the social and cultural heritage built by generations. In [3] states that the teaching profession is based on the best elements of the cultural heritage and defines it as the set of systematic actions carried out under processes of planning, development, monitoring, evaluation, and feedback during the educational process.

In this sense, the teaching performance is exercised in the personal mastery, in the space of learning, in the institutional field, and in the socio-cultural environment [8, 20–25]. In this order of ideas, it can be said that the professional teacher goes through a socio-cultural reality that guides the teaching-learning process. The beginning teacher acts in this scenario searching for a professional identity, becoming permeable to the integration of new ideas and experiences in the discovery of the developing teaching work [22, 26–30].

2.2 The Collaborative Learning: An Assertive Response to Education in Virtual Environments

The impact of the new technologies has opened a digital gap between the social sectors and the new generations in relation to the skills they feature to use the digital tools and their interpretation of the need to use them, replacing traditional forms of communication that have left their mark on the educational work. This context provides new opportunities for learning, unlearning and relearning in education, making necessary to reorganize the frame of knowledge and relationships of power that allow to transmit the message through networks in an adequate manner [3].

Such a reality has been impacted by a socio-cultural process mediated by technology evidenced in the global spaces that favor the entity of virtual communities marked by multiculturalism, generating a complex educational challenge by the presence of diversity of languages, beliefs, values, principles, and ways of understanding the educational work [31–33].

2.3 Collaborative Learning Spaces for Socio-Cultural and Technological Development: Initiation Challenge for the University Teacher

The socio-cultural constructivism serves as a framework of reference for the collaborative learning approach which today represents a significant advance in the construction of ideas and knowledge [10] and represents an easy handling instrument for the new generations of teachers who must develop their skills in the use of technologies.

In this regard, collaborative learning raises and responds to a global socio-cultural and technological scenario in a symbiotic relationship with the formation of the beginning teacher for their academic activities within the university.

In this scenario, the processes of team work for collaborative learning in virtual environments are developed, and the teacher's role is based on the socio-constructivism theory which proposes a mediator who promotes a kind of non-mediated relationship, stimulating the development of potentialities, and correcting deficient cognitive functions for the comprehensive formation of the individual [25].

To that effect, the beginning teacher faces the responsibility of transmitting and promoting knowledge in a rigorous socio-cultural language in front of a community of interests which is able to access to the knowledge embodied in the virtual global network updated with greater speed than the human learning [7].

In this order of ideas, [19] presented a model of learning community that requires the teacher to set common goals, targets, outcomes, and guidelines that will be socialized with people in the dynamics and processes for generating reflective spaces for the exchange of experiences and knowledge.

The university institutions involved in this global context face a process of radical transformation where teachers and students are required, by the socio-cultural and technological development, to pass from the traditional teaching systems to a virtual teaching work oriented toward the reflective spaces.

Another issue to consider in the initiation of the university teacher is the type of support received by the beginners to achieve their insertion into the academic world with the presence of a mentor for authors [17]. There are strategies as the classroom observation and reflection, collaboration in planning, and workshops with mentors that allow the novel teachers to be inserted into the reflective processes developed during their tasks.

The mentor or trainer provides support to the beginning teacher for solving problems and answering to questions by giving tips from the experience. In this sense, it is necessary to generate a relationship of trust to advance in the formation without fear. It is also necessary that the young professionals develop, with the support of their mentors, skills for critical reflection to analyze their work under conditions of creativity and originality. So, the mentor teacher must motivate the beginners to overcome their isolation and offer the possibility to develop the interactivity of learning as an essential step to connect with the collaborative processes [17].

Thus, the successful work of the beginning teacher in collaborative university virtual spaces will be marked by the ability to enter to the learning community under the responsibility of the mentor, developing a set of technical, human, professional, and digital competencies in response to a comprehensive formative nature compatible with other existing assessment instances along the university career [12].

3 Method

This paper is based on a non-experimental research with an analytical-descriptive approach in a qualitative perspective and a documentary phase. A theoretical comparison is carried out generating a reference for the elaboration of an instrument (in-depth interview) applied in a virtual way.

To that effect, a nonrandom sample to trial was selected, addressed to university beginning teachers belonging to several countries, particularly in Latin America and the Caribbean, who participated in the training process as teachers within virtual collaborative spaces.

In this regard, a total of twenty-five (25) teachers from universities in developing countries where they develop their teaching (Chile, Colombia, Peru, Venezuela, and Cuba) were interviewed. The data obtained were handled under the techniques of

content analysis and categorization to generate the analysis, discussion and evidences of the study.

4 Analysis and Discussion of the Results

Most of the beginning teachers (BT) must face the challenge of being teaching professionals without having even the specialized knowledge and expertise in the teaching profession. The theory basement of the present research is confirmed at Latin American and the Caribbean universities during the formation of the BT. These institutions are still focusing on face-to-face activities, offering courses about instructional strategies and techniques in the classroom and, to a lesser extent, to the activities of virtual and collaborative learning. The number of hours dedicated to offer a course for virtual training is restricted, putting aside the active participation between teacher-student, student-student, teacher-teacher that would contribute to the generation of innovative ideas in the teaching/learning process.

About the expectations of the BT, when observing the evidences of this reality in different countries, most of the teachers are aligned in the quest to prepare for their integration into the socio-cultural challenge which involves the university education. However, a small number of teachers are not clear about their true role as a teacher or a researcher.

Regarding the support received during their training as a BT, a significant number of them refer to the fact that they have not received any support or just having a group of teachers for consulting about the subject matter they administrate, but there is hardly a permanent accompaniment during the formation that guarantees help to the BT during that initial stage. Only a small number of participants refer the real accompaniment of the mentor as trainer of trainers, guaranteeing the proper use of technical daily language, the transmission of evaluative processes and the socio-cultural insertion within the management philosophy of the university.

When referring to the training received by the BT in virtual collaborative learning (VCL), it is evident that most of the participants did not have, in its initial formation, the deepening training in this field. The initiation in VCL has been developed in courses carried out in parallel ways to their training and as a result of individual initiative or throughout their college career where they achieved experiences in the following issues: interaction of knowledge, efficient use and management of time and the contents, contributions to the teaching/learning process in remote areas and with the absence of face-to-face spaces, compliance with the established planning, motivation for collaborative working and creating research teams. Likewise, most of the participants believe they have achieved efficiency in the management of VCL in areas such as the collective work in a set of disciplines, ensuring the inter and transdisciplinary creation of knowledge, and participating in controlled forums with motivation techniques in group.

About the values handled and the conduct of a proper use of language, the results show the presence of values of respect, responsibility, cooperation, collaboration and tolerance, in relation to the team work. Participants refer the importance of the appropriate use of language, the virtual forums and chats, recording and feedback of

interactive classes, training of the BT in VCL, study and development of language for VCL.

Finally, the interviewees, as an important contribution to the study, make the following suggestions: (a) sensitize university managers on the need to train on VCL as it represents a valuable tool for the teaching/learning process, (b) differentiate the cooperative learning from the collaborative learning, and (c) motivate the student as a part of the natural connection for the virtual processes.

5 Conclusions

The initial training of beginning teachers faces the challenge of a socio-cultural environment which remains uncertain and, at the same time, gives the opportunity to participate in collaborative learning spaces that reinforce their training requiring critical accompaniment of the pedagogical praxis on the part of the mentor, which provides the link between teaching and specialized knowledge.

In addition to this experience, the work processes for collaborative learning in virtual environments demand a role of the teacher becoming a mediator who requires a kind of unmediated interrelation. This proposal favors learning, stimulates the development of potentialities, improves cognitive functions, and moves all the actors to a space of potential development.

In this regard, the beginning teacher is aware of the importance of the VCL in the educational work, but there is no evidence of its relevance in training as a transforming shaft of the teaching work, which, in the case of most Latin American universities studied, is just a complement within the training strategies. However, the beginning teacher manifests its importance in the formation and discussion of new ideas within the knowledge field in the context of inter and transdisciplinary studies and, above all, in remote and without face-to-face experiences.

Finally, there is a need to continue studying this topic because its management urges to solve the individualism of the virtual contexts today, and invites to collaborate in an open manner in the discussion of ideas within one or more areas of knowledge, thus contributing to the formation of BT, and forming leaders in knowledge that motivate a generation characterized by the daily preference in the use of virtual networks and processes. These actions will guide the young university students in the need for confronting ideas, and where the BT becomes an active agent of the process of change, growth and integral formation of future generations.

It is important to promote strategies that promote the active participation of students through technologies, facilitating creativity, the exchange of ideas and experiences through virtual spaces for collaborative work. It is also significant to create peer learning contexts that allow communication so that mutual help and responsibility arise in group work tasks [29].

This environment of exchange of information obtained from various sources, makes possible the reflection and acquisition of new knowledge from the framework of autonomous and constructivist learning, always adequately valuing the times required by this type of educational process [30–33].

References

1. Bartholomew, R., Guiter, M.: La revolución de la enseñanza? El aprendizaje colaborativo en entornos virtuales. *Comunicar* **42**(21), 10–14 (2014)
2. Beca, C., Boerr, I.: El proceso de inserción en la docencia. En Aprendizaje y desarrollo, profesional docente. Metas educativas 2021, Organización de Estados Iberoamericanas. Fundación Santillana, España, pp. 109–118 (2010)
3. Delgado, K.: Aprendizaje colaborativo: teoría y práctica. Editorial magisterio. Bogotá, Colombia (2015)
4. Durán, R., Estay-Niculcar, C., Álvarez, H.: Adopción de buenas prácticas en la educación virtual en la educación superior. *Aula abierta* **43**(2), 77–86 (2015)
5. Expósito, C.: Valores básicos del profesorado. Una aproximación desde el modelo axiológico de Shalom Schwartz. *Educación y educadores*, pp. 307–325. Universidad de la sabana, Colombia (2018)
6. Ferrer, J.: Labor docente del profesor principiante universitario: reto de la universidad en espacios globalizados. Ponencia presentada en jornadas científicas Dr. José Gregorio Hernández. Universidad Dr. José Gregorio Hernández. Venezuela (2017)
7. Fondón, I., Madero, M., Sarmiento, A.: Principales problemas de los profesores principiantes en la enseñanza universitaria. En *Formación universitaria* **3**(2), 21–28 (2010)
8. Fontrodona, J.: Ciencia y práctica en la acción directiva. Ediciones Rialp, España (2003)
9. Gewerc, A., Montero, L., Lama, M.: Colaboración y redes sociales en la enseñanza universitaria. *Comunicar* **42**(21), 55–63 (2014)
10. Gómez, L., García, C.: Las competencias sociales como dinamizadoras de la interacción y el aprendizaje colaborativo. Ediciones hispanoamericanas. Universidad nacional abierta y a distancia, Colombia (2014)
11. Gros, B.: Aprendizaje, conexiones y artefactos de la producción colaborativa de conocimiento. Editorial Cedisa, España (2008)
12. Hernández-Sellés, N., González-Sanmamedy, M., Muñoz-Carril, P.C.: El rol docente en las ecologías de aprendizaje: análisis de una experiencia de aprendizaje colaborativo en entornos virtuales. Profesorado. *Revista de Currículum y Formación de Profesorado* **19**(2), 147–163 (2015)
13. Lombardi, G., Abrile, M.: Aprendizaje docente y desarrollo profesional. Metas educativas 2021. Organización de Estados Iberoamericanas. Fundación Santillana, España, pp. 57–66 (2010)
14. Marcelo, C.: El profesorado principiante. Inserción a la docencia. Ediciones Octaedro. Barcelona, España (2009)
15. Montenegro, I.: Perfil del docente investigador, para una educación de calidad. Editorial Génesis S.A.S. Bogotá, Colombia (2018)
16. Murga-Menoyo, M.Á.: Competencias para el desarrollo sostenible: las capacidades, actitudes y valores meta de la educación en el marco de la Agenda global post-2015. *Foro de Educación* **13**(19), 55–83 (2015)
17. Ochoa, L., Cueva, A.: Dificultades y retos de los maestros principiantes de español como lengua extranjera (ELE). En *Folios. Segunda época* (39), 3–11 (2014)
18. Onrubia, J., yEngel, A.: The role of teacher assistance on the effects of a macro-script in collaborative writing tasks. *Int. J. Comput.-Support. Collaborative Learn.* **7**(1), 161–186 (2012). Disponible en <https://www.redalyc.org/pdf/567/56741181010.pdf>
19. Palloff, R., Pratt, K.: Building Online Learning Communities. Effective Strategies for the Virtual Classroom, 2nd edn. Jossey-Bass, San Francisco (2007)

20. Pérez, M., Romero, M., Romeu, T.: La construcción colaborativa de proyectos como metodología para adquirir competencias digitales. *Comunicar* **42**(21), 15–24 (2014)
21. Pérez-Mateo, M., Guitert, M.: La dimensión social del aprendizaje colaborativo virtual. *RED. Revista de Educación a Distancia*, 18 (2007). Disponible en http://www.um.es/ead/red/18/perez_mateo_guitert.pdf
22. Pro Bueno, A., Valcárcel, M., Sánchez, V.: Viabilidad de las propuestas didácticas planteadas en la formación inicial: opiniones, dificultades y necesidades de profesores principiantes. *Enseñanza de las ciencias* **23**(3), 357–358 (2005)
23. Rodríguez, R.: Formación inicial del profesor novel universitario: Saberes del docente y cultura del aprendizaje organizacional. *Ciencias de la educación. Universidad Metropolitana (UNIMET)* **27**(49), 17–29 (2017)
24. Rodríguez Zamora, R., Espinoza Núñez, L.A.: Trabajo colaborativo y estrategias de aprendizaje en entornos virtuales en jóvenes universitarios. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo* **7**(14), 86–109 (2017)
25. Ruiz, E., Martínez, N., Galindo, R.: El aprendizaje colaborativo en ambientes virtuales. *Editorial centro de estudios e investigaciones para el desarrollo docente*, México (2015)
26. Salvat, B.G., Adrián, M.: Estudio sobre el uso de los foros virtuales para favorecer las actividades colaborativas en la enseñanza superior. *Educ. Knowl. Soc. (EKS)* **5**(1) (2015)
27. Valliant, D.: Políticas para un desarrollo docente efectivo. *Metas educativas 2021. Organización de Estados Iberoamericanas. Fundación Santillana, España*, pp. 29–38 (2010)
28. Zañartu, L.: Aprendizaje colaborativo: una nueva forma de Diálogo Interpersonal y en red. *Revista digital de educación y nuevas tecnologías. Contexto educativo. Nueva Alejandría. Argentina* (2011). <http://contexto-educativo.com.ar/2011/4/nota-02.htm>
29. Muñoz-Repiso, A.G.V., Gómez-Pablos, V.B.: Evaluación de una experiencia de aprendizaje colaborativo con TIC desarrollada en un centro de Educación Primaria. *Edutec. Revista Electrónica de Tecnología Educativa* (51), a291 (2015)
30. Fernández, M., Valverde, J.: Comunidades de práctica: un modelo de modelo de intervención desde el aprendizaje colaborativo en entornos virtuales. *Revista Comunicar* **42**, 97–105 (2014)
31. Vasquez, C., Torres, M., Viloria, A.: Public policies in science and technology in Latin American countries with universities in the top 100 of web ranking. *J. Eng. Appl. Sci.* **12** (11), 2963–2965 (2017)
32. Torres-Samuel, M., Vásquez, C., Viloria, A., Lis-Gutiérrez, J.P., Borrero, T.C., Varela, N.: Web visibility profiles of top 100 Latin American Universities. In: Tan, Y., Shi, Y., Tang, Q. (eds.) *Data Mining and Big Data, DMBD 2018. Lecture Notes in Computer Science*, vol. 10943, pp. 1–12. Springer, Cham (2018)
33. Viloria, A., Lis-Gutiérrez, J.P., Gaitán-Angulo, M., Godoy, A.R.M., Moreno, G.C., Kamatkar, S.J.: Methodology for the design of a student pattern recognition tool to facilitate the teaching – learning process through knowledge data discovery (big data). In: Tan, Y., Shi, Y., Tang, Q. (eds.) *Data Mining and Big Data, DMBD 2018. Lecture Notes in Computer Science*, vol. 10943, pp. 1–12. Springer, Cham (2018)



Competitions of Multi-agent Systems for Teaching Artificial Intelligence

Jesús Silva^{1(✉)}, Omar Bonerge Pineda Lezama², and Noel Varela³

¹ Universidad Peruana de Ciencias Aplicadas, Lima, Peru
jesussilvaUPC@gmail.com

² Universidad Tecnológica Centroamericana (UNITEC),
San Pedro Sula, Honduras
omarpineda@unitec.edu

³ Universidad de la Costa, St. 58 #66, Barranquilla, Atlántico, Colombia
nvarela2@cuc.edu.co

Abstract. This paper presents an approach based on competitions of multi-agent systems as the basis for teaching advanced topics in Artificial Intelligence. The method was applied in the Cognitive Robotics course with students of the 5th-year in Computer Science from the University of Mumbai in India, in the domain of Soccer. The championships are played between different teams to allow students to assess and compare the results. The motivation that is reached is fundamental for creating interest in the study of Artificial Intelligence techniques and in research. The developed experiences are described, as well as an analysis of the method and its impact for the academy and the research.

Keywords: Education · Artificial Intelligence · Cognitive Robotics · Robot soccer

1 Introduction

The curricula of undergraduate programs in Computer Science include topics about symbolic and non-symbolic Artificial Intelligence (AI), according to the suggestions of ACM/IEEE [1–3]. Teaching such topics represents a great challenge for teachers because of the hard work of providing a precise definition of AI, and because many of these issues are still developing. Most of today courses devote a great effort to the understanding of the different topics and less effort to integration and comparison of the various techniques. During the practices, students face a problem to be solved with some of the specific techniques, where the students present a poor knowledge to assess the appropriate technique and the way to support it with other tools to solve a given problem [4, 5].

There are few areas in Computer Science in which theory can be analyzed and implemented not just on reality simulators, but also with physical demonstrations. The area of AI is one of them, as it can provide real interactive experiences using robots, directly involving students. So, soccer is a multi-agent system application that allows the combination of several techniques that can be deployed on both simulators and on a

real environment, with development of a domain that is interesting and ludic at the same time [6–9].

Framed into a team game the teaching method was applied requiring the students to develop a multi-agent system with AI techniques in order to participate and win in soccer competitions. The importance of these competitions is reflected in the commitment made by students in the choice and application of AI techniques to develop their teams, in the initial contact of undergraduate students with research topics, and finally in the fun reached in an academic environment [10].

In this context, the University designed the optional course named Cognitive Robotics for Computer Science, which requires the participants to study and investigate topics in AI, choose the proper technique, develop a multi-agent system to play soccer, and assess and compare their results both in a simulator and in a real environment.

In recent years, the SimuroSot soccer simulator of FIRA was used in the AI course for studying search and planning [11–13]. However, the environment was redefined to perform the practices, restricting it to static and discreet characteristics [3]. On the other hand, the proposed exercises consisted of a single agent that should find a way from a starting point of the court to an end point, avoiding the obstacles that will be present in the way.

Unlike this first experience with AI in the Cognitive Robotics course, students implemented a multi-agent system in which the environment was not restricted (dynamic and continuous). The addressed topics are research issues in AI, so they helped reach motivation about accrediting the course, but the football competition was an incentive for the study.

Therefore, this paper proposes a design for teaching AI topics with a competition-based approach of multi-agent systems.

2 Method

The competition-based method was designed to be implemented in an optional course for advanced students of Computer Science. The main feature of this approach in AI teaching is that practices are organized with soccer as a common framework in which students can use various AI techniques to solve the same problem. Students designed, developed, and implemented a soccer team of robots through different projects, in which different AI techniques were integrated on the basis of simple reflex agents. It is important to note that, even when robots are used as an elementary resource, our purpose is not to teach robotics [14–16].

The difference lies in the fact that students must develop knowledge-based agents, instead of reactive agents that are then applied to the context of soccer, without focusing attention on the physical part of the robots. So, the purpose is to create “smart” agents, whose response times are adequate to be able to function in a dynamic and continued environment. In the design of the course under this approach, the study suggests three key milestones [14].

The first project aims at the study of a base team provided by the Chair, on which students will design, develop, and implement reflex players. The second project aims to investigate one or more topics about AI, selected from a list proposed by the Chair or

suggested by students, then make a report where the topic is developed, and finally, present the results. During the presentation of the topic by students, teachers encourage the discussion and analysis, comparing ideas to the contents that other students need to develop. In this way, students collaborate to build better solutions to the proposed problem, sharing experiences and partial solutions [2].

The third project aims to implement the techniques studied in the second project in the soccer player agents forming a multi-agent system: the team. In this project, students must submit the soccer team software, show skills acquired by implementing the technique, compare it with the initial team, study the computational complexity and draft a final report with paper format for explaining the development performed, then the analysis details and the findings of the project are presented.

The projects are developed by groups with a maximum of three members. A special class is given at the beginning and at the end of the academic term, where teams compete in a championship. The challenge of being the best team stimulates the students, particularly in the preparation of the team for the second championship. The evaluation of the course is carried out through the three projects. In the first case, students present the software and show the usually reactive behavior of the players. The simulators for the international federations are the selected platform for this exhibition. The second project is evaluated through the presentation-defense and the written report. Finally, the third project is evaluated in the laboratory through the simulators or the physical robots, as appropriate, and with the final report.

3 Results

Depending on the goals of the course and the designed method, the following activities were planned.

3.1 Activity 1

Presentation of the simulated RAKIDUAM soccer team as a pattern for the developments. The player agents are implemented in Ciao Prolog [4], language that offers all the advantages of programming in Logic and various mechanisms for interaction with other programming languages. The interface with the simulator was also provided to students. In the development of the interface with the simulator, the abstraction is the priority for the design of the agents in Prolog. This allows the agents to act both on the simulated platform and on the physical robot platform. This interface provides the independence of the programming language as additional flexibility. The strategies can be implemented in any language that supports communication using sockets.

Communication with the SimuroSot simulator of FIRA [2] was implemented through a dll developed in version 6.0 of the Visual Studio C++ environment [5]. A more detailed description of the interface can be found in [6] and [7]. Both the team and the interface have GNU General Public License [8], so students obtained the source codes of each of these programs. Students were suggested to use the LogViewer software [9] in order to analyze each move in the game to study the behavior of the player and team as a system.

3.2 Activity 2

The purpose of the First Project and the way to complete it was explained in the presentation. Teachers provided students with a general framework based on RAKIDUAM and with a module with a very simple strategy that would serve as an example. The main task in this phase was to rewrite the strategy.pl module that would implement a system of reactive agents. The RAKIDUAM system is organized in separate compilation modules. Its description is the following:

- Two modules: Navigation.pl and primitive.pl implement the predicates that perform the basic actions of the robots.
- Two other modules: command_server.pl and video_server.pl implement the interfaces with the command server and the video server respectively.
- The main.pl and environment.pl modules implement the drivers and the predicates that represent the internal state of the agents.
- Finally, the strategy.pl module contains the PROLOG rules that implement the game strategy of the robot agents.

3.3 Activity 3

First Soccer Championship. In the first project of the course, students had to design and implement the first team of robots in order to compete on the SimuroSot simulator of FIRA. The competition was implemented as a league system where each team faced the opponents twice. The evaluation of this project was carried out through competition, where the behavior of each player and team was observed, as well as the presentation of a first report for explaining the adopted strategies, the chosen knowledge representation, and all the design decisions among other features.

3.4 Activity 4

Introductory classes to the topics. As a preliminary step to the research project, the teacher introduced each of the items proposed for its development. The different techniques were analyzed from the point of view of applications and compared them with other similar. Finally, students were provided with the basic bibliography.

3.5 Activity 5

Research Project. The students selected a topic to research from those proposed by the chair. As a result of this study, students presented a class in which different multimedia resources were used in order to explain the topic to the classmates and teachers. In addition, they had to present a full report on the subject. In this sense, the teachers taught a class detailing some guidelines on research methodology and on the structure of the corresponding report. The topics proposed by the Chair were:

- Diffuse Control
- Reinforcement Learning
- Circumvention of obstacles - Navigation

- Continued Planning
- Fluent Calculus

Students selected and studied the last three topics. While each group specialized in a particular topic, the debate was encouraged so that all students take an active role and not only those who made the presentation. The fact that the research groups had already done a previous activity creating a soccer robot team was productive, since the study of these issues was carried out with a deployment goal in mind. The prior knowledge of the context to implement these techniques contributed to the understanding of the studied topics and the search for alternatives for the selected problem.

3.6 Activity 6

Second Soccer Championship. This is the latest project of the course. Students who specialized in the studied topic had to apply it to the domain of robot soccer. Each group improved its first soccer team, which was mostly reactive, with the studied technique. The group that analyzed the fluent calculus [10] implemented a knowledge base that allowed the team to change the game strategy based on fluents that described the situation of the game as favorable or not for the team, and in the relative success of each strategy [11].

The group that studied the techniques of circumvention of obstacles [6, 13, 16] implemented a suitable variant for the robot soccer, extending the available framework with the ability to use this necessary feature in the non-simulated environment [15]. Finally, the group that chose the continued planning study [17] implemented an integrated scheduler with the driver of the agents which produced an improvement in the behavior of the agents that is very difficult to achieve with reactive rules [18].

The competition was designed as a league system where each group faced all the other teams once, so that each group could compare the behavior of the team with all the other, evaluating the advantages and disadvantages of the different techniques. Also, the students submitted a final report in scientific paper format to explain the behavior of the team. The league ended with a ceremony with trophies for all teams.

4 Analysis of the Results

The implementation of the competition-based approach for the teaching of AI provided results in the domain of academy and research.

4.1 In Academy

Regarding the academy, the degree of participation and dedication to projects on the part of students highlights. Winning the competition games motivates students who spend more time in the study of different techniques for the development of the team. On the other hand, even all students wanted to win, the attitude changed from competition to collaboration. The difference in mood between the first tournament at the beginning of the course and the championship carried out after the research and

implementation of new techniques. In the first competition, students showed an extremely competitive attitude, while in the second competition, the desire to win and the competition itself step into the background.

4.2 In Research

The students had a first approach to research, particularly to that developed in the area of AI. Under the implemented method, students analyzed the basic bibliography of the topic and performed an advanced literature search guided by the teachers. They studied an AI technique that was later implemented in a multi-agent system and developed their first paper. In this sense, activities aimed at improving the scientific writing techniques, the structure of a scientific paper was explained, and finally teachers were the reviewers.

5 Conclusions

The competitions of multi-agent systems provide a teaching-learning environment that motivates students to overcome what was requested by the chairs, stimulating the identification of problems, the search for AI techniques, the generation and evaluation of solutions and the application of knowledge acquired in the course and in previous training.

From the activities of the course, the transfer of theoretical concepts into practice through projects stands out. The overall assessment of the method is positive, since students showed interest in the topics of the course, developed a research, conducted and developed technical reports and papers. For most of the students, this course was the first approximation to a scientific research, however, they successfully completed all the steps, from the field study, the implementation, and the writing of a scientific paper for a congress. Regarding the impact on research, it is important to note that many of the students are developing the final research of their careers in the Intelligent Robotics Research group.

References

1. Pineda Lezama, O., Gómez Dorta, R.: Techniques of multivariate statistical analysis: an application for the Honduran banking sector. *Innovate: J. Sci. Technol.* **5**(2), 61–75 (2017)
2. Viloria, A., Lis-Gutierrez, J.P., Gaitán-Angulo, M., Godoy, A.R.M., Moreno, G.C., Kamatkar, S.J.: Methodology for the design of a student pattern recognition tool to facilitate the teaching - learning process through knowledge data discovery (big data). In: Tan, Y., Shi, Y., Tang, Q. (eds.) *Data Mining and Big Data, DMBD 2018. Lecture Notes in Computer Science*, vol. 10943. Springer, Cham (2018)
3. Lee, A., Taylor, P., Kalpathy-Cramer, J.: A Tufail machine learning has arrived! *Ophthalmology* **124**, 1726–1728 (2017)
4. Yao, L.: The present situation and development tendency of higher education quality evaluation in Western Countries, p. 2006. Educ. Beef, Priv (2006)

5. Gregorutti, B., Michel, B., Saint-Pierre, P.: Grouped variable importance with random forests and application to multiple functional data analysis. *Comput. Stat. Data Anal.* **90**, 15–35 (2015)
6. Guo, Y., Hastie, T., Tibshirani, R.: Regularized linear discriminant analysis and its application in microarrays. *Biostatistics* **8**(1), 86–100 (2006)
7. Vásquez, C., Torres-Samuel, M., Viloria, A., Crissien, T., Valera, N., Gaitán-Angulo y, M., Lis-Gutierrez, J.: Visibility of research in universities: the triad producto-researcher-institution. Case: Latin American Countries. de Lectur Notes in Computer Scienicie (INcluding subseries Lectur Motes in Artificial Intellegent and Lectur Notes in Bioinformatics (2018)
8. Torres-Samuel, M., Vásquez, C., Viloria, A., Lis-Gutierrez, J., Crissien y, T., Valera, N.: Web visibility profiles of Top100 Latin American Universities. de Lectur Notes in Computer Scienicie (Including subseries Lectur Notes in Artificial Intelligent and Lectur Notes of Bioinformatics (2018)
9. ARWU: Ranking de Shanghái, [En línea]. <http://www.shangairanking.com/ARWU2018.html>. Último acceso 01 Dec 2018
10. QS: QS World University Ranking [En línea]. <https://www.topuniversities.com/university-rankings/latin-american-university-rankings/2019>. Último acceso 01 Dec 2018
11. Scimagoor: Scimago, Scimago Lab, [En línea]. <https://www.scimagoir.com/methodology.php>. Último acceso 01 June 2019
12. Webometrics: Ranking Web-Webometrics [En línea]. http://www.webometrics.info/es/Latin_America_es. Último acceso 30 Jan 2019
13. Torres-Samuel, M., Vásquez, C., Viloria, A., Hernández-Fernandez y, L., Portillo-Medina, R.: Analysis of patterns in the university Word Rankings Webometrics, Shangai, QS and SIR-Scimago: case Latin American. de Lectur Notes in Computer Science (Including subseries Lectur Notes in Artificial Intelligent and Lectur Notes in Bioinformatics (2018)
14. Vásquez, C., Torres-Samuel, M., Viloria, A., Lis-Gutierrez, J., Crissien, T., Valera, N., Cabrera y, D., Gaitán-Angulo, M.: Efficiency analysis of the visibility of Latin American universities and theri impact on the Ranking Web. de Lectur Notes in Computer Science (Including subseries Lectur Notes in Artificial Intelligent and Lectur Notes in Bioinformatics) (2018)
15. AgUILLO, I., Uribe y, A., López, W.: Visibilidad de los investigadores colombianos según sus indicadores en Google Scholar y ResearchGater. Diferencias y similitudes scon la clasificación oficial del sistema nacional de ciencia-COLCIENCIAS, Rev. Interam. Bibliot, vol. 40, no. 3, pp. 221–230 (2017)
16. Vásquez, C., Torres-Samuel, M., Viloria, A., Lis-Gutierrez, J., Crissien, T., Valera y, N., Cabrera, D.: Cluster of the Latina American universitiers Top100 according to Webometrics 2017. de Lectur Notes in Computer Scienicie (Including subseries Lectur Notes in Artificial Intelligent and Lectur Notes in Bioinformatics) (2018)
17. Melero y, R., Abad, F.: Revistas Open Access: Características, modelos económicos y tendencias, Lámpsakos, pp. 12–23 (2001)
18. Pinto, M., Alonso, J.C.J., Fernández, V., García, C., Garía, J., Gómez, C., Zazo y, F., Doucet, A.-V.: Análisis cualitativo de la visibilidad de la investigación en las Universidaes españolas a través de su página Web, Rev. Esp. Doc. pp. 345–370 (2004)



Implementation of an E.R.P. Inventory Module in a Small Colombian Metalworking Company

Jairo R. Coronado-Hernandez¹, Holman Ospina-Mateus²,
Danneris Canabal-Góñalez², Diana Peña-Ballestas²,
Javier Baron-Villamizar³, Nohora Mercado-Caruso¹,
Alfonso R. Romero-Conrado¹, Carlos Paternina-Arboleda⁴,
and Jesús Silva^{5(✉)}

¹ Universidad de la Costa, St. 58 #66, Barranquilla, Atlántico, Colombia

{jcoronadl8, nmercadol, aromerol7}@cuc.edu.co

² Universidad Tecnológica de Bolívar, Cartagena de Indias, Colombia

{hospina, t20050105, t20050745}@unitecnologica.edu.co

³ Escuela Naval de Cadetes “Almirante Padilla”, Cartagena de Indias, Colombia

jesus.garcia@unisimonbolivar.edu.co

⁴ Universidad del Norte, Barranquilla, Colombia

dfam@enap.edu.co

⁵ Universidad Peruana de Ciencias Aplicadas, Lima, Peru

jesussilvaUPC@gmail.com

Abstract. This paper aims to analyze the effect of implementing an inventory module of ERP Openbravo for the reduction of information flow time and customer response time, in a Colombian metalworking company. The processes structure and inventory management practices of the company were characterized and information flow time and customer response time were tested before and after implementing the inventory module. The main results were the reduction of 36% of information flow time and 41% of customer response time, so it can be concluded that obtained success is related to the active involvement of manager and workers' willingness to change.

Keywords: Customer response time · ERP · Information flow time · Inventory management

1 Introduction

Companies need to manage different kinds of resources and processes in order to obtain the best results, reducing the opportunity costs and the unnecessary expenses of time and raw materials. Enterprise Resource Planning systems (ERP) have been helpful in maintaining a real-time control and follow-up of each of the company's processes and resources. The American Production and Inventory Control Society APPICS defines ERP as a tool for planning and managing all the resources that are necessary to take, perform, and send customer orders in a company.

At the end of the 1980s and early 1990s, E.R.P. appeared as new software systems in the market, specifically targeting large and complex companies, but then, over the

years and the globalization of competitiveness, the target market of the E.R.P. has expanded from large companies to small and medium-sized enterprises (SMEs) [1]. Meanwhile, [2] considered ERP as the most innovative development of information and communication technologies (ICT) of the 1990s.

ERP systems have evolved and have suffered deep changes like programming language and the simplification of user interfaces. ERP modules can be added or exchanged when it is needed.

According to [3] some examples of ERP system modules include human resources, finances, sales, accounting, inventories, production, customer response, among others.

On the other hand, [4] have classified ERP modules in three groups: modules of the financial area, the logistics area and modules of the human resources area (See Fig. 1). Additionally, there are modules as particular solutions to specific sectors of the industry.

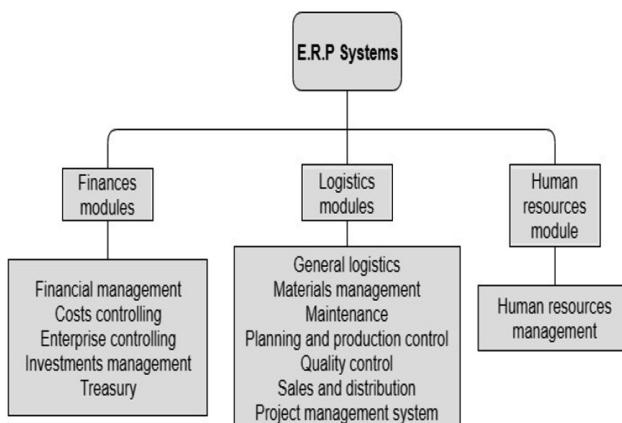


Fig. 1. Basic E.R.P. modules grouped by categories. Adapted from [4].

Authors in [5] sustain that the great advantage of the ERP systems is that they allow sharing information among different areas of the company, reducing the time spent in the generation of duplicated information. For example, the financial area and the inventory area require sales data information, which would cause them to have to duplicate that information and pass it to the other areas, while in an E.R.P. system the information is stored in the same database and is shared among the different modules.

The advantages of the implementation of an ERP system include improvements in the traceability of processes, the reduction of decision-making time [6]. In contrast, [7] exposes that the main disadvantages or barriers for ERP systems are the low commitment of managers or bosses and workers resistance to changes.

Multiple studies related to the use and implementation of ERP. have been focused mainly on the identification of success factors [8, 9], implementation and evaluation of success [4, 10–13], however, there is a lack of research for specific modules of ERP systems and focusing on evaluation of the reduction of times of flow of information and customer response.

2 Methodology

The present study was divided into three parts, with a simple empirical methodological design. The first stage of the study was to collect and characterize information about the operations and processes of the chosen mechanical metal company. In the second, the ERP was installed, and the staff of the company's area was sensitized for its use, demonstrating the importance and advantages of this. In the third and final stage, Measurements of information flow time were made between areas of the company, in addition to measuring the customer response time, timing them before implementing the ERP system. The calculation of the ideal time for the production process of a unit was carried out and after implementing the inventory module of the ERP system, the information flow time and response to the client was timed.

With the collected data, a simple comparison was made regarding the reduction in information flow times and customer response. The flow of information was counted from the request of the client in the commercial area, going through production and purchases and ended up in storage process.

3 Results

The chosen metalworking company is located in an important industrial sector of the Colombian Caribbean coast, close to where its main clients are located. The company has a building equipped with cutting equipment with computer numerical control (CNC) and other tools related to the cutting and maintenance of metal pieces. The selected company has 33 employees, and it is considered as a small company according to the local commercial regulations, therefore, it is inferred that there is a disposition of the company towards the technological improvement of its processes even though its current number of employees.

There was evidenced of the meticulous control of the quality of raw materials and inputs (See Table 1), however, once the inputs are entered and complete the quality tests, those are stored with little order, and the input and output formats of materials from the warehouse were generally outdated, which caused the absence of real control over the quantities of each input and/or raw material at the time of needing that information.

The company has six work areas identified, corresponding to Administrative area, Lathe and cut area, Furnace area, welding area, Painting area, and storage area.

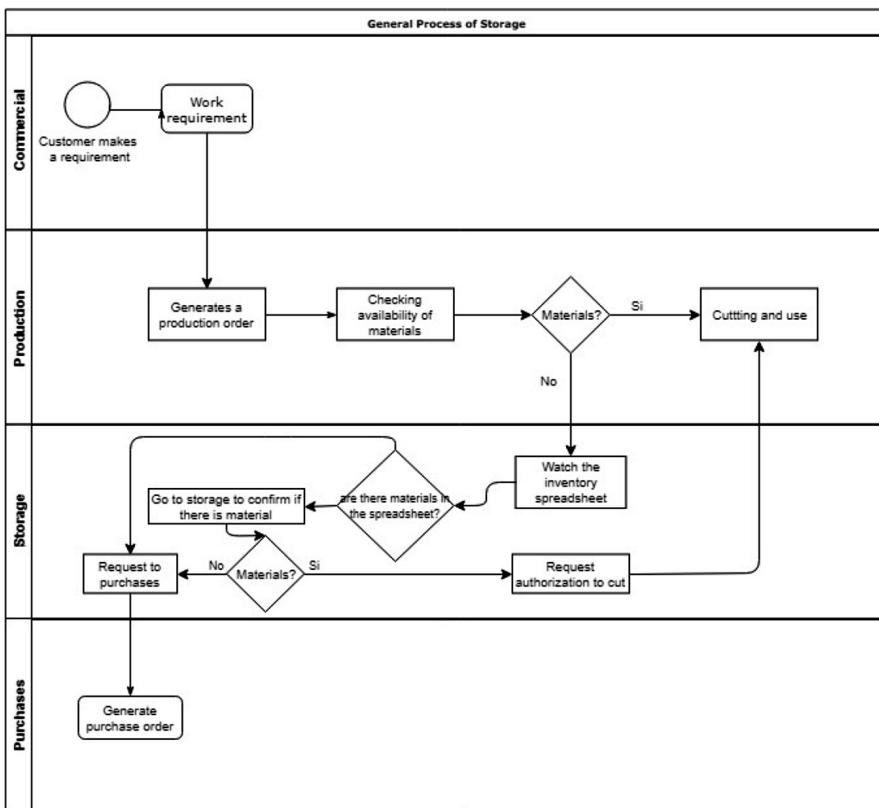
The company is limited to the acquisition of new clients, the loyalty of current customers, reception of orders, reception of recommendations and complaints, use of distribution channels to publicize their products and the quality they offer.

Evaluation of information flow times and customer response. The response time to customer requests varied from 5 to 10 h, as shown in Tables 2 and 3, so after the initial evaluation a similar exercise was done after implementing the inventory module during a period of 10 months.

It can be attributed that up to 95% of the reduction seen in the times of information flow and customer response is due to the implementation of the ERP inventory module, because, during the investigation, there were not introduced other changes to the processes, supply lines, procedures, different from those made at the time of implementing the module.

Table 1. SIPOC Reception of materials and tools of the metallurgical company analyzed.

Suppliers	Inputs	Process	Outputs	Customers
Suppliers	-Steel (feedstock) -Inputs -Tools	<pre> graph TD Start(()) --> Reception[Reception of materials and Quality test] Reception --> Decision{meets the quality requirements?} Decision -- No --> Return[Return order] Return --> Reception Decision -- Yes --> Accepted[Raw material / tool is accepted] Accepted --> Requisition[Generate customer requisition] Requisition --> End(()) </pre>	<ul style="list-style-type: none"> - Feedstock, raw materials, supplies and/or tools that meet the quality requirements. - Return order 	<ul style="list-style-type: none"> -Storage area -Sales department

**Fig. 2.** Diagram of inventory and storage process when a customer requirement is performed in the metalwork company analyzed.

3.1 Inventory and Storage

During the extensive analysis of the storage process, there were identified weaknesses in the organization of the materials in storage area, because in many cases the labeled materials were in locations that did not correspond to them, which caused that purchase orders for new raw material and other supplies were generated, even though it did not reach the minimum limits in stock established by the company.

In addition, when it was necessary to remove stored materials, the warehouse manager made several checks to determine whether or not there was any specific material required, having to go in most cases to personally check the existence or not of them. In Fig. 2 can be seen the production and storage sections, in which are redundant or unnecessary processes, which generate an unnecessary time spending.

-Requests, complaints and claims the information of all the complaints and claims made to the evaluated metalworking company was analyzed, during 10 months, obtaining as a result, 70.4% of the complaints were related to delay in the delivery times of the purchase orders, while the remaining 29.6% of complaints were related to unconfirmed production orders and re processes, among others causes.

The results obtained have been positive and there can be identified success characteristics (SC or SF, for success factors) at the time of implementing the ERP system, such as the direct involvement of general manager, and the interest generated in the workers of the chosen metalworking company, factors that [14], as well as [15–19] identified as success factors to implement ERP systems.

Table 2. Average delivery times and information flow of the analyzed company before implementing the Openbravo ERP inventory

Measurement of times											
Evaluated aspect	Unit.	Jan.	Feb.	Mar.	Apr.	May.	Jun.	Jul.	Aug.	Sep.	Oct.
Total production	Unit	44	49	47	40	41	52	44	49	48	45
Delayed deliveries	Unit	8	7	5	6	7	5	3	4	2	2
Information flow time	Min	56,7	51,3	48,2	52,6	53,7	51,6	50,2	46,2	39,7	37,5
Customer response time	Min	420,3	525,6	455,7	347,6	592,7	623,9	453,6	632,8	425,7	662

Table 3. Average delivery times and information flow of the company analyzed after implementing the Openbravo ERP inventory module.

Evaluated aspect	Monthly average	Reduction
Total production	49	
Delayed deliveries	2	
Information flow time	31,28	36%
Customer response time	303,25	41%

It can be attributed that up to 95% of the reduction seen in the times of information flow and customer response are due to the implementation of the ERP inventory module, because during the investigation, there were not introduced other changes to the processes, supply lines, procedures, different from those made at the time of implementing the aforementioned module.

The results obtained have been positive and there can be identified success characteristics (SC or SF, for success factors) at the time of implementing the ERP system, such as the direct involvement of general manager, and the interest generated in the workers of the chosen metalworking company, factors that [14], as well as [15–17] identified as success factors to implement ERP systems.

4 Conclusions

According to the information presented in this document, it can be concluded that the strategy to have control of the inventories and their processes was based on establishing and documenting the process of storage and control of inventories, supported by the definition of procedures and formats of control.

The real information was made available quickly, when installing the ERP with the intranet of the company, the management and the other areas of the organization had information of the state of the warehouse in real time, which allows to reduce time, that before the Implementation of the inventory module of the ERP Openbravo was time wasted completely.

It can also be concluded that the reorganization of the warehouse when implementing the ERP, allowed the information or reports that the ERP throws to be real, creating virtual shelves that had the same order as the metalworking shelves.

Through the analysis of times, it was possible to establish times for the flow of information and for customer response. In this way, the management area/administration was able to establish a range of time in which they can fulfill the order.

It has been possible to facilitate the areas related to storage in real time, due to the fact that during the time when the start-up of Openbravo was evaluated, there was no need to make unnecessary orders due to the exhaustion of material, because the purchasing department of the company, reviewed the system daily, for when it was necessary to place orders, making the purchase order.

From the analysis of time, it was observed that through a good administration of the inventories, the response time to the client is improved to more than 40% of the time used for the same activities before implementing the inventory module.

Finally, it can be concluded that the success in implementing the Openbravo ERP inventories module was due to the good disposition of senior management and the openness to change of workers, accompanied by the training given to each of the plant members. of the company.

References

1. Rashid, M., Hossain, L., Patrick, J.: The Evolution of ERP Systems: A Historical Perspective (2002)
2. Al-Mashari, M.: Enterprise resource planning (ERP) systems: a research agenda. *Ind. Manag. Data Syst.* **102**(3), 165–170 (2002)
3. Monk, E., Bret, W.: Concepts in enterprise resource planning (2012)
4. Benvenuto, Á.: Implementación de sistemas ERP, su impacto en la gestión de la empresa e integración con otras TIC. *Capiv* **4**, 33–48 (2006)
5. David, R., Sandhyaduhita, P.: Analysis and design of Enterprise Resource Planning (ERP) system for Small and Medium Enterprises (SMEs) in the Sales Business Function Area. In: 2013 International Conference on Advanced Computer Science and Information Systems, ICACCSIS 2013,no. March 2015, pp. 255–260 (2013)
6. Gupta, A.: Enterprise resource planning: the emerging organizational value systems. *Ind. Manag. Data Syst.* **100**(3), 114–118 (2000)
7. Khaparde, V.M.: Barriers of ERP while implementing ERP: a literature review. *IOSR J. Mech. Civ. Eng.* **3**(6), 49–91 (2012)
8. Parr, A.N., Shanks, G., Darke, P.: Identification of necessary factors for successful implementation of ERP systems. In: Proceedings of the IFIP TC8 WG8.2 International Working Conference on New Information Technologies in Organizational Processes: Field Studies and Theoretical Reflections on the Future of Work, The Netherlands, pp. 99–120 (2002)
9. Krasner, H.: Ensuring e-business success by learning from ERP failures. *IT Prof.* **2**(1), 22–27 (2000)
10. Ilin, V., Ivetić, J., Simić, D.: Understanding the determinants of e-business adoption in ERP-enabled firms and non-ERP-enabled firms: a case study of the Western Balkan Peninsula. *Technol. Forecast. Soc. Change* **125**(June), 206–223 (2017)
11. Hustad, E., Haddara, M., Kalvenes, B.: ERP and organizational misfits: an ERP customization journey. *Proc. Comput. Sci.* **100**(1877), 429–439 (2016)
12. Ruiz Usano, R., Framiñán Torres, J.M.: Sistemas ERP (I): Características y evolución histórica. *Rev. Alta Dir.* **38**(226), 433–440 (2002)
13. Romero-Conrado, A., et al.: A tabu list-based algorithm for capacitated multilevel lot-sizing with alternate bills of materials and co-production environments. *Appl. Sci.* **9**(7), 1464 (2019)
14. Ramirez, P., García, R., Arenas, J.: El éxito de los sistemas ERP. In: El comportamiento de la empresa ante entornos dinámicos: XIX Congreso anual y XV Congreso Hispano Francés de AEDEM, p. 55 (2007)
15. Holland, C.P., Light, B., Gibson, N.: A critical success factors model for enterprise resource planning implementation. In: Europe Council of International Schools, pp. 273–287 (1999)
16. Coronado-Hernandez, J.R., Simancas-Mateus, D., Avila-Martinez, K., Garcia-Sabater, J.P.: Heuristic for material and operations planning in supply chains with alternative product structure. *J. Eng. Appl. Sci.* **12**(3), 628–635 (2017)
17. Rius-Sorolla, G., Maheut, J., Coronado-Hernandez, J.R., Garcia-Sabater, J.P.: Lagrangian relaxation of the generic materials and operations planning model. *Cent. Eur. J. Oper. Res.* **1**–19 (2018)
18. Amelec, V.: Validation of strategies to reduce exhausted shelf products in a pharmaceutical chain. *Adv. Sci. Lett.* **21**(5), 1403–1405 (2015)
19. Amelec, V.: Methodology to increase the adaptability and flexibility of the supply chain of automotive company through lean manufacturing. *Ad. Sci. Lett.* **21**(5), 1517–1520 (2015)



Simulation Model of Internal Transportation at a Container Terminal to Determine the Number of Vehicles Required

Carlos J. Uribe-Martes¹, Doris Xiomara Rivera-Restrepo²,
Ángelica Borja-Di Filippo³, and Jesús Silva⁴(✉)

¹ Universidad de la Costa, Barranquilla, Colombia
curibe6@cuc.edu.co

² Groupe Robert, Longueuil, Canada
xiomara.rivera@robert.ca

³ Universidad Autónoma del Caribe, Barranquilla, Colombia
aborjad@gmail.com

⁴ Universidad Peruana de Ciencias Aplicadas, Lima, Peru
jesussilvaUPC@gmail.com

Abstract. The operating efficiency of a container terminal is largely determined by the number of vehicles available for internal transportation. This article presents a discrete event simulation model, combined with scenario analysis, to help determine the adequate number of vehicles to satisfy the demand for internal container movements at a port in the city of Barranquilla. The model assesses the container movements performed by Straddle Carriers (SC) between the container loading/unloading dock and the storage and inspection yards. The results of the experiments performed indicate that when demand increases by more than 10%, the number of vehicles currently available may be insufficient to cover operating requirements in an efficient manner. The simulation model tests the effectiveness of a set of strategies that may be implemented at the studied terminal.

Keywords: Scenario analysis · Container terminal · Discrete event simulation · Straddle Carriers

1 Introduction

Container terminals operate as nodes that link different transportation modalities. They provide storage space to temporarily hold containers that arrive (in ships) and depart (to a ship). The operating efficiency of a container terminal depends on several factors. One of them is the internal movement of containers between different locations on land. The most common locations at terminals are the loading/unloading dock and the container storage yards. A simple illustration of the operation is displayed in Fig. 1. In Colombia, there is an additional intervening factor related to illegal drug trafficking, due to which the authorities require additional internal movements in order to perform full inspections of containers in a specific area inside the terminal.

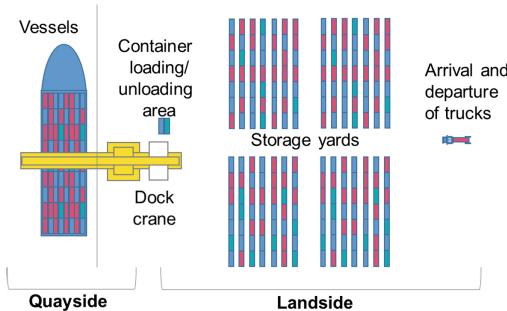


Fig. 1. Internal transportation of containers between the loading/unloading dock and the container yards are performed using Straddle Carrier vehicles.

Research aimed at improving efficiency at container terminals varies widely in terms of scope and technique [1]. Some studies focus on operating issues, such as space assignment for containers, dispatching and routing of container handling equipment [1]. Other studies focus on solving the problem of SC assignment in combination with other decisions such as the assignment of storage positions [2] or the assignment of SC to dock cranes [3]. In [4] was used a full mixed lineal programming model to reduce delays at the terminal, focusing on the internal transportation modalities. In [5] a simulation model with optimization is presented for programming of container loading. Another issue that has been frequently studied is the assignment of dock cranes [6]. Authors in [7] study operating performance depending on the equipment assignment strategy used for moving containers to the dock cranes.

Other studies focus on strategic problems, such as [8], who use discrete event simulation to design the layout of positions and distribution of container blocks, and to determine the number and capacity of SCs required for the operation. The analytical model presented by [9] addresses the container layout design by estimating the distances travelled by the SCs in different yard configurations.

Approaches for solving complex problems such as container terminals fall in three broad categories: Exact algorithms, Metaheuristics, and Simulation. Among the exact methods are linear and integer programming, branch-and-bound, and goal programming [10]. Metaheuristics include simulated annealing, ant colony optimization, tabu search, and population-based models such as evolutionary algorithms [11]. Discrete event simulation is an adequate method for modeling complex environments [12].

This paper presents a discrete event simulation model designed to help determine the number of Straddle Carriers (SC) required at the port terminal in the city of Barranquilla. The terminal has a fleet of 8 SCs to cover internal moving requirements. However, given a forecast increase in demand, it is possible that these vehicles will be insufficient to cover requirements in the short and medium term. In this context, a set of scenarios and strategies were reviewed aimed at improving efficiency. The rest of the article is organized as follows: Sect. 2 presents the general considerations for the formulation of the simulation model. Section 3 displays the results, and Sect. 4 presents a discussion. Lastly, Sect. 5 presents the conclusion of the study.

2 Methodology

For the effects of determining the number of Straddle Carriers (SC) required for terminal operations, the methodology of [13] and [14] was adapted to perform simulation studies as displayed in Fig. 2. Firstly, the problem was formulated, and study objectives were defined. In this case, the aim was to determine the number of vehicles required to perform the terminal's container movements without excessive delays. Subsequently, an assessment was performed of several scenarios that would possibly arise at the terminal in the short or medium term.

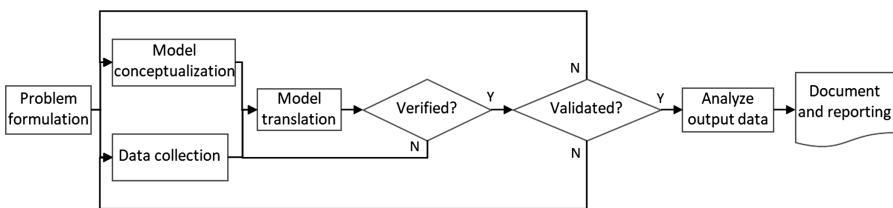


Fig. 2. The employed methodology was adapted from [13] and [14]

2.1 Definition of Assumptions, Variables and Parameters

In studying complex systems such as port terminals it is sometimes necessary to make simplifying assumptions to enable modeling. The variables and control parameters that were considered relevant for internal operating efficiency of the terminal were defined.

2.2 Data Collection

Based on current terminal operations and the study of various information sources, adequate values for the variables and parameters of interest for the terminal model were determined.

2.3 Programming and Verification of the Simulation Model

Specialized software for simulation of discrete events was selected to build the model. The model developed in this manner was submitted to the opinion of an expert to ensure that the model's logic was aligned with the current terminal design.

2.4 Model Validation

The model was validated by comparing certain performance measurements produced by running the simulated model against the values of reference obtained from the terminal.

2.5 Analysis of Scenarios

In order to explore scenarios, changes were made to certain control variables, such as the percentual increase in demand (10%, 25%, 50%), the vehicle assignment strategy (random selection, nearest vehicle), the probability that a container would be inspected (75% for export containers EC and 50% for import container IC, 90% for export containers EC and 75% for import container IC). Observations were made on how these changes affected vehicle utilization rates. The replication results were consolidated in ARENA reports, and confidence intervals were established for the performance measurements.

3 Results

In order to ensure the efficiency of port terminal operations it is necessary to determine the adequate number of vehicles required for internal container transportation. By developing a simulation model in ARENA ® it was established that the vehicles available at the studied terminal (8 SC) can cover current demand (79% utilization, 1.5 h wait at the dock). In fact, 7 SC would also suffice to cover demand (95% utilization and 1.52 h wait at the dock).

3.1 Definition of Assumptions, Variables and Parameters

The terminal currently has one dock where containers are loaded and unloaded, 4 container storage yards and one additional yard for customs inspections. The terminal also has 8 SC vehicles, under the assumption that their speeds are known. Another assumption is that the distances they travel, and their associated times are deterministic and known. It was also assumed that vehicle maintenance is previously planned, and that there is a fixed probability that a container will be inspected.

3.2 Gathering of Information

The data was gathered from different sources. SC speed with load was based on the manufacturer's information. The dates of arrival of containers by land and sea over the last three years were provided by the terminal, based on historical information from the transactions log database. The same database was used to determine the time during which the containers remain in the storage yards, the yards at which each container was located and the probability of being selected for inspection. The distances between the various locations of the terminal were determined based on drawings.

3.3 Programming and Verification of the Simulation Model

The model was then programmed using the ARENA ® simulation software. Four terminal operations areas were established (Dock, Container Yards, Maintenance Area, Inspection Yard). The model was verified by comparing the model's output to the corresponding terminal operations areas. Afterwards, 30 replications were made, each with duration of 30 days and a 10-day warm-up period. A confidence interval of 95%

was established for the evaluated performance measurements, primarily the percentage of time during which the vehicle was assigned to an operation over the total time of the simulation (Table 1).

Table 1. To validate the model, the performance measurements of the actual system were compared to those of the simulated model

Performance measurement	Actual system	Simulated model
Utilization percentage	85%	79%
Operating times	>1 h	1 h
Confidence level		95%
Percentage of error		1%

3.4 Model Validation

Validation was performed by comparing the times in operation (>1 h) and the utilization percentage (85%) estimated by the person responsible for operations at the workshop against the estimations of the simulation run (79% vehicle utilization, operating time of 1 h). The differences found were considered acceptable in order to move on to scenario analysis.

3.5 Scenario Analysis

In a scenario of a 10% increase in demand, 8 vehicles would suffice to fulfill demand based on utilization (<1). Any larger increase in demand would require adding more vehicles, as shown in Fig. 3.

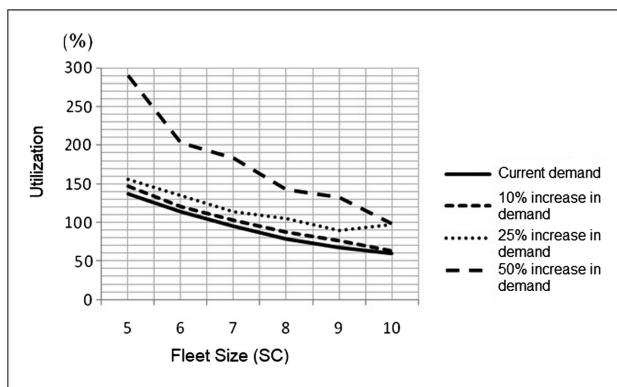


Fig. 3. If demand increases by more than 10%, at least 9 SC vehicles would be required.

In the scenarios that test an increase in the probability of customs inspections movements, it was found that the current number of vehicles is sufficient to cover demand, as indicated in Fig. 4.

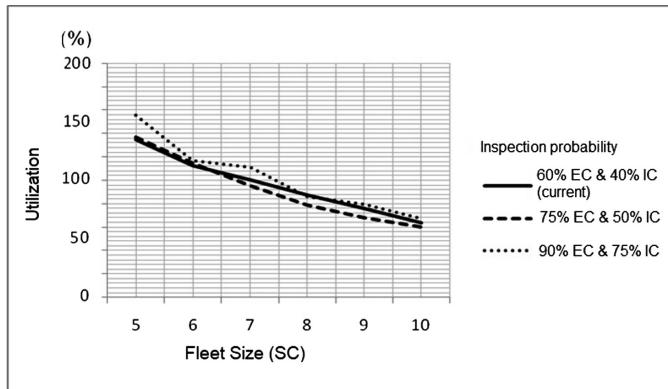


Fig. 4. An increase in the probability of inspection movements does not significantly change utilization

Changing the vehicle assignment strategy from random selection to using the nearest vehicle does not significantly change utilization. Figure 5 shows that for the tested scenarios, both criteria have similar results.

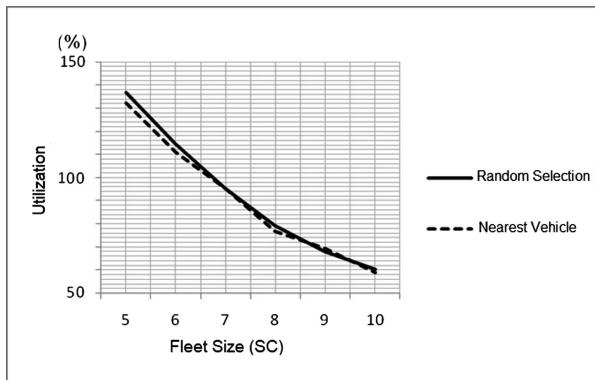


Fig. 5. Changing the vehicle assignment strategy from Random Selection to Nearest Vehicle does not affect utilization

Expanding infrastructure by enabling an additional yard that is currently used in a warehouse could produce operating efficiencies, as shown in Fig. 6.

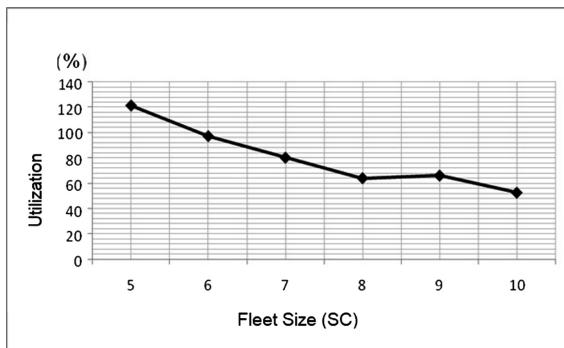


Fig. 6. Use of an additional yard improves operating efficiency

4 Discussion

At a container terminal it is important to have an adequate number of vehicles for internal transportation in order to ensure operating efficiency. In this case study, it was found that the number of Straddle Carriers (SC) available is adequate for current demand. However, if demand should increase by more than 10%, the current fleet may prove to be insufficient and the terminal should consider the acquisition of additional vehicles, or the expansion of infrastructure by enabling an additional yard. Both strategies proved to be efficient in the simulated scenarios.

Additionally, simulations of scenarios involving changes in the number of movements for inspections, or using different vehicle assignment strategies, indicate that such variables are not relevant in terms of operating efficiency. Lastly, the validity of the model could be enhanced that taking into consideration certain factors that were not included. On the one hand, additional variables and restrictions could be included in vehicle and route programming, such as the operating times of the cranes at the sea dock, the yards' capacity and the specific location of the containers within each yard. On the other hand, the models that were used assume that the routes and times of travel are deterministic, but models that consider variations of these factors could also be considered.

5 Conclusions

The use of discrete event simulation and analysis of scenarios proved to be a useful tool to determine the appropriate number of vehicles required for the internal transportation of containers that ensures operating efficiency. They take into consideration the effects of possible increases in demand, changes in customs inspection policies and changes in vehicle assignment strategies. Some initial hypotheses were rejected, such as that the percentage of movements for customs inspections, or that the vehicle assignment strategy, would influence efficiency under the tested load volumes and the studied

scenarios. A strategy that was found to be relevant was that of enabling an additional yard for container storage.

References

1. Carlo, H.J., Vis, I.F.A., Roodbergen, K.J.: Transport operations in container terminals: Literature overview, trends, research directions and classification scheme. *Eur. J. Oper. Res.* **236**(1), 1–13 (2014)
2. Dkhil, H., Yassine, A., Chabchoub, H.: Multi-objective optimization of the integrated problem of location assignment and straddle carrier scheduling in maritime container terminal at import. *J. Oper. Res. Soc.* **69**(2), 247–269 (2018)
3. Canonaco, P., Legato, P., Mazza, R.M., Musmanno, R.: A queuing network model for the management of berth crane operations. *Comput. Oper. Res.* **35**(8), 2432–2446 (2008)
4. Zehendner, E., Rodriguez-Verjan, G., Absi, N., Dauzère-Pérès, S., Feillet, D.: Optimized allocation of straddle carriers to reduce overall delays at multimodal container terminals. *Flex. Serv. Manuf. J.* **27**(2–3), 300–330 (2015)
5. Zeng, Q., Yang, Z.: Integrating simulation and optimization to schedule loading operations in container terminals. *Comput. Oper. Res.* **36**(6), 1935–1944 (2009)
6. Al-Dhaheri, N., Jebali, A., Diabat, A.: A simulation-based Genetic Algorithm approach for the quay crane scheduling under uncertainty. *Simul. Model. Pract. Theor.* **66**, 122–138 (2016)
7. Soriguera, F., Robuste, F., Juanola, R., Lopez-Pita, A.: Optimization of handling equipment in the container terminal of the port of Barcelona, Spain. *Transp. Res. Rec.: J. Transp. Res. Board* **1963**, 44–51 (2006)
8. Legato, P., Mazza, R.M.: A simulation model for designing straddle carrier-based container terminals. In: 2017 Winter Simulation Conference (WSC), pp. 3138–3149. IEEE (2017)
9. Wiese, J., Suhl, L., Kliewer, N.: An analytical model for designing yard layouts of a straddle carrier based container terminal. *Flex. Serv. Manuf. J.* **25**(4), 466–502 (2013)
10. Orejuela Cabrera, J.P., Flórez González, A.: Balanceo de líneas de producción en la industria farmacéutica mediante Programación por metas. *INGE CUC* **15**(1), 109–122 (2019)
11. Romero-Conrado, A., Coronado-Hernandez, J., Rius-Sorolla, G., García-Sabater, J.: A tabu list-based algorithm for capacitated multilevel lot-sizing with alternate bills of materials and co-production environments. *Appl. Sci.* **9**(7), 1464 (2019)
12. Varela, N., Fernandez, D., Pineda, O., Viloria, A.: Selection of the best regression model to explain the variables that influence labor accident case electrical company. *J. Eng. Appl. Sci.* **12**(1), 2956–2962 (2017)
13. Banks, J., Carson II, J.S., Nelson, B.L., Nicol, D.M.: Discrete-Event System Simulation, 5th edn. Pearson, London (2014)
14. Law, A.M.: Simulation Modeling and Analysis, 5th edn. McGraw-Hill, New York (2015)



Internet of Things Enabled Device Fault Prediction System Using Machine Learning

Kotte Bhavana, Vinuthna Nekkanti, and N. Jayapandian^(✉)

Department of Computer Science and Engineering,
CHRIST (Deemed to Be University), Kengeri Campus, Bangalore, India
Jayapandian.n@christuniversity.in

Abstract. Internet of Things (IOT) started as a niche market for hobbyists and has evolved into a huge industry. This IoT is convergence of manifold technologies, real-time analytics, machine learning and Artificial Intelligence. It has given birth to many consumer needs like home automation, prior device fault detection, health appliances and remote monitoring applications. Programmed recognition and determination of different kinds of machine disappointment is a fascinating process in modern applications. Different sorts of sensors are utilized to screen flaws that is discovers vibration sensors, sound sensors, warm sensors, infrared cameras, light cameras, and other multispectral sensors. The modern devices are becoming ubiquitous and pervasive in day to day life. This device is need for reliable and predicate algorithms. This article is primarily emphases on the prediction of faults in real life appliances making our day to day life easier. Here, the database of the device includes previous faults which are restored in online by using cloud computing technology. This will help in the prediction of the faults in the devices that are to be ameliorated. It additionally utilizes Naïve Bayes calculation for shortcoming location in the gadgets. The proposed model of this article is involves the monitoring of each and every home appliance through internet and thereby detect faults without much of human intervention.

Keywords: Internet of Things · Sensors · Cloud computing · Home appliance · Machine learning · Naive Bayes

1 Introduction

The modern internet world everything is linked with internet network. The same concept is also involved in electrical and electronic device that means all the devices interlinked with internet connection in the name of Internet of Things (IoT). That device is various field that is electrical, electronics, mechanical and health sector device. In modern lifestyle almost 90% of our home appliance is also interconnected with this IoT technology [1]. Example of this appliance is sensor based washing machine, IoT based air conditioner and Internet based electricity controller. This technology is working with the help of internet, cloud computing and sensors [2]. Cloud computing is a new technology that has become increasingly important and had developed into a great potential for the business world. It has come into existence since 2000 and is currently on a great demand. Cloud computing gives us access to servers, storages, databases, and a broad set of application services over the internet. It helps us

to innovate in a faster approach than any other technology [3]. In this article cloud computing has an immense role in the storage of the device information which includes previous fault detections, controls, and makes use of prediction algorithms for efficiency. Disappointments lead to framework breakdown or shut down of an appliance. That as it may, disperse figuring and along these lines, distributed computing is described by the idea of fractional disappointments [4]. An issue may happen in any constituent hub, procedure or system segment. This prompts a halfway disappointment and thus, execution debasement rather than a total breakdown. Despite the fact that this outcomes in vigorous and reliable frameworks, deficiencies ought to be taken care of adequately by appropriate adaptation to non-critical failure systems for better performance. This cloud computing data processing is deal with some third party service provider [5]. Customers expecting reliable service at the same time higher speed. The main purpose of using this technology is not required for special software installation and not need for any maintenance. This cloud computing is mainly used for data storage apart from this they provide platform and infrastructure service [6]. This technology is used for various fields like education, social media, healthcare industry and government sector [7]. The time of introducing cloud computing is used for industry and the IT field, now it is slowly interlinked with human day to day life.

Internet of Things is a booming shift in IT epoch. The internet uses TCP/IP protocol suites for interconnecting the computer networks in our global system. In our day to day life internet plays a crucial role for exchanging of data, news and technologies. Internet states about the data created by people, while the new-born is about data created by things. "IOT is an open and encyclopedic network of intelligent quick-witted devices that have the ability to share data, resources, technologies, acting in the real time situations and reacting to the changes in environment". This is a huge network which can allow the communication between humans-to-things, things-to-things and vice versa by providing a unique identity for each and every person or for a device [8]. It describes about the eye-witted intelligent connection and communication in our global system. IOT devices receives input through sensors which are highly miniature via technology and sends the output information through wired and wireless interfaces to cloud. For example: A smartphone application acknowledges the end user, to monitor the exact location of the vehicle, and views the route path using google maps (GPS) and helps the user to reach exact location. It even shows the arrival time of the vehicle. Ensuring safety and arrival time the prediction algorithm is used for the computation of arrival time. The software applications can continuously monitor the devices and update the faults to the end user. IoT technology is implemented in various real life products. For example, our heart beat is automatically monitored and send the data to cloud server. In modern healthcare sector is used in this IoT in various purposes. IoT based home automation is latest innovation in construction sector. This technology should help to monitor electricity, water flow and home appliance. This project comes under the smart city; smart city is another booming field to interlink with entire city by using IoT [9]. This home automation is working with IP gateway connected with smart mobile phone and other internet enabled devices. Artificial intelligence is a branch of science which aims to invent intelligent machines which can react and work like human beings without any action of the technological industry [10]. It has become the heart of the modern science. This develops a main difference between the human decisions and

smart machines. AI has shown its significance in machine learning (ML) and deep learning (DL) in modern systems. This can automate the responses and processes of the systems. As per the analysis, companies spend around 70% on AI workers and compounded annual will reach \$57.6 billion by 2021. The companies that fail to adapt AI and ML are fated to be left. There are some traditional problems in AI which includes reasoning, planning, learning and perception. AI can generate automated responses for the action given by any device or network without any human interaction by using ML and DL [11]. According to the analysis AI can completely replaces the employment where this is going to be a danger to humanity. The world is going to show the transformation of our vehicles to self-driven vehicles. This plays a crucial role in this paper where it needs to generate automated responses of the devices for our prediction. Despite the software engineers putting great efforts for developing fault detection models, fault detection gives us various challenges. Naïve Bayes is an integrated machine learning algorithm that has proven high-performance for this problem. It helps in the prediction of faults in the devices and is one among the most practical approaches for solving problems. This algorithm makes use of the database which comprises of previous faults that have occurred in the appliance, analyzes various cases by which the faults have occurred and thereby provides a prior information regarding the future faults that might occurred and alert the users. The following is the idea behind which the probable fault data is given.

2 State of Art

In the last decades, dependency on software has increased in our daily lives. Now a days it is very difficult to imagine human life without software. Every domain like medical, railway signal, home appliances has started to work with software. Here software reflects the meaning of devices working using AI, IOT, ML technologies. The development of the appliances in each domain is challenging a problem of failure. The impact of these failures, leads the human life into a miserable condition. Therefore, there is a growing solution to ensure the devices without undergoing faulty conditions [12]. The work initiated by Air Force's Rome laboratory was one of the best efforts made to predict the faults in the devices. Number of factors is selected by the research to measure the fault rates. Devices may have several problems such as wireless connection, no power capacity, interrupts. These interrupts undergo certain operation, by causing the device failure or a system failure. Markov chain model helps us to analyze the devices and its current state with a monitoring technique if a device is faulty [13]. Through monitoring resource information can calculate the fault tolerance. But if wrong information is provided to our devices then there is a chance of facing an accuracy problem. There is a model called push and pull model to detect the device nature. In the push model, the user sends information to the device, and then the device starts working if there is no fault. In the pull model the device sends a signal to user by stating the problem in a device. So by the prediction method the device problem can be resolved.

The most intelligent fault prediction system is based on internet of things, this aims at growing the efficiency of devices and detecting the faults. There are three steps need to be followed to ensure the working of a device. The first step is to monitoring the set-

up of the devices, which is connected to the AI, ML. The second step is to identify the fault of the device and diagnosing the fault. Third stage is to resolve the problem by modifying the device or the procedure which is done in setup. Fault prediction is a large safety key according to the IOT, and this is one large safe operation to prevent the faults. The work on fault prediction has been done in many countries. There are some groups in the industry to predict and diagnosis the fault in devices. The MFDT (Machinery Failure Prevention Technology) in the USA had founded the prediction group. The major applications of IoT are its increasingly being used in the manufacturing industry. More specifically, productivity improvements enabled by IoT technology have major impact on economy and competitiveness in manufacturing industry. Especially the mankind are entering the fourth phase of industrialization with the use of cyber-physical systems to monitor, analyse, and automate business. In particular, industrial maintenance contributes largely to this competitiveness through reliability and availability of production equipment. Especially in continuous production industries. The ratio “maintenance costs/added value product” is even higher than 25%. Apparently, defect components or process failures can stop the whole production and significantly impact the competitiveness in manufacturing industry. The effect of IoT in the business segment brings about noteworthy upgrades in proficiency, efficiency, gainfulness, basic leadership and adequacy [14]. IoT is changing how items and administrations are created and circulated. The foundations are overseen and kept up; it is additionally rethinking the communication among individuals and machines. IOT is about making your information meet up in new ways. Take of information with IOT dashboards reveal actionable realization. And modernize how you work together. IOT is an idea and a worldview that look prevalent attendance in the environment of a variety of things that from wireless and cable associations. One of a kind addressing schemes are capable to react with one another and coordinate with different things to make new usage/administrations and achieve shared target. In this setting the research and expansion challenges to make an intelligent world are large. A world where the true, digital and the practical are converging to make clever environments that make transport, power, town and many else regions very smart. Internet of Things is to can things to be linked, anywhere, anytime, with anything and anybody in a perfect use any path and any management. Alongside the quick improvement of Internet of Things and the country's strong support, innovations for IOT are connected to different fields.

Cloud computing is an engineering for encouraging registering administration through the web on necessity and pay per use access to a gathering of mutual assets specifically arranges, capacity, servers, administrations and applications, without physically procuring them [15]. Cloud DBMS is a conveyed database that gives processing as an administration. It is sharing of web framework for assets, programming and data over a system. The cloud is utilized as a capacity area where database can be gotten to and figured from anyplace. Cloud computing has gotten expanding enthusiasm from undertakings since its origin. It has inventive data innovation (IT) administrations conveyance model. Cloud computing could increase the value of endeavors. Cloud computing presents exceptionally concerning interior and outside issues. Cloud Computing frameworks inquire about motivation to investigate the already under-explored regions with respect to cloud computing appropriation factors and procedures.

3 Problem Statement

A fast and reliable method to detect faulty IoT devices is indispensable in IoT environments. To lessen the term of blackouts and limit reaction time to real blames, and to advance unwavering quality of supply. It is unavoidable for individuals to think of another innovation to look for minimal effort conveying gadget which sends an alarm to the screen which can imply us right on time to set it up. The individuals are seeking after regularly developing high caliber of their lives today. This issue prompts increasingly more bother to offices and home apparatuses including into their structures. Generally ordinary divider switches are situated in various corners of house, structures and workplaces. Consequently, when something goes off then entire framework is harmed alongside the switch. So as opposed to putting these changes to on or off, it wants to utilize the robotized gadgets which can distinguish the issue and inform us before something turns out badly. There is a lot of failure crisis in current situation of our country. Moreover, people have become negligent in proper utilization of the devices in proper way. People often forget to turn off the light sources and home appliance while staying out from home, even this may lead to the outage of appliance. Even in those situations, application of fault detection makes it possible to control them and to change the appliance.

4 Proposed IoT Based Fault Prediction System

The modern device is working with electronic based technology. The proposed system is electronic based technology also it will increase the performance and reduce the device cost. The proposed system comprises of various components that help in the detection of faults. The components include controller, database, smart phone, Control Unit, home appliances and Fault Maintenance Unit. Control unit is to monitor the home appliances, whether their working condition is normal. If the software application is turned open, Control Unit starts to track the data received from the controller which stores the up-to-date database of the appliances. Hence, the abnormal condition in the appliances can be detected and stored in the Fault Maintenance Unit using the naïve bayes algorithm. Furthermore, the alert message is generated to the end user (smart phone) from the control unit after a deviation from the normal working of the appliances is predicted. Control Unit has non-volatile memory and the data are retrieved from the controller every day. It stores the data in cloud using cloud computing technology. The data stored is used by algorithm to compute the faults that occurred or going to occur. This is the main functional unit of the entire system. The purpose of this control unit is to maintain the protocol structure of the proposed system. The concept of this proposed system is to connect the home appliance by using internet with interconnection of IoT technology. The working mechanism of this washing machine is monitored with the help of IoT sensor that means water utilization, machine running time and spinning time. This timing is monitored and sends this data to control unit. The controller notices if any home appliances are turned ON or OFF. If the appliance is ON, then it starts working to check if appliance is working or not. The control of each device is taken care of by controller by supplying the required amount of power for

working of the devices. The controller is maintained by the Control Unit through checking the faults in appliances. Controller stores the data of each and every fault occurred in appliances. It has volatile memory and so the details are stored until then the Control Unit retrieves the information from the controller.

The Fig. 1 is discussed proposed fault identification system using machine learning algorithm. The major unit of our proposed system is Machine Learning Algorithm Unit, this unit is using Naïve Bayes algorithm. The basic working principle of this algorithm is probabilistic classifier method. This algorithm is interlinked with the concept of Bayes concept. The basic structure of machine learning algorithm is to predict the future based on existing data set. This Bayes theorem is to split or cluster the data based on similarity. This cluster data set is stored in one particular database then future this data set is used to predict the result. This algorithm is also working in support vector mechanism. This method to find the similarity of different data, based on the similarity this system helps to predict the future. This mechanism is implemented in the IoT enabled home appliance, to maintain both with fault and without faulty device history. The purpose of maintain both the data is finding the similarity. Inside of this unit another major unit is also working that is named as software unit. Software application is used to find all the databases of all the home appliances. When the users enroll in the application with their residential address, they have allowed this application. The users can view the power consumption and the power wastage of each

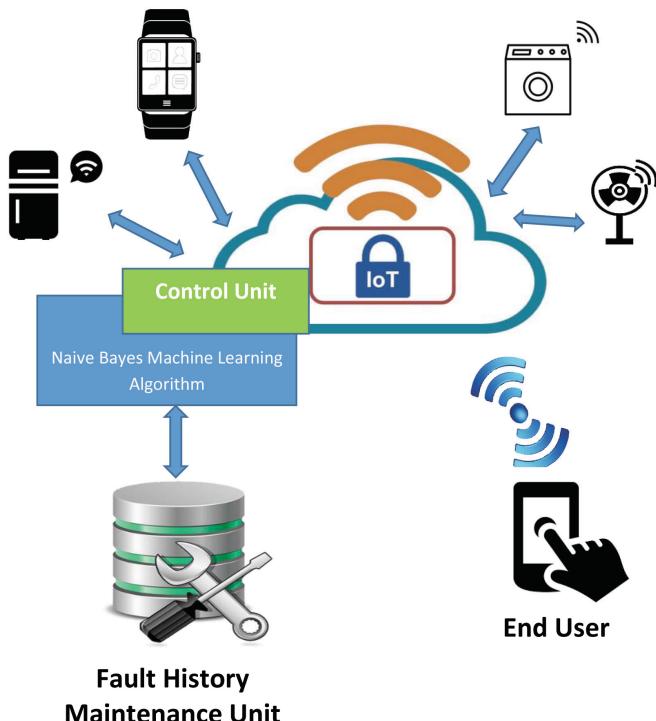


Fig. 1. IoT enabled fault history maintenance architecture

home appliance and also the occurrence of the fault in the device. Any change in the database table leads to the intervention of the user for alert. Hence this software is helpful to reduce the wastage of electric power that may occur during the fault period.

Here we can consider washing machine, fan, refrigerator as home appliances connected to Control Unit and cloud. These devices are controlled by Control Unit. The Control Unit and cloud allows to perform any tasks automatically. These can interact seamlessly and securely with any of the devices. These appliances play a key role in every home automation area. The Control Unit helps the appliances to connect directly to the software for detecting the faults. IoT based fault history maintenance unit helps to maintain these existing fault data and current machine situation. This is a cloud based database storage server. This is database system is dynamic with automated system, when small changes are observed that is updated in this unit. This particular unit is the heart of this proposed method. The reason is that without this particular unit is not able to predict the future fault. The major advantage of fault history maintenance unit is error free server. The working method of proposed system is home appliances generate data that means performance of that machine. This data is collected by using IoT technology, after that data is send it to machine learning algorithm unit. Here Navie Bayes algorithm is used to predict the future fault. Then that particular data is stored in separate database that is named as Fault History Maintenance Unit. That database is connected with cloud server, this prediction process is done with the help of machine learning algorithm unit, it is similar to the work of processor. The computer processor do the process in system input, similar to that device data is analyses and predict the future fault. Then this information is shard in end user. That end user look into this information by using mobile application. End user may be any smart device like a mobile phone or a PC used by us, which comprises of the software that keeps a record of the database of the devices and alerts the users when an abnormal condition or a deviation has been noticed in the working of an appliance.

5 Conclusion

A framework that distinguishes and recognizes flawed gadgets is basic in smart homes to give solid administrations to clients. Monitoring of home appliances using controller helps the Control Unit to monitor and maintain the maximum number of home appliances at the same time. Hence, this proposed system helps in the detection of faults without any intervention of human effort and also saves a lot of time. In this proposed system is implemented with the help of cloud computing, Internet of Things and Mobile App. This is a multi-technology environment, because more than one technology is involved in this proposed system. In future, this method can be implemented to improve industrial appliance.

References

1. Stojkoska, B.L.R., Trivodaliev, K.V.: A review of Internet of Things for smart home: challenges and solutions. *J. Cleaner Prod.* **140**, 1454–1464 (2017)
2. Jayapandian, N., Rahman, A.M.Z., Poornima, U., Padmavathy, P.: Efficient online solar energy monitoring and electricity sharing in home using cloud system. In: Proceedings of Online International Conference on Green Engineering and Technologies (IC-GET), pp. 1–4. IEEE (2015)
3. Wu, J., Ping, L., Ge, X., Wang, Y., Fu, J.: Cloud storage as the infrastructure of cloud computing. In: Proceedings of International Conference on Intelligent Computing and Cognitive Informatics, pp. 380–383. IEEE (2010)
4. Dikaiakos, M.D., Katsaros, D., Mehra, P., Pallis, G., Vakali, A.: Cloud computing: distributed internet computing for IT and scientific research. *IEEE Internet Comput.* **13**(5), 1–13 (2009)
5. Jayapandian, N., Rahman, A.M.Z., Gayathri, J.: The online control framework on computational optimization of resource provisioning in cloud environment. *Indian J. Sci. Technol.* **8**(23), 1–13 (2015)
6. Zhang, J., Wang, B., He, D., Wang, X.A.: Improved secure fuzzy auditing protocol for cloud data storage. *Soft. Comput.* **23**(10), 3411–3422 (2019)
7. Jayapandian, N., Pavithra, S., Revathi, B.: Effective usage of online cloud computing in different scenario of education sector. In: Proceedings of International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp. 1–4. IEEE (2017)
8. Xiao, G., Guo, J., Da Xu, L., Gong, Z.: User interoperability with heterogeneous IoT devices through transformation. *IEEE Trans. Ind. Inform.* **10**(2), 1486–1496 (2014)
9. Jayapandian, N.: Threats and security issues in smart city devices. In: Secure Cyber-Physical Systems for Smart Cities, pp. 220–250. IGI Global (2019)
10. Li, B.H., Hou, B.C., Yu, W.T., Lu, X.B., Yang, C.W.: Applications of artificial intelligence in intelligent manufacturing: a review. *Frontiers Inf. Technol. Electron. Eng.* **18**(1), 86–96 (2017)
11. Li, H., Ota, K., Dong, M.: Learning IoT in edge: deep learning for the Internet of Things with edge computing. *IEEE Netw.* **32**(1), 96–101 (2018)
12. Siegel, J.E., Pratt, S., Sun, Y., Sarma, S.E.: Real-time Deep Neural Networks for internet-enabled arc-fault detection. *Eng. Appl. Artif. Intell.* **74**, 35–42 (2018)
13. Oliver, N.M., Rosario, B., Pentland, A.P.: A Bayesian computer vision system for modeling human interactions. *IEEE Trans. Pattern Anal. Mach. Intell.* **22**(8), 831–843 (2000)
14. Atzori, L., Iera, A., Morabito, G.: Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. *IEEE Trans. Pattern Anal. Mach. Intell. Ad Hoc Netw.* **56**, 122–140 (2017)
15. Ni, J., Zhang, K., Lin, X., Shen, X.S.: Securing fog computing for internet of things applications: challenges and solutions. *IEEE Commun. Surv. Tutorials* **20**(1), 601–628 (2017)

Author Index

A

- Aarthi, A., 38
Aditya, M., 115
Agarwal, Piyush, 606
Agarwal, Srijan, 392
Ahlawat, Priyanka, 766
Aishwarya Lakshmi, T., 684
Akhtar, Iram, 606
Alkhaldi, Salwa, 711
Anand, Niketha, 801
Anand, Vishal, 450
Ananth, C., 441
Angel Cerli, A., 523
Anil Kumar, B., 104
Anitha Reddy, S., 653
Anitha, V., 362
Anuraj, K., 132
Aparna, Manikonda, 702
Arjaria, Arundhati, 79
Asanambigai, V., 587
Ashwini, L., 87
Asim, Mohammed, 606

B

- Bakthula, Rajitha, 209
Balakrishnan, Mathivanan, 758
Balasubramanian, M., 556
Bansal, Malti, 730
Baron-Villamizar, Javier, 905
Batni, Priya, 808
Beena Bethel, G. N., 653
Behara, Bhagyashree, 123
Bhalke, Nisha V., 38
Bharathy, G. T., 594
Bharati, Subrato, 297

B

- Bhargavi, G., 594
Bhattu, S. Nagesh, 240
Bhavana, Kotte, 920
Bhavana, V., 661
Bhavanisankari, S., 594
Bilaiya, Riya, 766
Bindu, V. R., 342
Bipin, B., 692
Borde, Sheetal, 847
Brahmane, Anilkumar V., 874
Budhiraja, Sugandha, 150
Busygin, Volodymyr, 191

C

- Canabal-Gonzalez, Danneris, 905
Cañas, José María, 423
Chaitanya Krishna, B., 874
Chaitanya, D. L., 104
Chaithanya, S., 362
Chana, Inderveer, 161
Chandran, Ruthesh, 677
Chourasiya, Uday, 79
Coronado-Hernandez, Jairo R., 905
Cuenca-Jiménez, Pedro, 423

D

- Daniel, D., 323
Das, Arunav, 48
Dethe, C. G., 29
Devakunchari, 749
Devakunchari, R., 801
Dixit, Priyanka, 79
Donga, Jayna, 374
Dua, Mohit, 646
Dubey, Akanksha, 458

Dubey, Shivendra, 79
 Duttagupta, Subhasri, 306

E
 Eklarker, Ravindra V., 579
 Evhen, Fedorov, 191

F
 Faizal, N., 351
 Farheen, Shaista, 669
 Fernández-Conde, Jesús, 423
 Ferrer, Juliana, 890
 Filippo, Angélica Borja-Dí, 912

G
 Gahlot, Yamini, 279
 Gaitán, Mercedes, 890
 Ganapathy, Murugesan, 637
 Gautam, Apurv Singh, 279
 Gayathri, R., 782
 Gianey, Hemant, 272
 Gnana Prakasi, O. S., 315
 Gomathy, C., 506

H
 H, Sivasankari, 489
 Hamsagayathri, P., 11
 Hariharan, Balaji, 677, 684
 Harsha, B. K., 248
 Hegde, Gayatri, 723
 Hemavathi, D., 476
 Hirekurabar, Rajashekhar Ningappa, 67
 Holia, M. S., 374
 Honnavalli, Prasad B., 738
 Hussana Johar, R. B., 414

I
 Indumathi, G., 248
 Itare, Ravikant, 827
 Ityala, Saiteja, 738

J
 Jaiganesh, M., 794
 Jain, Aaditya, 382, 458
 Jain, Ashish Kumar, 827
 Jayalatchumy, D., 774
 Jayapandian, N., 920
 Joglekar, Jyoti, 174
 Jose, Rinu Rani, 622
 Joshi, Harish, 579
 Joshi, Kalyani, 847
 Joy, Vijo M., 615

K
 K R, Venugopal, 489
 Kadhirvelu, D., 774
 Kalaiselvi, K., 523
 Kamat, Pooja, 279
 Kanjalkar, Pramod, 59
 Kanmani, P., 315
 Kapoor, Piyush, 232
 Karthik, J., 569
 Karthikeyan, M., 441
 Karthikeyini, S., 530
 Kedare, Ashutosh K., 94
 Khanam, Zeba, 711
 Khiani, Simran R., 29
 Kirmani, Sheeraz, 606
 Koundinya, Ch., 306
 Krishnakumar, S., 615
 Krishnan, Akash, 392
 Kulkarni, A. D., 263
 Kumar, Akkrabani Bharani Pradeep, 201
 Kumar, Binu P., 18
 Kumar, Devesh, 815
 Kumar, N. V. Narendra, 240
 Kumar, Sumit, 225
 Kumari, Swati, 808

L
 Lalitha, C. V. N. S., 115
 Lavanya, R., 782
 Lezama, Omar Bonerge Pineda, 883, 898
 Lilly Florence, M., 467
 Lis, Jenny Paola, 890
 Loyola Samraj, S., 38

M
 Madhavi, K., 630
 Maheshwari, Shyam, 815
 Maheswari, R., 232
 Malik, Prakhar, 749
 Manakattu, Sheeja Shaji, 67
 Maurya, Akhileshwar, 392
 Menon, Maya, 392
 Mercado-Caruso, Nohora, 905
 Mercy, S., 794
 Mhetre, Manisha, 123
 Mohan Vaishnav, P. S., 306
 Mohananthini, N., 441
 Moroz, Boris, 191
 Mulla, Badshaha, 331
 Mundada, Kapil, 94
 Muneeswari, G., 323
 Murugesh, Shivakumar, 67, 225

N

- Nagaraja, R., 794
Nair, Panchami S., 351
Nalini, N., 702
Natarajan, K., 323
Nekkanti, Vinuthna, 920
Ningombam, Hemarjit, 286
Nirmala Devi, M., 18

O

- Olena, Kholod, 191
Ospina-Mateus, Holman, 905

P

- Padmanabhuni, Venkata Nageswara Rao, 201
Pai, Vasudeva, 183
Palwe, MeghRaj V., 59
Panda, Manoj, 115
Pande, Karrrmany, 232
Paternina-Arboleda, Carlos, 905
Patil, Rajendrakumar, 847
Patsariya, Mohan, 827
Pavan Sankeerth, V., 661
Peña-Ballestas, Diana, 905
Phaneendra, H. D., 263
Podder, Prajjoy, 297
Pooja, T. L., 1
Poongodi, C., 11
Poorna, S. S., 132
Potluri, Avinash, 240
Prabhu, E., 38
Pragnavi, R. S. D., 392
Prakash, Amit, 858
Prasadula, Vasudeva Rao, 225
Puspha, S., 556

R

- R, Amutha, 489
Raja, K., 467
Rajamani, V., 556
Rajesh, A., 569
Rajiv Suresh, M., 547
Rama Krishna, C., 331
Ramasamy, Madhumathi, 758
Ramesh, G., 630
Rameshkumar, R., 255
Ramya, P., 11
Rani, Rinkle, 150
Rao, Bharath N., 392
Rao, Madhuri, 723
Rekha, K. S., 263
Rekha, P., 677, 684
Rishabh, 272
Rivera-Restrepo, Doris Xiomara, 912

- Robiul Alam Robel, Md., 297
Romero-Conrado, Alfonso R., 905
Rouf, Mohammad Abdur, 297
Roy, O. P., 286

S

- Sai Haneesh, K., 306
Sai Srikanth, Ch., 306
Salim, A., 622
Sankar, Devi S., 351
Sanket, Shashwat, 232
Santosh Markandeya, V., 661
Sarmah, Priyanshu, 48
Shahriar Parvez, A. H. M., 297
Shaheen, Bushra, 218
Shankar, S., 530
Shanthi, M. B., 808
Sharan, S., 351
Sharma, Bhuvnesh, 382, 458
Sharma, Oshin, 738
Sharma, R. K., 840
Sharma, Yogesh Kumar, 865
Sheela Sobana Rani, K., 782
Shrivastav, Suyash V., 232
Shruthi, M. L. J., 248
Shukla, Mukul, 827
Shvachych, Gennady, 191
Siddiqui, Farheen, 218
Silva, Jesús, 883, 890, 898, 905, 912
Singh, Upendra, 815, 827
Singh, Utkarsha, 161
Singh, Varsha, 450
Solanki, Narendra, 815
Solano, Darwin, 883
Sornalakshmi, K., 476
Sosa, Jignasha, 174
Sourabh, 749

- Sowmya Priya, K., 630
Sri Ranga, E., 661
Sridevi, S. V. G., 865
Srimathi, H., 476
Srinath, R., 38
Srinivas, Kethavath, 646
Srivastava, Gaurav, 730
Srivastava, Rajiv, 138
Srividya, L., 404
Stanley, Alphyn, 840
Subedha, V., 547
Subramanyam, R. B. V., 240
Sudha, P. N., 404
Suganthi Devi, S., 587
Suja Mary, D., 431
Sujatha, B. R., 414
Sunitha, N. R., 87

Supreetha, M., [1](#)
Suriakala, M., [431](#)
Swaminathan, J. N., [255](#)
Swathi, Y., [808](#)
Swetha, N., [104](#)

T
Tamilselvi, T., [594](#)
Tarannum, Suraiya, [669](#)
Tariq, Ariba, [209](#)
Tellis, Neetha Janis, [183](#)
Tetyana, Khollova, [191](#)
Thakare, V. M., [29](#)
Thakor, Jayraj, [232](#)
Thakur, Satyendra Singh, [138](#)
Thambidurai, P., [774](#)
Thangaraj, Chithrakumar, [758](#)
Thirupathi, Nallela, [630](#)
Tickoo, Raj Kumar, [331](#)
Tom, Linz, [342](#)

U
Uribe-Martes, Carlos J., [912](#)
Uthayasuriyan, K., [782](#)

V
Valarmathi, R. S., [11](#)
Valiveti, HimaBindu, [104](#)
Vankhede, Vikas, [815](#)
Vardhan, Aditya, [48](#)
Varela, Noel, [898](#)
Vedhanayaki, Anusha, [801](#)
Vinodhini, R., [506](#)
Visishta, Y. J., [801](#)

Y
Yadav, Dilip Kumar, [858](#)
Yadav, Raj Kumar, [606](#)
Yadav, Sakshi, [827](#)