Advances in Intelligent Systems and Computing 638

Daya K. Lobiyal
Vibhakar Mansotra
Umang Singh *Editors*

Next-Generation Networks

Proceedings of CSI-2015

Springer

Advances in Intelligent Systems and Computing

Volume 638

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing.
The publications within "Advances in Intelligent Systems and Computing" are primarily textbooks and proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

Daya K. Lobiyal · Vibhakar Mansotra
Umang Singh
Editors

Next-Generation Networks

Proceedings of CSI-2015

Springer

Editors
Daya K. Lobiyal
School of Computer and Systems Sciences
Jawaharlal Nehru University
New Delhi, Delhi
India

Umang Singh
Institute of Technology and Science
Ghaziabad, Uttar Pradesh
India

Vibhakar Mansotra
Centre for IT
University of Jammu
Jammu
India

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-981-10-6004-5 ISBN 978-981-10-6005-2 (eBook)
https://doi.org/10.1007/978-981-10-6005-2

Library of Congress Control Number: 2017949999

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

The last decade has witnessed remarkable changes in IT industry, virtually in all domains. The 50th Annual Convention, CSI-2015, on the theme "Digital Life" was organized as a part of CSI@50, by CSI at Delhi, the national capital of the country, during—December 2–5, 2015. Its concept was formed with an objective to keep ICT community abreast of emerging paradigms in the areas of computing technologies and more importantly looking its impact on the society.

Information and communication technology (ICT) comprises of three main components: infrastructure, services, and product. These components include the Internet, infrastructure-based/infrastructure-less wireless networks, mobile terminals, and other communication mediums. ICT is gaining popularity due to rapid growth in communication capabilities for real-time-based applications. New user requirements and services entail modified ICT architecture along with next-generation networks (NGNs). CSI-2015 attracted over 1500 papers from researchers and practitioners from academia, industry, and government agencies, from all over the world, thereby making the job of the Programme Committee extremely difficult. After a series of tough review exercises by a team of over 700 experts, 565 papers were accepted for presentation in CSI-2015 during the 3 days of the convention under ten parallel tracks. The Programme Committee, in consultation with Springer, the world's largest publisher of scientific documents, decided to publish the proceedings of the presented papers, after the convention, in ten topical volumes, under ASIC series of the Springer, as detailed hereunder:

1. Volume # 1: ICT Based Innovations
2. Volume # 2: Next-Generation Networks
3. Volume # 3: Nature Inspired Computing
4. Volume # 4: Speech and Language Processing for Human-Machine Communications
5. Volume # 5: Sensors and Image Processing
6. Volume # 6: Big Data Analytics
7. Volume # 7: Systems and Architecture

8. Volume # 8: Cyber Security
9. Volume # 9: Software Engineering
10. Volume # 10: Silicon Photonics & High Performance Computing

We are pleased to present before you the proceedings of Volume # 2 on "Next-Generation Networks." The development in communication technology has transformed all information and services (e.g., voice, text, images, video) through next-generation networks rather than telephone-centric approach. The main focus of NGN depends upon evolution of Internet in context of variety of services offered to users. Its rapid successful growth is due to continual refinement in efficient communication medium including related algorithms, efficient computing resources, and mass storage capabilities which have revolutionized the methods of data extraction and acquiring, storing, transmitting, and exchange of information among users dispersed across the geographical boundaries by taking all the important parameters for performance evaluation (security, power, battery life, load balancing, reliability, etc.) into account.

In today's scenario, developing countries have made a remarkable progress in communication by incorporating latest technologies. Their main emphasis is not only on finding the emerging paradigms of information and communication technologies but also its overall impact on society. It is imperative to understand the underlying principles, technologies, and ongoing research to ensure better preparedness for responding to upcoming technological trends. By taking above point of view, this volume is published, which would be beneficial for researchers of this domain.

The volume includes scientific, original, and high-quality papers presenting novel research, ideas, and explorations of new vistas by focusing on conceptual and practical aspects of wireless networks, mobile ad hoc networks, wireless sensor networks. The aim of this volume is to provide a stimulating forum for sharing knowledge and results in theory, methodology, applications of ad hoc, sensor networks, and its emerging trends. Its authors are researchers and experts of these domains. This volume is designed to bring together researchers and practitioners from academia and industry to focus on extending the understanding and establishing new collaborations in these areas. It is the outcome of the hard work of the editorial team, who have relentlessly worked with the authors and steered up the same to compile this volume. It will be useful source of reference for the future researchers in this domain. Under the CSI-2015 umbrella, we received over 200 papers for this volume, out of which 57 papers are being published, after rigorous review processes, carried out in multiple cycles.

On behalf of organizing team, it is a matter of great pleasure that CSI-2015 has received an overwhelming response from various professionals from across the country. The organizers of CSI-2015 are thankful to the members of *Advisory Committee, Programme Committee, and Organizing Committee* for their all-round guidance, encouragement, and continuous support. We express our sincere gratitude to the learned *Keynote Speakers* for support and help extended to make this event a grand success. Our sincere thanks are also due to our *Review Committee*

Members and the *Editorial Board* for their untiring efforts in reviewing the manuscripts, giving suggestions and valuable inputs for shaping this volume. We hope that all the participated delegates will be benefitted academically and wish them for their future endeavors.

We also take the opportunity to thank the entire team of Springer, who have worked tirelessly and made the publication of the volume a reality. Last but not the least, we thank the team from Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi, for their untiring support, without which the compilation of this huge volume would not have been possible.

New Delhi, Delhi, India — Daya K. Lobiyal
Jammu, India — Vibhakar Mansotra
Ghaziabad, Uttar Pradesh, India — Umang Singh
March, 2017

The Organization of CSI-2015

Chief Patron

Padmashree Dr. R. Chidambaram, Principal Scientific Advisor, Government of India

Patrons

Prof. S.V. Raghavan, Department of Computer Science, IIT Madras, Chennai
Prof. Ashutosh Sharma, Secretary, Department of Science and Technology, Ministry of Science of Technology, Government of India

Chair, Programme Committee
Prof. K.K. Aggarwal, Founder Vice Chancellor, GGSIP University, New Delhi

Secretary, Programme Committee
Prof. M.N. Hoda, Director, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi

Advisory Committee

Padma Bhushan Dr. F.C. Kohli, Co-Founder, TCS
Mr. Ravindra Nath, CMD, National Small Industries Corporation, New Delhi
Dr. Omkar Rai, Director General, Software Technological Parks of India (STPI), New Delhi
Adv. Pavan Duggal, Noted Cyber Law Advocate, Supreme Courts of India
Prof. Bipin Mehta, President, CSI
Prof. Anirban Basu,Vice President-cum-President Elect, CSI

Shri Sanjay Mohapatra, Secretary, CSI
Prof. Yogesh Singh, Vice Chancellor, Delhi Technological University, Delhi
Prof. S.K. Gupta, Department of Computer Science and Engineering, IIT Delhi, Delhi
Prof. P.B. Sharma, Founder Vice Chancellor, Delhi Technological University, Delhi
Mr. Prakash Kumar, IAS, Chief Executive Officer, Goods and Services Tax Network (GSTN)
Mr. R.S. Mani, Group Head, National Knowledge Networks (NKN), NIC, Government of India, New Delhi

Editorial Board

A.K. Nayak, CSI
A.K. Saini, GGSIPU, New Delhi
R.K. Vyas, University of Delhi, Delhi
Shiv Kumar, CSI
Shalini Singh Jaspal, BVICAM, New Delhi
Anukiran Jain, BVICAM, New Delhi
Anupam Baliyan, BVICAM, New Delhi
Vishal Jain, BVICAM, New Delhi
Ritika Wason, BVICAM, New Delhi
Shivendra Goel, BVICAM, New Delhi

Contents

About the Editors

Dr. Daya K. Lobiyal is currently working as Professor at the School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India. He received his Ph.D. and M.Tech. (Computer Science) from the School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India, in 1996 and 1991, respectively, and B.Tech. (Computer Science and Engineering) from Lucknow University, India, in 1988. His research interests include wireless networks, mobile ad hoc networks, wireless sensor network, wireless multimedia networks, vehicular ad hoc networks (VANETs), and natural language processing. Dr. Lobiyal has published papers in international journals and conferences including IEEE, Wiley & Sons, Springer, Inderscience, WSEAS, IGI Global, and ACM.

Prof. Vibhakar Mansotra did his Masters in Physics in 1986 and M.Phil. Crystal Growth (Physics) in 1988 and also one-year PGDCA in 1990. After completing his M.Phil. and PGDCA, he Joined the Department of Computer Science and IT, University of Jammu, as Ad hoc Lecturer in the year 1991 (February) and later got confirmed in the same Department in the year 1992 (October). In the year 1997, he went to the Indian Institute of Technology Delhi (IIT Delhi) for completing his M. Tech. Computer Science and completed the same in December 1998. After acquiring his M.Tech. degree from IIT Delhi, he took over as Head of the Department in April 2012 and remained in this position for 3 years up to April 2015. During his tenure as the Head of the Department, he contributed a lot to the growth of his Department and brought the Department on the national map as one of the best departments in the country. During his tenure as Head, he also started an M.Tech. program in the Department of Computer Science, thereby bringing more laurels to the Department at the national level. During his tenure as Head, he got the Best Teacher Award in Information Technology (IT) by Amar Ujala B-School Excellence Awards held in Bombay on November 23, 2012, and also the Best Professor Award in Information Technology (IT) by LOKMAT National Education Leadership Awards held in Bombay on February 13, 2015. Besides his teaching achievements, he has contributed extremely well to the design of new courses and

programmes and has earned a name in his region. He has remained an active member of various academic bodies of the University and various neighboring universities.

Dr. Umang Singh IBM RAD Certified "Associate Developer," has completed her doctorate from University School of Information, Communications and Technology Department, Guru Gobind Singh Indraprastha University (GGSIPU), Delhi. Currently, Dr. Umang is working as an Assistant Professor at the Institute of Technology and Science, Ghaziabad, UP, and has experience of more than 12 years in academics. She is an active researcher having interest in the area of mobile ad hoc networks, sensor networks, vehicular ad hoc networks (VANETs), software management, and software engineering. She is guiding M.Tech./Ph.D. students of various reputed universities. She has organized various conferences/seminars and faculty development programmes and has also worked as Editor and Joint Editor in journals and conferences. She has also authored a book titled "Real Time System" and co-authored the title "MCA IV Handbook" published by Pragati Publication, Meerut (UP). She is an active member of various societies and professional bodies including IEEE and a life member of the Computer Society of India (CSI). She has delivered lecture talks on the area of information security, mobile communications, vehicular networks, sensor networks, ad hoc networks and its implementation in ns2. She has more than 40 research papers in esteemed national/international conferences and journals including ACM, IEEE, IET credited to her name and is also a reviewer of national/international journals.

100 Gbps High-Speed Broadband Networks

S.C. Gupta

Abstract Information and communication technology (ICT) is growing rapidly due to large demand of voice, data, Internet, and intranet. Internet is growing at a rate of 150% per annum, whereas voice/data communication is growing at a rate of 50% per annum. Hence, large bandwidths and high-speed transmission are required to match above growth. High-end technology based on optical fiber communication is now extensively used for communication using optical coherent transmission at 40, 100 Gbps in Japan, Singapore, Hong Kong, USA, and Europe. The trend is to deploy 400 Gbps optical fiber networks during 2015–16. The optical coherent transmission with low form factor, low power consumption, and high reliability is used in high-speed network due to development of low power DSP, pluggable optical modules on single package. Hence, miniaturization of optical devices is required. 25 Gbps Ethernet (25 GbE) and 50 Gbps Ethernet (50 GbE) are used in data center network equipment for connectivity of systems at data rate as high as 100 Gbps. This paper deals with optical coherent transmission technology with coherent detection used in 40 and 100 Gbps networks. The 100 Gbps data centers are now extensively used in metro-access networks, core network, whereas higher data rates based on 400 Gbps systems are going to be used in near future. These are deployed in high-speed broadband networks to achieve maximum transmission at 4 Tera bits per second using DWDM.

Keywords Laser source · DSP · DWDM · EDFA amplifier · Coherent detection · High-speed broadband network · Single-mode fiber · Avalanche photodiode · Dispersion compensated module · PM-QPSK

S.C. Gupta (✉)
Raj Kumar Goel Institute of Technology, Ghaziabad, India
e-mail: gupta_subhash@yahoo.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_1

1 Introduction

The multiplexing of audio, video, data, and text requires higher and higher bandwidth and fast speed of communication [1]. The demand of Internet is growing at a rate of 150% per year due to need of instant information happening anywhere in the world [2]. The speed of communication has increased from Gbps to Tbps. The electronic signals are degraded as soon as the speed of communication is increased above 10 Gbps.

Hence, optical fiber communication is deployed when the speed exceeds 10 Gbps. The photonics using photons with optical multiplexing, amplification, and add/drop converters are used at speeds above 10 Gbps. 40 and 100 Gbps optical data centers are being developed to meet expansion of Internet and intranet. This paper is dealing with state of art technology used in optical fiber broadband communication link at 100 Gbps [3]. Advantages of polarization multiplexing-quadrature phase-shift keying (PM-QPSK) and coherent detection are included in the development of 100 Gbps optical fiber link.

2 Modulation

In the design of 100 Gbps long-haul communication and interfaces, coherent polarization multiplexing-QPSK (PM-QPSK) has been used due to higher optical signal-to-noise ratio (OSNR) performance. There is >2 dB improvement in OSNR in PM-QPSK as compared to direct detection formats. Spectral efficiency (SE) and tolerance of intersymbol interference (ISI) are much higher in PM-QPSK modulation.

In the polarization multiplexing (PM-QPSK)-quadrature phase-shift keying, erbiumdoped fiber amplifier (EDFA) as an optical amplifier is used to amply the signal level in the wavelength range of 1530–1570 nm generated by a coherent laser source. EDFA is pumped by an external laser source of either 980 nm or 1480 nm wavelength to produce signal gain of value 30 dB or more (10^3 times amplification) [4]. It is purely an optical amplifier and works without converting signal from optical to electrical and reconverted it from electrical to optical. It is light to light amplification.

3 Dense Wavelength Division Multiplexing (DWDM)

Dense wavelength division multiplexing (DWDM) is used for wavelength multiplexing with a resolution of 0.8 nm wavelength spacing which is equivalent to 100 GHz in frequency spacing [5]. It is given by

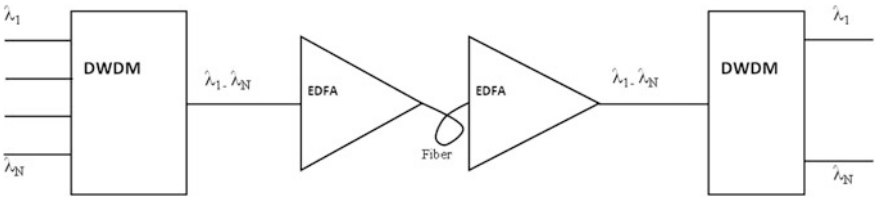


Fig. 1 Dense Wavelength Division Multiplexing

$$\frac{\Delta\lambda}{\Delta f} = \frac{\lambda}{f}$$

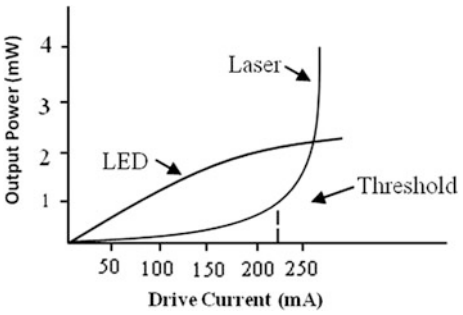
DWDM is working in the wavelength range of 1530–1570 nm range using a laser fundamental wavelength of 1550 nm where fiber provides optical window of minimum loss (<0.2 dB). Figure 1 shows wavelength division multiplexing with optical amplification.

The channel spacing in frequency can be reduced to 50 GHz which is equivalent to $\Delta\lambda$ of 0.4 nm. This increases the multichannel transmission capacity of the system. 160 wavelength channels can be transmitted over one fiber which allows transmission at 1–40 Tbps.

4 Light Source

Light source in the form of LED or laser diode (LD) can be used. Characteristics of both are given in Fig. 2. Laser diode offers higher output power, narrow spectral width, smaller numerical aperture (NA), faster switching speed, and long life while operating at 1310 nm or 1530 nm. These are used for complex and long-haul applications due to several benefits of high-speed transmission even though the cost of LD is high [6]. LED is used when small distance communication is required at low cost.

Fig. 2 Characteristics of LED versus Lased Diode



The modulation of laser diode can be direct modulation or by using external $LiNbO_3$ modulator.

InGaAs detectors are used as receiver to convert light signal into electrical signal. The quantum efficiency of 90% has been achieved in these detectors.

5 Coherent Detection

Coherent detection provides better performance [7]. In coherent detection, the received optical signal is mixed with signal of an optical local oscillator and the sum of two signals is detected by InGaAs photodiode.

It can be either used as homodyne detection or heterodyne detection using an intermediate frequency. So, the weak signal field is mixed with strong local oscillator signal field and is fed to InGaAs avalanche photodiode. Coherent detection can be used with all types of modulations such as PSK, QPSK, BPSK, QAM modulations. Figure 3 shows coherent detection.

The problem of signal degradation at the receiver end is due to fluctuations of light caused by state of polarization generated in the fiber. Dispersion compensation and polarization management are required due to nonlinear effects in the fiber.

Various techniques using high spectral efficiency modulation formats are analyzed. With high SE formats, the speed of trans-receiver electronics can be adjusted. These high SE formats are suitable to chromatic dispersion and polarization mode dispersion (PMD) since they enhance the bit rate using the same bandwidth (BW).

It is essential to use polarization multiplexing-QPSK (PM-QPSK) technology along with DSP devices to take care of polarization management. In PM-QPSK modulation scheme, following components and devices are required as explained above.

- Two coherent lasers, one for transmitter and another for local oscillator.
- Mach–Zehnder modulators with dual polarization.
- Driver amplifiers—four.
- Photodiodes—four balanced.

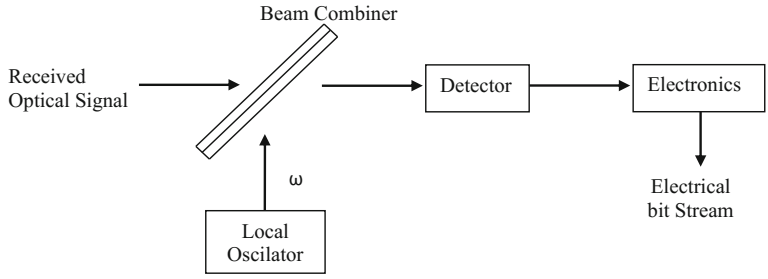


Fig. 3 Coherent Detection

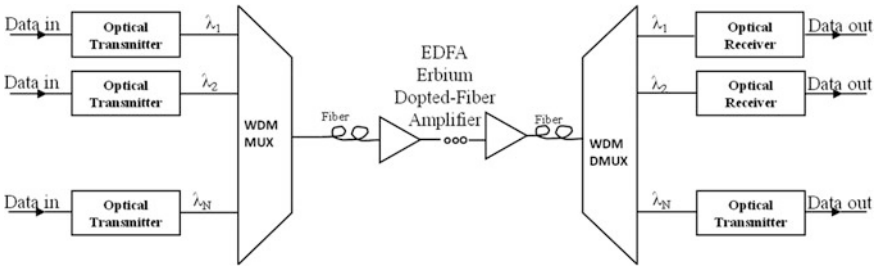


Fig. 4 Block Diagram of Multi Channel Optical-Fiber System

- Polarization beam combining optical components.
- Two numbers of 90° hybrids.
- Avalanche photodiode.
- DSP modules.

Figure 4 shows block diagram of multichannel optical fiber system.

So, penalty in the weak signal is reduced using coherent detection. Coherent detection offers 2–3 dB OSNR improvement in long-distance applications. Direct detection is used in 40 Gbps, whereas QPSK modulation and coherent detection are used in 100 Gbps PM-QPSK link.

6 Comparison of PM-QPSK

Next generation 100 Gbps per channel optical fiber system is being investigated using modulation based on PM-QPSK and coherent detection in which two QPSK signals are multiplexed in the polarization domain. Since it can reduce the symbol rate to ¼ of the data transmission rate, it can take care of digital signal processing speed and amplification bandwidth.

Figure 5 shows various types of optical modulation formats.

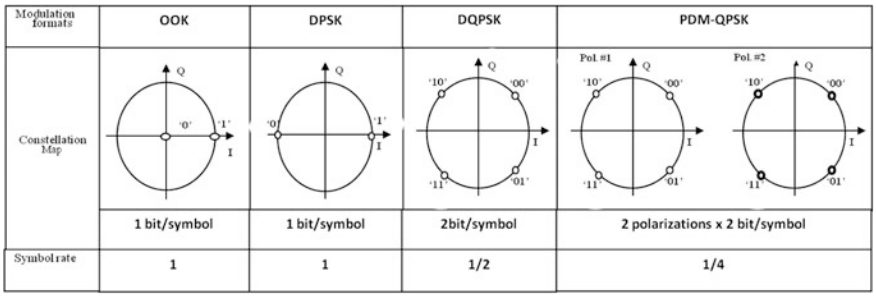


Fig. 5 Different Types of Optical Modulation Formats

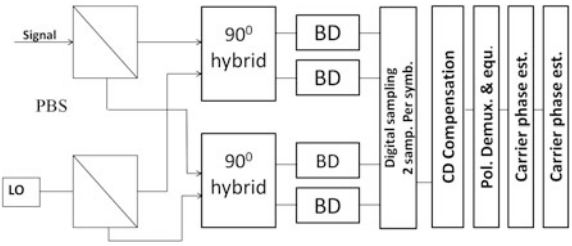


Fig. 6 PM-QPSK Transmitter

In PM-QPSK transmitter, two quadrature phase shift modulators and a polarization beam combiner (PBC) are used to multiplex two orthogonal polarizations in the form of two outputs. Similarly at the receiver end, the received optical signal is split into two orthogonal polarization tributaries using a second polarization beam splitter which are then mixed with the output of a local optical oscillator in a 90° hybrid structure (in phase and quadrature components of both polarizations) and are then detected by four photodiodes connected in balanced manner as shown in Fig. 6. This is then converted to digital signal to analog to digital converter. In this way, OSNR exceeding 15 dB (OSNR > 15 dB) with 0.1 nm resolution bandwidth is achieved.

7 Conclusion

In coherent 100 Gbps PM-QPSK fiber optical system with soft-decision forward error correction (SD-FEC) and electronic dispersion compensation by DSP devices, there is a 6 dB improvement for coherent detection, 3 dB improvement for FEC, and 1–2 dB improvement in chromatic distortion (CD) and polarization mode distortion penalties. So, there is net improvement of 10 dB in OSNR with respect to 10 Gbps link and 3 dB in OSNR with respect to 40 Gbps link. 100 Gbps fiber link will replace all 10 and 40 Gbps optical links in near future.

References

1. Arumugam, M.: Optical fiber communication. Pramana J. Phys. **57**(5 & 6) (2001)
2. Birk, M., Gerard, P., Curto, R., Nelson, L.E., Zhou, X., Magill, P., Schmidt, T.J., Malouin, C., Zhiang, B., Ibragimov, E., Khatana, S., Glavanovic, M., Lofland, R., Marcoccia, R., Saunders, R., Nicholl, G., Nowell, M., Forghieri, F.: Coherent 100 Gb/s PM-QPSK field trial. IEEE Commun. Mag. (2010)
3. Birk, M., Gerard, P., Curto, R., Nelson, L.E., Zhou, X., Magill, P., Schmidt, T.J., Malouin, C., Zhiang, B., Ibragimov, E., Khatana, S., Glavanovic, M., Lofland, R., Marcoccia, R., Saunders, R., Nicholl, G., Nowell, M., Forghieri, F.: Field trial of a real-time, single wavelength, coherent 100 Gbit/s PM-QPSK channel upgrade of an installed 1800 km link, IEEE Xplore, July 2010

4. Vand Den Borne, D., Sleiffer, V., Alfiad, M.S., Jansen, S.L., Wuth, T.: POLMUX-QPSK modulation and coherent detection: the challenge of long-haul 100G transmission. In: ECOC 2009, Vienna, Austria, IEEE Xplore, 20–24 Sept 2009
5. Hranilovic, S., Kschischang, F.R.: Optical intensity-modulated direct detection channels: singal space and lattice codes. IEEE Trans. Inf. Theor. **49**(6) (2003)
6. Ben Ezra, Y., Lembrikov, B.I., Zadok, A., Halifa, R., Brodeski, D.: All-optical signal processing for high spectral efficiency (SE) optical communication. In: N. Das (ed.) Optical Communication, Intech. ISBN 978-953-51-0784-2
7. Xie, C.: WDM coherent PDM-QPSK systems with and without inline optical dispersion compensation. Opt. Express **17**(6), 4815 (2009)

Author Biography

Dr. S.C. Gupta is a reputed professional in the field of Electronics and Communication. He was awarded Ph.D. from Delhi University and completed postdoctoral research from University of HULL, England. He was leader of PPC team deputed by Hindustan Aeronautics Ltd. at Ferrant Ltd, UK in the year 1980 and 1982. He has served in leading industrial Public Sector Undertakings (PSUs) for more than two decades and was Founder Director of Northern India Engineering College (NIEC), IP University, Delhi, for 10 years before joining RKGIT as Director (Academics). He has authored four engg. books and published 66 research papers in national and international journals/proceedings. He has successfully developed nine instruments that are being used in India and Europe. He has received various awards for outstanding contribution in optoelectronics and excellence in education.

Performance Variation of Routing Protocols with Mobility and Scalability in MANET

Manish Kumar, Chetan Sharma, Arzoo Dhiman and Ajay Kumar Rangra

Abstract The network in which nodes are mobile and these nodes communicate with each other by a wireless system not including any infrastructure is known as Mobile Ad HOC Network. Due to mobility of the nodes in MANET, routing a packet from source to destination becomes more difficult. So, many routing protocols have been purposed with reference to MANET but in a scenario of large nodes with high mobility no protocol is proved to be that efficient due to some particular limitation of that protocol. Therefore, mobility and scalability are alarming issue in mostly all protocols which support routing. The routing depends on the protocol; therefore, mobility and scalability of different routing protocols DSR, AODV and OLSR are evaluated in different network sizes with varying mobility rate. Firstly, the simulation environment is provided by varying some important parameters like pause time, speed and variation in number of nodes together. Then comparison between the three protocols is done to determine the best protocol in real-time scenario. Performance when measured on high scalability on a simulation of OLSR protocol as compared to that of AODV and DSR, the results deduced were far better.

Keywords MANET · Mobility · Scalability · AODV · DSR · OLSR

M. Kumar (✉) · C. Sharma · A. Dhiman · A.K. Rangra
Chitkara University, Baddi, Himachal Pradesh, India
e-mail: sharma.ycoe@gmail.com

C. Sharma
e-mail: chetanshekhu@gmail.com

A. Dhiman
e-mail: arzoodhiman89@gmail.com

A.K. Rangra
e-mail: ajay.rangra@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_2

1 Introduction

A Mobile Ad hoc Network is a network which does not need any infrastructure and configures itself by wireless link for communication of mobile nodes. As in a network which follows such type of strategy to communicate, nodes are free to move in any direction independently. So, wireless links keep on changing very frequently which help to complete the communication process. So, basic challenge faced in a MANET is to keep all the devices updated with the information further required for routing purpose. The position of the mobile nodes (which kept on changing in case of MANET) and their ability of transmission power play a major role in deciding the topology of network. Overall creation, organization and administration in a MANET are done by network itself [1, 2].

2 Categories of Routing Protocols

Some of the protocols which have been developed with context to MANET [3–6] can be classified into the following three categories [7] as shown in Fig. 1.

2.1 On-Demand Routing Protocols

In case of on-demand protocols, routes are searched only in case when some nodes need to communicate with each other. The process to discover the route terminates when it ends in finding a route or not at all any route. So, due to this feature of route maintenance this is also known as reactive protocol. Some popular routing protocol

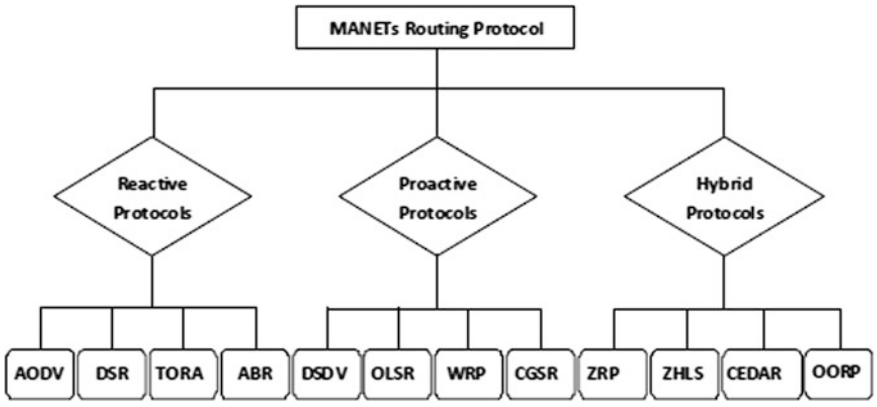


Fig. 1 Classification of routing protocols

which use this reactive technique for communication in MANET are dynamic source routing (DSR), ad hoc on-demand distance vector (AODV) routing protocol and temporally ordered routing algorithm (TORA).

2.1.1 Ad Hoc On-Demand Distance Vector (AODV)

In this protocol, the route reply packet is transmitted back to the origin node and target node gets the routing data packet. AODV protocol uses two steps for communication purpose that is discovery and maintenance of route. When any node wants to send the packet, the process of route discovery get initiated by sending route request packet to its adjacent nodes. If route exists to the target node from these adjacent nodes then a route reply packet will be returned back. In case when these adjacent nodes don't have any route to the target nodes, it will further send a route request packet to its own adjacent nodes excluding the origin node which started the communication process. If a node goes out of network then the corresponding routing table is updated by the process of route maintenance.

2.2 Table Driven Routing Protocols

The table driven routing protocol is also known as proactive protocol. These protocols keep their routing table information updated besides the need of data transfer. This feature of keeping updated routes help in finding the shortest path which leads to reduced delay.

2.2.1 Optimized Link State Routing (OLSR)

The OLSR determine and broadcast the link state information by using topological control message and "hello" interval. Every node uses this link state information to calculate the hop count so that shortest path to the destination is found. The advantage of OLSR is its ability to adapt the changes in network with no overhead of control message creation.

3 Analysis Factor in MANET

3.1 Mobility

Mobility means competence to sustain the network while nodes of the network keep changing their location.

There exist four popular models to support mobility i.e. random way point, random point group mobility, manhattan mobility model and freeway mobility model. We have selected Random Waypoint Model in our research work. In this model, there is a uniform distribution of velocity from zero to max (max is the highest velocity which can achieve by any node), which is randomly chosen by a node to reach any arbitrary location. The pause time parameter decides the duration of node to stop after reaching arbitrary location.

3.2 Scalability

A network has some limiting parameters like its size and traffic rate. But the ability of network to sustain its performance even with the increase of these parameters is known as scalability.

4 Performance Metrics

The following are some performance metrics which play a major role while deciding the efficiency of MANET routing protocols: average jitter, packet delivery ratio, normalized routing load, average throughput and average end-to-end delay. All these metrics must be calculated by varying some parameters related to the network like: network size, average connectivity, topological rate of change, mobility, link capacity. We have used the following two metrics for work which we found most important.

4.1 Average End-to-End Delay

The average time taken to reach from origin to target node by data packets including various delays is known as average end-to-end delay.

4.2 Average Throughput

The data packets fruitfully transferred per unit time is known as average throughput of the network.

5 Previous Work

In the previous research, most of the researcher focus was on analyzing scalability and mobility separately, but actually both these factors influence the network performance at the same time. So, I have decided to analyze the routing protocols considering scalability and mobility together.

6 Problem Statement

A collection of nodes which change their locations randomly and vigorously is denoted as Mobile Ad Hoc network. This random and vigorous movement leads to change in connections among them. Even though various routing protocols can be used to implement Mobile Ad Hoc network but there is no standard algorithm which perform efficiently with various issues like variation in network size, node mobility pattern and load of traffic. Therefore, choosing a protocol to implement MANET with above issues is an immense challenge. By variation in the number of nodes and their mobility, the performance of the network may decline. As the performance of MANET depends upon the protocols used for routing, so to determine which protocol gives better performance with change in mobility and scalability, we need to compare these protocols.

7 Objective

The primary objective of our research work is to study three routing protocols: dynamic source routing (DSR), ad hoc on-demand distance vector (AODV) and optimized link state routing (OLSR). We compared these protocols on two parameters which are scalability and mobility. The performance of these two parameters on the simulator. The simulator is provided with various number of nodes and the speed is managed by the simulator. Finally, find the best protocol for large number of nodes with varying speed.

8 Research Methodology

Statistical data for analysis produced in the current paper are results of experimentations and investigations performed using simulation. Research carried out using these process/experiments is called quantitative research.

9 Simulation Tool

The current research work has been carried out on Optimized Network Engineering Tool (OPNET) Modeller 14.5 which provides virtual network communication environment. The model is widely used and accepted across research fraternity as it is appropriate for the research studies, network modelling and engineering and performance analysis. Apart from being a leading environment for network modelling, this tool has been used in number of industry standards, networking protocols and devices [8].

10 Network Model Design

The OPNET modeller provides a blank scenario to run the configurations and simulations [9, 10]. The blank scenario is created using the set-up wizard provided in the modeller which generates a workspace. Now for simulation environment, drag and drop feature of the workspace is used wherein we get the application configuration, profile configuration along with mobility configuration and nodes. These configurations utility are picked from the object palette provided in the work space (Fig 2).

10.1 Application Configuration

Application configuration is an integral part of a network scenario. It is used to generate the required type of traffic in the network. Among the available choices of applications provided in the application configuration, namely FTP, email, HTTP, database and print, we have chosen HTTP Web application. The heavy browsing feature of the HTTP Web application is used as shown in Fig. 3.

10.2 Profile Configuration

To generate application traffic, user profiles need to be created. The user profiles can be created using the profile configuration utility provided in the simulator. Using the same, we can generate multiple profiles. As per our user design requirement, restrictions can be placed on the usage of nodes placed in the network environment. In this research, we have created only one profile named “Profile1” as shown in Fig. 4.

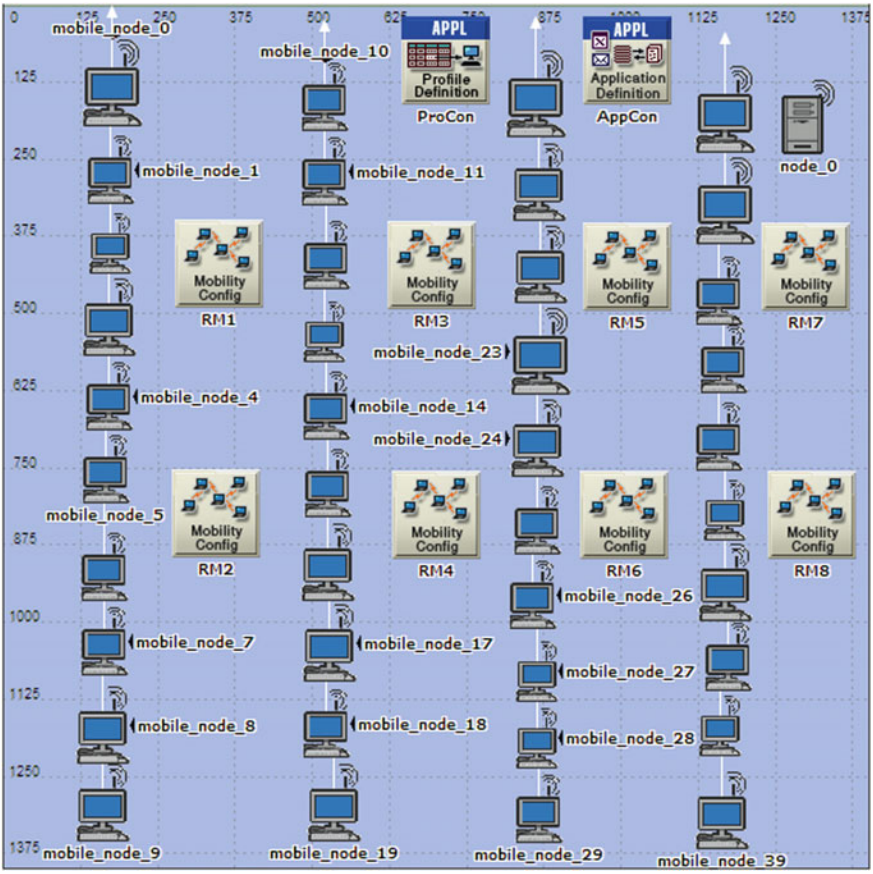


Fig. 2 An example of network model design of MANET using 40 nodes

Attribute	Value
name	node_0
Application Definitions	(...)
Number of Rows	1
HTTP	
Name	HTTP
Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	(...)
Print	Off
Remote Login	Off
Video Conferencing	Off
Voice	Off

Fig. 3 Application configuration attributes

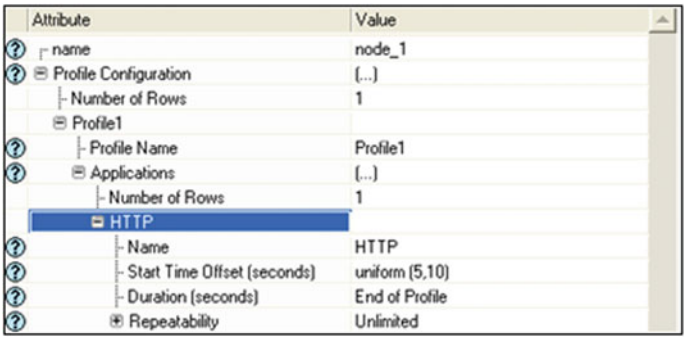


Fig. 4 Profile configuration attributes

10.3 Mobility Configuration

A control environment of mobility model is provided in the mobility configuration. The control on the nodes is managed by maintaining the parameters such as speed, start time and stop time of a given node. In this proposed work, I have varied speed and pause time of the nodes. The speed of the nodes is changed from 0 to 24 m/s. To ensure that the mobile nodes are configured with mobility, I have chosen random waypoint mobility model in this current work.

11 Scenarios and Parameters

In this research work, simulation mainly considers the performance of routing protocols with variation in the number of nodes and their speed. Here, we have taken 20, 40 and 60 number of nodes under nine different scenarios for simulation in context to AODV, DSR and OLSR. Application and profile configurations are used to generate the traffic for hyper text transfer protocol. Table 1 describes the values taken for different simulation parameters while observing three MANET protocols.

Parameters for individual protocols also varied from default setting except OLSR, because the OLSR gives best performance with these parameters. Table 2 show the parameters and their respective values.

Table 1 Simulation parameters

Attribute	Value	Attribute	Value
Maximum simulation time	600 s	Transmit power (W)	0.020
Interface type	Wireless (ad hoc)	Buffer size (bits)	1,024,000
Network area	1000 * 1000 m 1400 * 1400 m 1725 * 1725 m	No. of nodes	20, 40, 60
Mobility model	Random way point	Protocols	DSR, AODV, OLSR
Data rate (bps)	11 Mbps	Traffic generation application	HTTP (heavy browsing)

Table 2 DSR, AODV and OLSR parameters

DSR parameters		AODV parameters		OLSR parameters	
Route expiry time	300 s	Route request retry	5	Willingness	Willingness always
Max buffer size	Infinity	Route request rate limits (packets/sec)	10	Hello interval (seconds)	2.0
Expiry time	30 s	Gratuitous route reply flag	Enabled	TC interval (seconds)	5.0
		Active route timeout (seconds)	10	Neighbour hold time (seconds)	6.0
		Hello interval (seconds)	Uniform (1, 1.1)	Topology hold time (seconds)	15.0
		Allowed hello loss	10	Duplicate message hold time (seconds)	30.0
		Timeout buffer	2	Addressing mode	IPv4

11.1 DSR Parameters

See Table 2.

12 Performance Evaluation Metrics

Due consideration is given to important metrics for analyzing the performance of various routing protocols for mobility with the combination of scalability. The metrics chosen for this particular simulation are:

Average Throughput

The data packets fruitfully transferred per unit time are known as average throughput of the network. In our study, messages delivered per second are considered to evaluate throughput.

Average End-to-End Delay

The average time taken to reach from origin to target node by data packets including various delays is known as average end-to-end delay.

All the above metrics must be calculated by varying some parameters related to the network like:

- Network Size
- Average Connectivity (Average degree of node)
- Mobility
- Link Capacity (bits/sec)

In this research work, we have chosen speed of the nodes, pause time and network size as the varying parameter as we are evaluating the scalability and mobility of the MANET routing protocols.

13 Performance Comparison of Protocols

The following record analysis describes the performance comparison of protocols based on the mobility and scalability.

13.1 Network Delay

Figure 5 shows the delay for network packets transmission in AODV, DSR and OLSR for 20, 40 and 60 nodes, respectively. In the above analyzed scenarios,

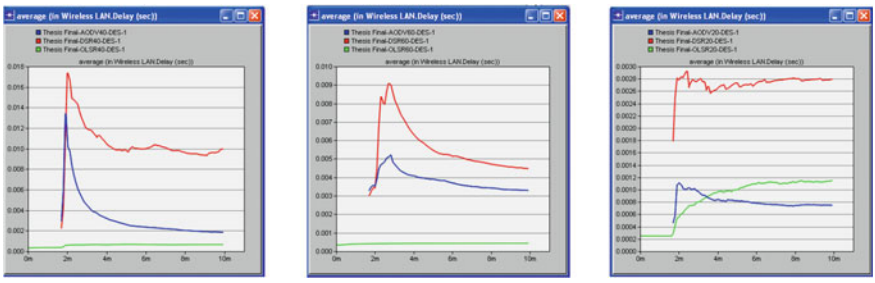


Fig. 5 Network delay for 20, 40 and 60 nodes (DSR, AODV and OLSR)

AODV and OLSR are showing very less network delay as compared to DSR. So, DSR is lacking in performance among these three protocols. The basic fact which leads to failure of DSR is use of caching hard line. Even when more than one choice is available DSR lacks in finding the fresh routes due to its inability to run out the decayed routes. We can observe that AODV delay is low in fewer numbers of nodes and mobility but increased as the number of nodes and mobility rate increases. This is due to the reason that there is less overhead for RREQ and RREP for fewer nodes but very higher as the number of nodes and mobility grow.

OLSR outperformed DSR and AODV in consideration of network delay in general. The table driven approach of OLSR is basic reason for these results. The delay in transmission is low because the extra work to discover the new route is not required in case of OLSR. Therefore, in terms of network delay OLSR and AODV are more scalable and mobile than DSR protocol.

13.2 Throughput

Figure 6 depicts the throughput of all three protocols for 20, 40 and 60 nodes, respectively. In our comparison study of three protocols, DSR is lacking in all the parameters chosen. DSR is far behind than OLSR and AODV in case of throughput. First reason is high cache of routes maintained by DSR. Secondly, the routes which are no longer in use do not deleted by DSR and it leads to problem in determining fresh routes.

If we change the number of nodes with variation in their speed, AODV protocol performs moderately in reference to throughput parameter. AODV keeps track of multiple routes from source to final node which leads to discovering an optimal route almost in each case. In determining new routes, AODV compromises with increased latency to manage the control of traffic. There is no doubt that AODV compromises with latency for controlling the network traffic.

The OLSR outperformed the AODV and DSR in our simulation in context to throughput also. Basic reason for this performance is use of proactive technique by

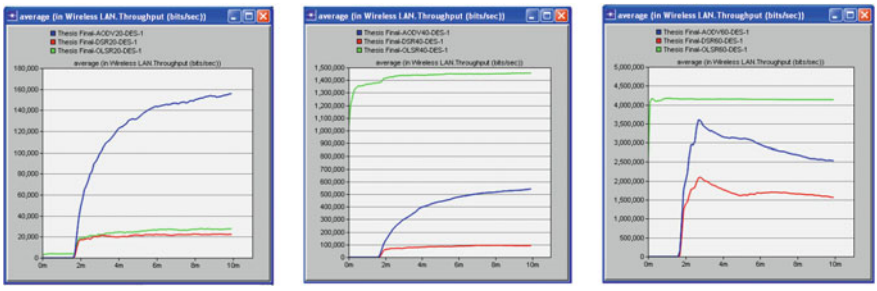


Fig. 6 Throughput for 20, 40 and 60 nodes (DSR, AODV and OLSR)

OLSR where MPR is used to update the various links which leads to control the overall overhead in network traffic. This does not affect the performance of OLSR when the network contains the small number of nodes but as the number of nodes increases with mobility it limits the performance of the protocol to some level. But, we can analyze that efficiency of the OLSR is great in case of network with high density of nodes.

14 Results and Conclusion

The simulation results conclude that the performance varies from protocol to protocol with mobility and scalability. The network's average end-to-end delay increased for all three routing protocols as and when the number and speed of the nodes increased. With the increase in number of nodes and their varying speeds, a delay has been observed in the network. Ultimately, under all the scenarios used OLSR performed far better than DSR and AODV has minimum network delay in high mobility and more number of nodes. In both the metrics, DSR's performance was not satisfactory even after using cache. But OLSR showed best results as compared to DSR and AODV in context to throughput. AODV is just behind the OLSR in case of performance in throughput but its reaction is very quick while operating as it maintains the overhead involve in routing better. All this analysis is based upon comparing the different routing protocols by varying their speed parallel with increase in number of nodes to determine the best possible protocol in real-time scenario so that cost involved can be minimized with best possible routing of network packets.

15 Future Work

For future consideration, other routing protocols apart from DSR, AODV and OLSR can be evaluated such as ZRP which belongs to hybrid routing category. Various parameters have been varied and tested during the work such as number of nodes, network area, mobility and pause time. Other parameters such as data rate and traffic applications are kept constant. It would be interesting to see the behaviour of the routing protocols by varying these parameters.

References

1. http://www.di.inf.pucrio.br/~endler/courses/Mobile/papers/MANET-Challenges
2. Schiller, J.: Mobile Communication, 2nd edn. Pearson Publications (2007)
3. www.csd.uoc.gr/~hy539/Spring%202005/lectures/adhoc

4. http://www.eexploria.com/manet-mobile-ad-hoc-network-characteristics-and-features/
5. Adhoc On-Demand Distance Vector (AODV) Routing. http://tools.ietf.org/html/rfc3561
6. Optimized Link State Routing Protocol (OLSR). http://www.ietf.org/rfc/rfc3626.txt
7. Roy, R.R: Handbook on Mobile Ad-hoc Networks for Mobility Models. Springer Publication (2011)
8. OPNET University Program. http://www.opnet.com/services/university/
9. Kumar, S., Sharma, S.C., Suman, B.: Simulation based performance analysis of routing protocols using random waypoint mobility model in mobile ad hoc network. Glob. J. Comput. Sci. Technol. **11**(1) (Version 1.0) (2011)
10. Barakovi, S., Barakovi, J.: Comparative performance evaluation of mobile ad hoc routing protocols. In: MIPRO 2010—33rd International Convention, 24–28 May 2010

Variations in Routing Protocol Resulting in Improved Energy Utilization in WSN

Chandandeep Kaur, Chetan Sharma, Arzoo Dhiman and Akansha Sharma

Abstract With advancements in technology in the twenty-first century, tiny and cheap but intelligent sensors networked using wireless links and internet are being deployed in physical areas. These are popularly named as WSN; WSNs are powered by microelectronic mechanical systems (MEMS) and wireless communication technologies. Each sensor node is accompanied with a battery which easily gets discharged with time and thus needs to be replaced or recharged. The lifetime expectancy of a WSN can be maximized by reducing the energy or power that is being consumed. Even then, ample amount of energy is wasted by idle node components (CPU, radio, etc.). Sometimes, power management schemes thus suggest turning the node components off when not in use. At an extensive level, there are three strategies: duty cycling approaches, data-driven techniques, and mobility approaches. In this paper, we contemplate on data-driven approaches. Data which is sampled by the sensor nodes is processed, but of all duty cycling approach is insensitive to data sampled. Hence, data-driven approach has been followed as it has been seen to improve the energy efficiency when compared to the other techniques.

Keywords Wireless · Protocol · Sensor network · WSN

C. Kaur (✉) · C. Sharma · A. Dhiman · A. Sharma
Chitkara University, Baddi, Himachal Pradesh, India
e-mail: chandandeepkalra@gmail.com

C. Sharma
e-mail: chetanshekhu@gmail.com

A. Dhiman
e-mail: arzoodhiman89@gmail.com

A. Sharma
e-mail: akankshasrpsharma@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_3

1 Introduction

Figure 1 shows the arrangement of a traditional sensor network [1]. Life of a node in a WSN is directly correlated to the current usage profile of the battery being used. If we can somehow estimate the energy that is being consumed by the node at any particular time, the choice of the routing protocols and sensing of the data can be made such that the informed decisions can be made to enhance the life of the sensor node as well as the network. However, it is not feasible practically to measure the energy consumption on a node. Each sensor node is accompanied with a battery which easily gets discharged with time and thus needs to be replaced or recharged. The lifetime expectancy of a WSN can be maximized by reducing the power consumption during network activities. The nodes that are being used with these networks are, however, not that expensive, and thus it is more cost effective to replace the entire node than to locate and recharge the battery supply [2].

A traditional wireless sensor node endures of basically four components:

- A subsystem with sensing capabilities for data acquisition purposes;
- A system with processing capabilities including a microcontroller and memory for local data processing;
- A radio subsystem for wireless data communication;
- A battery.

2 Problem Definition

WSNs are the networks that consist of numerous numbers of tiny sensor chips where each sensor node is a low-power computing device which is capable of data processing, wireless communication, and sensing features. Sensor nodes are capable of sensing physical environmental changes, processing the data attained at two

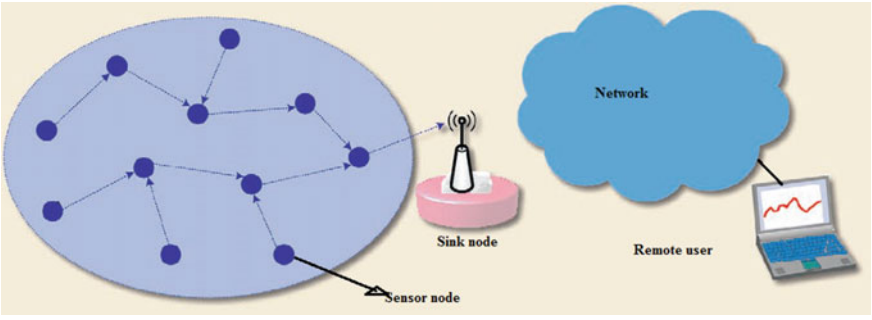


Fig. 1 Typical sensor network architecture

levels the unit and cluster, and transmit the fallout to the cluster as well as to one or more collection points, named as energy sinks or base stations.

As the nodes used are battery driven, therefore, battery power consumption is one of the main considerations of the deployment of these networks. Certain applications demand long network lifetime along with high quality of service, and this demands high consumption of battery power leading to frequent replacements or recharging of batteries which is not possible in all the cases. Efficient energy management strategies must be fabricated even at the finer levels to perpetuate the life of the network as much as possible.

Our research focuses on assumption that each feature specimens a sensor in the wireless sensor network; various data sets with multiple features have been designed to show that the changes in the routing configuration and traffic flow could play a key role in the reduction of the power consumption. We aim to minimize the number of sensors for energy efficient management which is equivalent to minimizing the number of features which have been considered.

Battery power consumption in a sensor node could be because of two types of sources either "useful" or "wasteful" [3].

- Energy from useful sources is consumed because of transmission and receiving of data, processing of query requests, and forwarding queries and data to neighbor nodes [4].
- Energy from wasteful source is consumed due to one or more of the following factuality.
- One of the major origins of energy waste is
  - Firstly, idle listening, i.e., auscultates an idle channel in order to analyze conceivable traffic that can be encountered [5].
  - Second reason for energy being consumed extravagantly for no purpose is collision or clashes, when a node receives more than one packet at the same time; these packets conflict with each other. All these packets that get collide have to be discarded, and retransmissions of these packets are required which further increases in boosting up the energy wastage [6].
  - The next reason for energy being consumed but serving no purpose is because of overhearing a node; in such cases, a node receives packets that are not destined to that particular node but to the other neighboring nodes.
  - Fourth reason encountered is control packet overhead [7].
  - Finally, over-emitting or duplicate emitting is another reason for the energy loss, which is caused by the transmittal/re-transmittal of a packet when the terminal node even prepared for the receiving.

Thus, by making the comparisons of certain parameters which are the deciding factors for the routing protocol and for the management of the traffic flow, we will try to efficiently manage the energy consumption of each individual node.

The results are obtained through OPNET using AODV routing protocol [8]. The variation in the routing protocol for different scenarios yields different results. The protocol used for traffic flow is an FTP (File Transfer Protocol), and the experiment

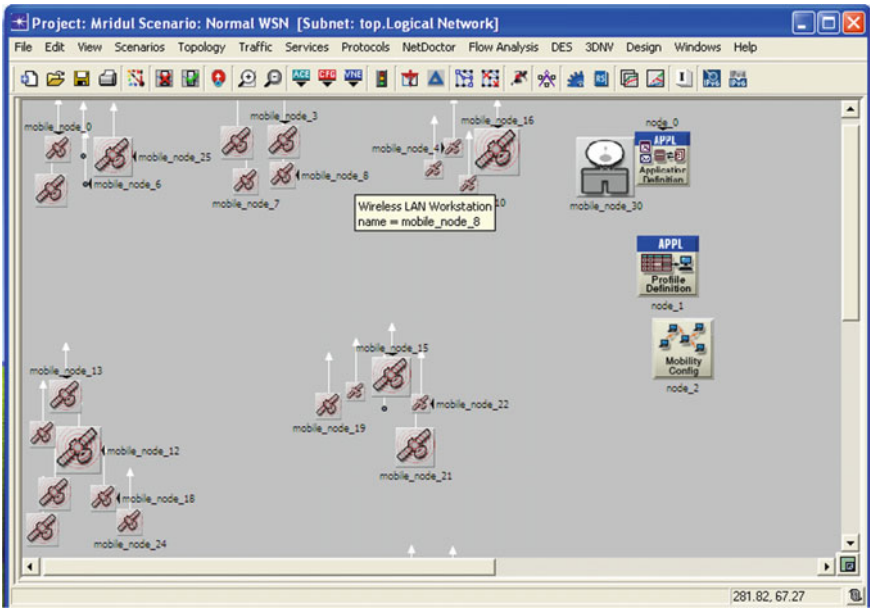


Fig. 2 Normal WSN 32 nodes

is performed on random nodes [9]. The experiment is performed in the uniform environment, and the results for the different parameters are shown in different figures.

As shown in Fig. 2, nodes are arranged in clusters, and these clusters are acting as clients to collect data from the surroundings, and then the data is transmitted.

The nodes are arranged in clusters acting as clients to collect data from the surroundings, and then each client sends data to the server node for processing. Figures 3 and 4, however, show the incremented number of nodes so as to make the network highly reliable, but it can be seen that due to power leakage some of the nodes get failed.

3 Parameters Analyzed

3.1 Throughput

Throughput is the average rate of successful message delivery over a communication channel. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

In Fig. 5, the comparison between the throughput for normal WSN and timely improved WSN has been established. The number of nodes used is 32. It is shown

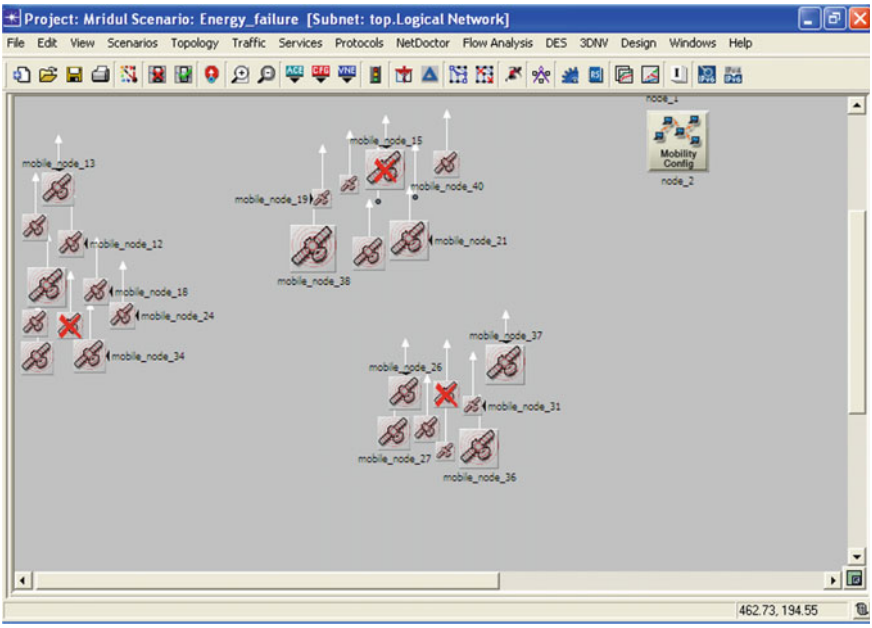


Fig. 3 WSN with more number of nodes (50 nodes)

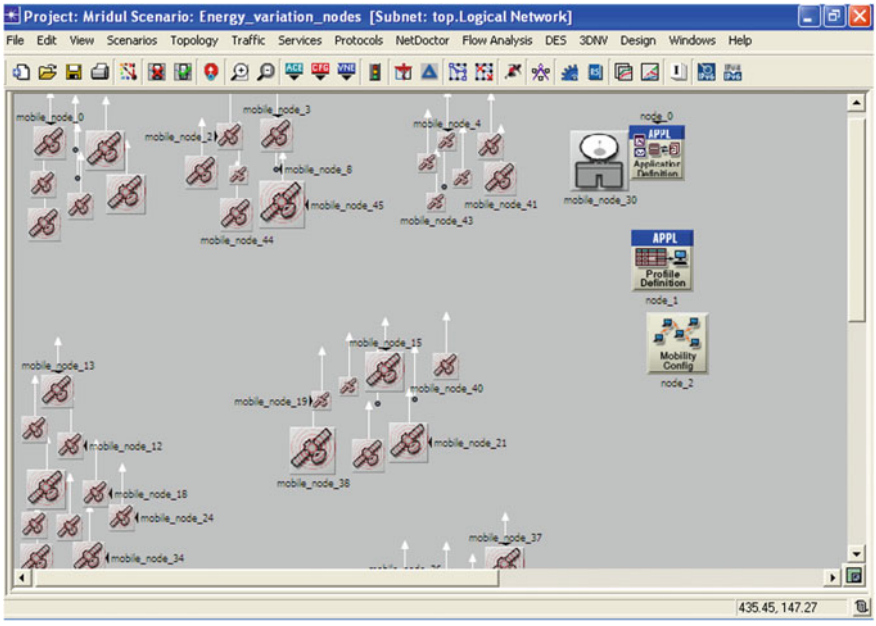


Fig. 4 WSN with some failure nodes (44 nodes)

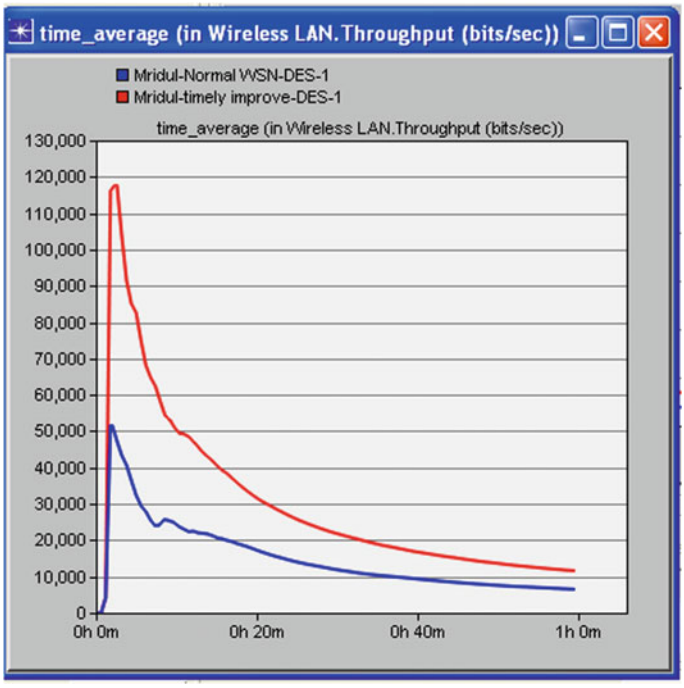


Fig. 5 Throughput comparison between normal (32 nodes) and timely improved (32 nodes) WSN

that the throughput for the improved WSN increases considerably within the same time interval. This is because of the changes made in the routing configuration.

In Fig. 6, the comparison between the throughput for the normal WSN and the WSN with energy management has been established [9]. The number of nodes in both the networks remains the same, i.e., 32. The graph clearly shows that the network can now send more number of packets in the same time interval, and in this way the battery lifetime of the network has increased.

Fig. 7 depicts the comparison of normal WSN and the WSN with varied number of nodes. The number of nodes is increased to 50 in the network, and then the throughput of the network has been calculated. The results show that the throughput of the network with varied number of nodes increases at a very high rate. This is due to the fact that the data sent by the less number of nodes in normal WSN has now been sent by more number of nodes in the same time interval [10].

In Fig. 8, comparison between normal WSN and the WSN with some of the failed nodes has been established. The count of nodes available in the network with failure nodes in each cluster is 44 and in normal WSN is 32. The network with some of the failed nodes in each cluster has more throughput rate as compared to the normal WSN. This is because when some of the nodes in the cluster fail, the packets sent by that node are distributed among other nodes in the cluster and the traffic channel capacity remains the same. Therefore, each node can send more

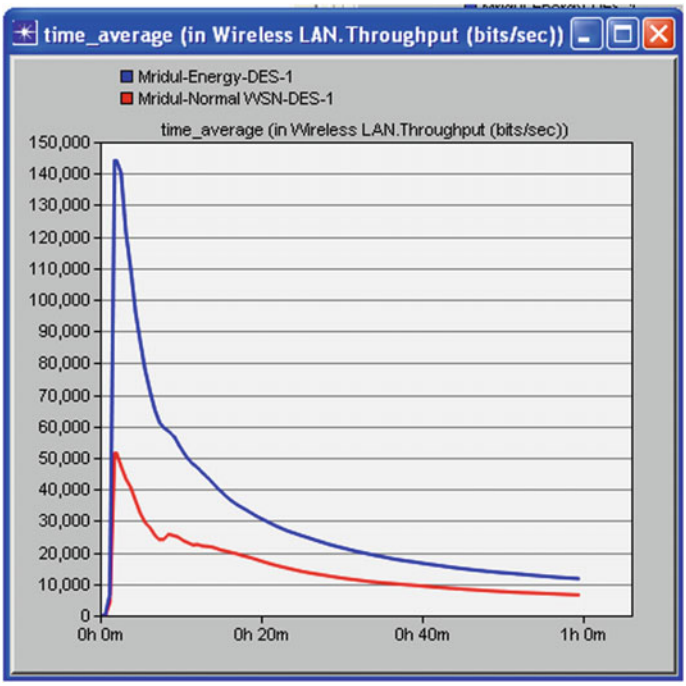


Fig. 6 Throughput comparison between normal (32 nodes) and energy managed (32 nodes) WSN

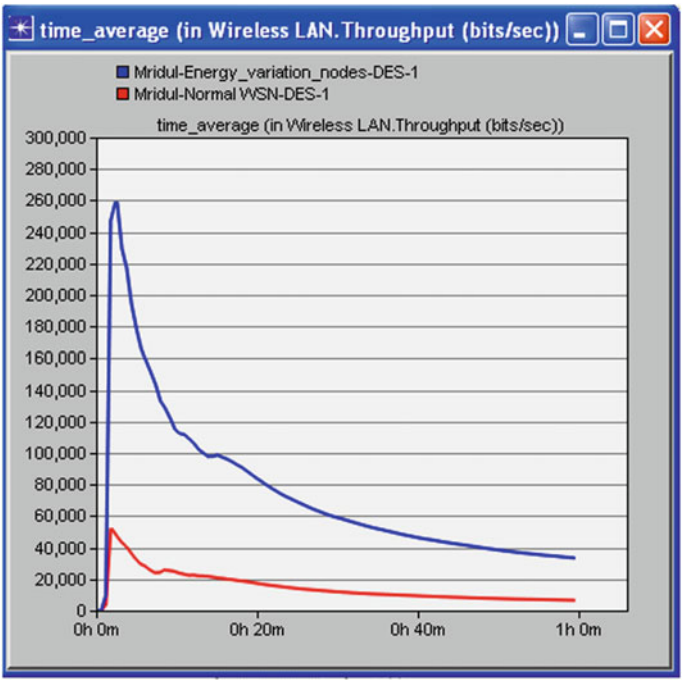


Fig. 7 Throughput comparison between normal (32) and varied number of nodes (50 nodes) WSN

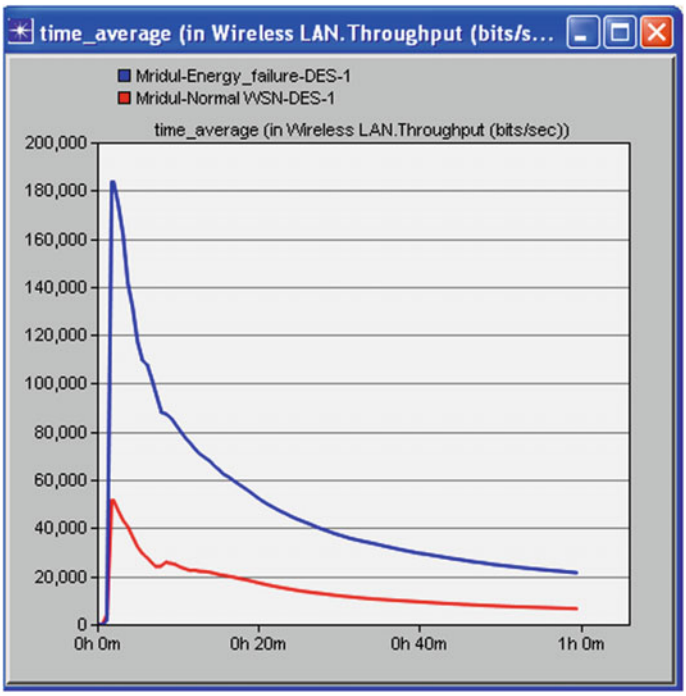


Fig. 8 Throughput comparison between normal WSN (32 nodes) and WSN with failure nodes (44 nodes)

number of packets on the same channel as compared to the network with all nodes working. Therefore, the data can be sent at a faster rate than the normal network [11].

Hence, the normal WSN gives low throughput as compared to all other networks.

4 Conclusions

For the proposed work, we have made changes in the configuration of the on-demand protocol with less time to live, less hello interval, and less hello loss. In the first scenario, we have proposed a timely based improvement in sensor network so that energy consumption should be less and lifetime of the network can be increased. In the second scenario, we have used an energy saving technique with improvement in transmitting energy and threshold energy parameters on cluster heads. In the third scenario, we have done variation in the number of nodes for testing the performance of the network. Finally in the last scenario, we have

considered a scenario with node failure for checking the performance of the network. The variation of performance has been shown in terms of comparison of graphs.

References

1. Alippi, C., et al.: Energy management in wireless sensor networks with energy-hungry sensors. IEEE Instrum. Meas. Mag. 16–23 (2009)
2. Sharma, Amit, et al.: Energy management for wireless sensor network nodes. IJAET Int. J. Adv. Eng. Technol. **1**(1), 7–13 (2011)
3. www.airccse.org
4. Zheng, J., Jamalipour, A.: Wireless sensor networks—a networking perspective. 978-0-470-16763-2
5. Chaturvedi, P.: Introduction to wireless sensor networks. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **2**(10), 33–36 (2012)
6. Yick, J., et al.: Wireless sensor network survey. Int. J. Comput. Telecommun. Netw. **52**(12), 2292–2330 (2008)
7. Anastasi, G., et al.: Energy conservation in wireless sensor networks: a survey. Ad Hoc Netw. **7**(3), 537–568 (2009)
8. Akyildiz, I.F., et al.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
9. Laki, S., Shukla, R.N.: Deployment in wireless sensor networks. Int. J. Adv. Res. Electron. Commun. Eng. (IJARECE) **2**(2), 108–111 (2013)
10. Singh, G., Arora, H.: Design and architectural issues in wireless sensor networks. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **3**(1), 28–32 (2013)
11. Gowrishankar, S., et al.: Issues in wireless sensor networks. In: Proceedings of the world congress on engineering, vol. 1. 978-988-98671-9-5 (2008)

Genetic Algorithm-Based Routing Protocol for Energy Efficient Routing in MANETs

Pawan, Rajendra K. Sharma, A.K. Sharma and Vinod Jain

Abstract Genetic algorithm is a very popular optimization technique in artificial intelligence. In mobile ad hoc networks (MANETs), all the devices are battery operated. The power consumption at nodes in transferring the data is a big issue in MANETs. In this paper, a new protocol for routing in MANETs using genetic algorithms is proposed. This protocol uses the power of genetic algorithms to find a path that consumes minimum power in transferring the data from source to destination node. Simulation results prove that the proposed algorithm performs better than the previous algorithms.

Keywords Wireless ad hoc networks · MANET · Power consumption · Power-aware routing protocols · Genetic algorithms · Crossover · Mutation

1 Introduction

Mobile ad hoc networks (MANETs) are infrastructure less dynamic networks. Nodes can be added or removed dynamically from these networks. Further nodes may move from one location to another location in MANETs. Because of mobility of nodes routing is very difficult in MANETs. In most of the MANETs, devices connected are battery operated. So power consumption of these devices is a very critical factor while calculating the performance of routing algorithms for MANETs. The energy level of the devices falls rapidly and a node may die very

Pawan (✉)
Al-Falah School of Engineering and Technology, Al-Falah University, Faridabad, India
e-mail: pawanbhadana79@gmail.com

R.K. Sharma
Faculty of Engineering & Technology, Agra College, Agra, India

A.K. Sharma · V. Jain
Department of Computer Science & Engineering, B.S. Anangpuria Institute of Technology and Management, Faridabad, India

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_4

soon if routing algorithm do not perform well or do not perform efficiently in MANETs. Genetic algorithm is a very popular optimization technique in artificial intelligence. The power of genetic algorithm can be used to efficiently route the traffic in MANETs so that the power consumed in transferring data from one node to another can be optimized (minimized).

1.1 Energy Efficient Routing Protocols

In literature, many power-aware routing protocols have been proposed by many authors [1–11]. Abolhasan et al. [1] discuss a review on various routing protocols for mobile ad hoc networks. Cui and others [4] provide an approach to increase the lifetime of the ad hoc network by using a utility-based algorithm. Ramanathan and others [8] provide challenges and directions to improve the performance of mobile ad hoc networks. Wedde and others [11] proposed Bee Ad Hoc that works on bee behavior to improve the performance of mobile ad hoc networks. D.E. Goldberg published a paper in 1989 [5] that focused on how genetic algorithm can be used in optimization problems. Authors provide a detail description about working of genetic algorithm and its various operators such as selection, crossover, and mutation. After having a look on this literature, it has been concluded that genetic algorithm can also be used to improve the performance of routing algorithms in mobile ad hoc networks.

2 Genetic Algorithm

Genetic Algorithm (GA) is an optimization technique which uses special operators such as selection, reproduction, and mutation to solve problems which are difficult to solve by using traditional techniques. GA works on some optimization function which may be a minimization function or a maximization function. The basic idea of genetic algorithm has been taken from medical science where characteristics of one population forwarded into next population. Before applying the genetic algorithm, a problem must be able to be represented in genetic form so that genetic operators can be applied on it.

The genetic algorithm is a special generate and test algorithm. It starts from a set of sample solutions to the problem called the initial population. This initial population can be generated randomly. Then different genetic operators such as selection, recombination, and mutation can be applied on the population repeatedly till some terminating criteria do not meet. Genetic algorithm is an optimization technique and does not guarantee to provide the best solution in given time. Generally, GA works on approximation and provides optimal or near optimal solution in the specified time. The amount of time GA takes to provide the solution depends on the

convergence of the genetic algorithm. In literature, there are methods that provide techniques to improve the convergence of genetic algorithms.

Some features of genetic algorithm are as follows:

1. GA uses populations which is a set of candidate solutions.
2. GA uses genetic operations to generate new population.
3. GA is stochastic in nature.

The major components of genetic algorithm are as follows:

1. Representation of problem in genetic form (initial population creation).
2. Calculating the fitness of different candidate solutions of the population.
3. Selecting parents to participate in recombination.
4. Applying crossover and mutation operators.
5. Survivor selection to create the next population.

3 Simulation Design and Implementation

3.1 Experimental Setup and Proposed Algorithm

In MANETs, the transmission power PR of a route depends mainly upon the distance between the two nodes and on some other factors of the network and the environment. PR is mainly function distance mathematically transmission power PR = k(distance)2

The value of k is assumed to be one.
Transmission power PR = k(distance)2

In this paper, genetic algorithms have been applied in finding a path to transfer the data from source to destination. We assume that every node have all the information about their neighbors.

Algorithm for cross_over()
{

1. Take two parents that will participate in crossover process.
2. Find an intermediate node that is common in both the parents. This node will be used as a meeting point in these two parents to perform one point crossover.
3. Generation of child1—Copy all the nodes from parent 1 into child1 up to the meeting point and then copy remaining nodes from parent2 into child-1.
4. Generation of child2—Copy all the nodes from parent2 to child2 up to the meeting point and then copy remaining nodes from parent1 into child-2.
5. Repeat the process of crossover in the same way in all the iterations.

}

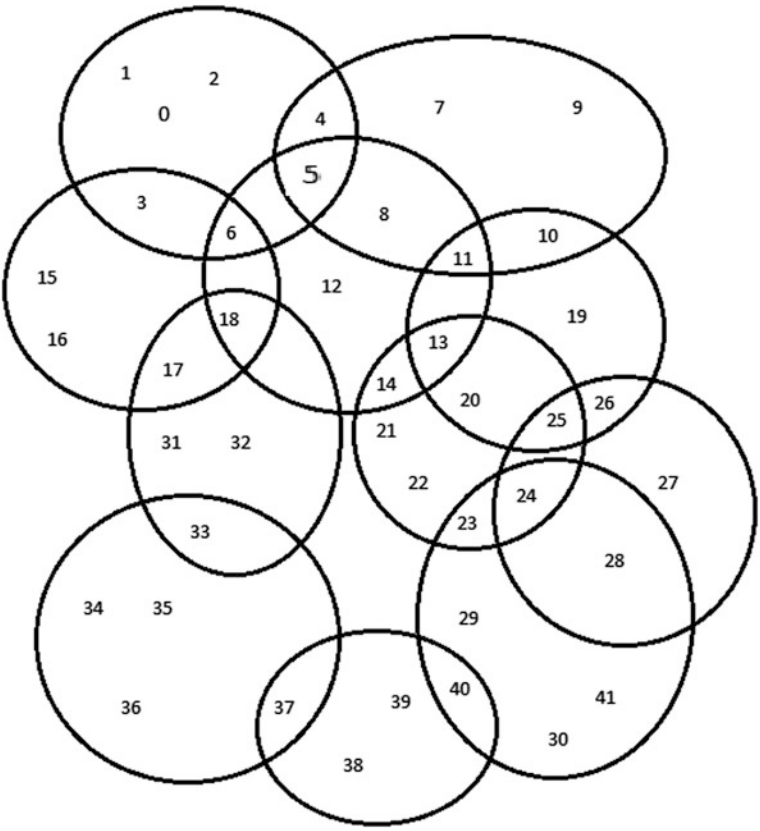


Fig. 1 Sample mobile ad hoc network

Consider the sample network shown in Fig. 1.

Let us consider that node-1 wants to send a data packet to node-41.

Sender node: 1
Receiver node: 41

Encoding: A permutation encoding has been done to represent the problem in a form suitable for application genetic operators like crossover and mutation.

A path from source to destination will become a chromosome. Following is an example of a valid chromosome:

Path: [1, 5, 4, 11, 9, 10, 26, 24, 41]

It is assumed that the network will store the cost of sending data from a node to all its neighbors. So every node creates a cost matrix to send data from this node to all of its neighbors.

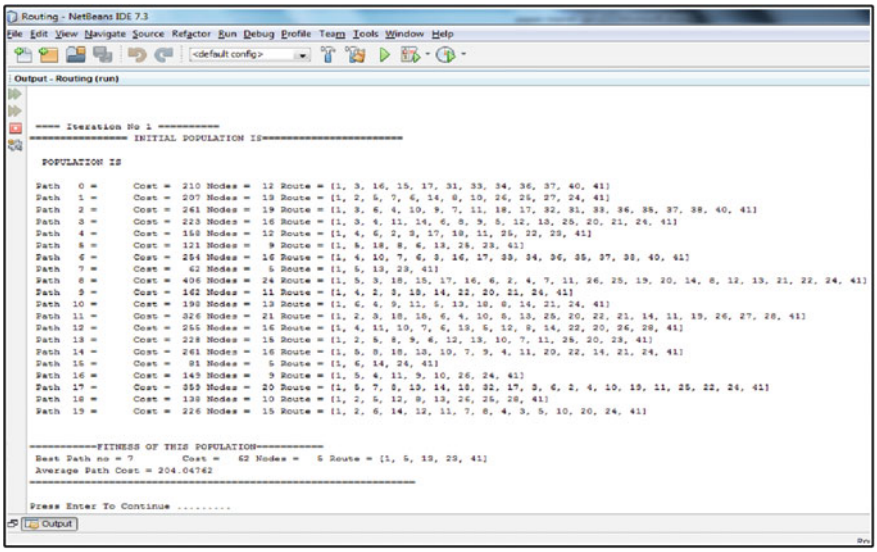


Fig. 2 Initial population

A random cost matrix has been created for the implementation and testing of the protocol.

The initial population of 20 paths has been created randomly. Every path is starting from node-1 (the sender node) and ends at node-41 (the receiver node).

The random population is given in Fig. 2.

3.2 Experimental Result

The average path cost in initial population is 204.04 and the cost of best path is 62.

Path no. 7 in the population is the best path which is as follows:

Cost = = 62 Nodes = 5 Route = [1, 5, 13, 23, 41]

3.3 Cross Over Operator

This operation selects two parents from the population and generates new children. While performing the crossover operation a common node in both of the parents

has been sleeted. The route traversed after that node in two parents is swapped to generate two children. The example is as follows:

parent1 = 3 Cost = 139 Nodes = 11 Route = [1, 3, 2, 5, 11, 12, 8, 13, 20, 23, 41]
parent2 = 10 Cost = 131 Nodes = 10 Route = [1, 6, 12, 14, 13, 19, 20, 22, 24, 41]

Node Selected For Cross Over = 12

Child1 = Cost = 147 Nodes = 13 Route = [1, 3, 2, 5, 11, 12, 14, 13, 19, 20, 22, 24, 41]
Child2 = Cost = 123 Nodes = 8 Route = [1, 6, 12, 8, 13, 20, 23, 41]

For example let us explain how child-2 has been generated:

First of all route traversed in parent 2 till node-12 has been copied in child-2, i.e., = [1, 6, 12]. After that route traversed in parent 1 after node-12 has been copied in the remaining part of the child, i.e., [8, 13, 20, 23, 41]

So finally child 2 = = [1, 6, 12, 8, 13, 20, 23, 41]

In the same way child-1 has been generated.

It can be observe that the crossover operation generates a new path (child 2) which is having less path length as compared to both of the parents. Thus, this process will improve the fitness of the population in every iteration.

Population after five iterations is shown in Fig. 3. The average path cost in this population is reduced to 108.04 and the cost of best path is 62. Path no. 19 in the population is the best path (same as the first initial population) which is as follows:

Cost = 62 Nodes = 5 Route = [1, 5, 13, 23, 41]

After this population, some more paths have been added in the population that can be used as alternate paths if there is any problem in sending the data through the best path.

4 Results and Discussion

Power-aware routing algorithm for mobile ad hoc networks can be optimized using GA genetic algorithm. GA can be used in finding a path that cost minimum in transferring data in MANETs. The work has been implemented in java on a sample network of 42 nodes. It has been observed that GA finds best paths very quickly in little iteration. It also finds some alternate paths that can also be used if one path failure occurs by any reason. In future, the proposed algorithm can be tested on a mobile ad hoc network having thousands of nodes.

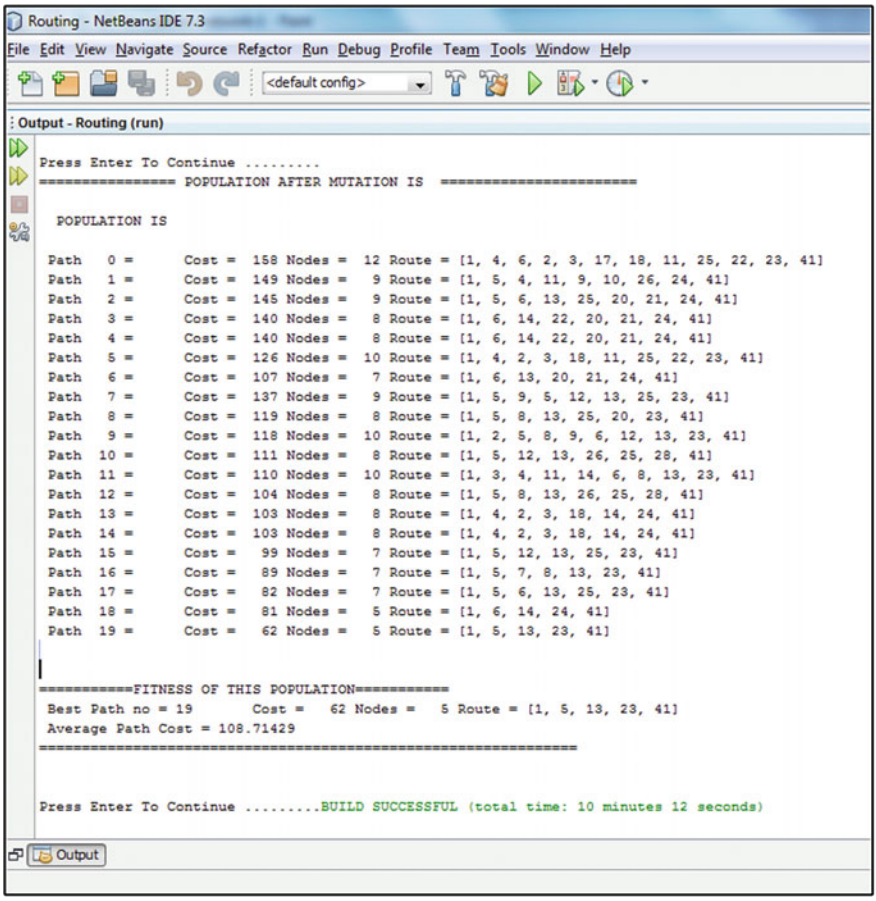


Fig. 3 Population after 5 iterations

5 Conclusion and Future Work

Genetic algorithm is a useful technique in finding path between two nodes in a mobile ad hoc network (MANET). An optimal solution to the problem can be find using GA that will find a path to transfer a packet from node-1 to node-41. GA process find a solution with cost = 63 in only five iterations. So it is concluded from this paper that genetic algorithms can be used to solve routing protocols in MANETs. However, the performance of GA with other existing techniques has to be justified in future.

6 Figures

See Figs. 1, 2, and 3.

References

1. Abolhasan, M., Winsock, T.A., Dutkiewicz, E.: A review of routing protocols for mobile ad hoc networks. Ad Hoc Netw. **2**(1), 1–22 (2004)
2. Basagni, S., Conti, M., Giordano, S., Stojmenovic, I.: Mobile Ad Hoc Networking. Wiley-IEEE Press (2004)
3. Brown, W.W., Marano, V., MacCorkell, W.H., Krout, T.: Future combat system-scalable mobile network demonstration performance and validation results. MILCOM, IEEE Volume 2, Issue, 13–16 Oct 2003, pp. 1286–1291 (2003)
4. Cui, Y., Xue, Y., Nahrstedt, K.: A utility-based distributed maximum lifetime routing algorithm for wireless networks Vehicular Technology. IEEE Trans. Veh. Technol. **55**(3), 797–805 (2006)
5. Goldberg, D.E.: Genetic Algorithms in Search, Optimization & Machine Learning. Addison-Wesley (1989)
6. Ingelrest, F., Simplot-Ryl, D., Stojmenovic, I.: Energy-Efficient Broadcasting in Wireless Mobile Ad Hoc Networks Resource Management in Wireless Networking, pp. 543–582. Springer, Berlin (2005)
7. Johnson, D.B., Maltz, D.A., Hu, Y.C.: The dynamic source routing protocol for mobile ad hoc networks (DSR) http://tools.ietf.org/id/draft-ietf-manet-dsr-10.txt (2004)
8. Ramanathan, R., Redi, J.: A brief overview of ad hoc networks: challenges and directions. IEEE Commun. Mag. **40**(5), 20–22 (2002)
9. Ross, P., Marin-Blazquez, J.G., Schulenburg, S., Hart, E.: (2003) Learning a procedure that can solve hard bin-packing problems: a new GA-based approach to hyper-heuristics. Genetic and evolutionary computation - GECCO 2003, Springer, Berlin, LNCS 2724, pp. 1295–1306
10. Tseng, Y.C., Ni, S.Y., Chen, Y.S., Sheu, J.P.: The broadcast storm problem in a mobile ad hoc network Wireless Networks, vol. 8. Short version in MOBICOM 99, pp. 153–167 (2002)
11. Wedde, H.F., Farooq, M., Pannenbaecker, T., Vogel, B., Mueller, C., Meth, J., Jeruschkat, R.: BeeAdHoc: an energy efficient routing algorithm for mobile ad hoc networks inspired by Bee Behavior. In: Proceedings of Genetic and Evolutionary Computation Conference, pp. 153–160 (2005)

IPv6 Security Issues—A Systematic Review

Atena Shiranzaei and Rafiqul Zaman Khan

Abstract IPv4 has been used over 30 years. It proved robust, interoperable, and easy implementation. The number of users is raising dramatically, the growth and development of IPv6 are vital. This protocol provides many new features like larger address space, auto-configuration, QoS, IPsec, easier TCP/IP administration, mobility, etc. In addition to these features, IPv6 development brings new security issues; however, many attacks were inherited from IPv4, which harm IPv6 networks. Those attacks affect both IPv4 and IPv6 networks. This paper explains and analysis the common threats in IPv4 and IPv6, security threats which introduced by new features of IPv6, and transition threats.

Keywords IPsec · IPv6 · Network security · IPv6 security issues · Transition mechanisms

1 Introduction

Internet Protocol version 4 (IPv4) is the first version of Internet protocol which has been used widely. It deployed at 1981. It demonstrated roughly easy implementation, robust, and interoperable. But, the growth of Internet causes new requests which IPv4 does not have the capacity to satisfy all users around the world. Most important problems are shortage of address, address configuration, security, etc. To remove these problems, Internet Protocol Version 6 (IPv6) was produced. Internet protocol version 6 is known as the next generation of IP. The development of IPv6 was integrated in 1997 [1] and standardized in 1998 by the IETF [2]. IPv6 represents many features to improve the performance of IPv4. IPv4 address length uses 32 bits. IPv6 address provides 128-bit length [3]. It generates 3.4 * 1038 unique

A. Shiranzaei (✉) · R.Z. Khan
Department of Computer Science, Aligarh Muslim University, Aligarh, India
e-mail: atena.shiranzaei@gmail.com

R.Z. Khan
e-mail: rzk32@yahoo.co.in; rzkhan.cs@amu.ac.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_5

addresses. Over 1027 globally unique addresses to every individual on the earth in the year 2050 can be made available by the increased address space [4]. As well as it eliminates NATing and allows every TCP/IP devices to acquire a public address. End-to-end communication is supported by IPv6. This allows the development of network applications like multimedia and VoIP. In IPv4, when a mobile device changes its location, then it will lose its IP address and whatever it has done so far. To eliminate this limitation, IPv6 brings a new feature which is named "mobility." This feature uses MIPV6 with handover, hierarchical mobility, and faster routing. IPv6 provides two types of IP address configuration, which are stateful and stateless auto-configuration. Stateful auto-configuration generates an IP address by using DHCPv6. Stateless auto-configuration uses network prefix and hardware address to obtain the IP address. In stateless auto-configuration, the key player is neighbor discovery protocol (NDP). NDP is defined in RFC 4861 [5]. The function of NDP is similar to ARP in IPv4 [6]. After configuration of IP address, NDP is used by a node for discovering other nodes that are in the same link. NDP allows the node to maintain neighbor reachability through discovering routers and gateway devices. Internet Control Message Protocol version 6 (ICMPv6) contains Neighbor Discovery Protocol messages, which are provided for performing diagnostics, reporting errors, and carrying multicast membership [7]. Those messages are Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA), and redirect message.

The rest of paper is organized as follows: second section presents IPsec in details. Third section discussed security threats in IPv4 and IPv6 networks. Fourth section concentrates on specific threats on IPv6. Fifth section presents the security which is related to transition mechanism.

2 IPsec

The IP security is used for making secure communications on IP networks by various security services. It protects the data is traveling among public or private IP network. IPsec provides (1) Data confidentiality: the packets are encrypted before transmission. (2) Data integrity: probably the data of packets has been changed during transmission. This function makes ensure that the data is free-altered. (3) Data origin authentication: the source of origin packet is authenticated by data origin authentication. (4) Anti-replay: it discovers and rejects the duplicated packets to prevent replay attacks. (5) Access-control to service or system [7]. IPsec comprises two security protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). Authentication header provides data integrity, authentication, and anti-replay service. Confidentiality is not provided by AH, it means that the data is sent without encryption. Hence, the data is readable but the modification is not allowed. In IPv6, the authentication header should be located before all headers which are processed at the destination node [8]. Encapsulating Security Payload provides data integrity, authentication, anti-replay service, and

confidentiality [9]. ESP protects only the data or IP payload which is being delivered. ESP must be placed behind the headers need to be processed by intermediate nodes. IPsec defines two securing traffic modes: transport mode and tunneling mode. Transport mode uses AH or ESP header to encrypt the IP payload. Transport mode is used for communication between two endpoints like client, server, etc., in Tunnel mode, the payload and IP headers are encrypted by IPsec. It protects the whole IP packet by AH or ESP. Tunnel mode is used when the traffic should pass via a security gateway.

For secure communication between two parties, they should agree with a form of encryption which is supposed to be used. For accomplishing this task, IPsec architecture involves key exchange and key management protocol [6]. IPsec connection's end systems should agree on the authentication algorithm and key, and the way that how the keys are going to be changed as well as updated overtime. IPsec provides IKE to define key exchange mechanism [6].

AH and ESP headers contain Security Parameters Index (SPI) field. This is a 32-bit number that is used to identify a particular Security Association (SA). SA is like an agreement between two parties regarding how to protect information during communication. As it mentioned earlier, it identifies which SA should be used to check the security of the received packet [8].

3 Common Security Threats in IPv4 and IPv6 Networks

3.1 Sniffing Attacks

Sniffing attacks are a device or a program which capture the data being sent via a network. The sniffing target is stealing password, email text, and files in transfer.

3.2 Application Layer Attacks

One of the most common attacks is application layer attacks. This type of attacks is present in both IPv4 and IPv6. Application layer attacks directed to the application server by making a fault in the operating system of network or application, then the attacker is able to delete, add, read, modification of data, introduce virus, etc.

3.3 Flooding Attacks

The procedure of this type of attacks is flooding a huge number of network traffic to a host or network devices, then the target is not able to process and becomes out of service or unavailable.

3.4 Rogue Devices

Rogue devices are some devices like laptop, switch, router, DNS server, DHCP, or wireless access point. These devices are introduced into the network, but they are not authorized.

3.5 Man-in-the-Middle Attacks

In this type of attack, the data is sent from source to destination without data origin authentication, the data is sent by user is grabbed by attacker. Attacker is able to monitor and read the data. Then user receives the data from attacker.

4 IPv6 Specific Security Threats

4.1 Reconnaissance Attack

The target of reconnaissance is the first step of attack. Attacker gains essential information regarding victim network by reconnaissance attacks. Attacker grabs essential information regarding victims such as hosts, interconnection in the network, and network devices. Hacker starts attacks by ping probes to find IP addresses which are in use in targeted network, after that it starts port scan. Some software is provided to perform these actions such as NMAP, HalfScan6, and Storbe [8]. Reconnaissance can be done by checking DNS, checking public looking glasses, checking registries, checking Routing Arbiter DataBase (RADB), using popular search engines, and checking traceroute discovery to finding hosts takes a lot of time because the subnets of IPv6 are extremely large (it is 64 bits be default); therefore, attacker must make 264 probes, that many scanning software do not have an ability to scan an IPv6 subnet, in such a way, there are some multicast addresses have been used which helps attacker together some resources from the victim network.

4.2 Hop-by-Hop

Hop-by-hop is one type of headers in IPv6. It is processed by the routers which should be visited by packet to reach the destination. This header is located before all headers in extension header. It might involve number of options and each may appear several times with different sizes. Thus, an attacker can make DoS attack by manipulating inconsistent options [10]. If an IPv6 packet consists a lot of options so that the packet could be in a problem because the options of packet should be looked by every routers and if all routers get affected by DoS attack, then the transmission of packet will be a trouble. In addition, Router Alert option is a potential security issue. It causes performance difficulty for a router that receives a large number of packets with Router Alert hop-by-hop option [6]. Because the router should look closer at the content of packet header so it consumes about all resources. But the resources should be preserved for important tasks [6].

4.3 Routing Header Attacks

7Routing header is a list of one or more intermediate nodes which a packet should visit them until it reaches the destination. Therefore, the address of destination is replaced at each layer-3 hop which processes routing header and the source of packet will be the final destination node. Routing header attacks reroute and redirect traffic [11] before it reaches the destination intermediate nods. It causes the destination node thinks that the traffic was forwarded by intermediate node [10, 11]. Routing Header 0 (RH0) and Routing Header 1 (RH1) are two types of routing header. RH0 is used for source routing indication, and RH1 is used for mobile IPv6 [6].

4.4 Fragmentation Header Attacks

Internet protocol packet transmission delivers an Internet protocol packet from source to destination. For carrying large amount of data, it is more appropriate to send a few large packets than many small packets. The capability to transmit packets is defined by Maximum Transmission Unit (MTU). If the size of packet is bigger than MTU, it should be broke by fragmentation. Fragmentation is used for breaking the packet into defined capability of transmit packet and sent separately. Fragmentation header in IPv6 deals with some security vulnerability which is not in IPv4. The first one occurs when the fragment overlap is not specified in RFC 2460. It helps attackers to bypass the filtering, and the second one is the value of fragment identification field which is predictable [10].

4.5 ICMPv6 and Multicast

ICMPv6 is used to report errors occurred in processing packets and to perform Internet layer functions. IPv4 block ICMP messages to provide security in IPv4. However, there are some ICMPv6 message which should not be blocked. These messages are related to some important mechanisms like NDP and path MTU discovery mechanisms. As the result, to proper network operation, some ICMPv6 messages should be allowed. ICMPv6 allows some messages to be sent to multicast address. Attacker can use this fact and modify a message directed to multicast addresses. In this way, attacker receives information to find key systems on which to target attacks [6, 7].

5 Security Issues Related to Transition Mechanism

The quite migration from IPv4 to IPv6 is impossible due to a large number of users in many IPv4 environment, and there are many techniques for migrating from IPv4 to IPv6 or for supporting their coexistence [9]. Those techniques are dual stack, traffic tunneling, and protocol translation.

5.1 Dual Stack

The most popular mechanism to migrate from IPv4 to IPv6 is dual stack. It involves two protocol stacks, IPv4 and IPv6 protocol stacks. Both IP versions are able to coexist on the same network. And all hosts as well as network devices run IPv4 and IPv6 protocol stacks. In dual stack, when a client is interested to connect to a server, first it sends a request to DNS server to find the address of server. The list of addresses is replayed to the client, then it selects the address to connect the server (IPv6 address is selected by default). The main drawback of dual stack is that most of operating systems uses IPv6 by default and IPv6 security policies are not forced. Thus, the attacker can launch and then attack. And another drawback is dual stack hosts which are accessible to local IPv6 attacks even a network does not run IPv6.

5.2 Tunneling

Tunneling is another transition mechanism. According to Fig. 1, IPv6 packets are allowed to transfer through an IPv4 cloud to an IPv6 host in another cloud. This method requires each tunnel end points should support both protocols (IPv4 and IPv6).

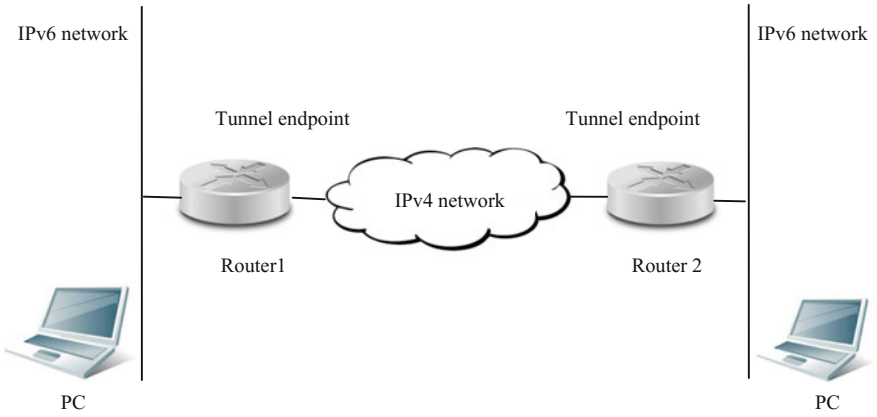


Fig. 1 How tunneling works

So, the end points can be configured as dual stack. Figure 1 depicts how tunneling mechanisms work [12].

Tunneling mechanisms are threatened by some attacks while IPv6 security methods are without authentication, confidentiality, and integrity [13]. One type of attack is Tunnel injection which makes an attacker as a legitimate user to inject traffic in the tunnel by spoofing internal IPv6 and external IPv4 addresses [6]. The next attack is Tunnel sniffing. In this case, attacker sniffs the IPv4 routing path then he can control the tunnel of IPv6 and execute man-in-the-middle attacks. Moreover, the data without knowledge of legitimate user can be redirected [13].

5.3 NAT-PT

Network address translation protocol translation allows communication between native IPv4 hosts and native IPv6 hosts [14], as well as vice versa. NAT-PT device is located at the boundary of IPv4 and IPv6 networks. This device involves Application Level Gateway (ALG). ALGs rewrite IPv6 addresses to IPv4 addresses. This mechanism is not appropriate when dual stack or tunneling can be used. NAT-PT slows down packet flow and exploits some capabilities of both protocols. The attacks which exploit NAT-PT are reflection attacks and DoS attacks.

6 Conclusion

IPv6 is the next generation of Internet protocol. Everyday IPv6 is accepted and used more and more via global. IPv6 provides many features which improves the functionality and security functions over network. Despite IPv6 brings new security functionalities, it also raises new security challenges which has presented in this paper. IPsec is a mandatory field provided by IPv6 which increases authentication, integrity, and confidentiality. IPsec offers better security; however, it is not able to eliminate the security problems all over. In this investigation, we highlighted various existing attacks in IPv6. These attacks are surveyed and investigated deeply. In this paper, we discussed about IPv6 protocol, IPsec, the common threats in both IPv4 and IPv6, IPv6 specific security threats, and the issues which are relevant to transition methods.

References

1. Shiranzaei, A., Khan, R.Z.: A Comparative Study on IPv4 and IPv6. Int. J. Adv. Inf. Sci. Technol. (IJAIST) **33**, 6–19 (2015)
2. Turiel, A.: IPv6: new technology, new threats. Netw. Secur. **8**, 13–15 (2011). doi:10.1016/S1353-4858(11)70085-X
3. Shiranzaei, A., Khan, R.Z.: Internet protocol versions—a review. In: 2nd International Conference on "Computing for Sustainable Global Development", pp. 11–15 (2015)
4. Radhakrishnan, R., Jamil, M., Mehfuz, S., Moinuddin, M.: Security issues in IPv6. In: 3rd International Conference on Networking and Services pp. 0–5, ICNS (2007). http://doi.org/10.1109/ICNS.2007.106
5. Simpson, W.: RFC **2461**, 1–97 (2007)
6. Hogg, S.: IPv6 security (2011)
7. Caicedo, C.E., Joshi, J.B.D., Tuladhar, S.R.: IPv6 security challenges. Computer **42**(2), 36–42 (2009). doi:10.1109/MC.2009.54
8. Minoli, D., Kouns, J.: Security in an IPv6 environment (2009)
9. Žagar, D., Grgić, K., Rimac-Drlje, S.: Security aspects in IPv6 networks—implementation and testing. Comput. Electr. Eng. **33**(5–6), 425–437 (2007). doi:10.1016/j.compeleceng.2007.05.008
10. Supriyanto, Murugesan, R. K., Ramadass, S.: Review on IPv6 security vulnerability issues and mitigation methods. Int. J. Netw. Secur. Its Appl (IJNSA), 4, 173 (2012)
11. Shah, J.L., Parvez, J.: Security Issues in Next Generation IP and Migration. Networks **17**(1), 13–18 (2015). doi:10.9790/0661-17131318
12. Hagen, S. (2006). IPv6 essential
13. Chasser, J.M.: Security concerns in IPv6 and transition networks. Inf. Secur. J.: A Global Perspect. **19**(5), 282–293 (2010). doi:10.1080/19393555.2010.514653
14. Srisuresh, P. (2000). No Title, 1–21

Authors Biography

Ms. Atena Shiranzaei is a research scholar in the Department of Computer Science; Aligarh Muslim University, Aligarh, India. She joined her Ph.D. course on 28-05-2014. Her research interest includes Networking and Security. She did Bachelor Degree in Computer Software from Islamic Azad University of Zahedan, Iran. M.Sc. in Computer Science from Osmania University, Hyderabad, India.

Dr. Rafiqul Zaman Khan is presently working as an Associate Professor in the Department of Computer Science at Aligarh Muslim University, Aligarh, India. He received his B.Sc. Degree from M.J.P. Rohilkhand University, Bareilly, M.Sc., and M.C.A. from A.M.U. and Ph.D. (Computer Science) from Jamia Hamdard University. He has 20 years of teaching experience of various reputed International and National Universities viz King Fahad University of Petroleum and Minerals (KFUPM), K.S.A., Ittihad University, U.A.E., Pune University, Jamia Hamdard University and AMU, Aligarh. He worked as a Head of the Department of Computer Science at Poona College, University of Pune. He also worked as a Chairman of the Department of Computer Science, AMU, Aligarh. His research interest includes Parallel and Distributed Computing, Gesture Recognition, Expert Systems, and Network Security. He has published about 50 research papers in International Journals/Conferences. He is the member of Advisory Board of International Journal of Emerging Technology and Advanced Engineering (IJETAE), Editorial Board of International Journal of Advances in Engineering and Technology (IJAET), International Journal of Computer Science Engineering and Technology (IJCSET), International Journal in Foundations of Computer Science and Technology (IJFCST) and Journal of Information Technology, and Organizations (JITO).

Moderating Bandwidth Starvation Using PQDWRR

Arti Singh, Ambar Yadav and Aarti Gautam Dinker

Abstract High throughput and reduced delays are the basic necessities of next-generation networks which use multimedia applications (ftp, videoconferencing, VoIP, etc.). In order to make the network function efficiently, these necessities should be improved and maintained at a desired level. This provides a better quality of service (QoS) to the traffic which ensures a maximum customers' satisfaction. These basic necessities are provided by using the appropriate scheduler mechanism at the router. The data are handled in the form of packets in the required manner. Presently, the scheduler mechanisms which are used have still some drawbacks in them. Therefore, they cannot handle the packets in a proper way in next-generation networks which are real-time applications. In this paper, various existing scheduling techniques are explained like First-In First-Out (FIFO), Priority Queue (PQ), Fair Queue (FQ), and Deficit Weighted Round Robin (DWRR). A new scheduling technique is introduced in this paper which is a combination of PQ and DWRR. Then a comparative analysis of the scheduling technique, i.e., PQ and proposed scheduling technique, i.e., PQDWRR is performed. PQDWRR technique provides a better QoS than the existing queuing mechanisms.

Keywords DWRR · PQ · WLAN · PQDWRR · QoS

1 Introduction

From the mid-90s to till date, telecommunication networks are undergoing rapid growth and change in terms of infrastructure, services, and customers. The nature of service is evolving from TDM voice calls, email, and Web services to enhanced

A. Singh (✉) · A.G. Dinker
School of Information and Technology, Gautam Buddha University, Greater Noida, India
e-mail: allimpdocuments@gmail.com

A. Yadav
Department of Electronics and Communication, HBTI, Kanpur, India

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_6

multimedia services such as videoconferencing, mobile presence management, and IPTV.

The major difficulties faced in the next-generation networks are the increasing expectations of end users and demands with volatile bandwidth and delay-boundary demands from new higher data rate services, such as high-definition television (HDTV), video teleconferencing, multimedia streaming, voice over IP (VoIP), file transfer, and online gaming. Thus, multimedia applications have experienced an explosive growth.

The various parameters of QoS are packet loss, delay, jitter, and throughput. Different queue scheduling algorithms have been proposed in establishing a better QoS of the network. But still there are some limitations of these mechanisms which need to be moderated in order to further improve the performance of network.

Queueing is not only something to store it but also to process it. In a network, when data packets are sent out from a source to destination, they enter a queue and at the router queue scheduling algorithms are used. Scheduling algorithms decide which packets from that queue should be processed. Different types of scheduling algorithms like Priority Queue, Round Robin, Weighted Fair, and Weighted Round Robin (WRR) can be implemented.

Priority Queuing (PQ) algorithm is a more popular technique used in the NGN for delay sensitive traffic. PQ classifies packets according to their preferences and thus provides the best service to the highest priority packets. But simultaneously the lower priority packets are starved of bandwidth. Thus, a large amount of bandwidth is wasted. For this reason, we proposed a new scheme for bandwidth allocation to lower priority traffic (LPT) and simultaneously increasing throughput by using a combination of PQ and DWRR mechanism.

The combination of PQ + DWRR algorithms provides low delay for low-priority queues and high throughput of the network. If the high-priority class does not exceed the available output capacity other classes are serviced as classical DWRR. There is also the possibility to limit the priority queue to a fixed rate. Then the queue serviced using PQ will use the bandwidth required by the traffics assigned to this queue up to this limit. Other packets will remain waiting in the queue, and other queues will be serviced using DWRR. When setting an accurate value of the limit we can avoid starvation of lower priority queues.

Next section of the paper describes the QoS parameters which are responsible for a network performance. Section 2 presents the various queue scheduling mechanisms FIFO, PQ, FQ, and DWRR along with their limitations. In Sect. 3, the related work is explained. The proposed algorithm is described in Sect. 4. Simulation results and their analysis are presented in Sects. 5 and 6, respectively. Finally, conclusion and future scope are presented in Sect. 7.

2 Queue Scheduling Mechanisms

Queuing scheduling mechanisms are required mainly during congestion. While congestion, there is no sequence of packet transmission through router.

The various queuing mechanism can include:

(a) First-In First-Out (FIFO) Queuing,
(b) Priority Queuing (PQ),
(c) Fair Queuing (FQ),
(d) DWRR Queuing.

2.1 FIFO Queuing

The basic queue scheduling mechanism is First-In First-Out (FIFO). In this, no configuration is required at the interface of the router. The packets are forwarded in the order in which they arrive at the router. In case the queue becomes saturated, new packets are dropped (tail drop).

2.2 Priority Queuing (PQ)

Priority Queue discriminates between the packets according to their priority. Packets are mainly classified into four priority queues as high queue, medium queue, normal queue (the default queue), and low queue. Packets of high-priority queue are processed first by the router.

2.3 FQ

Fair Queuing (FQ) provides equal access to the bandwidth to the packets of each queue. Each queue gets equal bandwidth irrespective of its traffic flow pattern and its packet size. As the number of queues increases, the amount of bandwidth provided to each queue decreases.

2.4 DWRR

In Deficit Weighted Round Robin (DWRR) algorithm, scheduler determines the number of bytes in the packet at the head of the queue by visiting each non-empty queue. The deficit counter is incremented by the quantum value. When the size of the packet is greater than the variable deficit counter, then the scheduler moves to service the next queue, and when the size of the packet is less than the variable deficit counter, then the deficit counter is reduced by the number of bytes in the packet and the packet is transmitted at the output port. The scheduler continues to dequeue the packets and decrements the variable deficit counter by the size of the transmitted packet.

3 Related Work

In communication networks, QoS is an important factor which affects the network performance. There are various QoS parameters like packet loss, delay, jitter, and throughput. Throughput is one of the important parameters of QoS which can be provided efficiently by scheduling mechanisms.

Zahirul and Rashed [1] discussed a comparative analysis of basic and hybrid queuing methods and their impact on the VoIP traffic delay within the network. Based on the simulation results, it was proved that PQ-CBWFQ was a low-latency queuing scheme and a proper solution for a VoIP time-sensitive application. Suardinata and Suanmali [2] proposed a new queuing scheduling algorithm based on PQ which reduced delay in VoIP network.

Bhaskaran and Parthasarathy [3] developed a priority queuing model which reduced the execution time of the jobs. A comparative analysis was made by Bhalla et al. [4] between FIFO and PQ scheduling mechanism.

Patel and Dalal [5] proposed a novel scheduling scheme called Controlled Priority Queuing (CPQ) with well-known RR and DRR algorithms. It was observed that CPQ throughput was found better in case of RTPS and NRTPS service class. Kochher and Chopra [6] presented various scheduling algorithms and concluded that they provide different services and with different QoS parameters with their queuing types to provide better QoS for end-to-end implementation.

4 Proposed Algorithm

The Bandwidth Starvation problem is eliminated by applying the proposed algorithm. In this scheme, a threshold is set for the bandwidth. The proposed algorithm is only practiced if the bandwidth consumed by higher priority traffic is less than 60%.

The simulation tool used in this work is NS-2.35 [7].

The pseudocode of the proposed algorithm is as follows:

Step 1 SET Threshold Traffic = 60%.
Step 2 IF Higher Priority Traffic < 20% THEN Packet Priority Technique = DWRR.
Step 3 ELSE IF 20% < Higher Priority traffic < 40% THEN Packet Priority Technique for Lower Priority Traffic more than Threshold value along with Higher Priority Traffic = DWRR Technique.
Step 4 ELSE THEN Packet Priority Technique = Dynamically Varying the Weights.
Step 5 ENDIF.
Step 6 ENDIF.

5 Simulations

According to our simulation scenario in Fig. 1, source 1 (blue packet) is provided a low priority, whereas source 2 (red packet) is provided a higher priority. Here, Priority Queue Scheduling is applied at the core router [8, 9]. The packets of node 0 are not forwarded until the queue of packets of node 1 is empty. Thus, the packets of node 0 have Bandwidth Starvation as they do not get the bandwidth until the queue of node 1 is empty.

In Fig. 1, it is seen that blue packets are stopped at the core router where they form a queue. They are not allowed to use the bandwidth. Hence, Bandwidth Starvation problem arises for packets of low-priority traffic (blue packet) in Priority Queue [10, 11]. In Fig. 2, by applying PQ + DWRR scheduling mechanism at the core router, it is seen that low-priority packets (blue packets) have the bandwidth provided to them.

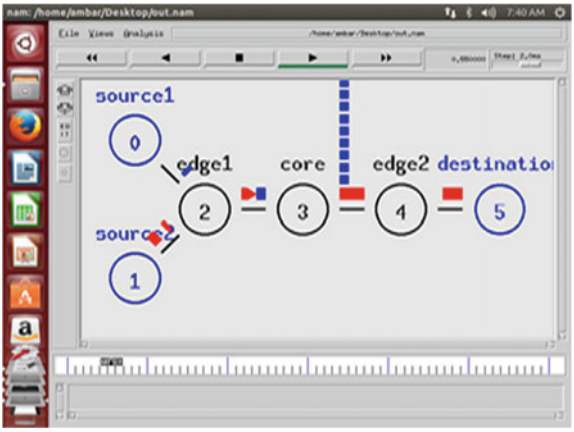


Fig. 1 Traffic generated when existing scheduler mechanism is used at router

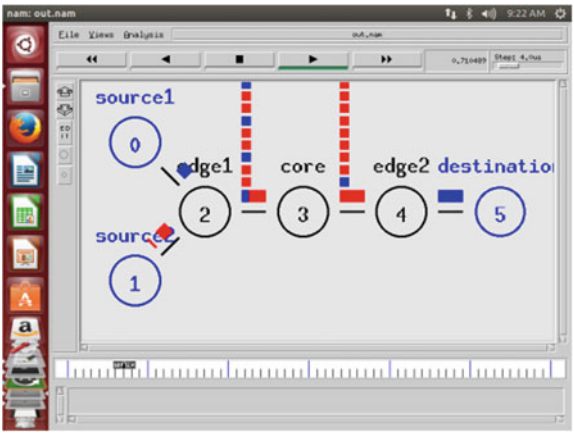


Fig. 2 Traffic generated when proposed scheduler mechanism is used at router

In our scheme, the threshold traffic at the core router is set at 60%. If the higher priority traffic is greater than threshold traffic, then only PQ scheduling mechanism is applied. But if the higher priority traffic is below threshold traffic, then the higher priority packets are sent according to the PQ while lower priority packets are sent according to the DWRR mechanism.

In our scenario, the higher priority traffic is less than threshold traffic. So, the blue packets are forwarded according to the DWRR mechanism as shown in Fig. 2. Hence, Bandwidth Starvation problem is resolved.

6 Result Analysis

Simulation scenario runs for 5 s. Here, the throughput is examined for the link between node 4 and node 5. Node 5 is the destination node.

In Figs. 3 and 4, the throughput is measured in terms of bits/TIL (time interval length, i.e., seconds). In the graph, throughput is increasing at a constant rate till 1 s. Then afterward, it acquires a constant rate which is equivalent to nearly 4.02×10^5 bits/s. Thus, it can be seen that much of the bandwidth is wasted here.

In proposed scheme, the throughput is again increasing at a constant rate till 1 s and then becomes constant. But in this case, the constant value is around 5×10^5 bits/s. Thus, much of the bandwidth is utilized as compared to the existing scheduling mechanism.

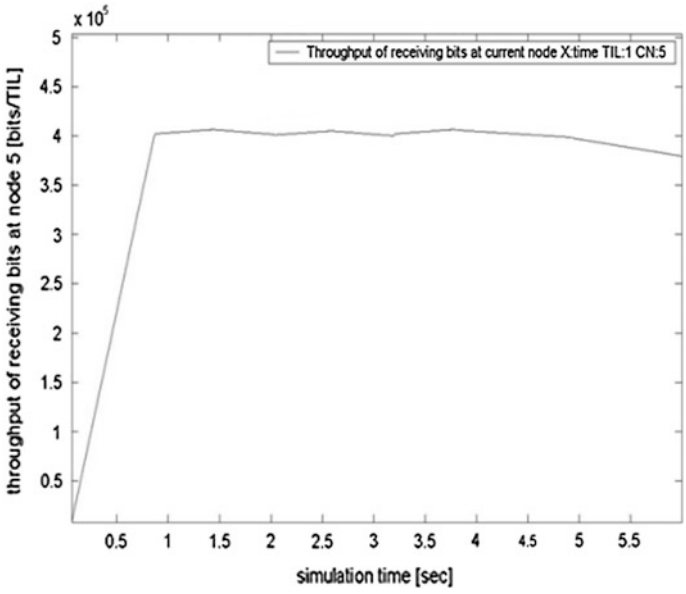


Fig. 3 Throughput of received bits at node 5 (proposed scheduler mechanism)

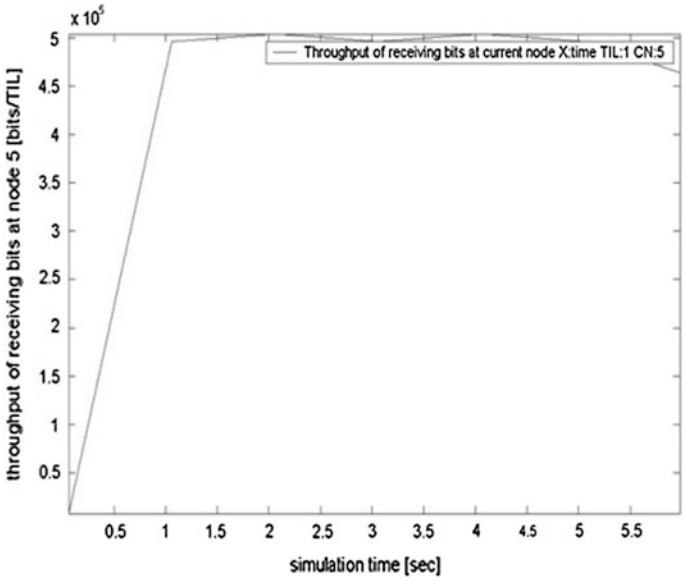


Fig. 4 Throughput of received bits at node 5 (existing scheduler mechanism)

Table 1 Result analysis

Parameter	Existing scheduling mechanism	Proposed scheduling mechanism
Bandwidth starvation	Exists	Does not exist
Throughput (10^5 bits/s)	4.02	5.05

The results of the above parameters can be analyzed now comparatively for both the scheduler mechanisms in Table 1.

7 Conclusion and Future Scope

In this paper, various queuing mechanisms have been studied. PQ and PQDWRR are comparatively analyzed. PQDWRR performs the best among other queue scheduling mechanism [12, 13]. PQ gives the best result for real-time application, but suffers due to Bandwidth Starvation problem. So PQDWRR gives good performance in optimizing network performance. These queuing mechanisms are applied in the network layer. In future, we will concentrate our work in the application layer which will further decrease the delay and hence optimize the network performance.

References

1. Islam, M.Z., Rashed, M.M.G.: A comparative analysis on traditional queuing and hybrid queuing mechanism of VoIP's QoS properties. Int. J. Adv. Innov. Thoughts Ideas
2. Suardinata, K.A.B., Suanmali, N.: Comparison process long execution between pq algorithm and new fuzzy logic algorithm for VoIP. Int. J. Netw. Secur. Its Appl. (IJNSA) **3**(1) (2011)
3. Bhaskaran, R., Parthasarathy, V.: An improved performance analysis of priority scheduling algorithm in modified ad hoc grid layer. Int. J. Distrib. Parallel Syst. (IJDPS) **3**(1) (2012)
4. Bhalla, S., Monga, K.S., Malhotra, R.: Optimization of computer networks using QoS. Int. J. Eng. Res. Appl. (IJERA), **2**(3), 2276–2281 (2012)
5. Patel, Z.M., Dalal, U.D.: Implementation and analysis of downlink scheduling for IEEE 802.16 using controlled priority queuing. In: Proceedings of International Conference on Advances in Computing Advances in Intelligent Systems and Computing, vol 174, pp. 399–406 (2012)
6. Kochher, R., Chopra, V.: Scheduling algorithm and IP queue types in WLAN. Int. J. Sci. Emerg. Technol. Latest Trends **1**(1), 24–30 (2012)
7. http://www.h3c.com; http://isi.edu.ac.in
8. Iyanda, J.N.: Analysis and evaluation of quality of service (QoS) router using round robin (RR) and weighted round robin (WRR). IISTE J. **5**(2) (2015)
9. Balogh, T., Medvecky, M.: Average delay and queue length model for WRRPQ. WSEAS Trans. Commun. **13** (2014)
10. Zhang, M.: Optimization of inter-network bandwidth resources for large-scale data transmission. J. Netw. **9**(3) (2014)
11. Mancas, C., Mocanu, M.: QoS optimization in congested multimedia networks. IEEE (2013)
12. Dhanal, R.J.: Queue-based traffic regulation on wireless 802.11 networks. Int. J. Innov. Res. Comput. Commun. Eng. **1**(4) (2013)
13. Kilkki, K.: Differentiated services for the Internet. Macmillan Technical Publishing, pp. 139–149 (2002)

Coordinate-Based Void Detection and Recovery in WSN

Shalu and Amita Malik

Abstract Wireless sensor networks (WSNs) have always been a fascinating area of research among the research fidelity. Random deployment, energy constrains, dynamic topology, physical damage may create the void areas in WSN where there is no coverage at all. This paper makes an attempt to identify and recover such regions based on the coordinate values of the nodes along the void region. The coverage on the right and bottom coordinate points at a distance equal to the sensing radius is calculated by comparing these points with the nearby sensing nodes coordinate values without broadcasting any message. The uncovered points can be clustered to give the rough estimates of the void region dimensions and location in the network. The recovery can be made by deploying more number of nodes in the estimated area.

Keywords WSN · Hole · Neighbor · Boundary

1 Introduction

With the recent advancements in the industry of integrated digital electronics circuits and micro-electro-mechanical systems (MEMS), the wireless sensor networks (WSNs) have become an important electronic component in our life. WSN is the collection of spatially dispersed sensors which senses some physical environmental conditions (like temperature, light, humidity, pressure, speed, and direction) and sends the collected information at some central location for further processing. A WSN consists of high density of randomly deployed nodes which can be static or dynamic in nature based on application. Due to the random deployment scheme and

Shalu (✉)
Computer Science Department, MSIT, New Delhi, India
e-mail: er_shalu2003@yahoo.co.in

A. Malik
Computer Science Department, DCRUST, Murthal, Haryana, India
e-mail: amitamalik.cse@dcrustm.org

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_7

battery limitations, a sensor network can be affected by some anomalies. One of the anomalies is the void problem in the sensing area under observation. The sensing area is required to be covered by some adequate number of nodes for the proper functioning of the network. Moreover, the nodes in the sensing area should be capable of covering the entire region. The situations occurring due to the absence of adequate number of sensor nodes may lead to the creation of the holes [1]. There is no direct provision of identification of such regions. A lot of energy can be saved if we can use the geometrical information of the nodes in the network. This paper is based on the identification of such void regions in the network using the coordinate information of the nodes near to the boundary of the said region.

The remaining part of the paper is organized as follows. Section 2 presents related work performed by other authors on the same problem. Section 3 presents the proposed algorithm used in the research. Section 4 shows various results and observations followed by conclusion and future scope in Sect. 5.

2 Related Work

There are lots of algorithms to find the void regions in the WSNs. Wang [2] used the Voronoi graph-based method for identification of void regions and recovers such areas by using mobile nodes. The mobility of nodes is achieved at the sake of consumption of large amount of energy. Li [3] in their research paper proposed the void recovery using only connectivity information. The algorithm works for the networks without location information. Gulling et al. [4] in their paper proposed the idea of using the Voronoi diagrams to find the coverage hole. The algorithm is suitable for the small networks but is not suitable for the larger networks. Ghrist [5] proposed the homology-based void area detection. The method is centralized, but is not suitable for larger networks. Algebra-based topology is used for getting the connection diagrams by Kanno [6] and can be applicable to the sensor nodes not having their coordinate positions information. Xin et al. [7] presents a boundary arc node discovery along the void boundary. Another interesting algorithm is path density-based algorithm given by Corke [8]. The algorithm is based on the path density across the neighbors of a dead sensor node. The algorithm can efficiently detect coverage holes remotely, but it requires more time and power consumption for detecting coverage holes in practice. Pearl and Amita [9] elaborated a very extensive survey on the various types of holes. They suggested the strengths and shortcomings of already existing coverage hole detection algorithms. On the basis of the study of the above-discussed research work, the paper is proposed titled as coordinate geometry-based void detection and recovery algorithm. The proposed paper aims to make cluster of the linear points along x- and y-axes around the boundary nodes. The detailed information is discussed in the upcoming sections.

3 Proposed Algorithm

This paper is based on certain assumptions that the sensors are distributed randomly [10]. There are certain terms used in the algorithm like sensing neighbor, intersection points, and critical points of intersection [1].

Definitions

Sensing Radius: The radius of the circular sensing area around a sensor node is called as sensing radius denoted by rs.

Sensing Neighbor: The sensing neighbors of a given node S are the set of all the nodes that are within a distance of twice the sensing range.

Intersection Point: For any two sensor neighbors the circular sensing disks intersect each other at two points called intersection points.

Critical Points of intersection: The intersection points which are not covered by any other sensor node in the network are called as critical points (Cp).

Is_covered: It is a function that takes a point as argument and returns true if the point is covered by one or more sensing neighbors.

Input

1. The location information of all nodes.
2. The coordinates information of the area under consideration, i.e., WXmin, WXmax, WYmin, Wymax.

Algorithm

This paper aims to identify the rectangular void area around critical point of intersection. The steps in proposed algorithm are as follows:

1. Collect the Location Information (i.e. X and Y Coordinates) of all the nodes in the sensor network.
2. Calculate the intersection points of the nodes with neighboring nodes.
3. Out of intersection points calculated at step 2 find all the critical points of intersection Cp and sort them in accordance with the Y Coordinate.
4. Calculate the Void region using the following steps:

   4.1 While not processed all the points in Cp begin
   4.2 Select a point P from Cp having Px and Py as the X and Y Coordinates respectively.
   4.3 Set the initial values of the parameters as Ymin=Ymax=Py, Xmin=Xmax=Px, Xright= Xleft=Px and Ydown=Py.
   4.4 Calculate the rightmost uncovered point as
   4.5 While not Is_covered(Xright, Ydown) and (Xright <WXmax) do Xright= Xright +rs.

4.6 Store the rightmost uncovered point Xright to update Xmax.
4.7 Calculate the rightmost uncovered point as
4.8 While not Is_covered(Xleft, Ydown) and (Xleft> <WXmin) do Xleft=Xleft - rs.
4.9 Store the leftmost uncovered point Xleft to update Xmin.
4.10 If not Is_covered(Px, Ydown) and (Ydown> <WYmin)
4.11 Set Ydown = Ydown-rs. Set Ymin = Ydown. Set Set Xright = Xleft = Px and goto 4.4
4.12 end of while loop at 4.1.
4.13 Plot a rectangle indicating the desired void region at the Coordinates Xmin, Xmax, Ymin, Ymax as calculated in step 4.1 to 4.13.

4 Simulation and Results

Our algorithm is simulated using MATLAB 7.0 nodes that are deployed randomly. The number of initially deployed nodes is around 10.

In Fig. 1, the initial set up of randomly deployed nodes is shown. The x-axis shows the x coordinate of nodes. The y-axis shows the y coordinate of nodes. The nodes are randomly deployed in the region under consideration. There are clearly shown void regions where there is no coverage. These areas have no single node present and the void is required to be recovered. In the next diagram, the critical boundary points are identified.

In Fig. 2, the intersection points have been identified and stored in the list and then critical intersection points are identified. Once this information is completed, next is to perform the recovery of such void regions. Figure 3 shows the coverage is improved by inserting the nodes on the calculated positions.

It is clearly shown that the void region is covered by the newly deployed nodes. The most important point of concern is to identify the proper location for the newly

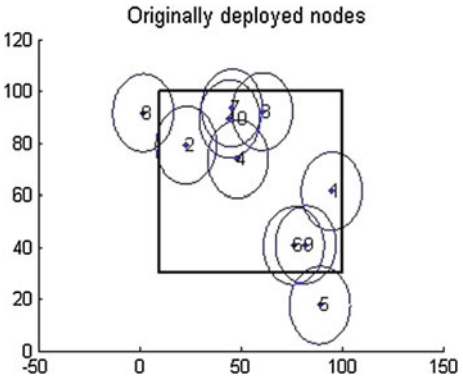


Fig. 1 Originally deployed nodes indicating avoid regions

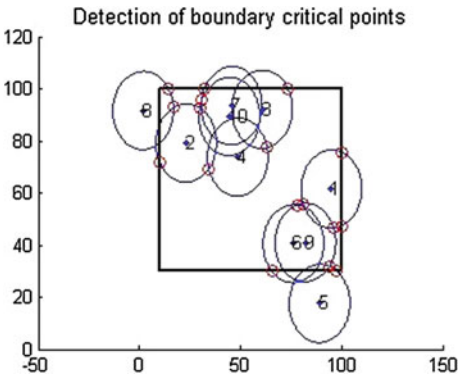


Fig. 2 Identification of the intersection points

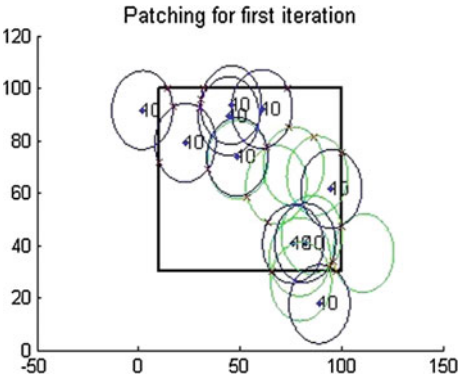


Fig. 3 Void recovery after patching

deployed nodes. The proposed algorithm clearly shows that the void locations have been identified and the nodes can be patched at suggested location to recover the void region.

5 Conclusion and Future Scope

This is clearly shown that the algorithm calculates the void region in the network by getting the location information of all the nodes. The algorithm locates the void region by checking the coverage of the points at one hop distance in the left, right, and the down position. The algorithm calculates the void region without passing messages in between the nodes but it can give enough good estimates about the uncovered regions. The patching using more sensor nodes helps to recover the void region. The work can be further extended to remove the redundant nodes in the void areas.

Acknowledgements The authors would like to thank University Grants Commission (UGC), Government of India, India, for providing the financial assistance for this work under grant number 41-626/2012 (SR).

References

1. Yan, F., Martins, P., Decreusefond, L.: Connectivity-based distributed coverage hole detection in wireless sensor network. In: Proceedings of Global Telecommunications Conference, pp. 1–6 (2011)
2. Wang, G., Cao, G., Porta, L.: Movement—assisted sensor deployment. In: Proceedings of Twenty-Third Annual Joint Conference of IEEE Computer and Communications Societies (2004)
3. Li, X., Hunter, D.K.: 3MeSH for full sensing coverage in a WSN without location awareness. In: London Communications Symposium (2005)
4. Guiling, W., Guohong, C., La Porta, T.: Movement assisted sensor deployment. In: INFOCOM 2004. In: 23rd Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 4, pp. 2469–2479 (2004)
5. Ghrist, R., Muhammad, A.: Coverage and hole-detection in sensor networks via homology. In: Proceedings of the 4th international symposium on information processing in sensor networks, pp. 254–260 (2005)
6. Kanno, J., Buchart, J.G., Selmic, R.R.: Detecting coverage holes in wireless sensor networks. In: Proceedings of 17th Mediterranean Conference on Control and Automation, pp. 452– 457 (2009)
7. Yue, X., Zhenjiang, Z., Yun, L.: A coverage hole detecting algorithm in wireless sensor networks. J. Convergence Inf. Technol. **6**(9, 201), 159–168 (2011)
8. Corke, P., Peterson, R., Rus, D.: Finding holes in sensor networks. In: Proceedings of the Workshop on Omniscient Space: Robot Control Architecture Geared Toward Adapting to Dynamic Environments at ICRA (2007)
9. Antil, P., Malik, A.: Hole detection for quantifying connectivity in wireless sensor networks: a survey. J. Comput. Netw. Commun. **2014**(969501), 11 (2014). doi:10.1155/2014/969501
10. Ma, H.C., Sahoo, P.K., Chen, Y.: Computational geometry based distributed coverage hole detection protocol in wireless sensor network. J. Netw. Comput. Appl. **34**, 1743–1756 (2011)

Optimized QoS-Based Node Disjoint Routing for Wireless Multimedia Sensor Networks

Vikas Bhandary, Amita Malik and Sanjay Kumar

Abstract Wireless multimedia sensor networks (WMSNs) are applicable in a wide range of areas including area monitoring, video surveillance. But due to unreliable error-prone communication medium and application-specific quality of service (QoS) requirements, routing of real-time multimedia traffic in WMSNs poses a serious problem. The proposed routing protocol, optimized QoS node disjoint (OQND) routing, tries to improve the performance of network by considering both average end-to-end delay and hop count for making route decisions and optimizing various resources such as energy, bandwidth. OQND finds two types of routes, and it can be restricted to find node disjoint routes only. Simulation results show that OQND outperforms ad hoc on-demand multipath distance vector (AOMDV) routing protocol.

Keywords Wireless multimedia sensor networks · Wireless sensor networks QoS routing · Latency-constrained routing · Real-time routing

1 Introduction

The advancements in various technologies have led to the creation of tiny and low-cost multimedia devices like video cameras and microphones, which can easily be integrated to form a sensor node. These devices are used in special types of wireless sensor networks (WSNs), called WMSNs [1, 2]. Using multimedia sensors in WSN, drastically improves event description capability of sensor networks [3].

V. Bhandary (✉) · A. Malik
Deenbandhu Chhotu Ram University of Science and Technology, Murthal, India
e-mail: vksbhandary@gmail.com

A. Malik
e-mail: amitamalik.cse@dcrustm.org

S. Kumar
SRM University Haryana, Sonepat, India
e-mail: skmalik9876@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_8

WMSN can sense and transfer scalar data as well as multimedia data, i.e. image, audio and video streams, in real time as well as non-real time. WMSNs inherit all the characteristics of WSN.

Routing in WMSNs is a complex problem due to application-specific quality of service (QoS) requirements and ad hoc nature of WSNs. Real-time streaming requires guaranteed end-to-end transmission delay and high bandwidth. Generally, multipath transmission is used in order to fulfil such high bandwidth requirements. On-demand routing protocols specifically designed for WSN (e.g. AODV [4], DSR [5], TORA [6]) focus only on energy efficiency, so they cannot be used for routing in QoS-bounded WMSNs due to dissatisfactory performance [7]. Latency-constrained routing protocols or multiconstrained routing protocols or location-based routing protocols (e.g. SPEED [8], MMSPEED [9], DARA [10], TPGF [11]) are more suitable for delivering multimedia streams in WMSNs due to timely delivery and less bandwidth consumption. In order to maintain QoS in WMSNs, routing protocols need to transfer extra routing packets to exchange network state information with all nodes.

The paper proposes an optimized QoS-based node disjoint (OQND) routing protocol. OQND is an on-demand routing protocol, which tries to find multiple node disjoint paths in a single route discovery. The novelty of OQND lies in the fact that it uses destination-initiated path metric update procedure, which helps in providing desired QoS. OQND uses five metrics in order to reduce end-to-end delay and hop counts and hence reduce the total number of transmission.

The remainder of the paper is organized as follows. Section 2 reviews work related to this paper. In Sect. 3, the proposed routing protocol is discussed in detail. Section 4 compares the performance of OQND with AOMDV [12]. Section 5 presents conclusion.

2 Related Work

On-demand routing protocols in sensor networks specifically maintain only needed routes and try to reduce routing overhead. Various on-demand routing protocols have been proposed in the literature (e.g. AODV [4], DSR [5], TORA [6]). In recent years, disjoint routing has been given much attention because of various applications, such as software testing [13], integrated circuit layout design [14]. Various on-demand disjoint routing protocols (e.g. split multipath routing (SMR) [15, 16], AOMDV [12]) have been proposed in the previous literature.

AOMDV [12] is an enhanced version of well-known routing protocol called ad hoc on-demand distance vector (AODV) [4] routing. It cannot be used in QoS-bounded WMSNs, but it is a multipath routing protocol. It finds multiple paths between source node and destination node in every route discovery. It reduces inter-nodal coordination overheads and ensures the disjointness of alternate paths. Thorough analysis of AOMDV [12] performed in [17] shows that its performance degrades with increase in packet rate.

3 Optimized QoS-Based Node Disjoint Routing

The optimized QoS-based node disjoint (OQND) routing protocol is an on-demand multipath QoS-based routing protocol for time-critical data streams. The protocol attempts to find multiple node disjoint routes to the destination and evaluates those paths to find best possible next hop using five routing metrics, i.e. average delay, average energy, average packet drop, average used bandwidth and hop count. Each intermediate node stores complete path to the destination, so that it can be used whenever needed. The protocol implements a destination-initiated update mechanism which updates route metrics after a constant interval of time.

OQND uses four different types of packets RREQ, RREP, UPD and RERR. RREQ packet is broadcasted by the source node when it does not have route to the destination node. RREP message is sent by destination node, which contains path information and accumulated route metrics. The destination node broadcast UPD message, which accumulates updated values of path metrics to make the right decision for selecting next hop. RERR packet is sent by an intermediate node to the source node, to inform when a node has stopped working.

OQND protocol tries to find node disjoint paths between source and destination. Two different types of paths which are discovered using OQND are a set of node disjoint paths and a set of split multipath. However, the algorithm can be restricted to find node disjoint paths only, by setting non-disjoint route maximum count equal to one.

A. *Data Structures*

- *Routing table*: Routing table used by the OQND protocol stores node list and route metrics parameters. Routing table is designed to store multiple paths. Table 1 shows sample routing table.
- *Broadcast table*: Broadcast table is used to store the route request broadcast message information such as source ID, broadcast Id and counter field. These entries are flushed after fixed interval of time.
- *Neighbour table*: Neighbour table is used to keep track of all the neighbours of a node. It stores only two fields: neighbour ID and expire.

B. *Algorithm*

The algorithm used by OQND routing protocol consists of six stages, namely initialization, route discovery, data transmission, path metrics updation, route maintenance and error recovery.

Initialization phase: In this stage, nodes initialize various constants and store neighbour ID received from HELLO messages. HELLO messages are sent by a node repeatedly after a constant interval of time. HELLO message stores node ID, timestamp and various other fields. HELLO messages are used to maintain the link status between two nodes.

Table 1 Sample routing table used in OQND

Destination	Flag	Route count	Valid paths	Route list						
				Node list	Hop count	Average energy	Average bandwidth	Average drop	Average delay	Expire

Route discovery: This stage starts, when a node needs to send packets to the other node. Steps taken in this stage by a node are:

- The node first checks whether it already has a route to destination. If yes, then node starts transferring the packets.
- If not, then the node sends a RREQ message with sum of energy of each traversed node, sum of packets dropped by each traversed node and sum of used bandwidth of each traversed node among other fields.
- The intermediate node checks whether it has already received the packet. If the received packet is new, then it inserts the sender's ID into a broadcast table and sets count attribute to 1. The node then checks whether hop count is greater than maximum hop count possible. If hop count is larger than MAX_SR_LENGTH, then the packet is dropped. MAX_SR_LENGTH is a constant defined in initialization phase, which denotes maximum source route length.
- After this, the node checks whether it is the intended receiver or not. If it is not the intended receiver, then it adds its ID into node list and adds the energy, packet drop and used bandwidth attributes in RREQ packet fields.
- If the current node is the intended receiver, then it checks whether the path is already present in the table or not. If the path is not present, then node adds a route entry in the table and sends a RREP message with the acquired information, to the previous hop on the node list.
- When the intermediate node receives a RREP message, it checks whether it has same path in their table, and if it is not present, then the RREP message is forwarded to the previous hop in node list.
- Finally, when the source node receives the RREP message, it checks whether the path is present or not. If it is not present, then it adds the path.

Data transmission: After path set-up, the data is transferred to the next hop. Selection of next hop, in QoS routing, is a complex issue. In OQND routing protocol, a factor α is calculated based on routing metrics: average path delay, average used bandwidth, average path energy, average packet drops and hop count [19]. This value is used to select next hop for the transmission of real-time data packets. The path with a maximum value of α is selected for data transmission. This decision is made at every node on the selected path.

This phase also performs various other operations such as α calculation, route validity check and next hop selection. Firstly, the route validity check procedure updates the status of paths in the table. After that, α for all valid paths is calculated using Eq. (1). Maximum value of α denotes the best possible path for desirable quality of services.

$$\alpha = c1 * \left(1 - \frac{\text{average delay}_i}{\text{maxdelay}}\right) + c2 * \left(1 - \frac{\text{average bandwidth}_i}{\text{maxdandwidth}}\right) + c3 * \left(\frac{\text{average energy}_i}{\text{maxenergy}}\right) + c4 * \left(1 - \frac{\text{average drops}_i}{\text{maxdrops}}\right) + c5 * \left(1 - \frac{\text{hop count}_i}{\text{maxhop count}}\right) \tag{1}$$

where $c1$, $c2$, $c3$, $c4$, $c5$ are constants which can be adjusted to get the preferred quality of service. This method used for path evaluation is the modified version of method proposed in [20]. In order to select path with minimum average delay, the ratio of average path delay and maximum delay is subtracted by unity, and then it is multiplied by constant c1; this makes the final value of α positive. Similar method is repeated for all adversely affecting route metrics.

Path metrics updation: OQND uses destination-initiated path metrics updation process, where each destination node is supposed to broadcast UPD message which contains destination ID, node list, hop count, sum of energy of each traversed node, sum of packets dropped by each traversed node, sum of used bandwidth of each traversed node and timestamp.

In order to reduce transmitted UPD messages, only those paths are updated which were used during a specific time interval. The path is updated only if the reverse path in the UPD message matches the path in routing table, otherwise the message is discarded. UPD message updates routing metrics which are needed to calculate α. The steps followed by nodes in this stage are:

(i) After a fixed interval, destination broadcasts UPD message by adding its node ID and updated values of other attributes such as energy, packet dropped, used bandwidth in UPD packet.
(ii) When an intermediate node receives UPD message, it first checks whether it is not outdated message by checking its timestamp attribute. If it is valid, then the node again checks whether it contains the path which is being updated. If the node contains path in the route table, then it again checks whether there is need to broadcast this message. If the current node is still intermediate node, then updated UPD message is broadcasted, which contains node ID in node list, and current node's attributes are added to UPD message.
(iii) When UPD message is received by the source node, it simply updates routing metrics and deletes the packet.

Route maintenance: OQND protocol uses HELLO messages and UPD messages to maintain the routes. HELLO messages are sent to maintain the link status between two nodes. If a node is unable to send a HELLO message within the maximum allowable time, then the node is considered faulty, and error recovery mechanism is used to remove the error.

UPD messages are used to maintain the validity of paths. After some fixed interval of time, the path becomes invalid and needs updated route metrics for calculation of α; therefore, invalid paths are not considered for data transmission. After receiving UPD message, node updates the route metrics and sets itself as valid route. So that next time, updates route metrics are used to evaluate the route.

Error recovery: Whenever a node detects a link failure, a procedure is called to handle the error. This procedure collects information about the faulty nodes and deletes the path in order to cause less packet drops. Now the node checks whether local route repair is possible, if it is possible, then it sends a RREQ message and

repairs the route otherwise it sends RERR message to report that a link is down. So source node checks whether the number of routes to destination is still equal to minimum required multipaths. If not, then the source node broadcasts a new RREQ message and starts route discovery.

4 Simulation Environment

OQND is implemented in Network Simulator 2 (NS2) version 2.35. OQND is compared with pre-established AOMDV [12] protocol.

4.1 Simulation Parameters

Table 2 shows simulation parameters. For performing simulation of OQND, two different scenarios are used to test the performance of OQND on different conditions. In scenario I, total number of nodes is fixed to 26, but the simulation time is varied from 10 to 300 s. Scenario I results will show how the performance of OQND will change with respect to time. In scenario II, total simulation time is fixed to 60 s, but the total number of nodes is varied. Scenario II results will show how the performance of OQND will change with respect to number of nodes. The size of sensing area is fixed to 2550 × 100 m square scenario I and 4072 × 100 m^2 scenario II. The nodes are assumed to be static. At the MAC layer, 802.11 is used. The transmission rate is set to 0.5 Mbps.

Table 2 Parameters of simulation environment

Simulation parameters	Scenario I	Scenario II	Simulation parameters	Scenario I/II
Sensing area size	2550 × 100 m^2	4072 × 100 m^2	Transmission rate	0.5 Mb
Propagation	Two-ray ground		Initial energy	1000 units
Antenna	Omnidirectional antenna		Idle power	1.0 units
MAC	802.11		Receiving power	1.0 units
Simulation time	10–300 s	60 s	Transmission power	2.0 units
Number of sensors	26	10–50	Packet size	1000 Kbits
Sensor mobility	Static		Tool used	NS2 (version: 2.35)
Transmission range	250 m			

4.2 Performance Metric for Simulation

The performance of both the scenario is measured in terms of average end-to-end delay, total hops, routing overhead and total energy consumed.

4.3 Simulation Results

Figure 1 shows average end-to-end delay versus simulation time graph. The total number of nodes in scenario I is fixed to 26, and the simulation time is varied, whereas Fig. 2 shows average end-to-end delay versus number of nodes graph. In both the simulation scenarios, OQND has outperformed AOMDV routing protocol. This is because of the reason that OQND selects next hop on the basis of α. The path which has maximum value of α gets selected every time when the node needs to forward data packets.

Figure 3 shows total hop versus simulation time graph, whereas Fig. 4 shows total hop versus number of nodes graph. In both the simulation scenarios, OQND has outperformed AOMDV routing protocol. In scenario I, the total hops are increasing at a constant rate. But in scenario II, total hops for OQND are less than total hops of AOMDV, but it is fluctuating. When new nodes are added, the total number of hops increases. This increase may affect the value of α, and the path with more hop count gets selected because of its low average end-to-end delay value. Therefore, total hops may increase or decrease, because of change in topology, but its value always remains less than total hops in AOMDV.

Figure 5 shows total routing packets versus number of nodes graph. In simulation scenario II, OQND transfers more routing packets as compared to AOMDV routing protocol. This is due to the reason that OQND broadcasts UPD packets to get up-to-date routing metrics values. Therefore, generally QoS-based routing protocols use more routing packets as compared to other protocols.

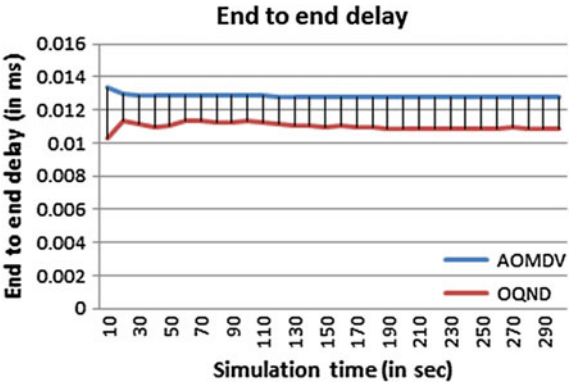


Fig. 1 Average end-to-end delay for scenario I

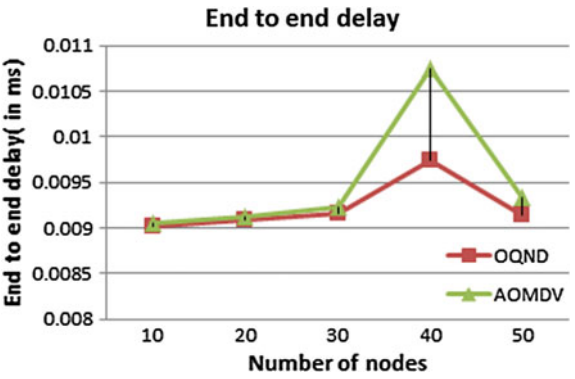


Fig. 2 Average end-to-end delay for scenario II

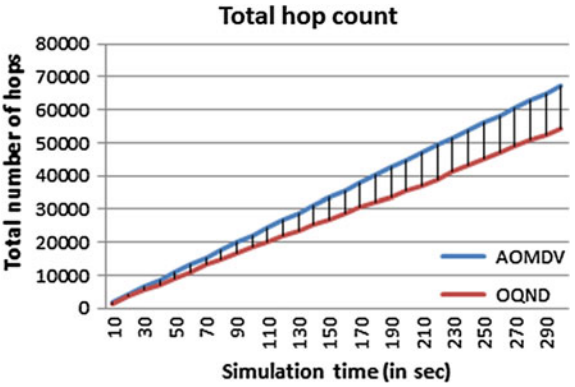


Fig. 3 Total hops graph for scenario I

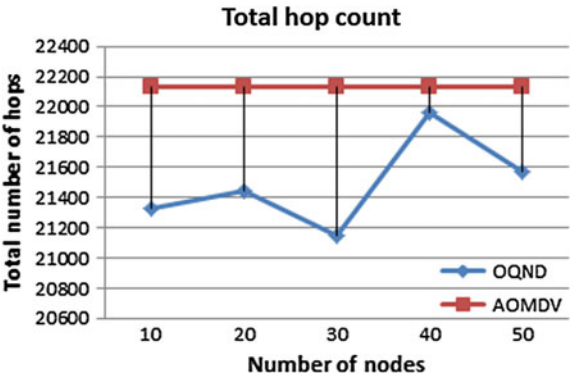


Fig. 4 Total hops graph for scenario II

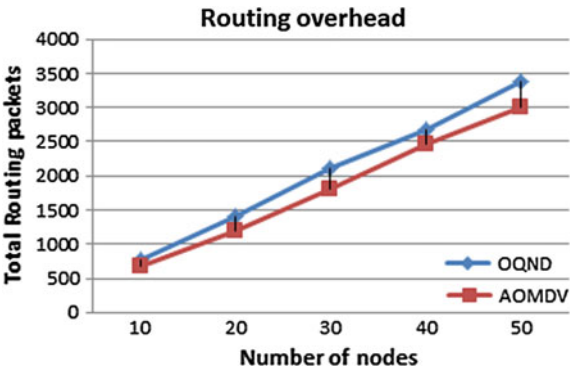


Fig. 5 Routing overhead graph for scenario II

5 Conclusion

Owing to the increase in applicability of WMSNs, researchers are more inclined to persuade research on WMSN routing protocols, in order to guarantee QoS and enhance energy efficiency of the system as a whole. We proposed a new approach to improve the efficiency of WMSN by implementing new method of routing, which consider average end-to-end delay and hop count for routing decision-making. OQND was implemented and analysed with AOMDV. The analysis was done on two different scenarios. The results clearly show that OQND minimizes the end-to-end delay and total hops. But OQND has too high routing overhead, due to unavoidable UPD message broadcast.

References

1. Akyildiz, I.F., Melodia, T., Chowdhury, K.R.: A survey on wireless multimedia sensor networks. Comput. Netw. **51**(4), 921–960 (2007)
2. Kumar, S., Dave, M., Dahiya, S.: ACO based QoS aware routing for wireless sensor networks with heterogeneous nodes. Emerging Trends in Computing and Communication, pp. 157–168. (2014)
3. Zhang, L., Hauswirth, M., Shu, L., Zhou, Z., Reynolds, V., Han, G.: Multi-priority multi-path selection for video streaming in wireless multimedia sensor networks. In: Ubiquitous Intelligence and Computing, pp. 439–452. Springer (2008)
4. Perkins, C.E., Royer, E.M.: Ad-hoc on-demand distance vector routing. In: Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100 (1999)
5. Johnson, D., Maltz, D.: Dynamic source routing in ad hoc wireless networks. Mob. Comput. 153–181 (1996)
6. Park, V.D., Corson, M.S.: A highly adaptive distributed routing algorithm for mobile wireless networks. In: Proceedings of INFOCOM '97, vol. 3, (1997)
7. 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 (2012)

8. He, T.H.T., Stankovic, J.A., Lu, C.L.C., Abdelzaher, T.: SPEED: a stateless protocol for real-time communication in sensor networks. In Proceedings of 23rd International Conference on Distributed Computing Systems, 2003, pp. 46–55 (2003)
9. Felemban, E., Lee, C.G., Ekici, E.: MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. IEEE Trans. Mob. Comput. **5**(6), 738–753 (2006)
10. Razzaque, M.A., Alam, M.M., Mamun-Or-rashid, M., Hong, C.S.: Multi-constrained QoS geographic routing for heterogeneous traffic in sensor networks. IEICE Trans. Commun. **E91-B**(8), 2589–2601 (2008)
11. Shu, L., Hauswirth, M.: Geographic routing in wireless multimedia sensor networks (2008)
12. Marina, M.K., Das, S.R.: Ad hoc on-demand multipath distance vector routing. Wirel. Commun. Mob. Comput. **6**(7), 969–988 (2006)
13. You, L., Fan, J., Han, Y., Jia, X.: One-to-one disjoint path covers on alternating group graphs. Theoret. Comput. Sci. **562**, 146–164 (2015)
14. Guo, Y., Kuipers, F., Van Mieghem, P.: Link-disjoint paths for reliable QoS routing. Int. J. Commun. Syst. **16**(9), 779–798 (2003)
15. Lee, S.J., Gerla, M.: split multipath routing with maximally disjoint paths in ad hoc networks. In: ICC 2001 IEEE International Conference on Communications. Conference Record (Cat. No. 01CH37240), vol. 10 (2001)
16. Nasipuri, A., Castaneda, R., Das, S.R.: Performance of multipath routing for on-demand protocols in mobile ad hoc networks. Mob. Netw. Appl. **6**(4), 339–349 (2001)
17. Kute, V.B., Kharat, M.U.: Analysis of quality of service for the AOMDV routing protocol. Eng., Technol. Appl. Sci. Res. **3**(1), 359 (2012)
18. Hop count [online]. Available: http://www.infocellar.com/networks/ip/hop-count.htm
19. Khiavi, M.V., Jamali, S., Gudakahriz, S.J.: Performance comparison of AODV, DSDV, DSR and TORA routing protocols in MANETs. Int. Res. J. Appl. Basic Sci. **3**(7), 1429–1436 (2012)
20. Rani, A., Dave, M.: Weighted load balanced routing protocol for MANET. In: Proceedings of the 2008 16th International Conference on Networks, ICON 2008 (2008)

Review of Industrial Standards for Wireless Sensor Networks

Seema Kharb and Anita Singhrova

Abstract Wireless sensor networks (WSNs) are the today's most interesting and exciting research area. It is supporting a large number of application domains and now planning for supporting wide industrial applications. As the requirements for industrial application domain are different from other WSN applications, hence, various standards are defined by some industrial alliances like HART, Zigbee to meet the requirements of industrial domain. This paper discusses various WSN standards specific for industrial domain along with their applications and limitations. It also lists and discusses various unsolved challenges in IEEE 802.15.4e industrial standard. Finally, a comparative analysis of these standards is provided and the research gaps are discussed.

Keywords Wireless sensor networks · Standards · TSCH · TSMP · Industrial automation

1 Introduction to Wireless Sensor Network (WSN)

WSN consists of sensor devices that are densely deployed in hostile environments to gather sensory information from temperature, pressure, humidity, wind direction and speed, illumination, sound and vibration intensity to pollutant levels, chemical concentration, and many more. Each sensor node has memory, communication device, controller, power supply and sensor/actuator that provide the capability to sense, process, and communicate data.

Initially, the sensor nodes have limited computing power and operate on batteries and are used only for military applications [1, 2]. But with the advancements in technology, wireless communication and batteries WSN eliminate the

S. Kharb (✉) · A. Singhrova
Computer Science & Engineering Department, DCRUST, Murthal, India
e-mail: seema016.phd@gmail.com

A. Singhrova
e-mail: nidhianita@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_9

need of human presence in dangerous and hostile environment, in addition to providing facility to monitor and collect data from these environments. Also they reduce the cost incurred due to placement and maintenance of wires. Therefore, the application domain of WSN is spreading from military applications to factory automation, disaster management (like wildfire), biodiversity mapping (observing wildlife patterns), intelligent buildings, home automation, industrial automation, facility management, machine surveillance, medicine, healthcare, traffic control and surveillance, environment monitoring [3, 4], underwater monitoring, and many more.

WSN used in industrial applications known as IWSN (Industrial WSN) [5] and is different from traditional WSN in terms of requirements. A general WSN has the requirement of small node size, low-cost low-power consumption, self-configuration, scalable, robust, adaptable, reliable secure, efficient channel utilization, and QoS support. In addition to these requirements, IWSN has the following requirements of interoperability, resistance to noise, coexistence, link reliability, deterministic latency, support for multiple source and sinks, service differentiation, predictive behavior, application-specific protocols and facility for data aggregation [6–8]. According to International Society of Automation, there are six classes of industrial systems, viz. safety systems (like fire alarm systems hence delay intolerant), closed loop regulatory and supervising systems (these are based on feedbacks with a difference whether feedbacks or measurements are periodically required or not), open loop control systems (WSN is used only for data collection and is human operated), next is alerting system (like temperature monitoring), and finally information gathering systems.

This paper focuses on various wireless standards that are specific for industrial applications of WSN like WirelessHART [9], ISA 100.11a [10], Zigbee Pro [11], 6LoWPAN [12], IEEE 802.15.4e [13].

Section 2 discusses briefly various industrial standards for WSN with detailed comparative analysis in Sect. 3 followed by conclusion in Sect. 4.

2 Industrial Standards for WSN

The basic requirements for an IWSN are low power, high administration, reliability, maintenance, easy deployment, and low cost. Considering these goals various standards like WirelessHART [9], ISA 100.11a [10], Zigbee Pro [11] have been established by various working groups like HART Communication Foundation (HCF) [14], Zigbee Alliance [15], and International Society of Automation [16]. All these standards are based on IEEE 802.15.4 [17]. This paper also discusses a MAC layer amendment to IEEE 802.15.4 for industrial applications known as IEEE 802.15.4e [13].

2.1 WirelessHART

WirelessHART is the industrial standard developed by HART Communication Foundation (HCF) based on HART communication protocol and IEEE 802.15.4-2006 for process automation. The protocol stack of WirelessHART as shown in Fig. 1a implements physical layer of IEEE 802.15.4-2006 with operational frequency of 2.4 GHz and modulation technique by combining frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) for efficient data transmission. At link layer, it extends the functionality of IEEE 802.15.4 MAC by adding the time slots of 10 ms and using Time Synchronized Mesh Protocol (TSMP) [18] that uses TDMA (Time Division Multiple Access) for channel access and reduces the number of collisions. For efficient channel usage, channel blacklisting (blacklisting the channels which exhibit large interference) and channel hopping are used. Network layer is responsible for routing and security. The network manager is responsible for creating, maintaining, and scheduling the network. WirelessHART employs redundant routing at the network layer. The basic features of WirelessHART, include self-healing and self-organization, robust, simple to implement, interoperable with other HART devices, energy efficient, scalability, can be achieved either by using multiple WirelessHART gateway or multiple access point, always on security, used for both star and mesh topologies, time synchronization.

Besides the various benefits of WirelessHART, it suffers from some drawbacks or limitations. Firstly, it is used for specific application domain of process automation and is not operable with other IEEE 802.15.4-based standards. Secondly, only dedicated links are present, and there is no provision related to shared links. Finally, the scheduling algorithm used is centralized scheduling algorithm.

<table>
<tr><th></th><th>(a)</th><th>(b)</th><th colspan="3">(c)</th><th colspan="2">(d)</th></tr>
<tr><td>Application layer</td><td>HART protocol</td><td>Services for appli cation layer & no process control applications</td><td colspan="3">Zigbee device objects</td><td colspan="2">Application layer</td></tr>
<tr><td>Session layer</td><td>Not defined</td><td>Not defined</td><td colspan="3">Not defined</td><td colspan="2">Not defined</td></tr>
<tr><td>Presentation layer</td><td>Not defined</td><td>Not defined</td><td colspan="3">Not defined</td><td colspan="2">Not defined</td></tr>
<tr><td>Transport layer</td><td>End to end reliability</td><td>UDP</td><td colspan="3">Not defined</td><td>UDP</td><td>ICMP</td></tr>
<tr><td rowspan="2">Network layer</td><td rowspan="2">Self healing network</td><td rowspan="2">6LoWPAN & IPv6</td><td rowspan="2">Security mgt.</td><td rowspan="2">Network mgt.</td><td rowspan="2">Routing mgt.</td><td colspan="2">IPv6</td></tr>
<tr><td colspan="2">Adaption layer</td></tr>
<tr><td rowspan="2">Data link layer</td><td>TSMP for time synchronization</td><td>Mac extension for channel hopping, time syn & graph routing</td><td colspan="3" rowspan="2">IEEE 802.15.4-MAC</td><td colspan="2" rowspan="2">IEEE 802.15.4-MAC</td></tr>
<tr><td>IEEE 802.15.4-MAC</td><td>IEEE 802.15.4-MAC</td></tr>
<tr><td>Physical layer</td><td>IEEE 802.15.4 PHY</td><td>IEEE 802.15.4 PHY</td><td colspan="3">IEEE 802.15.4 PHY</td><td colspan="2">IEEE 802.15.4 PHY</td></tr>
</table>

Fig. 1 Protocol stack of **a** WirelessHart. **b** Zigbee. **c** ISA 100.11a. **d** 6LoWPAN

2.2 ISA 100.11a

ISA 100.11a developed by ISA 100 working group provides robust and secure communication for process automation application domain [10]. ISA defines a protocol stack for ISA 100.11a which is built on top of IEEE 802.15.4 standard having same PHY (physical layer) features as WirelessHART, i.e., operates on 2.4 GHz frequency with DSSS and FHSS modulations. The data link layer extends the capability of IEEE 802.15.4 MAC features by supporting frequency hopping, graph routing and time slotted, time domain multiple access (a combination of TDMA and CSMA) that reduces interference and noise. Various channel hopping techniques are used by ISA 100.11a like slow, fast, and fixed hopping. The network and transport layers support the features of 6LoWPAN, IPV6, and UDP, respectively. The protocol stack of ISA 100.11a is depicted in Fig. 1b. It provides the following features that make it suitable for IWSN, i.e., determinism, reliability, security, support for multiple protocols and applications, flexibility, work in both star and mesh topologies, coexistence with other wireless technology, larger address space, configurable time slots.

Limitations. Following are some limitations of ISA 100.11a. It is not interoperable with other IEEE 802.15.4-based devices. There is high implementation cost and slow hopping results in increased power consumption as receiver remains on for a longer time.

2.3 Zigbee

Zigbee is the standard created by Zigbee Alliance suitable for control and monitoring applications. It is also built on top of IEEE 802.15.4 standard with 2.4 GHz operating frequency and can form star, mesh, and cluster tree topologies. It defines its own network layer for different networking capabilities, and application layer provides a framework for application development and communication. Two implementation options for a Zigbee standard are provided. One is for smaller networks (Zigbee) and other for larger networks (Zigbee Pro). The protocol stack is shown in Fig. 1c. The salient features of Zigbee can be summarized as supports star, cluster tree and mesh network topologies, robust, large number of nodes can be added, long range, easy deployment, supports low to medium data rates, low power and low cost, self-organizing and self-healing.

Limitations of Zigbee can be counted as they are interoperable with only Zigbee devices. There is no frequency diversity. They are prone to security threats. Static channel usages increase interference and hence delay. They support no path diversity, i.e., if a path is broken new path must be set up. It follows a random process for address assignments. Further, due to ad hoc on-demand distance vector (AODV) routing protocol there is lack of scalability. Finally, it also lacks energy-saving mechanism.

2.4 6LoWPAN

6LoWPAN, an acronym for IPv6 over low-power wireless personal area network, is developed by international engineering task force (IETF) and based on IEEE 802.15.4 PHY and MAC layer to integrate TCP/IP with WSN. It is developed for embedded applications that require deployment of large number of sensor nodes to cover a large geographic area with low cost, power, and computations. The integration of IPv6 provides Internet connectivity at low data rates with low duty cycle. The basic features of 6LoWPAN are smaller packet size, header compression, and fragmentation, scalable due to adopting adaption layer, supports mobility, and easy network management due to IPv6, reliable, and reduce latency. Its protocol stack is depicted in Fig. 1d. **Some limitations of 6LoWPAN are** they are more prone to link failures. Interference is present, and providing end-to-end security is still an open issue.

2.5 IEEE 802.15.4e

IEEE 802.15.4e [13] is the MAC layer amendment in the IEEE 802.15.-2011 [17] standard and released in 2012 to provide better opportunities for industrial applications and to become compatible with Chinese WPAN. Main ideas are taken from WirelessHART and ISA 100.11a. Major amendments in 802.154e can be categorized in two broad classes.

MAC Behavior Modes. These are specified for support of specific industrial application domains. These are briefed below.

TSCH, i.e., Time Slotted Channel Hopping is defined for application domains such as process automation. It takes some of its features from TSMP [18] like time slots (supports both dedicated and shared links) that are helpful in distributed transmission, time synchronization, multiple access. The main concepts of TSCH are the use of *slot frames* for data transmission and receiving, channel hopping to mitigate the effect of multipath fading and interference, a modified CSMA/CA algorithm for collision avoidance with in a slot.

But there are many drawbacks of TSCH like the maximum duration for a time slot is not specified by the standard also there is lack of proper Advertisement protocol. The author in [19] specifies a random advertisement protocol for Internet of Things (IoT) which is a generalization protocol specified in [20]. How the additional communication resources (slot frames and links) are allocated to devices. This issue is left for upper layers so in this concern some work is done in [21] and [22] where the authors specified a centralized (TASA-TSCH) and a decentralized algorithm to deal with this problem. But the issues with centralized and decentralized algorithms remain the same that is of static topology and mobility. *Deterministic and Synchronous Multi-channel Extension (DSME)* is designed specifically for industrial and commercial applications with stringent timeliness and

reliability requirements. It supports the features of multi-superframe (combination of superframes), multi-channel, and group acknowledgment for scalability, robustness, and flexibility. It also provides the features of distributed beacon scheduling and distributed slot selection for scalability and incorporates channel adaptation and channel hopping as channel diversity methods. The standard only explains the method of executing a schedule but it does not specify how that beacon schedule is formed and how to perform slot selection. The authors in [23, 24] represent a solution for this problem. *LLDN, i.e., Low Latency Deterministic Network* is used for applications requiring very low latency requirement (e.g., factory automation, robot control). It works in star topology only and uses beacon and assigned time slots to provide determinism. It is designed for small networks and small frames. *Radio Frequency Identification Blink (BLINK)* is used for identification, tracking, and location applications. *Asynchronous multi-channel adaptation (AMCA)* is restricted to application domains where large deployments are required *(e.*g., process automation/control, infrastructure monitoring). It works in non-beacon enabled mode. The issues with this approach are firstly, it works for single hop topology and secondly, the standard does not specify any method to determine the line quality indication (LQI) or receive signal strength (RSS).

General functional improvements. They are defined for supporting the MAC behavior modes to enhance their functionality. These are described below.

Low-energy (LE) protocol is introduced for allowing using minimal amount of energy very low duty cycle devices can send ad hoc data. There are two types of LE: coordinated sampled listening (CSL) which specifies how receiving devices periodically monitors the channel and receiver initiated transmission (RIT)—here, transmitting devices only transmit to a receiving device upon receiving a data request frame. *Information elements (IE*) are added to provide extensible MAC data transfers. These are useful in adding information to existing frame format without adding new frames. *Enhanced beacons (EB) and enhanced beacon requests (EBR*) are used to allow coordinator devices to send beacons with specifically requested data. EB is used with TSCH and DSME with relevant IEs. *The MAC multipurpose frame* provides the scalability and extensibility to allow standard to address new application needs with minimal MAC changes. *MAC performance metrics* provide upper layers with critical information on the quality of the communication links, and *FastA* reduces the time required to associate. It is optional and not defined in 802.15.4 devices.

3 Comparison of Different Industrial Standards for WSN

Table 1 compares the above-explained industrial standards [25–27] on the basis of various factors and provides an overview of their strength and limitations.

Table 1 Comparison of different industrial standards

Feature	IEEE 802.15.4e	WirelessHART	ISA 100.11a	Zigbee	6LoWPAN
Application domain	Process automation, factory automation, home automation, smart metering	Process automation	Process automation	Home automation	Internet of things and industrial monitoring
Topology	Star and mesh	Mesh, star (not recommended)	Mesh and star	Star, mesh, and cluster tree	Mesh
Physical layer	IEEE 802.15.4-2011	IEEE 802.15.4-2006	IEEE 802.15.4-2006	IEEE 802.15.4-2003	IEEE 802.15.4-2003
Operating frequency	Variable	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz
Modulation	DSSS and FHSS	DSSS and FHSS	DSSS and FHSS	DSSS and FHSS	DSSS and FHSS
IEEE 802.15.4 MAC layer mode	Both beacon enabled and non-beacon enabled	Non-beacon enabled based on TDMA	Non-beacon enabled based on TDMA and CSMA	Non-beacon enabled	Non-beacon enabled
Time synchronization	Yes	Yes	Yes	No	No
Addressing (in bits)	16 or 64	16 or 64	16, 64 or 128	16 or 64	128
Interoperability with other 802.15.4 devices	Yes	No, only with other HART devices	No, only coexistence with WirelessHART, 6loWPAN	No, only with other Zigbee devices	No
Routing protocol	N/A, applicability for higher layer	Redundant routing (source and graph routing)	Redundant routing (source and graph routing)	AODV	RPL

(continued)

Table 1 (continued)

Feature	IEEE 802.15.4e	WirelessHART	ISA 100.11a	Zigbee	6LoWPAN
Robustness	Present	Present	Present	Present	Present
Scalability	Unknown	Present either using multiple gateway or multiple access point	Present	Present	Present
Self-organization	Yes	Yes	Yes	Yes	Yes
Self-healing	Unknown	Yes using health reports	Yes	Yes	Yes
Security	N/A	Yes	Yes	Yes	Yes
Cost	Low	High	High	Low	Low
Data rate	Variable	250 kbps	Low data rates	250 kbps	20–250 kbps
Channel hopping	Yes	Yes [18]	Yes [18]	No	No
Channel blacklisting	Yes [28, 29]	Yes [18]	Yes [18]	No	No
Power consumption	Low	Low	Low	Low	Medium
Network management	Unknown	High	High	Medium	High

3.1 Research Gaps

The various research gaps that exist in these standards can be formulated as, firstly, because IEEE 802.15.4e is drafted in 2012 and provides details about physical and MAC layers only, so it provides procedure for executing a method like beacon scheduling but does not provide any algorithm to create and maintain them. Hence, there are many open issues remain unsolved till date regarding this standard. Secondly, the complete procedure for TSCH PAN Formation is specified but how the issues related to slot and link scheduling and assignment will be solved is left for upper layers. Thirdly, the advertisement protocol, i.e., how a PAN coordinator will determine the rate of advertisement and choose a suitable PAN identifier from a list of PANid is not specified. Finally, rest all the standards are interoperable with similar type of devices but they are compatible with other IEEE 802.15.4 based 219 devices.

4 Conclusion

This paper reviewed various industrial standards like WirelessHART, ISA 100.11a, Zigbee, 6LoWPAN, and IEEE 802.15.4e and compared them on various factors. Zigbee is suitable for applications that need low-power consumptions, short range, low complexity, and low data rates like chronic disease monitoring, home automation, Zigbee smart energy profile offers utility to handle demand response and provide control for load support but is not as suitable for industrial domain as other standards due to lack of determinism property, and it cannot provide QoS support for deterministic latency, and it cannot scale with large systems. Furthermore, it employs only DSSS that results in performance degradation in case of continuous noise. Similarly 6LoWPAN is the technology that offers low cost, easy deployment, and adaptability features but has comparatively high power consumption. It has its main application in Internet of Things (IoT) as it can connect to other IP-based technologies without additional routers or proxies. Therefore, HART Communication Foundation proposes WirelessHART as complete industrial solution by adding wireless interface, end-to-end reliability, secure communication and form a self-healing and self-organizing network properties to wired HART along with channel hopping and channel blacklisting features. It found its great applications in process automation and control. But again it lacks the deterministic latency feature required for commercial applications and cannot support multiple protocols. In contrast to this, ISA 100.11a is the standard that supports deterministic timing requirement needed for control applications such as reliable monitoring and alerting, predictive maintenance, condition monitoring, factory automation, asset maintenance, location services, and logistics. Hence, it is the much suitable standard but it is not backward compatible with other standards.

Although they all have same underlying principles based on IEEE 802.15.4, they are not interoperable with each other and are specific for a particular type of application domain either process automation or home automation or smart metering. Hence to overcome the issues related to these standards, IEEE task group 4 has amended IEEE 802.15.4 with the specific features of WirelessHART and ISA 100.11a and added some new features to it so that a generic standard can be formulated for industrial domain as presented it as IEEE 802.15.4e.

Acknowledgements This research has been supported by CSIR-Research Grants grant number—09/1063(0007)/2015-EMR-I.

References

1. Rahman, K.: A survey on sensor networks. JCIT **01**(01) (2010)
2. Khemapech, I., et al.: A survey of wireless sensor networks technology. In: Proceedings of 6th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (2005)
3. Romer, K., Mattern, F.: The design space of wireless sensor networks. IEEE Wirel. Commun. **11**, 54–61 (2004)
4. Akyildiz, I.F., et al.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
5. Shen, X., et al.: Wireless sensor networks for industrial applications. In: Proceedings of 5th World Congress on Intelligent Control and Automation, vol. 4, pp. 3636–3640 (2004)
6. Zand, P., et al.: Wireless industrial monitoring and control networks: the journey so far and the road ahead. J. Sens. Actuator Netw. **1**(2), 123–152 (2012)
7. Zheng, L.: Industrial wireless sensor networks and standardizations: the trend of wireless sensor networks for process automation. In: Proceedings of SICE Annual Conference, pp. 1187–1190 (2010)
8. Ajith Kumar S., et al.: An industrial perspective on wireless sensor networks—a survey of requirements, protocols, and challenges. IEEE Commun. Surv. Tutorials **16**(3), 1391–1412 (2014)
9. Chen, D., et al.: WirelessHART in a NUTSHELL. In: WirelessHART: Real-Time Mesh Network for Industrial Automation, 1st ed. Springer, New York, ch. 1–6 (2010)
10. Group, W.W.: Draft standard ISA100. 11a. In: Internal Working Draft, International Society of Automation, May 2008
11. Alliance, Z.: Zigbee specification. In: Zigbee Document 053474r13, Zigbee Alliance (2008)
12. IETF IPv6 over Low power WPAN (6LoWPAN). [Online]. Available http://datatracker.ietf.org/wg/6lowpan/documents/
13. IEEE Std 802.15.4eTM-2012: Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) (Amendment to IEEE Std 802.15.4-2011); IEEE Computer Society: New York, NY, USA, (2012)
14. http://www.hartcomm.org/
15. http://www.zigbee.org/
16. http://www.isa.org/
17. IEEE Std 802.15.4TM-2011: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs); IEEE Computer Society: New York, NY, USA, (2011)
18. Pister, K.S.J., Doherty, L.: TSMP: time synchronized mesh protocol. In: Proceedings of IASTED International Symposium on Distributed Sensor Networks, Nov 2008

19. De Guglielmo, D., et al.: A performance analysis of the network formation process in IEEE 802.15.4e TSCH wireless sensor/actuator networks. In: ISCC (2014)
20. Watteyne, T., et al.: OpenWSN: a standards-based low power wireless development environment. Trans. Emerg. Telecommun. Technol. (2012)
21. Palattella, M.R., et al.: Traffic aware scheduling algorithm for reliable low-power multi-hop IEEE 802.15.4e networks. In: Proceedings of IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications, Sydney, Australia, pp. 327–332, 9–12 Sept (2012)
22. Tinka, A., et al.: A decentralized scheduling algorithm for time synchronized channel hopping. ICST Trans. Mob. Commun. Appl. **11**, 1–13 (2011)
23. Jeon, Y.A., et al.: An adaptive superframe duration allocation algorithm for resource-efficient beacon scheduling. JIPS (2015)
24. Lee, W.Y., et al.: Distributed fast beacon scheduling for mesh networks. In: Proceedings of the 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '11), pp. 727–732, Oct (2011)
25. Lennvall, T., et al.: A comparison of WirelessHART and ZigBee for industrial applications. In: Factory Communication Systems, IEEE International Workshop, pp. 85–88 (2008)
26. Rodenas-Herraiz, D., Antonio et al.: Current trends in wireless mesh sensor networks: A review of competing approaches. Sensors **13**, 5958–5995 (2013)
27. Nixon, M.: A comparison of WirelessHART™ and ISA 100.11a. White Paper: HCF_SPEC-xxx, Preliminary A (2012)
28. Du, P., Roussos, G.: Adaptive time slotted channel hopping for wireless sensor networks. In: IEEE iCOST, Shanghai, China, 10–12 Oct 2011
29. Du, P., Roussos, G.: Adaptive channel hopping for wireless sensor networks. In: 2011 International Conference on Selected Topics in Mobile and Wireless Networking (iCOST) (2011)

Fairness and Performance Evaluation of Fuzzy-Based Resource Allocator for IEEE 802.16 Networks

Akashdeep

Abstract Intensification of mobile devices has triggered use of applications over the web. These applications even put scheduler performance of broadband wireless systems like WiMAX to test. The role of schedulers in such networks had become very challenging, and only adaptive schedulers can survive to fit in user's demands. This paper has evaluated working of dynamic fuzzy-based scheduler used for bandwidth allocation. The scheduler is implemented as component of the base station and works to grant bandwidth to traffic classes after analysis of their traffic share and quality of service parameters. The performance of proposed method is justified by drawing comparisons with established practices.

Keywords Fuzzy scheduler · WiMAX · IEEE 802.16 · QoS

1 Introduction

IEEE 802.16 is one of recent broadband wireless access standards for MANs, commercially popularized by WiMAX Forum with name of Worldwide Interoperability for Microwave Access (WiMAX) [1, 2]. WiMAX has been standardized to cater to needs of ever-growing number of applications on the web. The increase in number of these applications has been manifold because of popularity of smartphones from 122 million to 968 million in 2013 (stastica.com-2014). Resource distribution in such environments is always tedious task as pressure exerted by these multimedia-rich applications is much significant. The presence of real-time applications always tries to overpower resources of low priority non-real-time classes.

Bandwidth allocation mechanism in WiMAX has not been standardized by IEEE, and vendors can opt for any specific implementation according to their requirements. Quality of service is supported by implementing five scheduling

Akashdeep (✉)
Panjab University, Chandigarh, India
e-mail: akashdeep@pu.ac.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_10

services or traffic classes, namely unsolicited grant service (UGS), real-time polling service (rtPS), non-real-time polling service (nrtPS), extended real-time polling service (ertPS) and best effort (BE). The quality of service levels for these traffic classes maps to requirements of various user applications. The classifier sends incoming traffic to one of these classes, and bandwidth is allocated by schedulers according to implemented algorithm.

WiMAX implements a request-grant allocation mechanism scheme in which subscribers (SS) registered with the base station (BS) request bandwidth, and BS allocates these resources according to available channel conditions and requested bandwidth. The time gap between resource request and allocation can be a bottleneck in maintaining effectual QoS levels as during this period more admitted real-time applications can account for resources of non-real-time traffic classes. Role of scheduling structure and allocation policy gets much crucial in such circumstances and demands a ploy that shall be fair, intelligent and adaptive so that the performance of scheduling classes do not deteriorate. Design of such intelligent scheduling structure is only possible if most recent information from SS is incorporated into decision-making process. The most current state of traffic shall be made available to scheduler, and decisions regarding allocations shall be made accordingly. In this paper, authors have evaluated the performance of an adaptive method that utilizes fuzzy logic principles. The proposed system evaluates three qualities of service parameters from incoming traffic, and required number of slots are calculated according to these values. The performance analysis has been done by comparing the proposed method against established algorithms for four parameters of throughput, delay jitter and fairness. The paper is organized as follows: Sect. 2 summarizes latest studies in this field followed by formulation of problem. Section 3 introduces the proposed method followed by results and discussion in next section. Conclusion and future directions of work are provided in the last section.

2 Related Work

Use of fuzzy logic for resource allocation in WiMAX has found a limited number of studies in the literature, recently. It is one of hottest research areas, and few of these studies explored by authors can be found at [3–10]. Bchini et al. [11] and Simon et al. [3] used fuzzy logic concepts in designing handover algorithms. An intelligent call admission and control system for different traffic classes of WiMAX has been proposed by Shuaibu et al. [4]. Sadri et al. [5] implemented an interclass scheduler for 802.16 networks on basis of latency for real-time applications and throughput for non-real-time applications. Mohammed et al. [6] had implemented an adaptive version of DRR algorithm on basis of priorities of different service classes, latency and throughput requirements. Similar studies were also given by Hedayati et al. [7], Hwang et al. [8], Seo et al. [9] and Akashdeep and Kahlon [10].

The above-mentioned studies try to use fuzzy logic principles aiming to satisfy latency and throughput requirements of traffic classes. These do not consider request grant allocation mechanism used by WiMAX for bandwidth allocation which can lead to starvation of non-real-time flows. The proposed approach finds instantaneous information from various subscribers and makes allocation decisions accordingly. The approach calculates share of traffic in queues of real and non-real traffic together with latency and throughput requirements when system is up and running. The system then works to find an appropriate value for queue weight using fuzzy logic principles. This weight is utilized further for allocating bandwidth to queues of real and non-real traffic. Comparisons with reputable approaches are provided at end in order to justify the performance of proposed approach. Fairness of the system has also been explored and is found to be sufficiently good.

3 Proposed System

The standard resource allocation process for WiMAX consists of different subscribers requesting resources from the base station. The base station after evaluation of all requests and available resources makes the decision for slot allocation. This static process of allocation has been made adaptive by implementing fuzzy-based scheduler that makes decisions as per latest information available at various SS. The structure utilizes the latest information available at SS, senses changes in incoming traffic and modifies the allocation policy accordingly in order to satisfy requirements of both real as well as non-real-time classes. The proposed fuzzy system works on three input parameters: share of real-time and non-real-time traffic data, throughput requirements for non-real-time traffic and latency requirement for real-time traffic. The framework works adaptively by updating weights of queues serving these traffic classes. Fuzzy system has been implemented to automate weighted fair queuing (WFQ) algorithm for resource allocation on basis of parameters extracted from incoming bandwidth request packets and amount of traffic accumulated in queues of various SS. The output of the fuzzy system is weight for real-time traffic which is utilized to allocate slots to queues. Figure 1

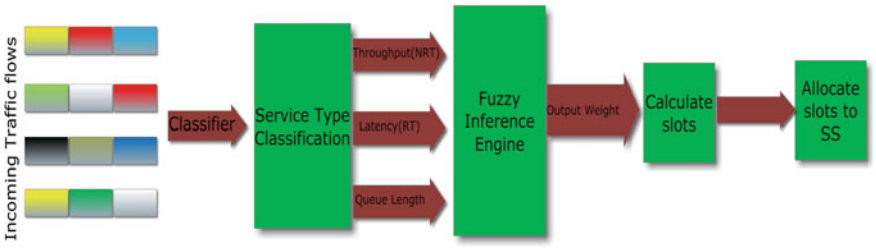


Fig. 1 Model of fuzzy logic-based resource allocator

shows the adopted methodology. The input and output variables have been defined with help of different linguistic levels. For latency and weight, we had defined five linguistic levels, whereas traffic share and throughput is measured on basis of three levels. This makes rules base to be used consisting of 45 different rules. The rules have been framed considering variable traffic patterns and nature of our variables. The dynamics of variables have been taken as ranging from (0) to +(1).

The allocation starts by assigning an initial weight to all flows (i) using Eq. (1)

$$w_i = \frac{R_{\min(i)}}{\sum_{i=0}^{n} R_{\min(i)}} \tag{1}$$

where $R_{\min(i)}$ is the minimum reserved rate for flow (i).

On receiving any bandwidth request from subscriber, the base station calls fuzzy inference system. The fuzzy system reads values of latency, throughput and queue length; performs fuzzification of these values against membership functions defined for these variables and applies the inference mechanism using fuzzy rule base. A final crisp value is generated after de-fuzzification using the centre of gravity method. This crisp-generated value is taken as weight for real-time traffic, and weight for non-real-time traffic is calculated using this generated value. Bandwidth to real and non-real-time traffic is allocated using these two weights according to Eqs. (2) and (3), respectively.

$$B_{\text{real}} = S_i \times \left(\frac{w_i}{\sum_{i=1}^{n} w_i}\right) \times \left(\frac{\text{Frame Duration}}{\text{Maximum Latency}}\right) \tag{2}$$

$$B_{\text{non-real}} = S_i \times \left(\frac{(w_j)}{\sum_{j=1}^{n} w_j}\right) \tag{3}$$

where S_i is the number of slots requested for that flow, w_i and w_j are weighted for real and non-real-time traffic queues. The overall performance of network has increased, and over all fairness and fairness towards non-real-time classes have also improved.

4 Results and Performance Evaluation

A simulating environment consisting of base station and multiple subscribers was set-up for performance evaluations. The simulating environment has one base station with increasing number of subscribers transmitting traffic according to five service classes of WiMAX. The subscribers transmit traffic for ertPS at rate of 10 frames/s, nrtPS traffic at 512 kbps with polling interval of 1s and web (BE) traffic. UGS class has an interval of 0.001 s. The requirement for rtPS has been taken as lower than 150 ms with all connections specifying their minimum

and maximum requirements. Experiments are conducted to evaluate the performance of proposed system against established approaches such as EDF (Extended deadline first), WFQ (weighted fair queuing) and WRR (weighted round robin) with concerns to parameters delay, throughput, jitter and fairness.

Figure 2 shows a plot of throughput and shows that system improves considerably in throughput. The fuzzy-based approach was quick to respond to requirements of real-time applications and provided allocation to non-real-time traffic in case requirement from real-time traffic are not rigid. This ability of fuzzy scheduler makes a positive impact on overall throughput value. Figure 3 plots average jitter for fuzzy system against other algorithms. The performance of all algorithms is similar till the number of subscribers is limited as resources are sufficient. The jitter variations are considerable as subscribers are increased further beyond 60. The proposed fuzzy system was successful in keeping jitter variations to minimum possible level.

Figure 4 indicates that proposed system was able to keep delay within permissible limits. This is because fuzzy-based system assigns major chunk of bandwidth to those connection which has comparatively smaller latency values. The fuzzy system is dynamic in nature, whereas other algorithms provide static allocations. The delay gets stable after subscribers reach about 105 which indicates system is able to meet requirements of all traffic classes, and weights are almost stable at this point.

One more experiment to verify the fairness of fuzzy-based approach was conducted in which fairness of different algorithms measured using Jain's Fairness Index was calculated and compared. Three service classes of rtPS, nrtPS and BE were considered for evaluation for reasons that these classes do not get dedicated allocations. Figures 5, 6 and 7 show plot of fairness observed by rtPS, nrtPS and BE classes, respectively. Figure 5 shows that out of all algorithms, EDF is more fair towards rtPS when number of connections are limited. Fairness deteriorates with increase in number of UGS and ertPS connections. The performance of WFQ and WRR is almost constant but shows a decline with increasing number of real-time

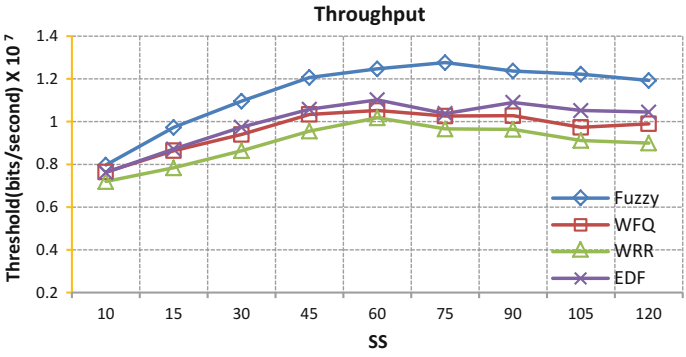


Fig. 2 Performance evaluation for throughput

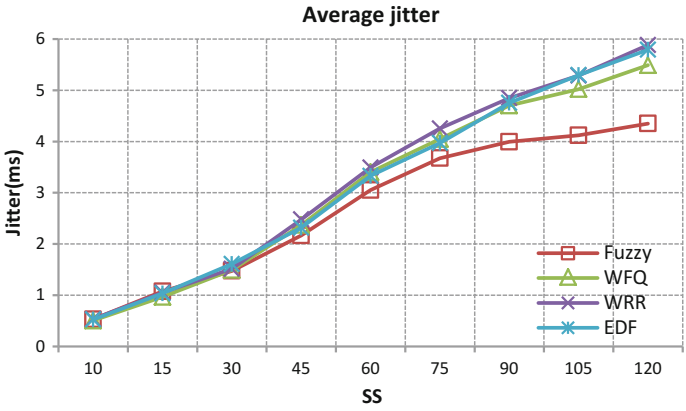


Fig. 3 Performance evaluation for jitter

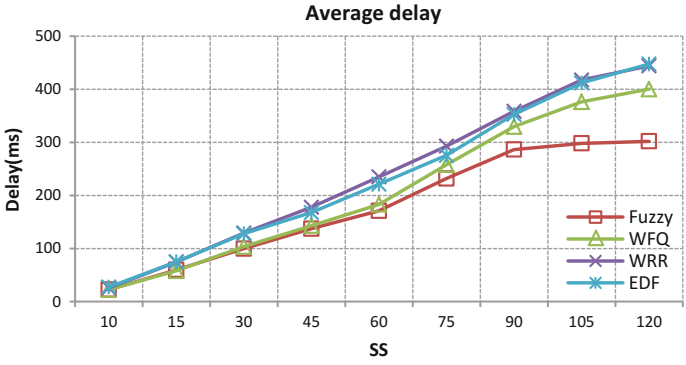


Fig. 4 Performance evaluation for delay

connections. WRR and WFQ are fairer but shows decline in fairness at relatively larger number of real-time connections.

Figures 6 and 7 suggest that proposed method is more inclined in fairness towards non-real-time traffic classes of nrtPS and BE. This may be because allocation to these classes is governed by relative variations in incoming traffic, and fuzzy scheduler increases amount of allocations whenever traffic from these classes tends to increase beyond a limit. This is a major reason for avoiding starvation of these classes, whereas other algorithms fail to adopt this policy, and therefore, the performance of these classes in other algorithms declines. Figure 7 shows that all algorithms have same values for limited amount of traffic but decrease substantially once traffic is increased. Out of all algorithms, WFQ and WRR provide relatively more fair level of performance to BE class. The performance of proposed method is also competitive.

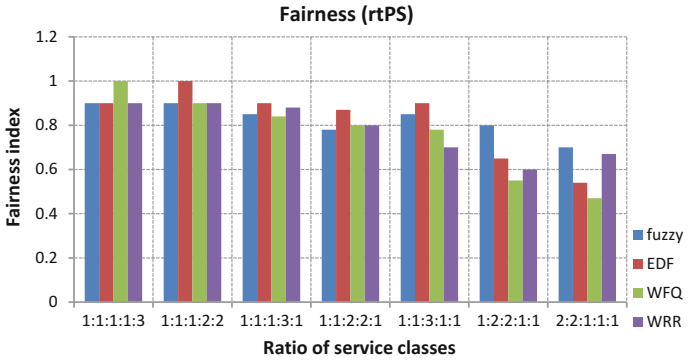


Fig. 5 Fairness comparison for rtPS

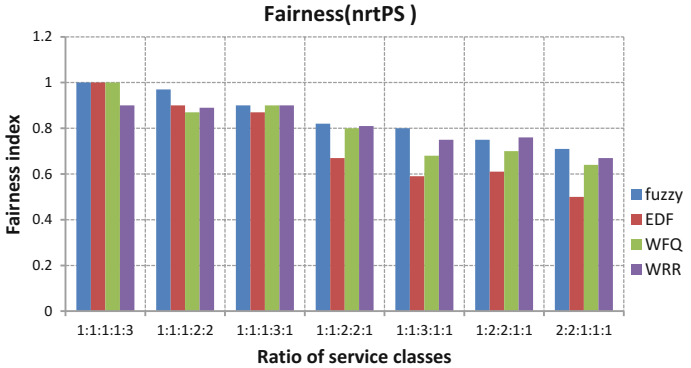


Fig. 6 Fairness comparison for nrtPS

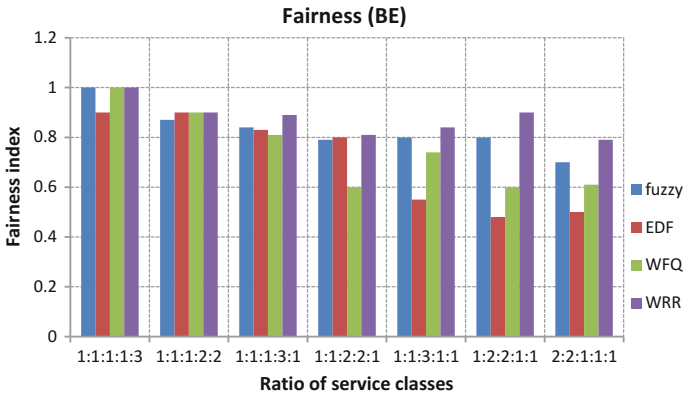


Fig. 7 BE fairness comparison

5 Conclusion

The above study has provided an evaluation of fuzzy logic-based resource allocator to be used in WiMAX networks in terms of different parameters. The approach is implemented to work adaptively using fuzzy logic vagueness. Decisions regarding resource allocation have been implemented using variables that are extracted at simulation time from incoming traffic. Use of fuzzy logic to implement an adaptive system has increased throughput of network. The delay and jitter variations of various service classes have been minimized, and low-prior non-real-time classes are not starved as system takes care of these flows on basis of their share. The approach was also tested for fairness, and results of the study are quite promising.

References

1. IEEE, Draft: IEEE standard for local and metropolitan area networks. 727 Corrigendum to IEEE standard for local and metropolitan area networks—Part 16: 728 Air interface for fixed broadband wireless access systems (Corrigendum to IEEE Std 729 802.16- 2004). IEEE Std P80216/Cor1/D2. 730 (2005)
2. IEEE, Draft.: IEEE standard for local and metropolitan area networks. 731 Corrigendum to IEEE standard for local and metropolitan area networks—732 Advanced air interface. IEEE P80216 m/D10, 1–1132 (2010)
3. Simon, J., Maria, D., Juan, A., Gomez, P., Miguel A., Rodriguez, A.: Embedded intelligence for fast QoS-based vertical handoff in heterogeneous wireless access networks. J. Per. Comp. (2014). http://dx.doi.org/10.1016/j.pmcj.2014.01.009
4. Shuaibu, D.S., Yusof, S.K., Fiscal, N., Ariffin, S.H.S., Rashid, R.A., Latiff, N.M., Baguda, Y. S.: Fuzzy logic partition-based call admission control for mobile WiMAX. ISRN Comm. Netw. **171760**, 1–9 (2010)
5. Sadri, Y., Mohamadi, S.K.: An intelligent scheduling system using fuzzy logic controller for management of services in WiMAX networks. J. Sup. Com. **64**, 849–861 (2013)
6. Mohammed, A.A., Borhanuddin, A.M., Noordin, N.K., Mohamad, H.: Fair uplink bandwidth allocation and latency guarantee for mobile WiMAX using fuzzy adaptive deficit round robin. J. Net. Com. Appl. http://dx.doi.org/10.1016/j.jnca.2013.04.004i. (2013)
7. Hedayati, F.K., Masoumzadeh, S.S., Khorsandi, S. SAFS.: A self adaptive fuzzy based scheduler for real time services in WiMAX system. In: 9th International Conference on Communications (COMM), pp. 247–250, 21–23 June 2012
8. Hwang, J., Youngnam, H.: An adaptive traffic allocation scheduling for mobile Wimax. In: Proceedings of IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC 2007, Athens, pp. 1–5
9. Seo, S.S., Kang, J.M., Agoulmine, N., Strassner, J., Hong, J.W.-K.: Fast: a fuzzy-based adaptive scheduling technique for IEEE 802.16 networks. In: Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on, pp. 201–208, 23–27 May 2011
10. Akashdeep, Kahlon, K.S.: An adaptive weight calculation based bandwidth allocation scheme for IEEE 802.16 networks. J. Emer. Tech. Web Inte. **6**(1), 142–147 (2014)
11. Bchini,T., Tabbane, N., Tabbane, S., Chaput, E. Beylot, A.: Fuzzy logic based layers 2 and 3 handovers in IEEE 802.16e network. J. Com. Comm. **33**, 2224–2245 (2010)

Intrusion Detection and Recovery of MANET by Using ACO Algorithm and Genetic Algorithm

Kuldeep Singh and Karandeep Singh

Abstract Mobile adhoc network (MANET) is a self-configuring agglomeration of wireless nodes with dynamically changing network topology that formed without using any preinstalled infrastructure or any central administrator. Intrusion detection is the security system that is used to automatically detect the problem when someone trying to break information system through violation of security policy. Alone intrusion prevention method is not sufficient because in MANET, network topology is continuously changing, so intrusion detection technique is used. This paper is based upon the intrusion detection in MANET based upon the different parameters of mobile nodes (MNs). Based upon some threshold values of parameters, ACO algorithm is used to detect the intrusion present in the network. And after that, genetic algorithm is used to recover the network.

Keywords MANET · MNs · IDS · ACO · GA

1 Introduction

Mobile adhoc network (MANET) is the rapidly growing area of research and most prominent technology of wireless network because the demand of wireless network is increasing day by day. There is no preinstalled and fixed infrastructure in MANET, and each node acts as intermediate router. Therefore, it becomes easy to attack such type of network in which there is no monitor or administrator. The various types of attack on MANET are flooding attack, warm hole attack, black hole attack, dropping attack, [1, 2] byzantine attack, passive eavesdropping, active interfering, data tampering, leakage of secret information, message replay, impersonation, message distortion, and denial of service (DoS) attacks. These types of

K. Singh (✉) · K. Singh
Department of Computer Engineering, Punjabi University, Patiala, India
e-mail: sidhu.kuldeep89@gmail.com

K. Singh
e-mail: karan_rob07@yahoo.co.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_11

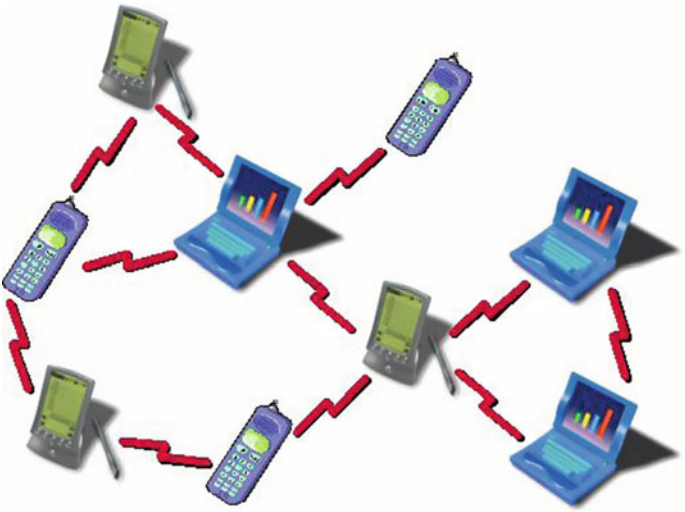


Fig. 1 Structure of mobile adhoc network

attack are not detected easily, so all mobile nodes (MNs) in MANET need much cooperation for proper functioning of network. In wired network, traffic can be monitored and analyzed through specified point or single administrator, but in case of MANET, it is very difficult to monitor and analyze the traffic because there is no central control over the network. Traffic can be analyzed in their radio transmission range only (Fig. 1).

2 Background

2.1 Intrusion Detection System (IDS)

Intrusion detection [3, 4] is the act of detecting action that used to break the confidentiality, integrity, and availability of the system and network resources. Intrusion detection system is mainly three types:

Network Intrusion Detection System (NIDS): In NIDS, whole network traffic is analyzed to determine the behavior of the network. Network traffic is continuously sensed to find the abnormal behavior. Once the attack is identified or abnormal behavior is detected, system alert can be sent to administrator by notifying that there is problem in the network.

Network Node Intrusion Detection System (NNIDS): In NNIDS, the analysis of traffic is done at specific node present in the network. Whole network traffic is not examined. Based upon the parameter values of that particular node, we can identify that there is problem in node or not.

Host Intrusion Detection System (HIDS): In HIDS, the current state of the host and previous state are compared, if the critical files of the system are decontaminate or modified, the alert can be sent that there is problem in that particular host.

2.2 Ant Colony Optimization (ACO)

Ant colony [5, 6] optimization algorithm is used to find the optimization paths, which is based on the behavior of ants' searching of foods. At first, ant wonders randomly, and when an ant finds source of food, it returns back leaving a marker (pheromones). That shows the path has food. When other ants come across the markers, they are likely to follow the path with a certain probability. If they do, then they populate the path with their own markers as they bring the food back. As more ants find the path, it gets stronger until there are a couple streams of ants traveling to various food sources near the colony.

Same way, we can apply ACO algorithm to find the intrusion present in the network. We are working with number of parameters of MNs like battery backup, throughput, packet delivery ratio, end-to-end delay, and packet drop ratio. These parameters have some threshold values. Based on these threshold values, we can detect whether the parameter is faulty or not.

Initially at first parameter of each node, ant wonders. If the value of the parameter is less than the specified values (threshold value) of node, then ant leaves markers (pheromones) and moves further. Likewise on all five parameters of each node, ants move and leave pheromones and then finally move one ant which counts all the pheromones on each node at all parameters. The accuracy of this algorithm depends upon the selection of parameters and threshold values.

2.3 Genetic Algorithm (GA)

Genetic algorithm [7, 8] is a heuristic search algorithm that is used to mimic the behavior of natural selection. It is inspired from biological immune system, and it is evolutionary algorithm. It uses chromosomes as a data that evolves through selection. Mainly the selection process is randomly chosen and crossover that is various recombination's of selected data to produce the better results and finally it uses mutation process to create the diversity in the selected population. The process is repeating until the best result is not obtained.

3 The Proposed Intrusion Detection and Recovery Technique

3.1 Parameter Extraction and Detection of Intrusion

Intrusion detection and recovery is the main goal of this technique. So first step is to select the *N* number of nodes, and after that, we need to detect the parameters of all *N* nodes. In this work, parameters used are battery backup, throughput, packet delivery ratio, end-to-end delay, and packet drop ratio. Intrusion detection is depending upon the efficient selection of parameters of nodes. As much the parameter will be strong, intrusion detection probability will be more (Table 1).

Next step is detection of intrusion. Intrusion detection can be done by ACO algorithm. Each parameter has some threshold value like battery backup has some threshold value BB_{th} and packet drop ratio has some threshold value PDR_{th}. Based on this threshold value, we can detect the problem in that node. Launch the iterations of and on first parameter of each node if the parameter value is less than the required value then ant leaves a pheromones and moves forward likewise second and is moved on second parameter of each node and identify that whether there is problem or not. At last, one ant is moved from first node of first parameter to last node of last parameter and counts the all pheromones leave by other ants. And hence, we can list the number of faulty parameters and can analyze how many nodes have problem due to intrusion present in the network (Fig. 2).

Algorithm Ant Colony Optimization for Intrusion Detection

Step 1 Randomly select number of nodes.
Step 2 Detection of parameter values of all nodes.
Step 3 Launch the iteration of ants on each parameter of all *N* nodes.
Step 4 If parameter value is less than or greater than specified values
Step 5 Then leave pheromones on that node and move forward.
Step 6 Else move ant forward without leaving pheromones.
Step 7 Repeat Step 3 to Step 6 until all parameters of all nodes are not processed.
Step 8 Leave single ant from first node of first parameter to last node of last parameter.
Step 9 Count the number of pheromones and move forward.
Step 10 Calculate how many parameters of all *N* nodes have problem.

Table 1 List of parameter used for intrusion detection system

Parameter	Threshold value
Battery backup	$>BB_{th}$
Throughput	$>NT_{th}$
Packet delivery ratio	$>PDVR_{th}$
End-to-end delay	$<EED_{th}$
Packet drop ratio	$<PDR_{th}$

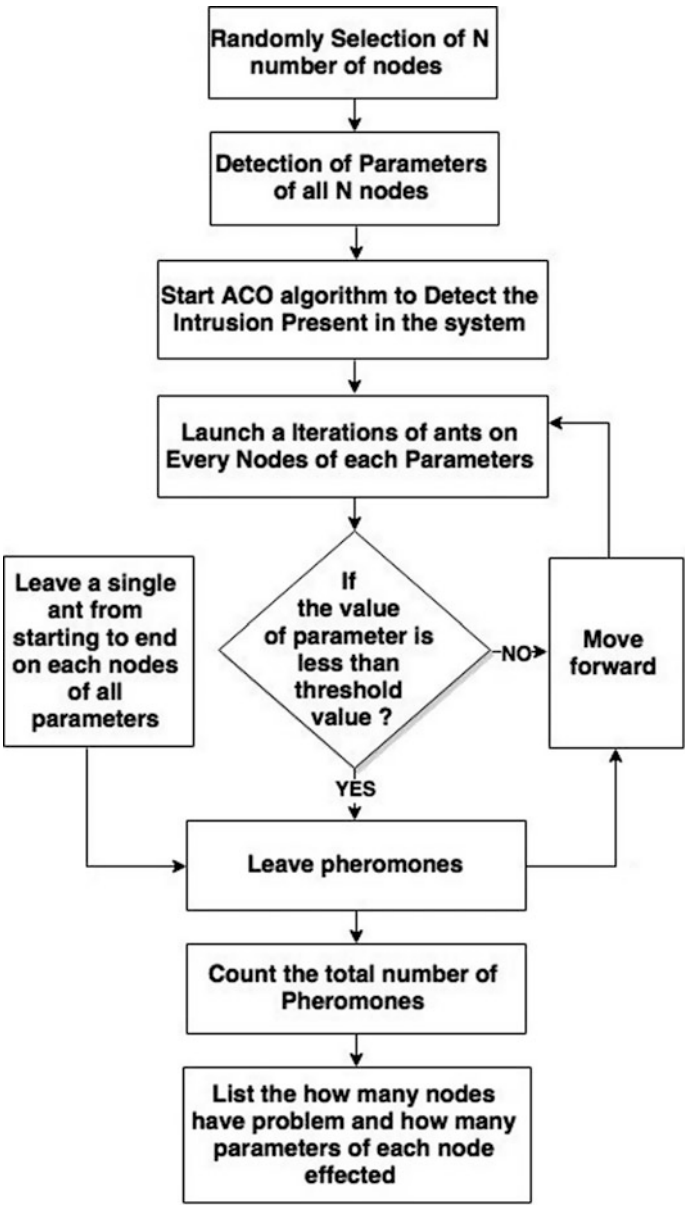


Fig. 2 Ant colony optimization algorithm flowchart

3.2 Recovery of Network from Intrusion

Intrusion is done by ACO algorithm. It lists how many parameters have fault. Genetic algorithm is used to recover the network. It uses all parameter values of all nodes as initial population. After that, it selects the populations of parameters from initial population and the techniques of selection are based on random procedure. The number of iterations can be performed to recover the problem, so we can provide that how many iterations we required to perform so that our result will be efficient. Crossover is the process that is applied after the selection process. In crossover process, various recombinations of selected chromosomes are made to recover the problem. We can perform one-point, two-point, and three-point crossover parameter values. After crossover, the newly obtained generation is stronger than previous generation. The final step of genetic algorithm is mutation. Before applying the mutation, we need to select the probability of mutation process. Mutation is mainly used to create the diversity in the selected population that is obtained after crossover process. After the total iteration, the result is obtained and analyzed that how many parameters have removed problem and how many parameters have still remained. Following is the algorithm that is used to recover the problem in mobile adhoc network due to the presence of intrusion (Figs. 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12).

Genetic Algorithm for Recovery of Nodes

Step 1 Take into account the population of all parameters of all N nodes.
Step 2 Select initial population in which algorithm is need to be applied.
Step 3 Select the number of iterations.
Step 4 Perform one-point, two-point, and three-point crossovers on selected population.
Step 5 Select mutation probability.
Step 6 Perform mutation to create diversity.
Step 7 If the number of iterations finishes.
Step 8 Calculate and analyze the result that how many nodes have removed problem and how many have still remained.
Step 9 Else repeat the Step 4 to Step 7.

4 Experimental Results

By using ACO algorithm, we identify that how many parameters have problem listed below as total number of faulty parameters, and for recovery, we use genetic algorithm. Each time we can select different number of iterations and with different probability of mutation listed as Mut_Pr(i) and after applying algorithm the number of parameters corrected listed as No. of Par_Cor. Experimental results for various numbers of node values have been listed.

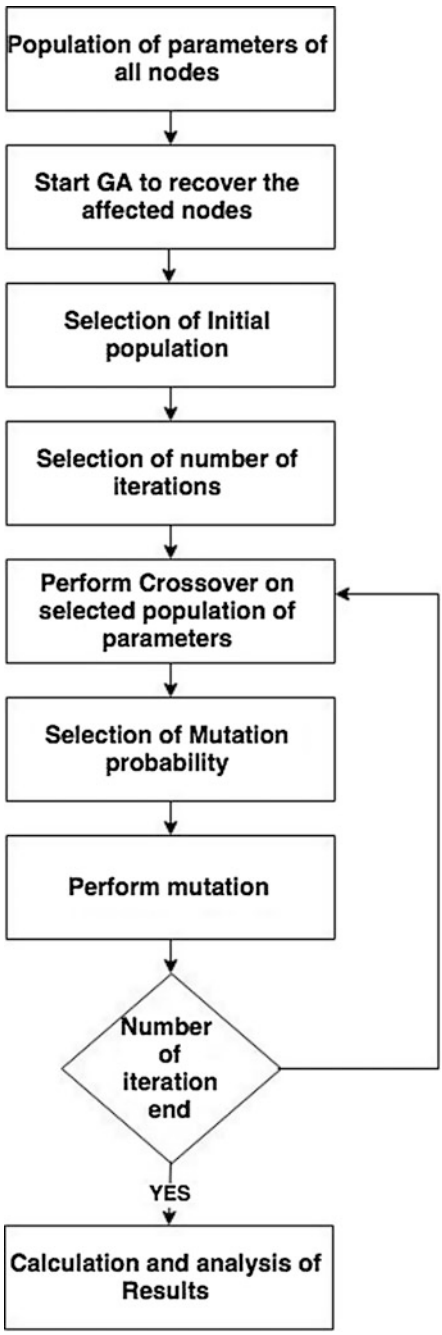


Fig. 3 Genetic algorithm flowchart

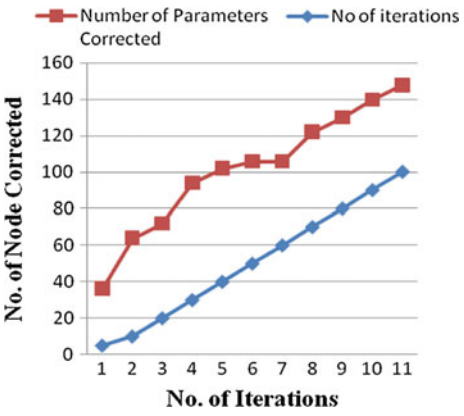


Fig. 4 Number of nodes corrected when mutation probability = 0.2

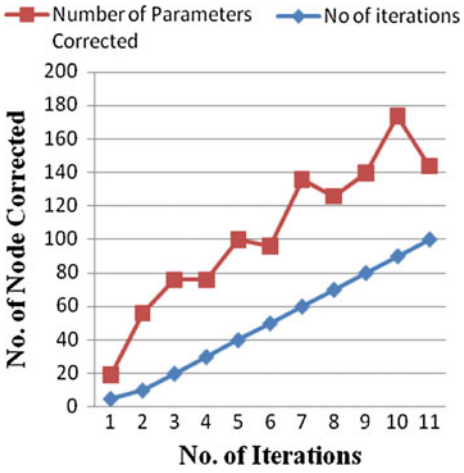


Fig. 5 Number of nodes corrected when mutation probability = 0.4

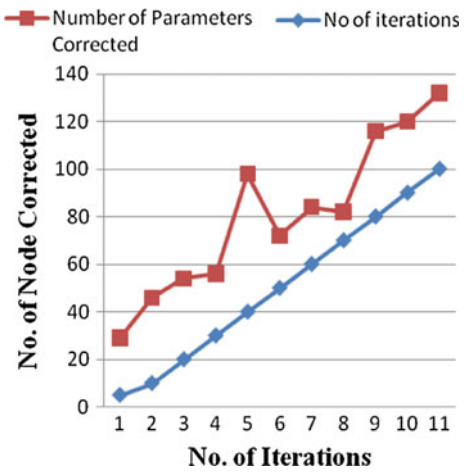


Fig. 6 Number of nodes corrected when mutation probability = 0.6

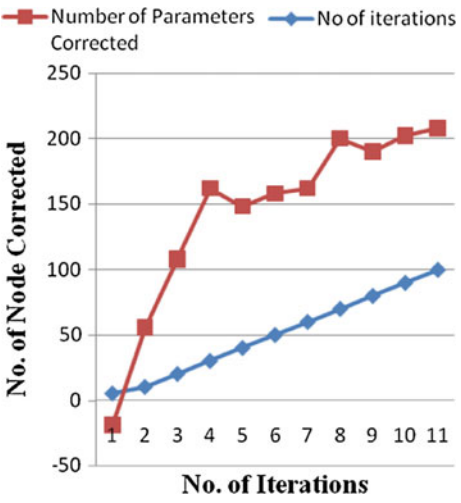


Fig. 7 Number of nodes corrected when mutation probability = 0.2

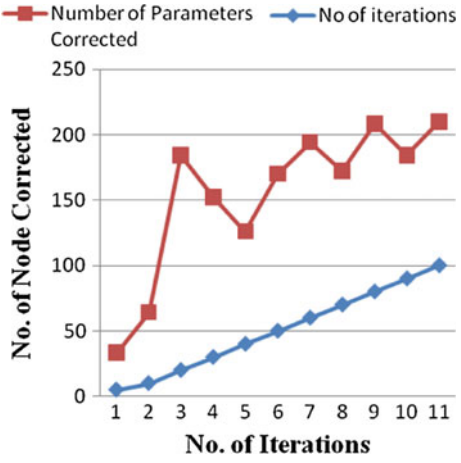


Fig. 8 Number of nodes corrected when mutation probability = 0.4

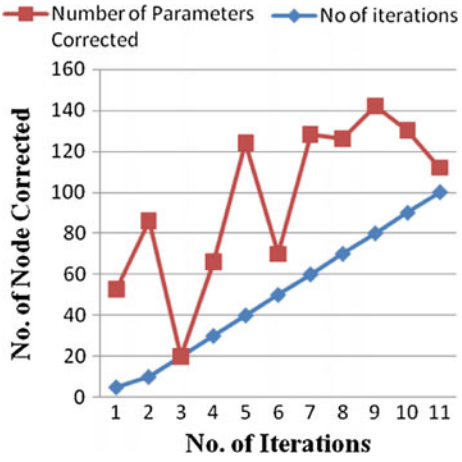


Fig. 9 Number of nodes corrected when mutation probability = 0.6

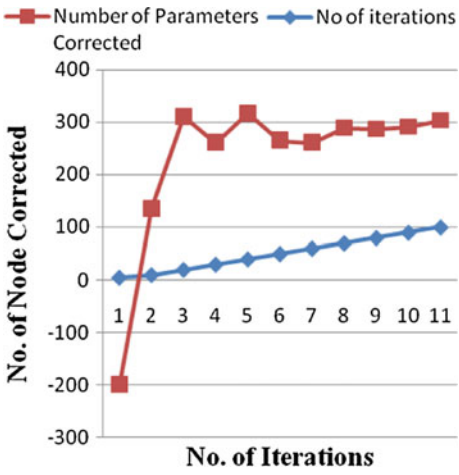


Fig. 10 Number of nodes corrected when mutation probability = 0.2

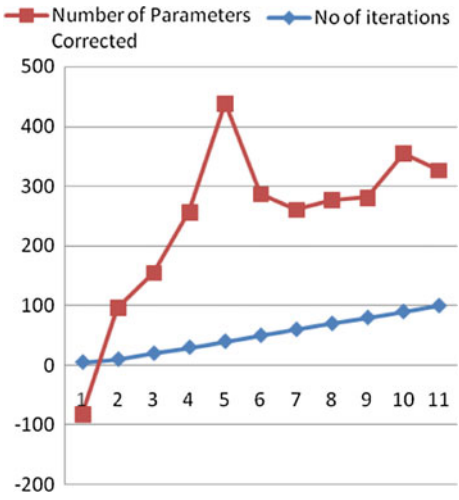


Fig. 11 Number of nodes corrected when mutation probability = 0.4

Total number of nodes—30
Total number of parameters—150
Total number of faulty parameters—106 (Table 2).
Total number of nodes—70
Total number of parameters—350
Total number of faulty parameters—242 (Table 3).
Total number of nodes—150
Total number of parameters—750
Total number of faulty parameters—489 (Tables 4).

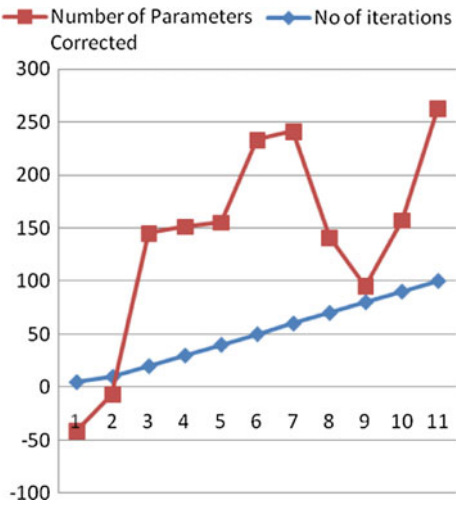


Fig. 12 Number of nodes corrected when mutation probability = 0.6

Table 2 Number of iterations with mutation probability and number of corrected nodes

No. of ite.	Mut_Prl	No. of Par_Cor.	Mut_Pr2	No. of Par_Cor.	Mut_Pr3	No. of Par_Cor.
5	0.2	31	0.4	14	0.6	24
10	0.2	54	0.4	46	0.6	36
20	0.2	52	0.4	56	0.6	34
30	0.2	64	0.4	46	0.6	26
40	0.2	62	0.4	60	0.6	58
50	0.2	56	0.4	46	0.6	22
60	0.2	46	0.4	76	0.6	24
70	0.2	52	0.4	56	0.6	12
80	0.2	50	0.4	60	0.6	36
90	0.2	50	0.4	84	0.6	30
100	0.2	48	0.4	44	0.6	32

Table 3 Number of iterations with mutation probability and number of corrected nodes

No. of ite.	Mut_Prl	No. of Par_Cor.	Mut_Pr2	No. of Par_Cor.	Mut_Pr3	No. of Par_Cor.
5	0.2	−24	0.4	28	0.6	48
10	0.2	46	0.4	54	0.6	76
20	0.2	88	0.4	164	0.6	0
30	0.2	132	0.4	122	0.6	36
40	0.2	108	0.4	86	0.6	84
50	0.2	108	0.4	120	0.6	20
60	0.2	102	0.4	134	0.6	68
70	0.2	130	0.4	102	0.6	56
80	0.2	110	0.4	128	0.6	62
90	0.2	112	0.4	94	0.6	40
100	0.2	108	0.4	110	0.6	12

Table 4 Number of iterations with mutation probability and number of corrected nodes

No. of ite.	Mut_Prl	No. of Par_Cor.	Mut_Pr2	No. of Par_Cor.	Mut_Pr3	No. of Par_Cor.
5	0.2	−205	0.4	−87	0.6	−47
10	0.2	125	0.4	87	0.6	−17
20	0.2	291	0.4	135	0.6	125
30	0.2	231	0.4	227	0.6	121
40	0.2	277	0.4	399	0.6	115
50	0.2	215	0.4	237	0.6	183
60	0.2	201	0.4	201	0.6	181
70	0.2	219	0.4	207	0.6	71
80	0.2	207	0.4	201	0.6	15
90	0.2	201	0.4	265	0.6	67
100	0.2	203	0.4	227	0.6	163

5 Conclusion and Future Scope

Intrusion detection is done by ACO algorithm, and recovery of network from intrusion is done by genetic algorithm. The accuracy of the algorithm depends upon the selection of parameters. As much the parameters will be strong, the result will be more accurate. Research work shows that best result can be obtained by using number of iterations between 10 and 80 and mutation probability within the range of 0.2–0.4 units. For future work, we can use different techniques for intrusion detection and can compare with this work. Like neural network can be used for intrusion detection system.

References

1. Nguyen, H.L., Nguyen, U.T.: A study of different types of attacks in mobile adhoc networks. In: 25th IEEE Canadian Conference on Electrical Computer Engineering (CCEC) (2012)
2. Narang, E.K., Sonal.: A study of different types of attacks in MANET and discussion about solutions of black hole attack on AODV protocol. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **2**(4) (2013)
3. Shakshuki, E.M., Kang, N., Sheltami T.R.: EAACK—A secure intrusion-detection system for MANETs. In: IEEE Trans. Ind. Electron. **60**(3) (2013)
4. Butun, I., Morgere, S.D., Sankar, R.: A survey of intrusion detection system in wireless sensor networks. IEEE Comm. Syst. Tutorials **16**(1) (2014) (First Quarter)
5. Muraleedharan, R., Osadciw, L.A.: An Intrusion Detection Framework for Sensor Networks Using Ant Colony. IEEE, Nov 2009
6. Li, W.S., Bai, X.M., Duan, L.Z., Zhang, X.: Intrusion detection based on ant colony algorithm of fuzzy clustering. In: International Conference on Computer Science and Network Technology, IEEE, Dec 2011

7. Hassan, M.M.M.: Network intrusion detection system using genetic algorithm and fuzzy logic. Int. J. Innovative Res. Comput. Comm. Eng. **1**(7) (2013)
8. Kashirsagar, V.K., Tidkem, S.M., Vishnu, S.: Intrusion detection system using genetic algorithm and data mining overview. Int. Comput. Sci. Inf. **1**(4), 2231–5292 (2012). ISSN (PRINT)

Avoiding Attacks Using Node Position Verification in Mobile Ad Hoc Networks

G. Krishna Kishore and K. Rajesh

Abstract A mobile ad hoc network is a collection of autonomous mobile devices that communicate with each other. This network may contain foe nodes and trustworthy nodes. Foe nodes imply attacker nodes which are malwares, threats, malicious nodes. To keep away from these nodes, we introducing node position verification protocol. This protocol is utilized for message exchange which is used for transmitting messages among the nodes and checks the location of each and every node in the network. The message exchange protocol manages the distinguishing proof of nodes that are in a communication range. Distance computation is in view of message transmission between the prover and its correspondence adjacent node. Calculated distance is utilized to confirm the location of communicating nodes in network. For node position verification, mainly three methods are utilized. This problem is implemented for mobile ad hoc network and simulation using NS2 tool. The benefit of this technique is to lessen the delay and accomplish the high throughput and can stop attackers not entering into information transmission nodes.

Keywords Node position verification (NPV) · Foe nodes · Symmetry test · Multilateration test

1 Introduction

In MANET, nodes have mobility and they have to announce their position in real time to the surrounding nodes. Malicious nodes can announce incorrect position information to threaten the network users or even collapse the network or even make the network behave unexpectedly. This can cause severe consequence, for example, by advertising forged positions, adversaries could bias geographic routing

G. Krishna Kishore (✉) · K. Rajesh
Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, AP, India
e-mail: gkk@vrsiddhartha.ac.in

K. Rajesh
e-mail: rajeshkalakoti@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_12

or data gathering processes, attracting network traffic and then eavesdropping or discarding it. Solutions to these attacks and threats have to be found using node position verification (NPV) protocol. By knowing the location, awareness has become an advantage in mobile devices. In a wide range of protocols and applications require knowledge of the node positions. These are all examples of services using node position information. Applications are geographic routing in spontaneous networks, data gathering in sensor networks, movement coordination among autonomous robotic nodes, location-specific services for handheld devices, danger warning, or traffic monitoring in vehicular networks.

2 Literature Survey

Hu et al. [1] Neighborhood discovery (ND) serves as central building blocks in mobile wireless systems. Obviously, ND empowers (multi-hop) communication [2], as it is vital for route discovery and data forwarding [3]. ND can also bolster a wide range of system functionality network access control, topology control, transmission scheduling, energy-efficient communication, as well as physical access control. Given the basic and multifaceted part of ND, its security and robustness must be guaranteed: ND conventions must distinguish as neighbors just those gadgets that really are neighbors, even in unfriendly situations. Then again, the very way of wireless mobile networks makes it simple to mishandle ND and along these lines bargain the overlying protocols and applications [4, 5]. Along these lines, giving strategies to moderate this susceptible and to secure ND is pivotal [6]. This literature focuses on this problem and provides the different types of neighborhood and ND protocol properties [7, 8, 9]. There are three neighborhood types: (1) Communication and physical neighborhood. (2) Partial and complete neighborhood discovery. (3) Neighborhood as a building block. In multi-hop wireless networks, a wide range of data communication and dissemination (one-to-one, one-to-many, or broadcast) depends on the thought of neighborhood.

3 Methodology

Attack scenario: Here we propose NPV protocol. The secure data transmission is possible with NPV protocol. Source discovers the position of every adjacent node utilizing the NPV protocol. In this protocol, prover shows the SELECT message to all adjacent nodes. The prover additionally stores the dispatching the SELECT message time for all adjacent nodes. Subsequent to getting SELECT message from prover, each and every adjacent nodes store the SELECT message acceptance time and RESPONSE to prover. The RESPONSE message contains every adjacent node ID. This likewise inside spares the dispatch the RESPONSE message time. Then DISCLOSE message is telecasted using prover's location. It contains a proof

that prover P is the creator of the first SELECT. After uncover message telecasted, every adjacent nodes reported the position to verifiers. The REPORT message incorporates the adjacent locations and dispatches the RESPONSE message time.

3.1 Notations Are Used in Algorithms

(1) P: prover. (2) A: Adjacent node. (3) Node_attacker: attacker. (4) adj_nodes: Number of adjacent nodes which are neighbors. (5) Next_ip: Next input to verifier. (6) Dispatch_ SELECT _Data: Dispatch the SELECT data. (7) Dispatch_time: Node dispatching the time. (8) Acceptance_time: Node acceptance time, (9) Node_id: Id of the node. (10) Dispatch_DISCLOSE_Data: DISCLOSE the dispatching data. (11) location_X: Node X's location. (12) dist[P][A]: Distance from the node prover to attacker. (13) dist[A][P]: Distance from the Adjacent to prover. (14) acceptance_time[P][A]:Time accepting from the prover to node Adjacent node. (15) acceptance_time[P]: Time acceptance of the node prover. (16) acceptance_time[A][P]: Time acceptance from the Adjacent node to prover. (17) acceptance_time[A]: Acceptance time of the adjacent node. (18) Postion_dist [P][A]: Distance between the positions of nodes from prover to adjacent node. (19) comm._range: Communication range. (20) Link_count: Count of the nodes which connected the prover. (21) Miss_ match_count: Count of the nodes which are not connected to prover.

Algorithm 1: Location of adjacent nodes

```
if ( prover==Next_ip)
 if find(adj_nodes,P)  then Dispatch_ SELECT _Data(P); Load Dispatch_time(P);
end-if
for( i=0;i<=Length(adj_nodes);i++)
   adj_nodes[i]= Load  Acceptance_time(SELECT _data);
adj_nodes[i]= RESPONSE (Node_id, Dispatch_time);
end-for
 if find(RESPONSE(adj_nodes))  then Dispatch DISCLOSE _Data(P); end-if
for( i=0;i<=length(adj_nodes);i++)
     adj_nodes[i]: REPORT(location_X, Dispatch_time(RESPONSE));
end-for
end-if
```

3.2 Position Verification

Each adjacent nodes of prover of the position is verified using three tests. They are

1. Direct symmetry test (DST)
2. Cross symmetry test (CST)
3. Multilateration symmetry test (MLT).

In DST verifier, the immediate connection nodes are confirmed with its corresponding adjacent nodes. The predictable adjacent will be checked by taking the criteria: (1) Time of Flight—(Time and speed-based) determined that separations are reliable with one another, (2) with the location publicized by the adjacent node, and (3) within communication range. In CST, test data commonly assembled by every pair of correspondence adjacent nodes are checked. Euclidian distance: It uses to calculate distance between nodes using the formula

$$P_{VN} = \left\{ (X_v - X_N)^2 + (Y_v - Y_N)^2 \right\}^{1/2} \quad (1)$$

Algorithm 2: Direct symmetry Test

```
if(prover==Next_ip)
        dist[P][A] =(acceptance_time[P][A] - acceptance_time[P] )*speed_node
        dist[A][P] =(acceptance_time[A][P] – acceptance_time[A] )*speed_node
   where distance=time*speed
    here distance calculation is based on location of the nodes
        Dist=[dist[P][A] – dist[A][P]];
    Postion_dist[P][A]= [(nodeX_P – nodeX_A)^2 + (nodeY_P – nodeY_A)^2 ]^1/2;
        Verification of the direct adjacent nodes of prover
    if((Dist>threshold_value) or
      (Postion_dist[P][A]- dist[P][A])>threshold_value) or
      (dist[P][A]>comm._range))
       Node _attacker;
end-if
```

Algorithm 3: Cross Symmetry Test

```
If(prover==next_ip) prover:Link_count[P]; /*number of adjacent nodes are
connected to prover checking for any pair of adjacent nodes
for (i=0;i<=Length(adj_nodes;i++)
        adj_nodes[i]:Link_count[i]++;
        adj_node[i]:REPORT(Link_count[i],adj_node_id);
  end-for;
if(Link_count[P]<=adj_nodes[i]) then Miss_match_count:Miss_match_count[i]++ ;
    Node_attacker;  end-if
```

Multilateration Test
In this method, the unidentified connections are tested.

Algorithm 4

```
            if(prover==next_ip)  Prover: Location(adj_nodes[i]); Load: Fake_attacker;
            No_of_attacker[i]: attacker_location;
    for (i= 0;i<= Length(adj_nodes;i++)
            each adjacent nodes gives other adjacent postions
            adj_nodes[i]: REPORT(Loacation_adj_nodes[i]) end-for;
        Node_attacker; end-if
end-if
```

4 Results

Node 0 is verifier or sender. Attacker nodes are indicated by red color. Remaining nodes are genuine nodes. Simulation area is 600 m × 600 m. Initially, verifier sending a SELECT message to neighbors in the network as shown in Fig. 1a. All neighbors sending RESPONSE (OWN ID) message to verifier, attackers (30, 33, and 36) also sending RESPONSE message to verifier is shown in Fig. 1b. Figure 2a shows that verifier sending DISCLOSE message to all adjacent nodes for position get from all adjacent nodes after receiving RESPONSE message. At that time, verifier also calculates the reception time of REPORT message for each adjacent node. Each adjacent node sends own (original) position to verifier. Attacker (node 16, 12, 39) also reports fake position (near to source) to verifier is shown in Fig. 2b.

The DST only detects the attacker node 36. But attacker nodes 33 and 30 are not detected. Because the attackers are 33 and 30 reception time of the distance is less similar to the within the communication range of reception time (Fig. 3). Therefore,

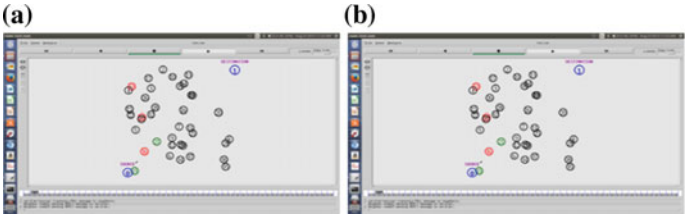


Fig. 1 **a** SELECT. **b** RESPONSE

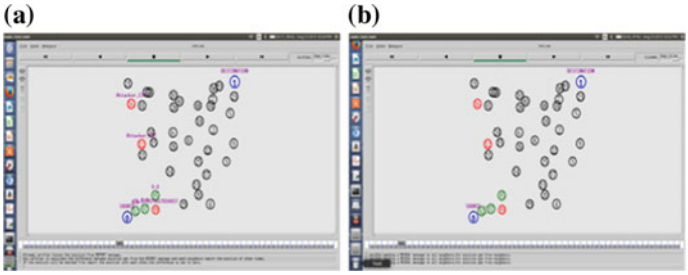


Fig. 2 **a** DISCLOSE. **b** REPORT

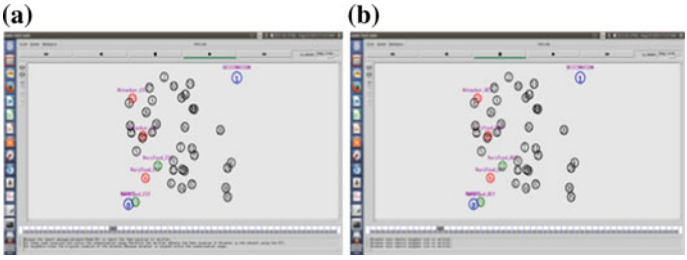


Fig. 3 **a** DST. **b** CST

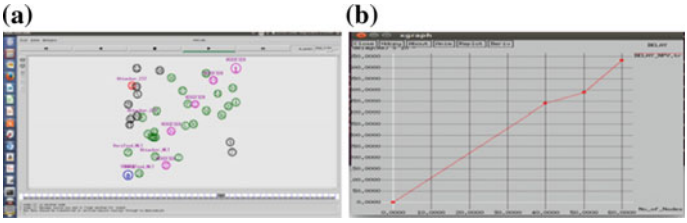


Fig. 4 **a.** MLT. **b** DELAY

the direct symmetry test only detects the attacker of original location distant away from the adjacent nodes of source node is shown in Fig. 4a. DST of 23 = Verified_DST, DST of 33 = attacker_DST The CST is only detecting the attacker 36 and the attackers 33 and 30 are not detected because these attackers 30 and 33 are placed within the communication range. So the attacker 33 is placed in all adjacent nodes (verifier's neighbor) node list as shown in Fig. 4b. Total number of verifier adjacent nodes = 7, Threshold = 6 CST of 33 = attacker_CST CST of 23 = Verified_CST MLT (Multilateration Test):Verifier compares the each neighbors reports the position of other nodes, Already verifier known the position from REPORT message. Then verifier calculates the difference between positions get from the REPORT message and each neighbors reports the position of other nodes.

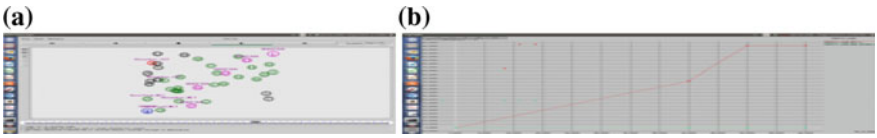


Fig. 5 **a** Verified path. **b** Traffic overload

If the position will be matched from report, the position with each other, then the difference is zero. Otherwise, the difference will be greater than zero. If the difference is greater than the zero, the attacker will find out as shown in Fig. 5a. Figure 5b shows the number of nodes versus delay.

Figure 5a shows result node 0 and node 1 are a source and destination. Here, the message has to pass from the source to destination through trusted nodes which are represented in pink color. Here, attackers are represented in red color nodes; finally, the path is set from source to destination through nodes 0, 27, 16, 22, 13, 1 which are helpful for data transmission from not entering attackers. Figure 6b shows the traffic overload in the network. But non-secure the attacker is not detected.

5 Conclusion

The proposed protocol is very durable to detect attacks and against to colluding foe nodes, even when attacks contain complete idea about the prover adjacent nodes and total information of whole network. Finally, we can transmit the data securely using NPV protocol through NS2 simulation tool. We can say NPV protocol is more efficient in data transmission with low delay.

References

1. Hu, Y.-C., Perrig, A., Johnson, D.B.: Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. IEEE Infocom, S. Francisco, CA (2003)
2. Lazos, L., Poovendran, R.: HiRLoc.: high-resolution robust localization for wireless sensor networks. IEEE JSAC **24**(2), 233–246 (2006)
3. Papadimitratos, P., Poturalski, M., Schaller, P., Lafourcade, P., Basin, D., Capkun, S., Hubaux, J.-P.: Secure neighborhood discovery: a fundamental element for mobile ad hoc networks. IEEE Comm. Mag. **46**(2) (2008)
4. Chiang, J., Haas, J., Hu, Y.: Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration, ACM WiSec, Zurich, Switzerland (2009)
5. Capkun, S., Rasmussen, K., Cagalj, M., Srivastava, M.: Secure location verification with hidden and mobile base stations. IEEE Trans. Mobile Comput **7**(4), 470–483 (2008)
6. Zhong, S., Jadliwala, M., Upadhyaya, S., Qiao, C.: Towards a Theory of Robust Localization against Malicious Beacon Nodes. IEEE Infocom, Phoenix, AZ (2008)

7. Chiang, J., Haas, J., Hu, Y.: Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration. ACM WiSec, Zurich, Switzerland (2009)
8. Leinm¨uller, T., Maihöfer, C., Schoch, E., Kargl, F.: Improved Geographic Ad Hoc Routing through Autonomous Position Verification. ACM VANET, Los Angeles, CA (2006)
9. Capkun, S., Rasmussen, K., Cagalj, M., Srivastava, M.: Secure Location Verification with Hidden and Mobile Base Stations. IEEE Trans. Mobile Comput. **7**(4), 470–483 (2008)

Algorithm for Multi-Hop Relay in Mobile Ad Hoc Networks

G. Krishna Kishore and P. Sai Geetha

Abstract Mobile ad hoc network (MANET) is a collection of mobile nodes that are connected each other. Considering the potential relay nodes based on power constraint is a difficult problem to obtain efficient throughput. This problem can be solved by selecting the minimum distance nodes as relay nodes from destination. In the proposed method, the delay is analyzed by selecting the relay nodes in multi-hop. Relay nodes are selected when the destination node is not in the communication range. There exists more than one relay node between the source and destination in multi-hop. Thus, the packets are transferred from source to destination through these relay nodes. If the destination node is not in the transmission range, then consider one-hop neighbors of source and calculate the distance from destination to these one-hop neighbors. The network topology is designed using the NS2 tool which gives routing tables, to provide the information about neighbors and also about the selected next hop node. The node with minimum distance is taken as selected next hop node. This node is considered as a relay node. In this manner, relay nodes are selected between source and destination. We can reduce the packet loss and delay.

Keywords MANET · Delay · Multi-hop relay

1 Introduction

Mobile ad hoc network (MANET) is a collection of nodes consisting mobility without any infrastructure. These are mainly used in military, rescue operations, and personal area network. There are many challenges in mobile ad hoc networks such

G. Krishna Kishore (✉) · P. Sai Geetha
Computer Science & Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, AP, India
e-mail: gkk@vrsiddhartha.ac.in

P. Sai Geetha
e-mail: geethapamidimukkala@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_13

as dynamic topology, limited bandwidth, and power constraint. Every node in the network can act as both host and a router. Nodes have the ability to roam independently without any links, and they have the capability to change their links with other devices [1]. The network topology is dynamically changed, and routing protocols are used to manage this dynamic nature. Packets are transferred from source to destination by using different routing protocols. Usage of MANETs is increasing due to their mobility and less cost. If the destination is not in the transmission range of source, then relay nodes are selected.

Relay node is used in mobile ad hoc networks to include fault tolerance. Packets from sensor nodes are sent to the receiver through multi-hop paths. Relay nodes are responsible for packet transfer from sender to receiver. Relay nodes carry out three functions [2]. For transmitting or receiving, the information radio communication section (RCS) is used. Information recording section (IRS) is used for receiving sensor node information, and information destination is decided by information conveying section (ICS).

2 Literature Review

2.1 On the Delivery Probability of Two-Hop Relay MANETs with Erasure Coding

Yang [3] proposed a new algorithm for achieving delivery probability as 0 or 1. 0 indicates the packets are not delivered, and 1 indicates that the packets are delivered successfully. Two-hop relay algorithm explains that if destination is within the range, then source transfers the packets to destination directly or else a random relay node is selected. A model Markov chain is developed for transferring frames. Matrix method is used to calculate the delivery probability. But this paper does not explain the process of selecting relay node between the source and destination (Fig. 1).

2.2 Delay Control in MANETS with Erasure Coding and F-Cast Relay

Krifa [4] proposed new algorithm for controlling delay in mobile ad hoc networks. For reducing delay, erasure coding is combined with packet duplication process. Sending the same packets to more than one relay node consumes more space. Source node encodes the packets, and these packets are sent to different relays. At the destination node, these packets are decoded to get the original message. Matrix

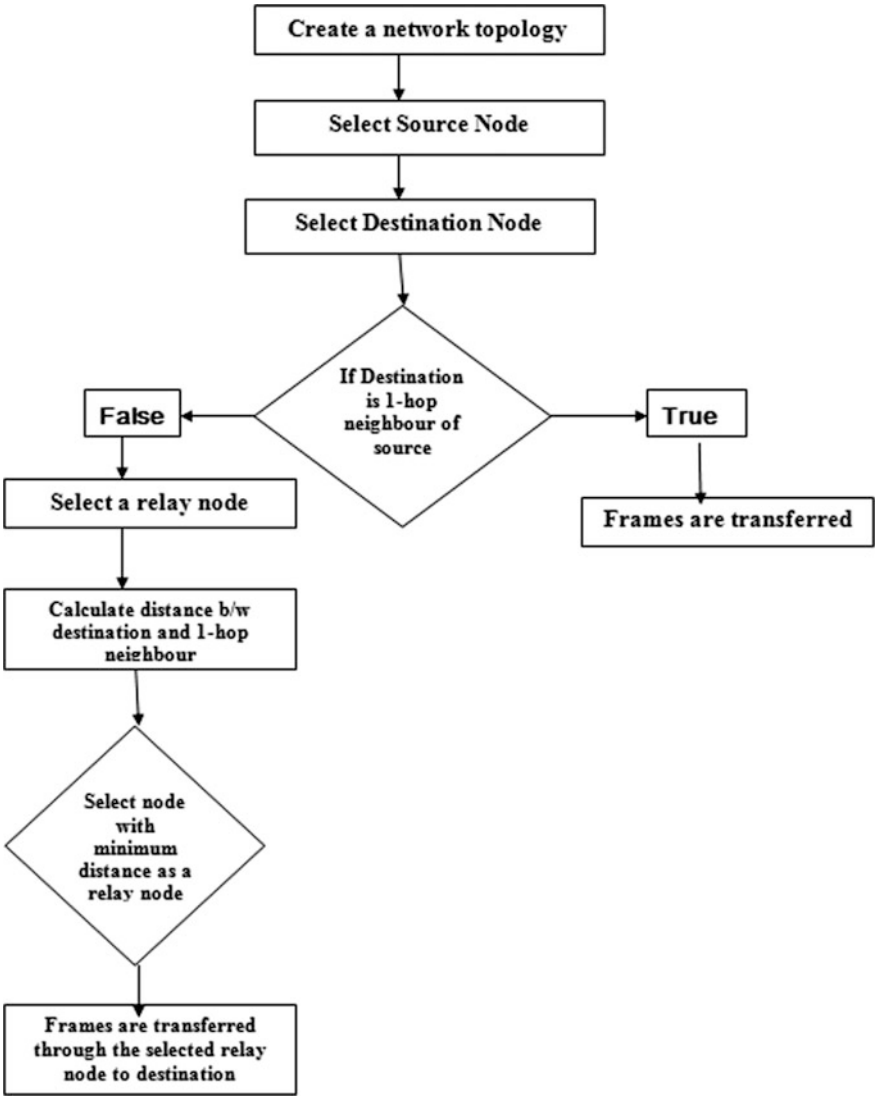


Fig. 1 Flowchart for multi-hop relay

technique is used to derive different expressions that are most important to reduce delay of packets. This paper contains the redundancy concept. So the buffer space required is more when compared to other methods. Overhead is also more in this concept.

2.3 Message Drop and Scheduling in DTNs

Liu [5] proposed algorithm for dropping of the messages and scheduling of that messages in delay-tolerant networks. The ordering of message is important to deliver the original message to destination. The solutions to buffer management and scheduling problems are that scheduling can be done by considering the node that should contain messages with the decreasing order of their usage. Message is of less utilized among the messages in buffer is dropped when a message arrives at node. In this paper, probability of delivering message rate is maximized and delay is minimized based on the optimality. But the disadvantage is that buffer has to maintain the entire history.

2.4 Delay and Capacity in Ad Hoc Mobile Networks with F-Cast Relay Algorithms

Liu [6] proposed two-hop relay algorithm in which packet is delivered to f distinct relay nodes. A new form is developed that indicates trade-off in between delay or capacity and *f*. Two-hop relay algorithm is developed in which $f + 1$ copies of packets exist at each node which include source node copy [7]. One queue is locally generated and waits for redundant copies (f) and that contain $n - 2$ relay nodes. Packets are transferred from source to destination if destination is one-hop neighbor of source or else relay nodes are selected. Here, sending number and receiving number of packets are considered in order to get the original message from source. But the selection of relay node is not specified.

3 Methodology

In MANETs, the main challenges are [8] limited bandwidth, dynamic topology, and power constraint. Finding the potential relays based on power constraint is a difficult problem. This problem can be solved by selecting the minimum distance nodes as relay nodes. In multi-hop relay, packets are transferred from source to destination through these relay nodes [9]. Relay nodes are selected in such a way that they are very near to particular desired location. The main objective of multi-hop relay is reducing delay of packets that are transferred from source to destination [10].

Neighbor Calculation: Consider source and destination. Calculate the one-hop neighbors of all nodes. All the nodes are within the transmission range, and then, they are considered as one-hop neighbors. If the destination is one-hop neighbor, then direct transfer of packets takes place or else a relay node is selected.

Selection of Relay Node: Note all the one-hop neighbors of source, and calculate the distance between the destination and these neighbors. Distance can be

calculated by using Euclidian distance formula. Consider two points, destination and source, with coordinates (X_1, Y_1) and (X_2, Y_2), respectively. If destination and source distance is d, then it is calculated as follows.

$$d^2 = (X_2 - X_1)^2 + (Y_2 - Y_1)^2 \quad (1)$$

This process is also continued for all relay nodes. Routing table contains the information about source and its neighbors. Consider the minimum distance node as relay node. This relay node becomes next hop node for source and that process is continued up to destination node. Similarly, all relay nodes are selected between the source and destination.

Traffic Flow: Packets are transferred from source to destination through intermediate relay nodes which have less distance from destination. So the packets are transferred effectively. Message from source is sent to relay nodes, and these relay nodes process the information.

3.1 Algorithm of Proposed System

1. Create a network topology.
2. Select source(S) and destination (D) nodes.
3. If the destination (D) is one-hop neighbor of source(S), then frames are directly transferred to destination. Otherwise, we have to select a relay node (R).
4. i ==S
5. While (i! = D)

   {
   Consider one-hop neighbors of node i.
   Calculate the distance between destination (D) and one-hop neighbors. Select the node that has minimum distance from the destination as a relay node(R).
   }

6. Packets are transferred from S to D through these relay nodes(R).

Network topology is created, and choose the source and destination nodes. If the destination is one-hop neighbor of source, then direct transmission takes place. If the destination is at larger distance from source, the intermediate relay nodes are selected as relay nodes. These relay nodes are selected based on the minimum distance from source and destination. Traffic is sent from source to destination through these relay nodes.

4 Results

Simulation Environment: Initially, the network topology is designed using the NS2 tool with 40 nodes and ranges 250 m. Using Simulation environment, packets are transmitted using relay node more effectively from source to destination. From this environment, we can say that accuracy is improved and delay reduced.

Figure 2a shows one-hop neighbors of each and every node that is calculated. If node is within the transmission range, then it is known as one-hop neighbor. One-hop neighbor calculation is used to know that the destination is one-hop neighbor or not. If the destination is one-hop neighbor, then frames are transferred from source to destination or else relay node must be selected. Figure 2b shows the single-hop transmission. Source node is 35, and destination node is 37. Node 37 is one-hop neighbor of 35. So, packets are transferred directly from source to destination. Packets are dropped when the packet size exceeds buffer limit. Figure 3a shows two-hop transmission in mobile ad hoc networks. Source node is 14, and destination node is 18. Node 17 is one-hop neighbor of source node 14, and it is having less distance from the destination node 18. Packets are dropped when the buffer size is less than the packet size. Figure 4b shows multi-hop relay in mobile ad hoc networks. Source node is 9, and destination node is 16. Node 11 is one-hop neighbor of source 9, and it is having minimum distance from destination. So, node 11 is selected as relay node. Packets are transferred from source to destination through these relay nodes. Packets are dropping at source 9 because of the packet size.

Figure 4a shows graph for end-to-end delay. Here, *x*-axis represents time, and *y*-axis represents delay. Figure 4b shows graph for packet loss. It contains single-hop, two-hop, and multi-hop transmissions in mobile ad hoc networks. Packet loss occurs when the size of packets exceeds the buffer limit. Here, *x*-axis represents time, and *y*-axis represents number of packets. Figure 4c shows graph for packet delivery ratio. It contains single-hop, two-hop, and multi-hop. *x*-axis represents time, and *y*-axis represents packet delivery ratio.

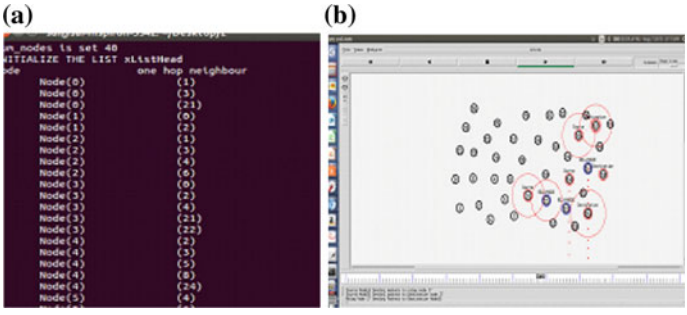


Fig. 2 **a** One-hop distance calculation, **b** single-hop transmission

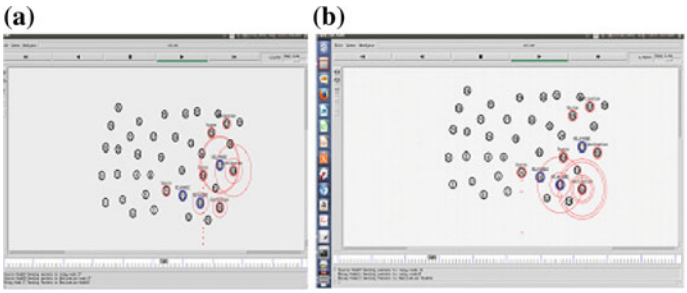


Fig. 3 **a** Two-hop transmission, **b** multi-hop transmission

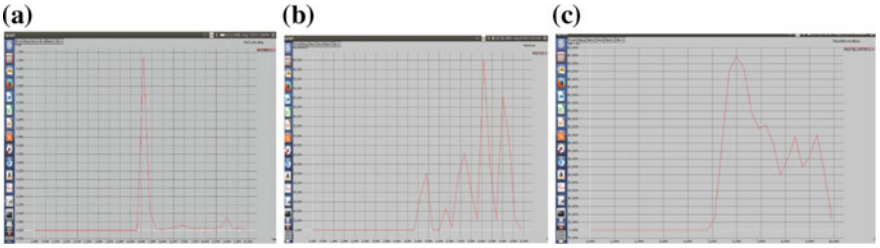


Fig. 4 **a** Delay graph, **b** packet loss, **c** packet delivery ratio

5 Conclusion

Mobile ad hoc networks (MANETS) are widely used because of their features like mobility and instant infrastructure. The research activities in mobile ad hoc networks are increased over the past few years. Our proposed method explains about the selection of relay node concept. When the destination is having larger distance from source, then relay nodes are used to process the message from source to destination.

References

1. Vallimayil, A., Sarma Dhulipala, V.R., Karthick Raghunath, K.M., Chandrasekaran, R.M.: Role of relay node in wireless sensor network: a survey. IEEE (2011)
2. Liu, J., Jiang, X., Nishiyama, H., Kato, N.: On the delivery probability of two-hop relay MANETs with erasure coding. IEEE Trans. Commun. **61**(4) (2013)
3. Yang, B., Gao, J., Zhou, Y., Jiang, X.: Delay control in MANETs with erasure coding and f-cast relay, Springer, July 2014
4. Krifa, A., Barakat, C., Spyropoulos, T.: Message drop and scheduling in DTNs: theory and practice. IEEE Trans. Mob. Comput. **11**(9) (2012)

5. Liu, J., Jiang, X., Nishiyama, H., Kato, N.: Delay and capacity in ad hoc mobile networks with f-cast relay algorithms. IEEE Trans. Wirel. Commun. **10**(8) (2011)
6. Liu, J., Jiang, X., Nishiyama, H., Kato, N.: Group-based two-hop relay with redundancy in MANETs, HPSR (2011)
7. Liu, J., Jiang, X., Nishiyama, H., Kato, N.: Exact throughput capacity under power control in mobile ad hoc networks. IEEE INFOCOM (2012)
8. Li, P., Fang, Y., Li, J., Huang, X.: Smooth trade-offs between throughput and delay in mobile ad Hoc networks. IEEE Trans. Mob. Comput. **11**(3) (2012)
9. Liu, J., Jiang, X., Nishiyama, H., Kato, N.: Group-based two-hop relay with redundancy in MANETs. In: IEEE 12th International Conference on High Performance Switching and Routing. (2011)
10. Whitbeck, J., Conan, V., de Amorim, M.D.: Performance of opportunistic epidemic routing on Edge-Markovian dynamic graphs. IEEE Trans. Commun. **59**(5), 1259–1263 (2011)

Comparative Performance of Multipath Routing Protocols in Wireless Mesh Network

Meenakshi Sati, Mahendra Singh Aswal and Ashutosh Dimri

Abstract The WMNs are coming up as a new networking trend for setting up a wireless networking infrastructure in metropolitan areas. Network operators prefer WMN because of easy installation and fast deployment of it. It may also result in reduction of monetary investment and cost of operation. The routing in WMNs is challenging task because of the unpredictable variations in the wireless environments. In this paper, three routing protocols, AOMDV, MOLSR, and MHRP, are compared in terms of their performance in WMN.

Keywords WMN · Multipath routing · MOLSR · AOMDV · MHRP

1 Introduction

The wireless mesh network (WMN) brought new opportunities and challenges, because of its dynamically self-organized and self-configured network. Generally, a WMN can be regarded as a set of wireless nodes which communicate with each other and forward each other's packets [1]. The nodes of a WMN are classified as mesh router or mesh client. Each node in the network is not only a host but also works as a router. It can forward the packets on behalf of other nodes that may be beyond the direct wireless communication range of their destinations.

A WMN is dynamic in nature with self-organizing and self-configuring the nodes, thus establishing and maintaining mesh connectivity automatically among

M. Sati (✉)
Department of CSE, NITTTR, Chandigarh, India
e-mail: meenakshi.nitttr@gmail.com

M.S. Aswal
Gurukula Kangri Vishwavidyalaya, Haridwar, India
e-mail: mahendra8367@gmail.com

A. Dimri
Jamia Hamdard, New Delhi, India
e-mail: ashutoshdimri85@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_14

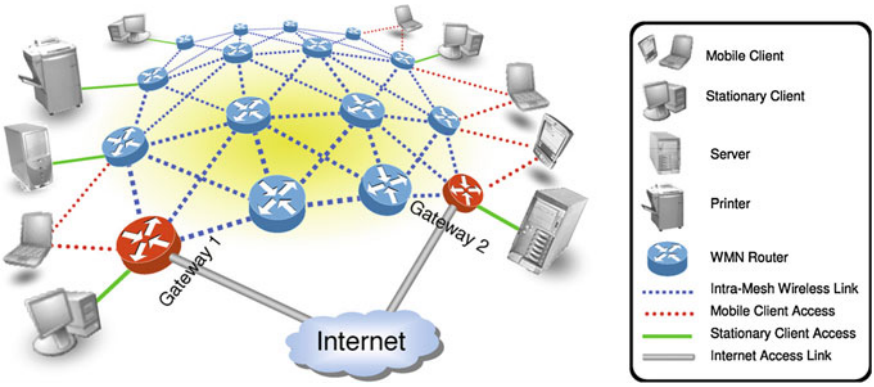


Fig. 1 Wireless mesh network comprising several stationary and mobile clients to the Internet [9]

the nodes. According to F. Akyildiz et al., these features provide many benefits of using WMNs like lower setup cost, simple network management, fault tolerant, and reliable service coverage. Figure 1 illustrates the architectural view of a typical wireless mesh network.

The routing algorithm used is a main aspect affecting the performance of a network. A number of single-path and multipath routing algorithms have been proposed for WMN. The important goal of multipath routing is to incorporate balancing of load and to achieve higher degree of fault tolerance. A number of paths are chosen between two communicating nodes. The packet flow is allowed through any one path. When a link becomes faulty on a path owing to a poor channel state or mobile conditions, next path is opted from the group of remaining paths [1].

The present paper studies the comparative performance of three multipath routing protocols namely AOMDV, MOLSR, and MHRP on the basis of different parameters. The rest of the paper is arranged in the following manner. The next section overviews the multipath routing in WMN. The third section elaborates the features of different multipath routing protocols. The section four discusses the results obtained after simulation, and section five contains conclusive comments.

2 Multipath Routing in WMN

A WMN is built with two kinds of nodes called *as* mesh router *and* mesh client. The locations of mesh routers are fixed, but mesh clients can change their locations and connect to network over other mesh routers and clients. S. Xuekang et al. investigated that in addition to performing the routing capability of a traditional wireless router for gateway/repeater functions, a mesh router node exhibits extra routing functions to enable mesh connectivity.

The multipath routing makes use of the resources of core network by setting up many paths between source–destination pair. The motives behind using it include

utilization of bandwidth, optimizing latency, making the network fault-tolerant, building reliability and equal load distribution. The purpose of using multipath routing is to employ the various valid routes to arrive at destination and not just the most suitable path. But the control overhead incurred in establishing these multipaths should be optimal [2].

The three phases of multipath routing are path exploration, traffic distribution, and path maintenance. The path exploration phase determines the existing paths for a node pair. During the traffic distribution phase, the number of paths for distributing traffic is selected. Path maintenance is responsible for generating paths again after exploring the initial path. It can be started either after the failure of one path or after the failure of all the paths [3].

A. *Path Exploration*
   Path exploration is the mechanism of finding out the existing path set for a given sender and receiver node. There are numerous issues which a protocol should take into consideration while deciding the subset of available paths it tends to generate in the exploration process.
   The one of the important issue here is that generated paths should be disjoint, which dictates the path independence in terms of shared resources.
B. *Traffic Distribution*
   There are a number of methods for allocating traffic to existing paths. A multipath protocol may choose to transmit the traffic using only the best path while keeping other explored paths as backups or using the paths in parallel. A pathfinding algorithm chooses a subset of available paths on the basis of a specific attribute of the paths. For instance, no. of hops is being used widely as a metric for a long time. Some other possible metrics are path reliability, path disjointedness, free bandwidth, degree of route interdependence, etc.
C. *Path Maintenance*
   Path maintenance can be stated as the mechanism of recreating the paths after the initial path discovery. Due to the resource constraints of the nodes, paths are highly error prone. Therefore, there should be mechanism for path reconstruction to reduce performance degradation.
   The path discovery can start in three following situations: failure of an active path, failure of all active paths, or failure of a subset of paths.

3 Multipath Routing Protocols

The primary aim of routing protocol is to choose the route from sender to receiver node. The protocol should be reliable, quick, and with less overhead. Some multipath protocols constantly supervise and keep track of quality or overall QoS metric of existing paths by using dynamic maintenance algorithms. The multipath Routing protocols can be classified as reactive, proactive, and hybrid [4].

A. *Reactive Protocols*

The paths are created only when desired by the source node. Some of the reactive protocols are:

- AODV-based decoupled multipath (AODV-DM)
- AODV-backup routing (AODV-BR)
- Ad hoc on-demand multipath distance vector protocol (AOMDV)
- Multipath dynamic source routing (MP-DSR)
- Split multipath routing (SMR)

AOMDV protocol works on the basis of distance vector and routes on step-by-step basis [5]. Moreover, AOMDV discovers multiple paths on request using a single pathfinding technique.

The route request (RREQ) propagates from the sending node to the receiving node and set up many return paths both at middle nodes as well as at the receiving node. Multiple route replies (RREPs) traverse back these reverse paths in order to construct multiple forward paths to the destination at the source and middle nodes. AOMDV also assigns alternate paths to middle nodes as they are considered to be helpful in minimizing route exploring frequency [5].

The main concept of the AOMDV protocol is to make sure that discovered multiple paths are disjoint and free from loop and that such paths are efficiently found using a flood-based routing method. Perkins et al. [6] proposed that AOMDV protocol depends to a large extent on the routing information which already exists in the under considered AODV protocol, thus reducing the delay resulted in finding multiple paths.

B. *Proactive Protocols*

Routing information is stored in one or more tables at every node within the network. The multipath optimized link state routing protocol (MOLSR) is a proactive protocol that tries to produce reduced delay and data loss by employing multiple path routing [7]. Xuekang et al. [2] investigated that OLSR restricts broadcasting by using multipoint relays and multipoint relay selectors. In MOLSR, multiple routes are found out and top two routes are selected as per the link metrics specified. The routes having two or more identical nodes are not taken into consideration.

MOLSR introduces the concept of cross-layer and the node discovery algorithm which is used to find out every node on the path in order to bypass disjoint path. The purpose of it is to reduce delay and packet drop ratio [7].

C. *Hybrid Protocol*

The hybrid routing protocols combine both proactive and reactive routing protocols. One of the main hybrid protocols for wireless mesh networks is multipath hybrid routing protocol (MHRP), where multipath is used to provide the backup mechanism [8]. MHRP has four building blocks:

- Intra-Region Routing Protocol—IRRP
- Router Infrastructure Routing Protocol—RIRP
- Region Gateway Routing Protocol—RGP
- Route Maintenance

As paths in the infrastructure mesh are comparatively fixed, RIRP is a proactive-based protocol. IRRP is a member of reactive routing protocols group that provide increased pathfinding and maintenance services using local communication inside the particular regional scope. The Region Gateway Protocol (RGP) [8] facilitates the routes between two ad hoc regions.

Before sending the data to a destination node, a node inquires if there exists a route to destination; if the route is absent, the node initiates the route exploration phase. The route exploration is performed in three stages: route request, route setup, and route response.

Siddiqui [8] stated that MHRP is a hybrid approach as it adopts both proactive and reactive methods in discovering the routes. Being a secure multipath routing protocol, MHRP reduces the control overhead arising out of it to a great extent by employing a simple mutual authentication mechanism [9, 10].

4 Simulation Environment

A. *Experimental Setup*

The simulation is done to analyze the performance of WMN routing protocols for selected evaluation parameters using NS2. The network simulator NS2 V 2.34 was used for simulation study. The network was simulated with 10, 20, 30… 40 nodes using square grid topologies for each experiment conducted. All nodes were distributed within the area of 1493 m × 734 m. The first node was configured as source, while the last node was configured as destination. The size of data payload was 512 bytes. The traffic type was constant bit rate type traffic. A simulated WMN having 30 mesh nodes randomly deployed over 1493 m × 734 m region is shown in Fig. 2.

The three protocols AOMDV, MOLSR, and MHRP are simulated using this simulation setup. The details of simulation parameter are given in Table 1.

In this simulation study, selected routing protocols are simulated for following four evaluation parameters:

- End-to-End Delay: The delay of a network enumerates the latency it takes for a bit of data to traverse the network from one node or endpoint to another.
- Throughput: It is the number of packets that were delivered during a specified time period.
- Packet delivery ratio: It is known as the ratio of the numbers of packets successfully arrived at a receiving node to the total number of packets sent by the sending node.
- Packet loss ratio: If one or more transmitted packets fail to reach at their destination, it is called as packet loss. The packet loss ratio denotes the percentage of transmitted packets that failed to reach the intended destination.

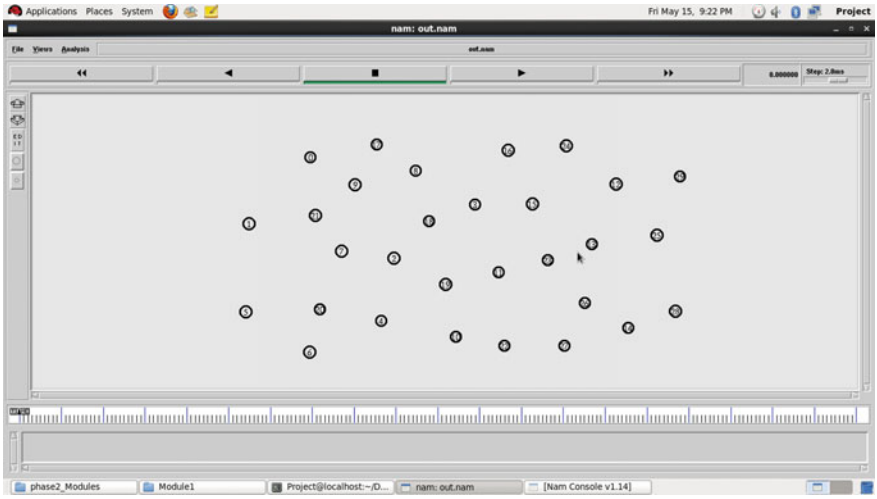


Fig. 2 WMN topology having 30 nodes with random placement using NS2

Table 1 Simulation parameters

Parameter	Value
Network simulator	NS2.34
Routing protocol	AOMDV, MOLSR, MHRP
No of nodes	10, 16, 25, 30
Simulation area	1493 m × 734 m
Simulation time	10/20/30/40/50 s
Traffic type	CBR
Packet size	512 bytes
Node deployment	Random
Mac type	802.11

B. *Result and Discussion*

Comparison of reactive, proactive, and hybrid protocol is performed using the measured parameters.

This simulation of AOMDV, MOLSR, and MHRP protocols was performed for four different evaluation parameters namely end-to-end delay, packet loss ratio, throughput, and packet delivery ratio.

The performance of protocols was analyzed for varying simulation time, and resulting values of throughput, end-to-end delay, packet loss ratio, and packet delivery ratio were measured for each protocol.

The results for throughput, packet loss, packet delivery ratio, and end-to-end delay versus time are shown in Figs. 3, 4, 5 and 6, respectively.

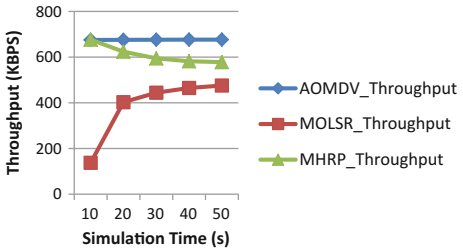


Fig. 3 Comparison of AOMDV, MOLSR, and MHRP for time versus throughput

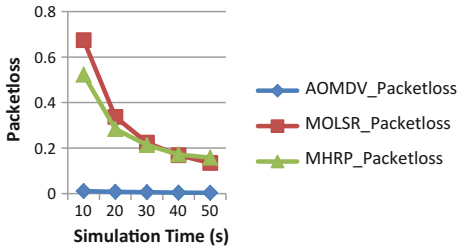


Fig. 4 Comparison of AOMDV, MOLSR, and MHRP for time versus packet loss

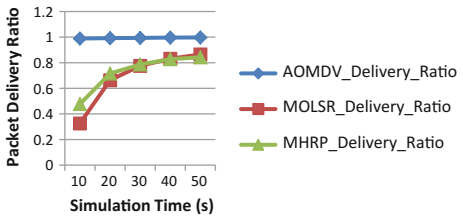


Fig. 5 Comparison of AOMDV, MOLSR, and MHRP for time versus packet delivery ratio

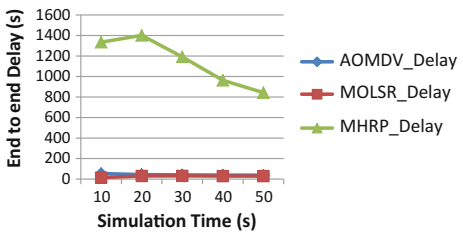


Fig. 6 Comparison of AOMDV, MOLSR, and MHRP for time versus delay

5 Conclusion

In this paper, performance of three multipath routing protocols for wireless mesh networks, namely AOMDV, MOLSR, and MHRP, has been compared. Simulations were performed using NS2 in different random topologies. The results show that AOMDV protocol provides better result than MOLSR and MHRP for packet

delivery ratio, throughput, and packet loss for the given simulation environment. However end-to-end delay of MOLSR is partially better than AOMDV and much better than MHRP. We can conclude that AOMDV performs better as compared to other two protocols for a WMN consisting of 10–30 nodes spread across the given area. Our future work includes the enhancement of AOMDV by improving the security features of it.

References

1. Akyildiz, F., Wang, X., Wang, W.: Wireless mesh networks: a survey. Comput. Netw. **47**, 445–487 (2005)
2. Xuekang, S., Wanyi, G., Xingquan, X., Baocheng, X., Zhigang, G.: Node discovery algorithm based multipath olsr routing protocol. In: International Conference on Information Engineering, pp. 139–142. (2009)
3. Manoj, B.S., Rao, R.R.: Wireless mesh networks: issues and solutions. In: Wireless mesh networking: architecture, protocols and standards. Auerbach Publications, (2007)
4. Ghahremanloo, P.: Multi-path routing challenging single-path routing in wireless mesh networks. In: International Siberian Conference on Control and Communication, pp. 12–15. (2011)
5. Das, M.M.: On-demand multipath distance vector routing in Ad Hoc networks. In: 9th International Conference on Network Protocols, (2001)
6. Perkins, C., Belding-Royer, E., Das, S.: Ad hoc on demand distance vector (AODV) routing. IETF, RFC 3561, (2003)
7. Valarmathi, K., Malmurugan, N.: Multi path routing protocol for improving reliability in IEEE 802.16 wireless mesh networks: In: International Conference on Trendz in Information Sciences and Computing, pp. 116–121. (2011)
8. Siddiqui, M.S., Amin, S.O., Kim, J.H., Hong, C.S.: MHRP: a secure multi-path hybrid routing protocol for wireless mesh network. In Military Communications Conference, pp. 1–7. (2007)
9. Zhang, W., Wang, Z., Das, S.K., Hassan, M.: Security Issues in Wireless Mesh Networks. In: Wireless Mesh Networks: Architectures and Protocols, Springer, (2008)
10. Network Simulator-ns 2 URL: http://www.isi.edu/nsnam/ns

Energy-Efficient Approaches in Wireless Network: A Review

Veenu Mor and Harish Kumar

Abstract Environment protection and reduction of operational cost are gaining popularity among researchers. Energy consumption has direct impact on both factors and follows an increasing trend of attentions in recent years. A number of energy-aware approaches have been found in research to trim down superfluous energy expenditure by embedding energy alertness in the protocols, devices and designing of wireless networks. This paper intends to provide a broad review of the various researches at protocol stack for minimizing energy consumption in wireless network.

Keywords Energy-efficient communication · Layer-based solutions · Cross-layer optimization

1 Introduction

Information and communication technology (ICT) plays vital role in reducing movement of people and products, to enhance efficiency of production and consumption of goods, etc. Increased use of ICT helps to reduce emissions of CO_2. But, on the other side, electricity consumption of ICT equipment itself is growing more rapidly contributing to carbon dioxide (CO_2) emission. ICT is found to be responsible for around 750 thousand tons of CO_2 production for every terawatt hour of energy dissipation. This sector is being reported to contribute for 2–3% [1] of the total CO_2 discharge of which mobile networks contribute about 0.2%. In developed countries, CO_2 emission rate is even higher. As ICT is the fastest growing sector, it can contribute significantly in enhancing energy efficiency of other sectors and hence in controlling average rise in temperatures.

V. Mor (✉) · H. Kumar
University Institute of Engineering and Technology, Panjab University, Chandigarh, India
e-mail: veenu.mor@pu.ac.in

H. Kumar
e-mail: harishk@pu.ac.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_15

Furthermore, future trend is toward wireless communications, and bandwidth requirements are increasing with launching of new bandwidth-hungry network applications. Increasing Internet Protocol (IP) traffic demands expanding infrastructure like switches, routers and hence more network equipments are leading to energy expenditure. Hence, the need for energy-efficient solutions in network has become apparent due to the immense increase in amounts of energy consumption and carbon footprints within ICT sector. Environmental aspects and the resulting energy cost of network operators are major motivators for the energy-efficient network solutions. Additionally, compared to hardware defined approaches like power amplifiers, highly integrated modules, software-based solutions have wider scope. So, this research work focuses on review of various ongoing solutions at protocol stack.

This study broadly provides a survey of the most applicable research trends for minimizing energy expenditure in wireless networks based on protocol stack layers. The paper is formulated into four sections. Introduction to field is discussed in Sect. 1. Section 2 represents various layer-based approaches ranging from physical to application, cross-layer approach has been found to be more promising field; Sect. 3 highlights trends of research work at protocol layers over last five years; finally, Sect. 4 provides conclusion and future work.

2 Layer-Based Approaches

Energy consumption in wireless network is affected by each layers of protocol stack. Hence, energy reduction should be considered throughout all layers. Apart from traditional stand-alone solutions at individual layers, interaction among layers can further reduce energy significantly. This section focuses on classification of energy-saving techniques based on Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack as depicted in Fig. 1. Application layer occupies top of stack followed by transport, network, data link, and physical layer.

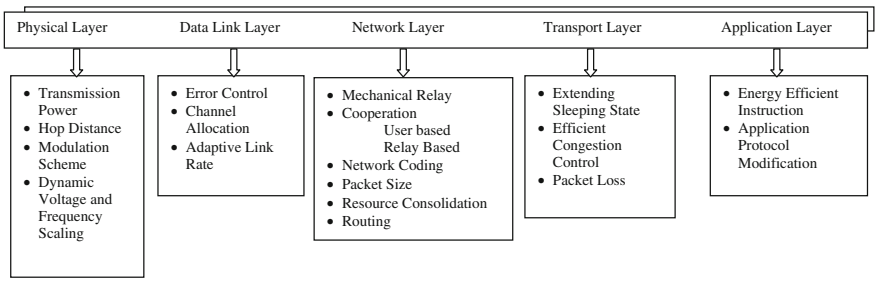


Fig. 1 Energy-efficient approaches at various layers of TCP/IP protocol stack

2.1 Physical Layer

Physical layer is accountable for real conduction of data over communication link in signal forms. Energy efficiency at physical layer can be achieved by optimal setup of various parameters like transmit power, hop distance, modulation scheme, dynamic voltage/frequency scaling. These parameters further depend on type of channel models like Gaussian noise, block Rayleigh fading.

Transmission Power: It determines coverage area, effecting chances of locating the receiver. Signal-to-noise ratio of the channel decides successful decoding of received transmission and is proportional to transmission power. Increases in transmission power decrease likeliness of error and enhance the chance of successful transmission. But on other front leads to higher probability of collision with other transmissions in neighbor. Hence, to achieve energy-efficient successful transmission, an optimal balance between the two needs to strike out. In [2], performance with respect to variable transmission power of a multi-hop network has been analyzed. Energy of beam-forming base stations is reduced significantly at cost of minor increase in consumption at user end. [3] has evaluated performance of variable transmission power control on energy, delay, throughput, etc., which shows better results for network performance and energy saving than common-range transmission control schemes.

Hop distance: On similar ground, optimal hop distance helps in minimizing per packet expended energy across a multi-hop network. It is based on rule that increase in hop distance increases chances of error, hence increases power consumption while reduces fixed circuitry cost due to less number of reception and transmission (due of less number of hops) and vice versa.

Modulation: It is a deciding factor for the probability of success of transmission as well as to achieve energy-efficient communication. Rosas and Oberli [4] have studied optimization of modulation size with respect to Signal-to-Interference-plus-Noise Ratio (SINR). It is reported that every modulation is associated with an optimum SINR value where energy consumption for one bit of data can be found to be minimum. In this scenario, binary phase shift keying and quadrature phase shift keying are the optimum options for high transmission distances. But with decrease in transmission distance, the optimal modulation size can be as high as 64-quadrature amplitude modulation (QAM). This study is based on an error-free environment for both backward and forward frames, i.e., ignore possibility of loss of data, and energy consumed at transmission and receiving are assumed to be equal. Whereas [5] has optimized the M-ary QAM constellation size in multi-hop linear networks with goal of minimizing the energy used per bit with in average bit error rate. Modulation size and routing paths are together optimized. The circuit, transmission, and retransmission energies have been considered. While, in [6], modulation scheme has achieved energy performance by dipping total of packet retransmission and hence the amount of bits.

Dynamic Voltage/Frequency Scaling (*DVFS*): Physical layer can also handle processors and radio parameters as per ongoing working environment. By utilizing

multiple voltages and frequency levels, energy eating can be reduced significantly. The voltage and clock frequency can be varied based on workload to meet preferred performance with minimum energy expenditure [6, 7]. It is one of the most useful techniques when low-power sleep is not an alternative. A number of work are found in the literature on DVFS, and approaches which work equally well in regular and irregular workload needs more attention.

Being closer to physical medium among all layers, physical layer has vital role in energy-efficient solutions, but network components may have varying properties. So building solutions at physical layer involve separate solutions for such different components.

2.2 Data Link Layer

Data Link layer (DDL) has potential to achieve energy-efficient operation. Error control, channel allocation, and adaptive link rate (ALR) have been identified as key components.

Error control: Significant number of studies has been reported on error control at logical link part of DDL. It can be achieved by error coding, e.g., forward error correcting (FEC) [8] and retransmission, e.g., automatic repeat request (ARQ) [9, 10]. FEC is a way to control errors of data transmission. Sender appends error-correcting code to original messages, whereas ARQ deals with errors through retransmission. In view of ARQ, utilizing current state of network conditions can help in making decisions in re-transmitting packets at favorable time and hence achieve energy savings. In [9, 10], transmitter nodes make intelligent decision to reduce retransmissions by utilizing channel quality information for achieving energy reductions.

Channel Allocation: Channels are scarce resource in wireless communication and must be allocated efficiently throughout network. Channel allocation can be achieved at media access control (MAC), and being an important parameter, it can contribute significantly in archiving energy-efficient communications. An energy-efficient MAC scheme should utilize benefit from both traffic and network characteristics. Channel access MAC approaches can be majorly classified into three types, i.e., contention-based, conflict-free, and hybrid. The contention-based approaches cover channel allocations using ALOHA, slotted ALOHA, carrier sense multiple access (CSMA), CSMA/CD, CSMA/CA, whereas FDMA, TDMA, FH-CDMA, DS-CDMA are conflict-free. PRMA and D-TDMA are part of hybrid channel allocation approaches. Numeral research works have been reported in the literature with green channel allocation strategy. For instance, Wu et al. [11] have jointly addressed both power and multi-channel issues to achieve energy efficiency at a node by controlling the transmit power to reach intended receiver during transmission. But this power control approach is found more effective when numbers of channels are lesser than a threshold. Misra et al. [12] have introduced learning automata-based distributed dynamic channel allocation approach with a

focus toward improving overall system performance by reducing dropping probability in a highly mobile scenario. It helps to achieve energy saving but study lacks in experimenting with different mobility patterns. In [13], energy-efficient MAC (EE-MAC) for ad hoc protocol without significantly reducing network performance is proposed. This approach is based on principle idea of electing some nodes to form a connected virtual backbone set to route packets, while other nodes named as slaves can stay in power-saving mode. Sheelavant and Sumathi [14] have proposed a channel interference limited routing protocol for delay sensitive traffic to meet throughput increase and energy saving of cognitive radio sensor networks. In [15], two energy-efficient strategies, namely altruistic DISH, in situ DISH for cooperative multi-channel MAC Protocols have been proposed. Approach is applicable for single radio per node and does not require time synchronization. Results demonstrate 40–80% energy saving without compromising at throughput part. But, in situ is found suitable for scenario with less density nodes or low traffic.

In wide, purpose of energy-efficient channel allocation is to limit packets collision for efficient channel utilizations and hence energy resource.

Adaptive Link Rate: It is an energy proportional computing scheme, which adopts data rate with objective of optimum performance and energy efficiency depending on traffic or channel conditions. It has less complex physical layer modulation so needs less-power consumption to decode. A variable data rate scheme is used in [16] to optimize total communication energy in body sensor network and wifi. It achieves 86% energy reduction with respect to fixed data rates solution. Furthermore, Nedevschi et al. [17] have proposed an energy-saving policy for link rate adaptation based on link utilization and buffer queue length. Results are compared with link sleep policy and found that during low link utilization, sleep state is more feasible than rate adaption.

As seen, DDL has good capability toward achieving energy-efficient networking. Adding mobility awareness in this layer will help in recovery of data due to path failure.

2.3 Network Layer

In wireless mobile networks, the network layer is accountable for routing packets under mobility constraints. Apart from traditional routings approaches, following techniques can be applied to achieve energy efficiency at this layer.

Mechanical Relaying (*Store and Forward*): It is a technique applicable in wireless mobile networks where communication is intentionally delayed till meeting favorable networking conditions (e.g., improved SINR, region of less prone to error). Mobile nodes can act as relay to carry data of its own and others node. They are facilitated with ability to store information while on move. Hence, in mechanical relay (MR), mobile nodes operate under a store-carry and forward paradigm [18, 19]. Transmitting at better locations allows efficient use of radio by reducing transmit power. It also leads to less interference to other nodes and hence

better SINR at receiver side. Hence, this feature of carrying data mechanically, communicating only at the best locations and within delivery deadlines helps to achieve significant reduction in energy consumption during transmission. Kolios et al. [20] proposed a MR to solve the problem of energy efficiency in cellular network and proved that mobility prediction can be beneficial in saving energy. But study is only limited to single cell, hence lacking intra-cell communication. Message forwarding decision policy and size of message are key factors for successful energy-efficient transmission. Policy can be applied in centralized or distributed, or hybrid manner. Cross-layer approach at application and MR at network layer can together achieve further performance gains.

Energy Efficiency with Cooperation: Utilization of cooperation between nodes of the network is one of successful technique to reduce energy consumption and to achieve better performance improvement of wireless transmission [21, 22]. Cooperation can be categorized into two types, first is relay cooperation (RC) [21], in which relay nodes assist the source in transmitting information to destinations, and second is user cooperation(UC) [22] which is more suitable in multicast scenario. UC is based on concept that destinations which receive data successfully and have better channel quality to other destination nodes than source node will further assist source in transmitting data to other remaining destinations. RC and UC both can decrease the total energy consumption of network. But RC requires installation of new relay node to network, hence expensive than UC. In UC, user's relay nodes may not always have better link quality with the remaining users than source node. Performance is not always assured in UC.

Energy Efficiency with Network Coding: Under this approach, router nodes mix content of different packets and broadcast the resulting packets. Network coding (NC) helps to achieve optimum usage of network resources. Hence, it is important to explore its effect on energy-efficient systems. Chen et al. [23] have shown that by applying NC bandwidth can be saved. It is more suitable for multicasting scenario. Chen et al. [24] have evaluated the potential of coding from perspective of throughput and energy efficiency. Energy-saving factor in unicast random networks is upper limited by 3, while throughput is lower bounded by a constant factor, but it is suspected that the constant factor can be even smaller. Blind flooding factor for achieving broadcast in NC can be improved by utilizing better broadcast mechanism. Keeping this in view, [25] has combined NC with connected dominating set (CDS)-based broadcasting approach to give network coding over connected dominating set (NCDS). Energy gains have been reported as 161% over blind flooding and 37% over CDS. In [26], network coding-based probabilistic routing scheme has been projected. Results of scheme in terms of energy efficiency and reliability have been found better than probabilistic routing and pure flooding.

Packet Size: It has relationship with loss probability and provides valuable information in adjusting different network conditions for optimum utilization of wireless resources [27]. Probability of packet delivery increases with small packets achieving energy efficiency. But when overhead bits are taken into account, highest energy efficiency exists for some optimal packet size [28]. In [29], packet size optimization is devised as a nonlinear constrained problem, solved with sequential

quadratic programming. In [30], the packet size and transmission power are decided as a function of distance between transmitter and receiver under varying modulation strategy. Data compression reduces transmission time of packets by reducing transmitted bits; it can be looked as a firm technique for energy reduction and can be applied at packet payload [31] and header part [32]. Additional computation cost incurred by data compression needs to be considered for energy saving. [33] has proposed a simple low computation power hungry algorithm.

Resource Consolidation: Networks are deployed keeping in view the quality of service for peak traffic demands. In scenario when traffic follows a pattern on periodical basis [34], resources are over-provisioned during low traffic periods. Networks need not to operate in full capacity and can be dynamically adjusted according to current traffic level. Resource consolidation (RC) is a kind of routing achieves this objective by consolidating the network load and traffic on a selected set of active network nodes and shutting down other lightly loaded nodes. Load is redistributed by cooperation among network equipment [35]. RC is an attractive means in fields like data centers, CPU, wired networks.

2.4 Transport Layer

Transport layer provides service for end-to-end communication. TCP/IP stack has been proposed keeping in view of wired connections. Performance of classical transport protocols degrades considerably in wireless network. It is necessary to consider energy efficiency behavior of the transport layer protocols. Extending sleeping state, efficient congestion control, packet loss recoveries are few of approaches which can be exploited under this layer.

Extending Sleeping State: Such, approaches control data traffic to achieve maximum sleep period. Few of early work has been addressed in [36–38]. In [36], energy/throughput trade-off of TCP has been considered. In [37], energy consumption for bulk data transfer under different TCP versions like Tahoe, Reno, and New Reno has been studied. In [38] TCP header has been modified for TCP sleep option. Before sleeping, client notifies server through this option. On seeing TCP sleep from client, server will store data received from the application and does not send it immediately. In [39], energy consumption of TCP data transfer by stretching the ideal period has been considered. Bursty communication over a wireless LAN can reduce the energy expenditure in TCP data transmit by around 60%. But analysis of energy saving with impact over delay has been ignored. Hu and Li [40] have studied cross-layer-based approach for energy competence of TCP in wireless cooperative relaying networks. Relay selection is solved by using primal-dual index-based heuristic algorithm. It is shown that the energy efficiency of TCP can be enhanced by adapting the lower layer parameter, e.g., modulation, coding, frame length, and limit on retransmission time.

Efficient Congestion Control and Packet Loss: Congestion can occur if packet arrival rate exceeds packet service layer. Factors like contention, bit error,

interference contribute toward packet loss and also add to congestion. In all both factors increase packet service time and degrade energy performance. They are as such important factors to be dealt under this layer. Suitable rate adjustment and retransmission techniques will help to mitigate this issue. In [41], adaptive duty cycle-based congestion control scheme has been projected.

Research for achieving energy efficiency is more centered toward lower layers; upper layers had been ignored. Further potential of transport layer for energy-efficient solutions needs to be explored for maximal gain in this direction.

2.5 Application Layer

Application layer consists of high-level setup services for the application program and acts as interface between user and network. As being most closed to end user, this layer is the best choice for utilizing application-specific information toward designing energy-efficient solutions.

Application Protocol Modification: Energy saving can be achieved by modifying particular application protocol and utilizing traffic pattern knowledge. For instance, existing Bit Torrent, a P2P technology, used in distribute digital content in decentralized architecture requires peers to be active all the time in spite of current load. Green BitTorrent [42] is an improved version of existing BitTorrent, which allows clients sleep in a swarm by disconnecting their TCP connections with peers when not actively downloading or uploading contents, yet still active member in peer lists. An assessment of Green BitTorrent with respect to energy savings and download time has been done. Energy savings of up to 25% with standard version are realizable, but with small increase in file download time. For backwards compatibility with existing BitTorrent method to signal type of peer, i.e., green or nongreen and to wake up the sleeping clients are not mentioned. From protocol modification perspective, [43] Telnet is redesigned with a green objective to give Green Telnet Protocol, allowing the client to go to sleep and recover later. Additional control messages are required to share power state changes to avoid losing data.

Energy-Efficient Instructions: It is other tool for achieving this goal, some work toward this direction has been presented in [44, 45]. In [44], a green framework has been proposed that supports energy-conscious programming using principled approximation for expensive loops and functions. A dynamic instruction scheduling logic has been discussed in [45]. It is based on grouping a number of instructions as a single dispatch entity. The proposed logic holds and sends off extra instructions without growing the size or number of ports. The results show energy cutback of 42, 50, and 44% for dispatch, select, and issue correspondingly. Green programming can be explored further for reducing programmer burden through more automated program approximation.

Energy-saving process can involve cross-layer cooperation as power consumption is affected by each aspects of system design, varying from hardware to

applications. Parameters of multiple layers like transmit powers, rates, link schedules, routing can be utilized for joint optimization objective across protocol stack with adjustability to required service, traffic load, and surroundings dynamics. A large number of different issues have been successfully addressed by cross-layer approaches in networking. Cross-layer solution can be seen as a very promising research area in field of energy saving [46].

3 Trends

A survey on IEEE Xplore for last five years has been carried out to find out the popularity of research in energy efficiency of TCP/IP protocol stack, and recorded observations have been listed in Table 1. The following query has been used on abstract, which is further refined by publication date and including discussed layerwise approaches. Though, results may vary with inclusion/exclusion of other keywords. The outcome clearly indicates that in energy-efficient wireless communication overall research trend is increasing.

> Abstract (((((Energy OR Green) AND (Efficiency OR Efficient OR Saving OR Aware OR Conservation OR Harvesting OR Performance OR Computing OR Communication OR Radio OR Modulation OR Performance OR Consumption)) AND Wireless Network))

Table 1 Trend in IEEE Xplore over last five years

Layer year	2011 (Jan–Dec)	2012 (Jan–Dec)	2013 (Jan–Dec)	2014 (Jan–Dec)	2015 (Jan–Aug)	Total
Physical layer	123	145	133	160	78	639
Data link layer	86	74	112	108	53	433
Network layer	483	520	493	486	210	2191
Transport layer	74	78	71	62	26	311
Application layer	8	13	8	13	1	43
Total	1583	1686	1730	1742	788	7528

4 Conclusion and Future Work

This study has highlighted solutions toward energy reduction within each layer of TCP/IP protocol stack. The overall energy consumption is influenced by the functionality of each layer. Future road map requires more coordinated energy control among all layers with due consideration toward energy consumption of solution itself. Based on survey, it has been acknowledged that inclination of research is increasing in energy efficiency. Functionality of network layers are most explored one in achieving energy-efficient solutions, and application layer is least targeted. Hence, being most closed to end user, there is plenty of scope of research for achieving energy efficiency at application layer.

References

1. Mingay, S.: Green IT: the new industry shock wave. Gartner. www.ictliteracy.info/rf.pdf/Gartner_on_Green_IT.pdf. Accessed on 26 June 2014
2. Shiwen He, Yongming Huang, Wenyang Chen, Shi Jin, Haiming Wang, Luxi Yang. Joint power and feedback bit allocation for energy- efficient design in limited-feedback coordinated beamforming systems. EURASIP Journal on Wireless Communications and Networking 2015; 126
3. Bouallegue, M., Raoof, K., Ben Zid, M., Bouallegue, R.: Impact of variable transmission power on routing protocols in wireless sensor networks. In: 10th international conference on wireless communications networking and mobile computing (WiCOM 2014), pp 496–499 (2014)
4. Rosas, F., Oberli, C.: Modulation and SNR optimization for achieving energy-efficient communications over short-range fading channels. IEEE Trans. Wireless Commun. **11**(12), 4286–4295 (2012)
5. Chen, Q., Gursoy, M.C.: Energy-efficient modulation design for reliable communication in wireless networks. In: 43rd Annual Conference Information Sciences and Systems 2009. CISS 2009., 2009; 811-816
6. Zheng, G., Krikidis, I., Masouros, C., Timotheou, S., Toumpakaris, D.-A., Ding, Z.: Rethinking the role of interference in wireless networks. IEEE Commun., Mag. **52**(11), 152–158 (2014)
7. Lai, C.F., Lai, Y.X., Wang, M.S., Niu, J.W.: An adaptive energy-efficient stream decoding system for cloud multimedia network on multicore architectures. IEEE Syst. J. **8**(1), 194–201 (2014)
8. Huo, Y., El-Hajjar, M., Maunder, R.G., Hanzo L.: Layered wireless video relying on minimum-distortion inter-layer FEC coding. IEEE Trans. Multimedia **16**(3), 697–710 (2014)
9. Yao, X., Gao, Q., Fei, L.: Impact of outdated channel state information on energy efficiency of co-operative hybrid automatic repeat reQuest in wireless sensor networks. IET Wireless Sens. Syst. **4**(4), 170–175 (2014)
10. Lombardo, A., Panarello, C., Schembra, G.: A model-assisted cross-layer design of an energy-efficient mobile video cloud. Multimedia **16**(8), 2307–2322 (2014)
11. Wu, S.L., Tseng, Y.C., Lin, C.Y., Sheu, J.P.: A multi-channel mac protocol with power control for multi-hop mobile ad-hoc networks. Comput. J. **45**(1), 101–110 (2002)
12. Misra, S., Krishna, P.V., Saritha, V.: LACAV: an energy-efficient channel assignment mechanism for vehicular ad hoc networks. J. Supercomput. **62**(3), 1241–1262 (2012)

13. Shi, Y., Gulliver, T.A.: An energy-efficient MAC protocol for ad hoc networks. Wireless Sens. Netw. **1**(5), 407–416 (2009)
14. Sheelavant, K., Sumathi, R.: Energy efficient reliable routing through dynamic spectrum management in cognitive radio sensor networks. In: International Conference Contemporary Computing and Informatics (IC3I), pp. 817–822, 27–29 Nov. 2014
15. Luo, T., Motani, M., Srinivasan, V.: Energy-efficient strategies for cooperative multichannel MAC protocols. IEEE Trans. Mobile Comput. **11**(4), 553–566 (2012)
16. Li, Y., Peng, G., Qi, X., Zhou, G., Xiao, D., Deng, S., Huang, H.: Towards energy optimization using joint data rate adaptation for BSN and WiFi networks. In: IEEE 7th International Conference Networking, Architecture and Storage (NAS), pp. 235–244 (2012)
17. Nedevschi, S., Popa, L., Iannaccone, G., Ratnasamy, S., Wetherall, D.: Reducing network energy consumption via sleeping and rate-adaptation. Fifth USENIX Symposium on Networked Systems Design and Implementation (NDSI 2008), pp. 323–336, USENIX Assoc., Berkeley, CA, USA (2008)
18. Gama, S., Walingo, T., Takawira, F.: Energy analysis for the distributed receiver-based cooperative medium access control for wireless sensor networks. Wireless Sens. Syst. **5**(4), 193–203 (2015)
19. Lalos, A.S., Antonopoulos, A., Kartsakli, E., Di Renzo, M., Tennina, S., Alonso, L., Verikoukis, C.: RLNC-aided cooperative compressed sensing for energy efficient vital signal telemonitoring. Wireless Commun. **14**(7), 3685–3699 (2015)
20. Kolios, P., Friderikos, V., Papadaki, K.: Energy-efficient relaying via store-carry and forward within the cell. IEEE Trans. Mob. Comput. **13**(1), 202–215 (2012)
21. Yang, D., Zhou, X., Xiao, L., Wu, F.: Energy cooperation in multi-user wireless-powered relay networks. IET Commun. **9**(11), 1412–1420 (2015)
22. Zou, Y., Zhu, J., Zhang, R.: Exploiting network cooperation in green wireless communication. IEEE Trans. Commun. **61**(3), 999–1010 (2013)
23. Chen, J., He, K., Du, R., Zheng, M., Xiang, Y., Yuan, Quan: Dominating set and network coding-based routing in wireless mesh networks. Parallel Distrib. Syst. **26**(2), 423–433 (2015)
24. Liu, J., Goeckel, D., Towsley, D.: Bounds on the gain of network coding and broadcasting in wireless networks. In: INFOCOM (2007) 26th IEEE International Conference on Computer Communications, pp. 724–732 (2007)
25. Wang, S., Vasilakos, A., Jiang, H., Ma, X., Liu, W., Peng, K., Liu, B., Dong, Y.: Energy efficient broadcasting using network coding aware protocol in wireless ad hoc network communications. In: IEEE International Conference (ICC), pp 1–5 (2011)
26. Rout, R.R., Ghosh, S.K., Chakrabarti, S.: Co-operative routing for wireless sensor networks using network coding. IET Wireless Sens. Syst. **2**(2), 75–85 (2012)
27. Zhihui, G., Anzhong, L., Taoshen L.: EEFA: energy efficiency frame aggregation scheduling algorithm for IEEE 802.11n wireless network. China Commun. **11**(3), 19–26 (2014)
28. Li, Y., Qi, X., Keally, M., Ren, Z., Zhou, G., Xiao, D., Deng, S.: Communication energy modeling and optimization through joint packet size analysis of BSN and WiFi networks. Parallel Distrib. Syst. **24**(9), 1741–1751 (2013)
29. Oto, M.C., Akan, B.: Energy-efficient packet size optimization for cognitive radio sensor networks. IEEE Trans. Wireless Commun. **11**(4), 1544–1553 (2012)
30. Wang, T., Heinzelman, W., Seyedi, A.: Link energy minimization for wireless networks. Ad Hoc Netw. **10**(3), 569–585 (2012)
31. Misbahuddin, S., Tahir, M., Siddiqui, S.: An efficient lossless data reduction algorithm for cluster based wireless sensor network. In: IEEE International Conference Collaboration Technologies and Systems (CTS), pp. 287–290 (2014)
32. Sengupta, A., Thakur, R., Siva Ram Murthy, C.: An efficient preamble compression for multi clock-rate sampling wireless devices. In: 19th IEEE International Conference Networks (ICON), pp. 1–6 (2013)
33. Marcelloni, F., Vecchio, M.: Enabling energy-efficient and lossy-aware data compression in wireless sensor networks by multi-objective evolutionary optimization. Inf. Sci. **180**(10), 1924–1941 (2010)

34. Qureshi, A., Weber, R., Balakrishnan, H., Guttag, J., Maggs, B.: Cutting the electric bill for internet-scale systems. In: ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM 2009), pp. 123-134, Barcelona, Spain (2009)
35. Ismail, M., Zhuang, W.: Network cooperation for energy saving in green radio communications. IEEE Wireless Commun. **18**(5), 76–81 (2012)
36. Tsaoussidis, V., Badr, H., Ge, X., Pentikousis, K.: Energy/throughput tradeoffs of TCP error control strategies. In: 5th IEEE Symposium on Computers and Communications (ISCC), pp. 106–112 (2000)
37. Zorzi, M., Rao, R.R.: Energy efficiency of TCP in a local wireless environment. Mobile Netw. Appl. **6**(3), 265–278 (2001)
38. Irish, L., Christensen, K.J.: A "green TCP/IP" to reduce electricity consumed by computers. IEEE Southeastcon 302–305 (1998)
39. Hashimoto, M., Hasegawa, G., Murata, M.: Energy efficiency analysis of TCP with burst transmission over a wireless LAN. In: 11th International Symposium Communications and Information Technologies (ISCIT), pp. 292–297 (2011)
40. Hu, Z., Li, G.: On energy-efficient TCP traffic over wireless cooperative relaying networks. EURASIP J. Wireless Commun. Netw. 78 (2012). doi 10.1186/1687-1499-2012-78
41. Lee, D., Chung, K.: Energy efficient congestion control in duty-cycled wireless sensor networks. In: Consumer Electronics (ICCE), 2010 Digest of Technical Papers International Conference, pp. 493–494 (2010)
42. Blackburn, J., Christensen, K.: A simulation study of a new green BitTorrent. In: First International Workshop on Green Communications (GreenComm) along with IEEE International Conference on Communications, pp. 1–6, Dresden, Germany (2009)
43. Blackburn, J., Christensen, K.: Green Telnet: modifying a client-server application to save energy. Dr. Dobb's J. **414**, 33–38 (2008)
44. Baek, W., Chilimbi, T.: Green: a system for supporting energy-conscious programming using principled approximation. Technical Report: MSR-TR-2009-89, Microsoft Research, July 2009
45. Sasaki, H., Kondo, M., Nakamura, H.: Energy-efficient dynamic instruction scheduling logic through instruction grouping. In: ACM International Symposium on Low power Electronics and Design (ISLPED 2006), pp. 43–48, Tegernsee, Bavaria, Germany (2006)
46. Al-Jemeli, M., Hussin, F.A.: An energy efficient cross-layer network operation model for IEEE 802.15.4-based mobile Wireless sensor networks. Sens. J. **15**(2), 684–692 (2015)

Developing Small Size Low-Cost Software-Defined Networking Switch Using Raspberry Pi

Vipin Gupta, Karamjeet Kaur and Sukhveer Kaur

Abstract Software-defined networking (SDN) is a new emerging technology for networking that separates the forwarding and control plane. With SDN static, inflexible and complex network are replaced by dynamic, scalable, and innovative networks. The motivation of developing low-cost portable SDN switch arose when we were developing load balancing and stateful firewall SDN applications during our research work. To test and measure the performance of our applications, we needed low-cost SDN testbed. Existing solutions were utilizing special hardware such as NetFPGA or real switches. But these were not suitable due to high costs and complexity involved. We could have tested these applications using Mininet emulator but there are performance issues. In this paper, we created a small size, low cost, portable SDN switch for testing our SDN applications using Raspberry Pi. Our low-cost switch supports OpenFlow Specification 1.0–1.4. Raspberry Pi is Linux-based small size low-cost device which can be used as a personal computer as well as for making low-cost portable SDN switch.

Keywords Open vSwitch · OpenFlow · Raspberry Pi · SDN · Controller

1 Introduction

Computer network consists of a large number of network devices such as routers, switches, and various middleboxes such as firewalls, load balancers, network address translators having complex protocols on them. Network operators are

V. Gupta
U-Net Solutions, Moga, Punjab, India
e-mail: vipin2411@gmail.com

K. Kaur (✉) · S. Kaur
AD College, Dharamkot, Punjab, India
e-mail: bhullar1991@gmail.com

S. Kaur
e-mail: bhullarsukh96@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_16

responsible for configuring individual network devices using configuration interface.

Software-defined networking is a new networking concept in which the data plane is decoupled from control decision plane [1]. Data planes are actually dumb merchant silicon boxes. We can turn them into a simple hub, learning switch, or a router by creating flow entries in flow tables. SDN in part represents logically centralized network intelligence in control plane and data plane become simple packet forwarding device that can be programmed via open interface. OpenFlow is a prominent example of such an interface [2, 3]. OpenFlow switch has flow tables that contain packet handling rules. When a rule matches with the incoming traffic, then corresponding action such as dropping, forwarding, and flooding is taken. According to the flow table rules, OpenFlow switch behaves like a switch, router, hub, or firewall [4].

SDN is getting a lot of attention from research community as well as industry [5]. Open network foundation (ONF) has been created for promoting SDN and standardizes the OpenFlow (Fig. 1).

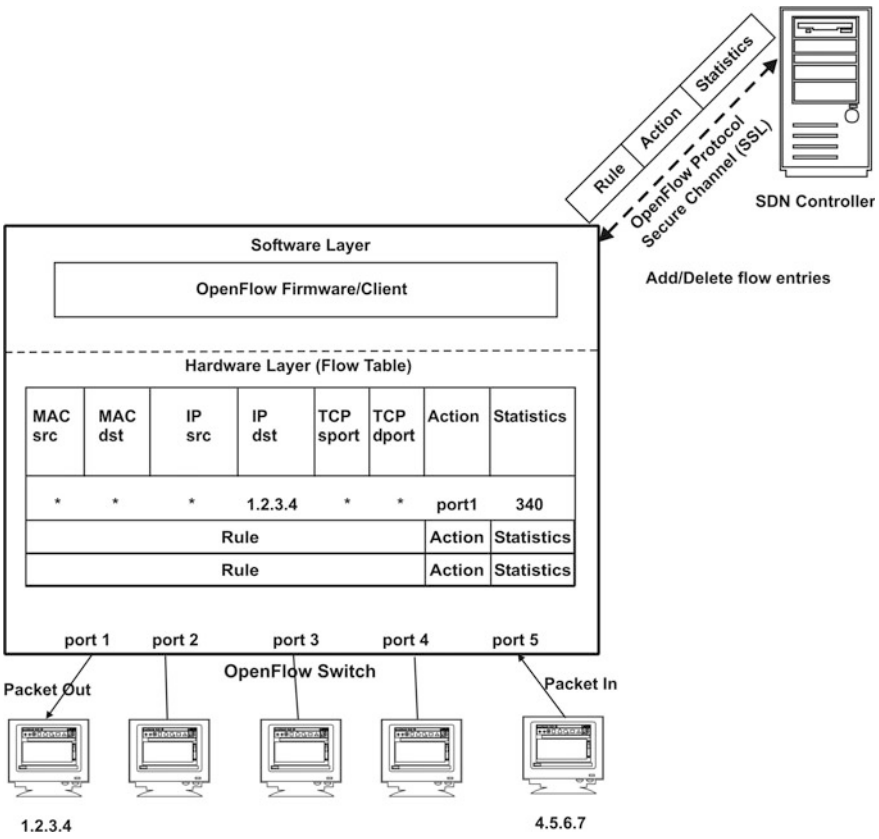


Fig. 1 SDN architecture

2 Related Work

Mininet [6, 7] is a emulator software that enables you in creating large networks on a simple laptop or virtual machine (VM). It allows you to create simple as well complex networking consisting of switches, controllers, hosts, and links. It provides a simple, robust mechanism for testing OpenFlow applications. But there are scalability issues and resource constraints when we run Mininet on a single system. Many other researchers use special devices such as NetFPGA for creating testbeds. But these SDN testbeds are not suitable due to higher cost and complexity [8]. Earlier work supported OpenFlow specification 1.0 [9], while in case of our work, it supports OpenFlow Specification 1.0–1.4.

Raspberry Pi is small size low-cost device which can be used as personal computer as well as for making low-cost SDN switch. Raspberry Pi is basically a device using embedded Linux.

3 Steps for Developing SDN Switch

Our switch was made using Raspberry Pi which comes preloaded with Raspbian operating system. For our switch, we used latest Raspberry Pi model B+ which also comes with 1 GB Ram instead of 512 MB Ram in earlier versions. The Raspberry Pi is a small, powerful, and lightweight ARM-based computer [9]. We loaded the latest Ubuntu MATE 15.04 on Raspberry Pi. Raspberry Pi contains only one LAN card. Since we wanted four ports SDN switch, so we ordered three USB-based low-cost LAN cards online. The following are the steps for converting our Raspberry Pi system to a SDN switch.

1. Attached three USB LAN cards to our Raspberry Pi system thus making total number of LAN cards available to four.
2. We downloaded a pre-built image of Ubuntu MATE which is available on the Internet [10]. We unzipped that image file and wrote the Ubuntu MATE image file on MicroSD card that comes along with Raspberry Pi system. It removed the default Raspbian image on MicroSD. We removed the Raspbian OS because it does not support the latest version of OpenFlow switch (Fig. 2).
3. We used the ‘apt-get install’ for installing the Open vSwitch packages on Raspberry Pi.
4. We used the ‘óvs-vsctl’ for making our Raspberry Pi as SDN switch and added four LAN cards as four ports of our SDN switch.
5. We attached four laptops to four ports of our Raspberry Pi SDN switch. One laptop was used as client system, one laptop as POX/RYU controller and two other laptops as servers.
6. First, we tested our load balancing application using POX controller [11, 12]. Our Raspberry Pi switch was properly working as a load balancer.

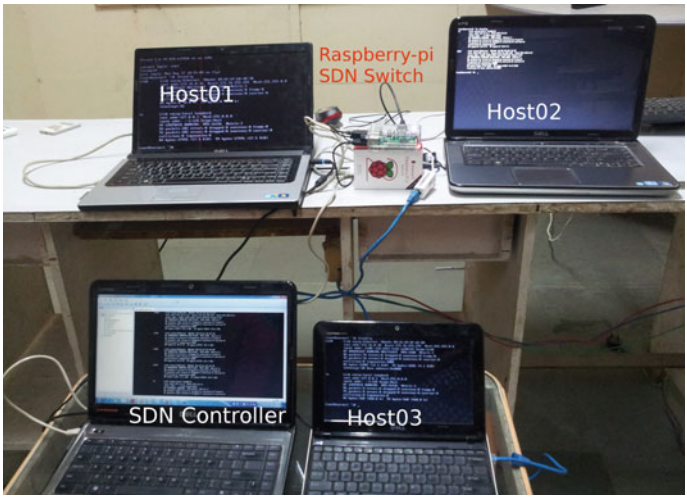


Fig. 2 Raspberry Pi-based SDN laboratory

7. Secondly, we tested our firewall application using RYU controller [13, 14]. Our Raspberry Pi switch was now properly working as firewall.

4 Laboratory Setup

For testing our switch, we created the laboratory as shown figure. Our switch ports were named eth0, eth1, eth2, eth3. We attached our POX controller on eth0 and hosts on eth1, eth2, and eth3 ports. We tested our Raspberry Pi-based SDN switch using load balancing application and firewall application (Fig. 3).

The load balancing architecture consists of OpenFlow switch network with a POX controller and multiple servers connected to the ports of the OpenFlow switch. Each server is assigned static IP address, and the POX controller maintains a list of live servers that are connected to the OpenFlow switch. Web service is running on each server on a well-known port 80.

A firewall allows or rejects a specific type of data. Our firewall application allows or restricts the traffic based on MAC addresses (Layer 2), source and destination IP addresses (Layer 3), ports (Layer 4). When a packet enters into the switch, the packet header is matched against the firewall rules.

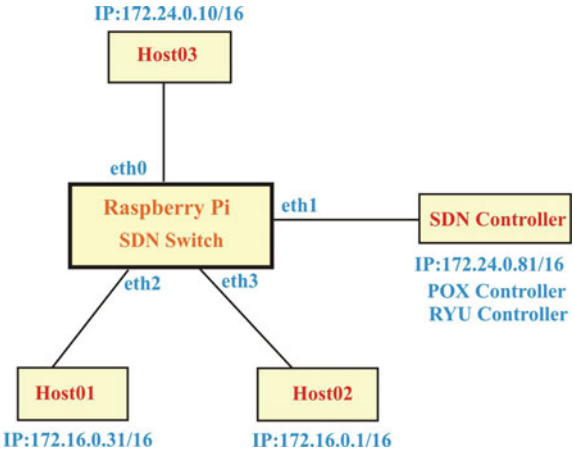


Fig. 3 Laboratory setup

```
root@sdn-raspberry-pi:~# ovs-vsctl show
11a26b40-ae15-4a50-98a0-601b7bad8a5e
    Bridge "sw0"
        Controller "tcp:172.24.0.81:6633"
        fail_mode: standalone
        Port "eth2"
            Interface "eth2"
        Port "sw0"
            Interface "sw0"
                type: internal
        Port "eth3"
            Interface "eth3"
        Port "eth1"
            Interface "eth1"
    Bridge br-int
        fail_mode: secure
        Port br-int
            Interface br-int
                type: internal
    ovs_version: "2.3.1"
root@sdn-raspberry-pi:~# _
```

Fig. 4 Switch ports for connecting hosts

We tested our load balancing application using POX controller installed on '172.24.0.81' host. Firewall application was tested using Ryu controller installed on '172.24.0.81'. Raspberry Pi SDN switch was configured to use remote controller as shown in figure. Both of these applications are working properly on Raspberry Pi-based SDN switch (Fig. 4).

5 Conclusion

Here we have successfully developed a SDN switch using Raspberry Pi by installing Ubuntu MATE Linux and other open source softwares. We were able to successfully test our load balancing and firewall applications. This switch is very low cost and portable as compared to other available alternatives in the market. Future work can involve creating a SDN testbed consisting of Raspberry-based switches and hosts.

References

1. Mendonca, M., Nunes, B.A.A., Nguyen, X.N., Obraczka, K., Turletti, T.: A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks (2013)
2. McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., Turner, J.: OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput. Commun. Rev. **38**(2), 69–74 (2008)
3. Hegr, T., Bohac, L., Uhlir, V., Chlumsky, P.: OpenFlow deployment and concept analysis. Adv. Electr. Electron. Eng. **11**(5), 327–335 (2013)
4. Lara, A., Kolasani, A., Ramamurthy, B.: Network Innovation Using Openflow: A Survey, pp. 1–20 (2013)
5. Feamster, N., Rexford, J., Zegura, E.: The road to SDN: an intellectual history of programmable networks. ACM SIGCOMM Comput. Commun. Rev. **44**(2), 87–98 (2014)
6. Handigol, N., Heller, B., Jeyakumar, V., Lantz, B., McKeown, N.: Reproducible network experiments using container-based emulation. In: Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies, pp. 253–264. ACM (2012)
7. Lantz, B., Heller, B., McKeown, N.: A network in a laptop: rapid prototyping for software-defined networks. In: Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, p. 19. ACM (2010)
8. Naous, J., Erickson, D., Adam Covington, G., Appenzeller, G., McKeown, N.: Implementing an OpenFlow switch on the NetFPGA platform. In: Proceedings of the 4th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, pp. 1–9. ACM (2008)
9. Kim, H., Kim, J., Ko, Y.-B.: Developing a cost-effective OpenFlow testbed for small-scale software defined networking. In: 2014 16th International Conference on Advanced Communication Technology (ICACT), pp. 758–761. IEEE (2014)
10. https://ubuntu-mate.org/raspberry-pi/
11. Kaur, S., Singh, J., Ghumman, N.S.: Network Programmability Using POX Controller
12. POX at https://openflow.stanford.edu/display/ONL/POX+Wiki
13. Shalimov, A., Zuikov, D., Zimarina, D., Pashkov, V., Smeliansky, R.: Advanced study of SDN/OpenFlow controllers. In: Proceedings of the 9th Central & Eastern European Software Engineering Conference in Russia, p. 1. ACM (2013)
14. Lin, T., Kang, J.-M., Bannazadeh, H., Leon-Garcia, A.: Enabling SDN applications on software-defined infrastructure. In: Network Operations and Management Symposium (NOMS), 2014 IEEE, pp. 1–7. IEEE (2014)

A Timestamp-Based Adaptive Gateway Discovery Algorithm for Ubiquitous Internet Access in MANET

Prakash Srivastava and Rakesh Kumar

Abstract Internet gateways are used for integration of mobile ad hoc network (MANET) with Internet to increase its usability. Mobile nodes in MANET need to discover an Internet gateway to obtain Internet connectivity. Existing gateway discovery approaches such as reactive, proactive, and hybrid suffer from low network throughput and performance trade-off. In the proposed gateway discovery scheme, proxy nodes are utilized to reduce network overhead as well as dynamically adjust proactive area of gateways according to traffic load on a gateway. The gateway selection scheme uses a timestamp factor besides hop count and queue length for selecting an optimal Internet gateway. The performance of the proposed approach is analyzed through simulation on the basis of routing overhead and gateway discovery time. Results show that our approach has been found outperforming to existing approaches.

Keywords Mobile ad hoc network · TTL (time-to-live) · Adaptive gateway discovery · Timestamp

This project is partially funded by University Grant Commission (UGC), India under major research project vide letter no. 42-140/2013 dated 14th March 2013 and Technical Education Quality Improvement Programme Phase II (TEQIP II).

P. Srivastava (✉) · R. Kumar
Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur, Uttar Pradesh, India
e-mail: prakash2418@gmail.com

R. Kumar
e-mail: rkiitr@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_17

1 Introduction

Mobile ad hoc network [1] and the fixed networks such as Internet are integrated to extend network coverage and also to enhance usability of such networks. The architecture of such network differs from Internet as it makes assumptions of various sorts on the structure, dynamic topology, and communication patterns. Due to these differences, integrating different networks to form a hybrid network is a challenging issue. Internet gateway acts as a bridge between a MANET and the Internet for achieving integration. Communication of mobile devices such as laptop, PDA, smart phones in an ad hoc network and a fixed device in Internet needs changes in MANET routing protocol such as AODV, DSR. The challenge in integration of MANETs to Internet originates from the need to inform mobile nodes about available Internet gateways. In this scenario, there is a great challenge of making an optimal consumption of scarce network resources such as bandwidth battery power. In the proposed approach, proxied adaptive is used for MANET-Internet integration in which some nodes in the MANET act as proxy nodes to minimize the load on gateway and also reduce network overhead as depicted in Fig. 1.

The organization of the rest of the paper is as follows. Related work about MANET-Internet integration and various gateway discovery approaches are described under Sect. 2. The proposed gateway discovery scheme is presented in Sect. 3. Section 4 presents performance evaluation using simulation. Finally, conclusions along with directions of future work are presented in Sect. 5.

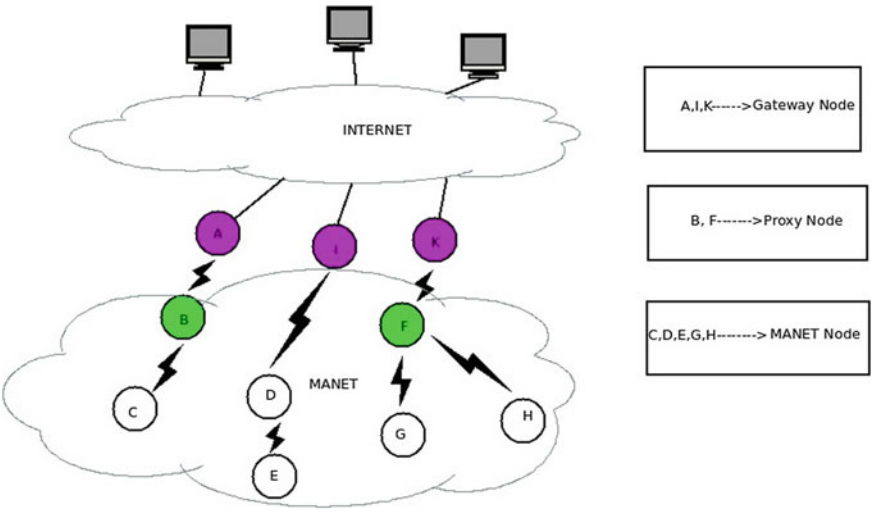


Fig. 1 MANET-Internet integration strategy

2 Related Work

Hamidian et al. [2] proposed a gateway discovery scheme for Internet access to mobile ad hoc networks. The AODV routing protocol used in the MANET domain was modified. They devised three gateway discovery approaches, namely reactive, proactive, and hybrid for Internet connectivity. All these three approaches are based on single hop count metric for gateway discovery.

A load-adaptive gateway discovery proposal was proposed by Park et al. [3], which resizes proactive gateway advertisements range dynamically and reduces gateway acquisition latency. For adjusting this area dynamically, access gateway should know the information like number of source nodes and network nodes that requires Internet connectivity and size of the network. This approach takes into account the load of the network while calculating the TTL value dynamically, but the problem of gateway advertisement messages periodicity are not addressed.

The existing solution for MANET-Internet integration was analyzed by Nordstrom et al. [4] but flexibility and robustness were found lacking. Authors come to the conclusion that interconnection scheme's inability to express indirection is the cause for routing failure. Another problem concerns state replication in which a route update does not succeed to replicate all the routing state required to forward packets to a gateway. The proposed scheme when combined with AODV enhanced the packet delivery ratio up to 20% which is shown through simulation.

Zaman et al. [5] discussed two important issues in MANET-Internet integration. First, the path load balancing during communication of mobile nodes with gateways. Second, mobile nodes register with a gateway before communication begins. This approach is focused on combining adaptive gateway discovery, balancing path load mechanism, and maximal source coverage [6] scheme. The simulation results show the improvement in normalized routing load but it does not show any significant improvement in packet delivery ratio and end-to-end delay as compared to other approaches.

Yuste et al. [7] proposed an adaptive gateway discovery scheme in which the frequency of gateway advertisement (T) is optimized using fuzzy logic system and TTL value is varied according to traffic load. However, this scheme does not focus on efficient handover scheme and determination of optimized proactive area which is also primarily important to improve network performance.

3 Proposed Gateway Discovery Mechanism

We call our scheme as timestamp-based proxy adaptive gateway discovery algorithm. This approach takes the benefit of local information provided by proxy which is gained by some mobile nodes in the network [8]. Since, adaptive gateway discovery scheme creates a reactive and proactive zone, gateway advertisement

Fig. 2 Modified gateway advertisement (GW_ADV) message format

Type	Reserved	Prefix size	Hop Count
Broadcast ID			
Destination IP Address			
Destination Sequence Number			
Source IP Address			
Lifetime			
Q			
N			
T			

(GWADV) does not require flooding across whole network [9]. Nodes which are intermediate acting as proxy in proactive zone border reply using a gateway reply (GW_REP) unicast to the originator and thereby reducing the overhead.

Majority of gateway selection schemes/approaches use minimum number of hops to select an optimal gateway [10–12], consequently under high traffic load, the nearest Internet gateway suffers from bottleneck, besides there is also some nodes which are congested along the gateway route. In our scheme, we introduce an additional metric, i.e., timestamp factor (T) as shown in Fig. 2 in gateway advertisement message (GW_ADV) format. Now gateway selection metric takes into account four metrics, and therefore now the composite metric gc is computed with the help of modified Eq. 1.

$$gc = hc + T + (N/N + 1) + (Q/Q + 1) \tag{1}$$

The source node always selects gateways having high response time, and the traffic is distributed evenly among other gateways resulting in lower chances of collision and packet loss due to high congestion.

3.1 Algorithm for Calculation of Proactive Area

```
1. Initialize
2. ttl ← A.η/N.2P
                n(Δt)   n(Δt)
3. Load, ρ  =   ∑ λi   . ∑ ζi
                i=1     i=1
                // Event advertisement timer expires
4. if ttl > 0 then
5. GW _REP.src = this gateway;
6. GW_REP.dst = broadcast;
7. GW _REP.ttl = ttl;
8. GW_REP.T=current time;
```

```
9. send GW_REP ;
10. end if    //Event receive GW_REQ (Route request)
11. set-up reverse route;
12. GW_REP.src = this_gateway;
13. GW_REP.T=current_time;
14. GW_REP.dst = GCREQ.src;
15. send GW_REP ;  //Event load estimation timer expires
16. γmax=ρ +0.005;
17. γmin= ρ – 0.005;
18. Estimate new load as
                n(Δt)      n(Δt)
        ρ   =   ∑ λi   .   ∑ ζi
                i=1        i=1
19. If ρ >γmax then ttl ← ttl + 1;
20. If  ρ < γmin then ttl← ttl -1; //Event receive DATA
21. communicate with DATA.src;
```

3.2 Algorithm for Congestion Mitigating Gateway Selection and Discovery Scheme

```
1. Initialize
2. G ←∅; where G set contains tuple of form (g,T) //g←set of gate-
ways    // T←Timestamp factor
3. last _reply_ time ← 0;// Event route to Internet lost
4. if (current_time – last_reply_time) >= time between periodic GCREP then
5. GW_REQ.src = this_node;
6. GW_REQ.dst = broadcast;
7. send GW_REQ ;
8. end if     //Event receive GW_REQ (Route request)
9. setup reverse route;
10. if G ≠ 0 then
11. let g is the selected gateway from this node according to metric gc;
12. gc = hc + T + (N/N+1) + (Q/Q+1)
13. GW_REP.src = g;
14. GW_REP.T=current_time - T of selected g from (g,T);
15. GW_REP.dst = GCREQ.src;
16. GW_REP.proxy = yes;
17. send  GW_REP ;
18. else
```

```
19. forward GW_REQ // Event receive GW_REP
20. Set up forward route
21. if GW_REP.dst ≠ this_ node then
22. forward GW_REP
23. if GW_REP.dst=broadcast then
24. last_reply_time = current_time
25. end if
26. end if
27. G ← G U GW_REP.src;
28. T ← current_time – GW_REP.T;
29. schedule active gateway timer for GW_REP.src;
        // Event active gateway g timer expires
30. G ← G/{g , T}; //Event data transmit
31. if G ≠ ∅ then
32. Select a g which belongs to G such that metric gc is minimum
33. gc =T+ hc + (N/N+1) + (Q/Q+1)
34. send data
35. else
36. send GW_REQ
37. end if
```

4 Performance Evaluation

The proposed approach is implemented using NS-2 simulator (NS 2.34 version). For performance comparison of our proposed approach with existing ones, common simulation parameters are given as per Table 1 [13–16].

4.1 Performance Metrics

The following performance metrics have been used.

- Routing Overhead: The total number of control messages, including gateway discovery generated is called routing overhead. It is computed by the formula given below:

$$R_{\text{overhead}} = \sum_{i=1}^{n} \text{Overhead}_i$$

Table 1 Simulation parameters

Parameters	Values
Number of mobile nodes	15 and 60
Number of sources	10, 20, 30, 40 and 50
Wireless transmission range	250 m
Number of gateways	4
Number of hosts	2
Topology size	1200 × 800 m
Traffic type	CBR
Packet size	512 bytes
Packet sending rate	5 packets/s
Mobility model	Random waypoint
Length of interface queue	50 packets
Link level layer	IEEE 802.11 DCF
Interval between successive GW_ADV advertisement	5 s
Speed of a mobile node	20 m/s
Simulation time	500 s

- Gateway Discovery Time: The times required to search and discover a gateway is known as gateway discovery time. It is computed by the formula given below:

$$T_{\mathrm{GWD}} = \text{searching time} + \text{delay latency}.$$

4.2 Results and Discussion

The routing overhead in case of our proposed scheme as shown in Fig. 3 shows less number of routing overhead messages as compared to other gateway discovery schemes due to proxy and less congestion due to timestamp factor which causes less packet drops and less retransmission, consequently less routing overhead.

If we are considering the fixed scenario of four gateways and increasing number of source nodes, the overhead caused by our proposed scheme in terms of number of message is less compared to other gateway discovery schemes as displayed in Fig. 4. The scalability of our proposed scheme is better due to our unique congestion mitigating scheme and integration of proxy node with gateways which does not cause overload situation on gateways.

The proactive algorithm shows less gateway discovery time in short time span and bad performance for longer time interval. Interval time is the time between successive solicitations. The discovery time for RMD scheme is relatively constant, as the frequency of solicitations depends on mobility condition. Our proposed gateway discovery scheme performs better in terms of gateway discovery time even in higher time intervals, and it is clearly reflected in Fig. 5.

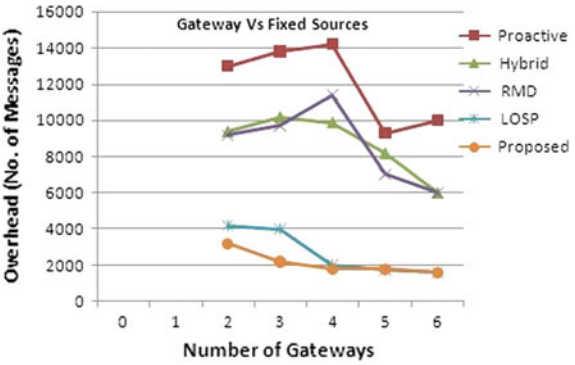


Fig. 3 Routing overhead when there is fixed number of sources

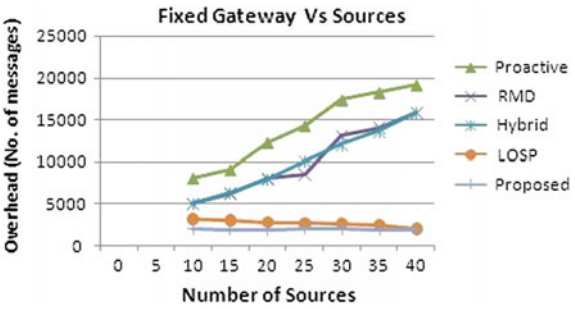


Fig. 4 Routing overhead when there is fixed number of gateways

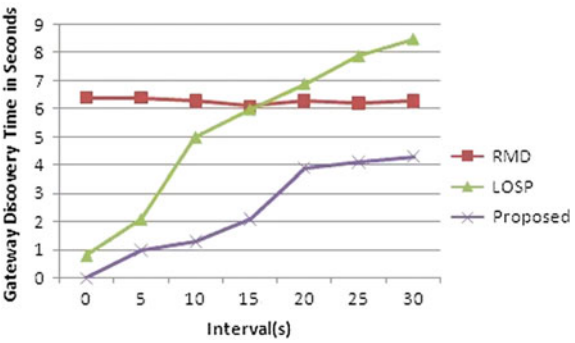


Fig. 5 Gateway discovery time

5 Conclusions and Future Scope

A new proxied adaptive algorithm is designed which exploits the traffic load on the gateway to dynamically adjust the proactive range. Mobile nodes use timestamp value which is set by a gateway in GW_REP message to calculate the composite metric *gc* and thus select an optimal gateway with least congested route. Our proposed protocol provides two benefits. First, it is scalable when the number of gateways and source node increases. Second, it can also help a node choose an efficient gateway among multiple available gateways with highest response time with lower packet loss due to congestion. The future works include incorporation of security mechanism to our modified proxy gateway discovery scheme. Further, improvement may also include calculation of more accurate optimal proactive zone.

References

1. Murthy, C.S.R., Manoj, B.S.: Ad Hoc Wireless Networks, Architectures and Protocols. Pearson Education (2004)
2. Hamidian, A., Korner, U., Nilsson, A.: A Study of Internet Connectivity for Mobile Ad Hoc Networks in NS2. Department of Communication Systems, Lund Institute of Technology, Lund University (2003)
3. Park, B.N., Lee, W., Lee, C.: QoS-aware Internet access schemes for wireless Ad Hoc networks. Elsevier J. Comput. Commun. **30**, 369–384 (2007)
4. Nordstrom, E., Gunningberg, P., Tschudin, C.: Robust and flexible Internet connectivity for mobile Ad Hoc networks. Elsevier J. Ad Hoc Netw. **9**, 1–15 (2011)
5. Zaman, R.U., Khan, K.U.R., Reddy, A.V.: Path load balanced adaptive gateway discovery in integrated internet-MANET. In: IEEE International Conference on Communication Systems and Network Technologies, pp. 203–206 (2014)
6. Ruiz, P.M., Gomez-Skarmeta, A.: Maximal source coverage adaptive gateway discovery for hybrid Ad Hoc networks. Lect. Notes Comput. Sci. **3158**, 28–41 (2004)
7. Yuste, A.J., Trivino, A., Trujillo, F.D., Casilari, E.: Using fuzzy logic in hybrid multihop wireless networks. Int. J. Wirel. Mobile Netw. **2**(3), 96–108 (2010)
8. Kumar, R., Mishra, M., Sarje, A.K.: A proactive load-aware gateway discovery in Ad Hoc networks for internet connectivity. Int. J. Comput. Netw. Commun. (IJCNC) **2**(5), 120–139 (2010)
9. Ruiz, P.M., Ros, F.J.: Low overhead and scalable proxied adaptive gateway discovery for mobile Ad Hoc networks. In: 3rd IEEE International Conference on Mobile Ad-hoc and Sensor Systems, Vancouver, Canada, pp. 226–235 (2006)
10. Shahid, M., Iqbal, A., Kabir, M.H.: Hybrid Scheme for discovery and selecting Internet gateway in Mobile Ad Hoc Network. Int. J. Wirel. Mobile Netw. (IJWMN) **3**(4), 83–101 (2011)
11. Das, S., Perkins, C.E., Belding-Royer, E.M.: Ad-hoc on-demand distance vector routing RFC 3561. In: IETF (July 2003)
12. Bouk, S.H., Sasase, I., Ahmed, S.H., Javaid, N.: Gateway discovery algorithm based on multiple QoS path parameters between mobile node and gateway node. J. Commun. Netw. **14** (4), 434–442 (2012)
13. Ruiz, P., Gomez-Skarmeta, A.: Adaptive Gateway discovery mechanisms to enhance internet connectivity for mobile Ad Hoc networks. J. Ad Hoc Sensor Wireless Networks **1**, 159–177 (2005)

14. Ghassemian, M., Friderikos, V., Aghvami, H.: On the scalability of internet gateway discovery algorithms for Ad Hoc networks. In: International Workshop on Wireless Ad Hoc Networks (2005)
15. Vanjara, R.K., Misra, M.: An efficient mechanism for connecting MANET and the internet through complete adaptive gateway discovery. In: 1st International Conference on Communication System Software and Middleware, pp. 1–5 (2006)
16. Attia, R., Rizk, R., Ali, H.A.: Internet connectivity for mobile Ad Hoc network: a survey based study. J. Wirel. Netw. Springer 1–26 (2015)

A Directed Threshold Signature Scheme

Manoj Kumar

Abstract Directed signature is a solution of such problems when signed information is sensitive to message holder/signature receiver. Generally, in a directed signature, the signer is a single entity. But, when a sensitive message is signed by an organization and needs the approval of more than one entity, threshold signature scheme is a solution of this situation. To keep in mind, this paper presents a threshold directed signature scheme.

1 Introduction

Physical signature is an old and natural tool to authenticate the communication, but it does not work in electronic messages and the signer has to rely on digital signature [1]. Digital signature is a cryptographic tool to solve this problem of electronic authentication. Basically, digital signature has a self-authentication property, which means that someone has public information related to the signature, will be able to check its validity, but he/she will not able to forge this signature for other messages. This self-authentication property [2] of digital signatures is definitely suitable for many applications such as broadcasting of announcements and publication of public key certificates, but it is quiet unsuitable for some situations [3].

In some conditions, when the message are very much sensitive to the signature, receiver/message holder such that her/his medical reports, income tax related information, any personal information or most personal business transactions are these messages [4]. For these conditions, the information is signed such that only the information holder will able to verify the signature and also able to prove the

M. Kumar (✉)
Department of Mathematics, Rashtriya Kishan Postgraduate College, Shamli 247776, India
e-mail: yamu_balyan@yahoo.co.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_18

validity of the signature to a third person, whenever it is required. These types of signatures are known as directed signatures [3–6]. In a directed signature scheme [3], the receiver always has full control over the process of signature verification. No other person can check the validity of this type signature without the help of signer/receiver [1].

In most situations, generally a single identity creates signature on the message. But there are so many conditions when the message is on behalf of a group/organization, that message may require the approval or consent of several people [2]. In these conditions, the signature is created by more than one identity rather than by a single identity [5]. In case of large bank transaction, which requires the signature of more than one person [7]. In such a condition, the problem can be solved by having a separate digital signature for every required signer, but this type of solution makes the verification process very typical [8]. This problem can be solved with the help of threshold signature [8]. The (t, n) threshold signature schemes [2, 7–10] are used to solve these problems. Threshold signatures are based upon the concept of threshold cryptography [9, 11, 12].

1.1 Paper Organization

Section 2 is about some basic tools. In Sect. 3, we present a threshold directed signature scheme. Section 4 discusses the security of the proposed scheme. An illustration of the scheme is discussed in Sect. 5. Conclusion is in Sect. 6.

2 Preliminaries: Some Basic Tools

2.1 In This Paper, We Will Use the Following Public Parameters

- p: a prime number.
- q: a prime number and $q|p - 1$.
- g: a generator [3] of order q in Z_P^*.
- h: one-way hash function [13].

It is assumed that user A selects an integer $x_A \in Zq$ and will be able to compute a relative value/integer $y_A = g^{x_A} \bmod p$. Here, the integer x_A is the secret/private key of the user A, and y_A is his/her public key.

2.2 Schnorr's Signature Scheme

In the above scheme, the signature of the signer A on a message m is given by a pair (r_A, S_A), where, $r_A = h(gk_A \bmod p, m)$, and $S_A = k_A - x_A \cdot r_A \bmod p$. The integer k_A is random and secret/private to A. The signature is verified by checking the equality.

$$r_A = h(gS_A y r_A \bmod p, m).$$

3 Directed Threshold Signature Scheme

This section presents a threshold directed signature scheme [13, 14]. Suppose a group G of n designated users, out of which any t members are able to signed a message m. In our scheme, the message holder/signature receiver B will be able to check the signature authenticity, and he/she can prove this message authenticity to a third person C, whenever it is needed. It should be noted that no one other than the message holder B can check the validity of this kind of signature without the help of holder B [14]. We describe a construction of threshold directed signature scheme for this situation as follows.

In our scheme, there exists a trusted share distribution center (SDC) [13, 14], which is able to determine the secrets parameters and the secret shares $v_i, i \in G$ for all members of the group. Again assume that H be a subset of G, containing t members. We also have a designated combiner DC for collecting partial signatures of each participant of subgroup H. Any shareholders in the group/subgroup have equal authority with respect to the main secret key for signature generation. In the proposed scheme, the generation of the required directed signature needs t signers out of n signers and interaction with DC. This scheme has the following steps.

3.1 Generation of Secret Key and Secret Shares for Group

(a) SDC also selects a polynomial

$$g(x) = a_0 + a_1 x + \cdots a_{t-1} x^{t-1} \bmod q, \text{ with } a_0 = K = g(0).$$

(b) SDC compiles group public key, y_G, as, $y_G = g^{g(0)} \bmod p$.
(c) SDC computes private shares v_i for each user in group G, as,

$$v_i = g(u_i) \bmod q.$$

Here, u_i is public information related to user i in the group G.
(d) SDC transfers v_i to each user in a secret manner.

3.2 Generation of Partial Signature by Any t Signer

Let any t signers out of n signers agree to sign a message m for receiver B, they generate the signature using following steps.

(a) Each member i randomly picks K_{i_1} and $K_{i_2} \in Zq$ and then computes

$$w_i = gK_{i_2} - K_{i_1} \bmod p \quad \text{and} \quad z_i = y_B K_{i_2} \bmod p.$$

(b) Each signer computes Z, W, and R as

$$W = \prod_{i \in H} w_i \bmod q, Z = \prod_{i \in H} z_i \bmod q, \quad \text{and} \quad R = h(Z, W, m) \bmod q.$$

(c) Each signer i modifies corresponding share, as

$$\mathrm{MS}_i = v_i. \prod_{j=1, j \neq i}^{t} \frac{-u_j}{u_i - u_j} \bmod q.$$

(d) Each signer i computes

$$s_i = K_{i_1} - \mathrm{MS}_i \cdot R \bmod q.$$

(e) DC collects the partial signatures and produces

$$S = \sum_{i=1,}^{t} s_i \bmod q.$$

(f) $\{S, W, R, m\}$ is desired directed signature.

3.3 Verification of Digital Signature {S, W, R, M}

(a) The signature holder B recovers $\mu = gS(y_G)RW \bmod p$ and recovers $Z = \mu x_B \bmod p$.
(b) The signature holder B checks the validity of signature by verifying $R = h(Z, W, m) \bmod q$.

3.4 *Proof of Validity by Signature Receiver to Any Third Party* C

(a) The signature holder B sends $\{S_A, W_B, r_A, m, \mu\}$ to third party.
(b) Third party checks if $r_A = h(Z_B, W_B, m) \bmod q$.
If this does not hold third party stops the process; otherwise goes to the next steps [13, 14].
(c) Signature receiver (in a zero-knowledge fashion) proves to C that $\log_{\mu} Z_B = \log_g y_B$ as follows.

- Third party selects randomly two values u and $v \in Zp$ and then finds $w = \mu u \cdot gv \bmod p$ and passes this value w to receiver.
- The signature receiver selects randomly a value $\alpha \in Zp$ and then calculates another value $\beta = w \cdot g\alpha \bmod p$ and $\gamma = \beta x_B \bmod p$, and then passes it to third party.
- The signature receiver verifies that $w = \mu u \cdot gv \bmod p$. The third party verifies $\beta = \mu u \cdot gv + \alpha \bmod p$ and $\gamma = Z_B u y_B v + \alpha \bmod p$.

In this way, the third party ensures himself that the signature receiver is an authentic user.

4 Security Discussion

This section is about the security aspect of the proposed scheme.

- Is it possible that an antagonist retrieves group secret key $g(0)$ with the help of group public key y_G? It is computationally infeasible because this is equivalent to solve a discrete logarithm problem.
- Is it possible that an antagonist recovers the secret information v_i, from the information u_i? No, it is computationally infeasible because g is selected randomly.
- Is it possible that an antagonist recovers the secret information v_i, K_{i_1} and s_i, from the equation $s_i = K_{i_1} - MS_i \cdot R \bmod q$? No, it is computationally infeasible because unknown parameters are three and the number of equation is only one.
- Is it possible that an antagonist recovers the group secret key $g(0)$ or any partial information from the equation, $S = \sum_{i=1}^{t} s_i \bmod q$? This is again computationally infeasible due the property of the equation.
- Is it possible that an antagonist impersonates a shareholder of subgroup H? To impersonate, an antagonist needs a related secret share v_i to generate corresponding secret value s_i. To obtain this secret information from the public information is computationally infeasible.

- Is it possible that an antagonist forges the digital signature $\{S, W, R, m\}$ by using the equation

$$\mu = [gS(y_G)RW] \bmod p?$$

  To recover S from the above equation is equivalent to solving a discrete logarithm problem.
- Is it possible that a group of antagonist act in collusion to recover the polynomial $g(x)$? Yes, this is possible, but this vulnerability is not a pitfall of the proposed scheme. Actually, this is the basic characteristic of the proposed scheme.

5 Illustration

To illustrate the proposed scheme, we consider that there are four users. Out of four users A, C, E, and F any two users, say, A and F can generate the directed signature for message m. The secret and public key pair $x_B = 6$, $y_B = 8$ of the receiver B. The following steps illustrate our scheme.

5.1 Generation of Group Secret Key and Partial Secret Shares

Let SDC choose $p = 23$, $q = 11$, $g = 18$, and $g(x) = 3 + 5x \bmod 11$, where $g(0) = 3$ is the group secret key. The public values u_i and corresponding secret shares v_i of users are as follows.

Users	Public value (u_i)	Secret share (v_i)
A	9	4
C	12	8
E	14	7
F	16	6

Now, the SDC computes the private/secret key as $g(0)$ and then recovers the group public key, y_G, as $y_G = 18^3 \bmod 23 = 13$.

5.2 Signature Generation by Any t Users

Users A and F out of four users agree to sign a message m for user B, then the signature generation has the following steps.

(a) The user A randomly selects $K_{a_1} = 2$, $K_{a_2} = 7$ and computes $w_1 = 3$, $z_1 = 12$. Similarly, the user F randomly selects $K_{f_1} = 5$, $K_{f_2} = 9$ and computes $w_4 = 4$, $z_4 = 9$.
(b) Both the users A and F make (w_1, w_4) and (z_1, z_4) publicly available through a broadcast channel. Once all (w_1, w_4) and (z_1, z_4) are available, each user in H computes the product Z, W, and R as

$$W = 12, Z = 16 \quad \text{and} \quad R = h(16, 12, m) \bmod 11 = 5(\text{let}).$$

(c) The users A and F compute their modified shares as $MS_A = 6$ and $MS_G = 8$.
(d) The user A uses his/her modified share $MS_A = 6$ and random integer $K_{a_1} = 2$ and calculates his/her partial signature $s_1 = 5$.
(e) The user F uses his/her modified shadow, $MS_G = 8$, and random integer $K_{f_1} = 5$ and calculates his/her the partial signature $s_2 = 9$.
(f) Both the users A and F send their partial signature to DC who produces a group signature $S = 3$.
(g) DC sends {3, 12, 5, m} to B as signature of the group G for the message m.

5.3 Signature Verification by B

(a) B computes $\mu = [18^3.13^5.\ 12] \bmod 23 = 3$ and $Z = 16$.
(b) B checks the validity of signature by computing $R = 5$.

5.4 Proof of Validity by B to Any Third Party C

(a) B sends {3, 12, 5, m, 3} to C, and C checks that $R = 5$.
(b) Now, B proves to C that $\log_3 16 = \log_{18} 8$ in a zero-knowledge fashion [15] by using the following confirmation protocol.

(i) C chooses at random $u = 11$, $v = 13$ and computes $w = 2$ and sends w to B.
(ii) B chooses at random $\alpha = 17$ and computes $\beta = 16$ and $\gamma = 4$ and sends β, γ to C.
(iii) C sends u, v to B, by which B can verify that $w = 2$.
(iv) B sends α to C, by which she can verify that $\beta = 16$ and $\gamma = 4$.

6 Conclusion

The security of this cryptosystem is [16–18] based on the discrete log problem. Only $t - 1$ shadows are not sufficient to obtain the group secret key and they will also get no information about the group secret key, until t individuals act in collusion. In this scheme, there is a designated combiner *DC* who collects the partial signature of the signer [19, 20]. We should note that there is no secret information associated with the *DC* [21–24]. Every user can compute his/her modified share under mod q. If q is not prime, then the calculation of the exponents is performed by mod $\Phi(q)$, which is not a prime. This implies that Lagrange interpolation for calculating the modified shadows will not work (except when $q = 3$, in which case we are not interested). Consider the situation, when $\prod_{j=1,j\neq i}^{t}(u_i - u_j)$ and q are co-prime. In this case, there is no way to find out the multiplicative inverse of $\prod_{j=1,j\neq i}^{t}(u_i - u_j) \bmod q$. There is only possibility of selecting the large prime q numbers in order for each person to get around this difficulty. These signature schemes are meaningless to any third party because there is no way for him to prove its validity. The only knowledge of Z is not sufficient to prove the validity of signature. Signature receiver also has to perform the confirmation protocol in a zero-knowledge fashion to prove the validity of signature [25–32]. No doubt, the communication cost of the proposed scheme is very high, so in future, we should try to reduce its cost without compromising the security of the scheme.

References

1. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Ingo. Theor. **31**, 644–654 (1976)
2. Desmedt, Y., Frankel, Y.: Shared generation of authenticators and signatures. In: Proceedings of Advances in Cryptology—Crypto 91, pp. 457–469. Springer, New York (1991)
3. Lim, C.H., Lee, P.J.: Security protocol. In: Proceedings of International Workshop, LNCS, vol. 1189. Springer, Cambridge, United Kingdom (1996)
4. Lim, C.H., Lee, P.J.: Modified Maurer-Yacobi, scheme and its applications. In: Advance in Cryptology—Auscrypt, LNCS, vol. 718, pp. 308–323 (1993)
5. Boyar, J., Chaum D., Damgard, I., Pederson, T.: Convertible undeniable signatures. In: Advances in Cryptology—Crypto 90, LNCS, vol. 537, pp. 189–205 (1991)
6. Chaum, D.: Designated confirmer signatures. In: Advances in Cryptology Euro crypt 94, LNCS, vol. 950, pp. 86–91 (1995)
7. Desmedt, Y.: Society and group oriented cryptography. In Proceedings of Advances in Cryptology—Crypto 87, pp. 457–469. Springer, New York (1988)
8. Harn, L.: (*t, n*) Threshold signature scheme and digital multisignature. In: Proceedings of workshop on cryptography and data security, 7–9 June, pp. 61–73. Chung Cheng Institute of Technology, ROC (1993)
9. Desmedt, Y.: Threshold cryptography. In: European Transactions on Telecommunications and Related Technologies. vol. 5, no. 4, pp. 35–43 (1994)

10. Gennaro, R., Jarecki Hkrawczyk, S., Rabin, T.: Robust threshold DSS signature. In: Proceedings of Advances in Cryptology—Euro Crypto 96, pp. 354–371. Springer, Berlin (1996)
11. Schnorr, C.P.: Efficient signature generation by smart cards. J. Cryptol. **4**(3), 161–174 (1994)
12. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
13. Lal, S., Kumar, M.: Application of directed signature scheme. South East Asian J. Math. Math. Sci. **2**(1), 13–26. Also available at http://arxiv.org/ftp/cs/papers/0409/o409050.pdf
14. Lal, S., Kumar, M.: A directed signature scheme and its applications. In: Proceedings of National Conference on Information Security, New Delhi, 8–9 Jan 2003, pp. 124–132. Also available at http://arXiv.org/ftp/cs/papers/0409/o4090036.pdf (2003)
15. Guillou, L.C., Quisquater, J.J.: A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory. In: Advances in Cryptology—Eurocrypt 88, LNCS, vol. 330, pp. 123–128 (1988)
16. Umaprasada Rao, B., Vasudeva Reddy, P.: ID-based directed multi-proxy signature scheme from bilinear pairings. Int. J. Comput. Sci. Secur. (IJCSS) **5**(1) (2011)
17. Zhang, J., Yang, Y., Niu, X.: Efficient provable secure ID-based directed signature scheme without random oracle. In: Proceedings of the 6th International Symposium on Neural Networks: Advances in Neural Networks, LNCS, vol. 5553, pp. 318–327. Springer (2009)
18. Vasudeva Reddy, P., Umaprasada Rao, B., Gowri, T.: ID-based directed threshold multisignature scheme from bilinear pairings. Int. J. Comput. Sci. Eng. **2**(1), 74–79 (2009)
19. Sun, X., Li, J., Chen, G., Yung, S.: Identity-based directed signature scheme from bilinear pairings. eprint.iacr.org/2008/305.pdg
20. Lu, R., Lin, X., Cao, Z., Shao, J., Liang, X.: New (t, n) threshold directed signature scheme with provable security. Inf. Sci. **178**(3), 756–765 (2008)
21. Lu, R., Cao, Z.: A directed signature scheme based on RSA assumption. Int. J. Netw. Secur. **2** (3), 182–186 (May 2006)
22. Wang, Y.: Directed signature based on identity. J. Yulin College **15**(5), 1–3 (2005)
23. Blakely, G.R.: Safeguarding cryptographic keys. In: Proceedings of AGIPS 1979 National Computer Congress, vol. 48, pp. 313–317 (1979)
24. Blake, I.F., Van Oorschot, P.C., Vanstone, S.: Complexity issues for public key cryptography. In: Skwirzynski, J.K. (ed) Performance Limits in Communication, Theory and Practice, NATO ASI Series E: Applied Science, vol. 142, pp. 75–97. Kluwer Academic Publishers [Proceedings of the NATO Advanced Study Institute Ciocco, Castelvecchio Pascoli, Tuscany, Italy] (1986)
25. Chaum, D.: Zero- knowledge undeniable signatures. Advances in Cryptology—Eurocrypt 90, LNCS, vol. 473, pp. 458–464 (1991)
26. Mullin, R.C., Blake, I.F., Fuji-Hara, R., Vanstone, S.A.: Computing logarithms in a finite field of characteristic two. SIAM J. Alg. Disc. Math. 276–285 (1985)
27. NIST.: Digital signature standard. GIPS PUB 186 (1994)
28. Okamoto, T.: Designated confirmer signatures and public key encryption are equivalent. In: Advances in Cryptology—Crypto 94, LNCS, vol. 839, pp. 61–74 (1994)
29. Odlyzko. A.M.: Discrete logs in a finite field and their cryptographic significance. In: Cot, N., Beth, T., Ingemarsson, I. (eds.) Advances in Cryptology—Eurocrypt 84, LNCS, vol. 209, pp. 224–314 (1984)
30. Rabin, T.: A simplified approach to threshold and proactive RSA. In: Proceedings of Advances in Cryptology—Crypto, vol. 98, pp. 89–104. Springer, New York (1998)
31. Yen, S.M., Laih, C.S.: New digital signature scheme based on discrete logarithm. Electron. Lett. **29**(12), 1120–1121 (1993)
32. Zheng, Y., Matsummoto, T., Imai, H.: Structural properties of one-way hash functions. In: Proceedings of Advances in Cryptology—Crypto 90, pp. 285–302. Springer (1990)

Comparing Mesh Topology-Based Multicast Routing Protocols in MANETs

Ashema Hasti and U.S. Pandey

Abstract In a network that is wireless, ad hoc, mobile, with forever differing topology, the need for a routing protocol arises for locating routes to nodes of the network so that a sender and a receiver can talk to each other via packets. An important task is to write a routing algorithm that will search, the cost-effective route, in terms of distance and overheads, between every source–target pair. In MANETs, there is a need for multicast routing because data packets are transmitted to dynamically changing groups. Therefore, multicast routing protocols should ensure that certain parameter values are achieved. In such networks, link breakage often happens. But when there are numerous paths available between the same pair of source and sink, the robustness of the network increases. This is the case with mesh-operated multicast routing protocols. This paper describes three of such protocols, compares them, and proposes a solution that overcomes the challenges in the existing protocols.

Keywords MANETs · Multicast routing · Mesh topology

1 Introduction

A mobile ad hoc network (MANET) is a wireless setup of nodes which are arbitrarily moving; they organize themselves into a network whenever there is a need to communicate. Such a network does not require any centralized infrastructure or any central access point [1]. For regular-wired networks, there are quite many multicasting routing protocols available. Since most of them are not meant for highly transient networks, such routing algorithms are unable to cope with the frequent

A. Hasti (✉)
Mewar University, Chittorgarh, Rajasthan, India
e-mail: ashema.hasti@gmail.com

U.S. Pandey
School of Open Learning, Delhi University, New Delhi, India
e-mail: us_pandey@hotmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_19

network mutations and sudden node movement in a wireless mobile ad hoc network.

In ad hoc wireless networks, link breakage often occurs due to mobility of nodes, which causes the path between the source and the destination to suffer. There are multiple paths between source and sink in case of multicast routing protocols which use mesh topology. Mesh-based protocols have an advantage of an enormously good packet delivery ratio. This leads to a sturdy network. Source tree and shared tree are two classifications of tree-based protocols [2]. Each router acts as a source of the multicast tree on a source-tree protocol [1]. In shared tree protocol, only one node acts as a core root node where all source nodes of a group share a single multicast tree. Such a protocol faces deep failures in performance in case core node stops operating. This is where mesh-designed protocol [3] gives flexibility. It gives a variety of paths for each pair of source–receiver. And hence, mesh-operated protocols are more resilient to failures as compared to tree-based protocols. The remainder of the paper is organized as follows in the form of four sections: Sect. 2 reviews background of multicast routing and mesh-based multicast routing, followed by Sect. 3 which describes three specific types of mesh-based routing protocols; after that, Sect. 4 elaborates on the significant comparison points among these three protocols, and then Sect. 5 gives the requirements for developing an optimum solution based on mesh-based multicast routing.

2 Mesh-Based Multicast Routing Protocols

2.1 Multicast Routing

For communication within a MANET network, whenever there are situations, wherein, we need to send or receive messages in a group of nodes, we need to do multicasting. This requires constructing a group with a set of member nodes. Each such collection has a unique multicast address. Now in case of a MANET network, the member nodes move around randomly as the topology keeps on changing. Thus, in such as case, packet delivery and group maintenance are hard to achieve [4]. Multicasting is the transmission of datagrams to a collection of zero or more hosts having a single destination address. A multicast datagram is delivered to all destination host group members with the same reliability as regular unicast packets. Multicasting reduces the communication cost for applications that send same data to multiple receivers rather than transmitting through multiple unicast. Multicasting brings down channel bandwidth and propagation delay. For most scenarios with realistic mobility levels and traffic loads in MANETs, the dominating part of overhead in the packet transmission is the misrouting overhead [5].

2.2 Mesh-Based Multicast Routing

The mesh-based protocols deliver more data packets as compared to tree-based due to the presence of multiple paths. Multicast routing protocols perform better in achieving parameter values of good packet delivery ratio, better reliability, less control overheads, and packet delays [6]. Mesh-based protocols work efficiently because they provide alternative routes and deliver packets with good success rates and they are less vulnerable to the loss of packets amid a network of nodes that are forever mobile. These structures are usually rooted at a core node (first sender or an elected node from multicast group receivers) [7]. The drawbacks in maintaining multicast trees in ad hoc network are frequent tree reconfiguration and non-shortest path in a shared tree. Multicast protocols using mesh networks usually provide multi-path links to nodes within a multicast group. And hence, mesh-based multicast routing protocols can respond quickly to link breakage due to mobility [8].

3 Description of Three Mesh-Based Protocols

3.1 ODMRP: On-Demand Multicast Routing Protocol

A mesh is formed by a group of forwarding nodes (intermediate nodes) within the multicast network. These nodes forward data packets between source and receiver and maintain message cache [9]. This cache discovers duplicity, if any, in data and control packets. In the mesh creation phase, a multicast mesh is made. Each source floods "Join Request" control packet periodically. Potential receivers can transmit back "Join Reply" packet through reverse shortest path. The route between source and destination gets formed once source gets the "Join Reply" packet (containing sourceId and forwarding nodeId) [10]. In the mesh maintenance phase, multicast mesh protects the communication from being affected by node mobility. A soft-state approach is used to maintain mesh, i.e., for refreshing routes. The source periodically floods JoinReq control packet [11]. See Fig. 1.

3.2 DCMP: Dynamic Core-Based Multicast Routing Protocol

In mesh creation phase, the protocol tries to reduce the count of sources flooding their "Join Request" packets. Sources are classified into passive, active, and core active nodes [10]. A passive source is bound with a node called core active source that forwards packets on behalf of passive source. Passive sources do not flood "Join Request" control packets. Just active and core active ones do that. The total tally of passive sources served by core active ones is limited (number of maximum

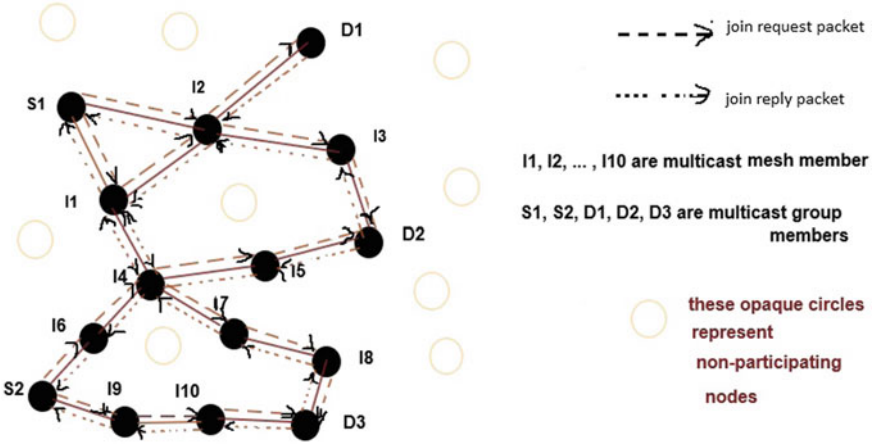


Fig. 1 Mesh topology in ODMRP

passive sources is fixed). Also, the distance between the two is also limited (maximum hop distance is fixed). In mesh maintenance, soft-state approach is used. It is recreated periodically. After timeout value, forwarding nodes that are not part of the mesh drop their forwarding status.

3.3 CAMP: Core-Assisted Mesh Protocol

This protocol eliminates flooding of control packets for increased bandwidth utilization. The receiver initiates mesh creation. In order to join the mesh, the receiver takes out core node ids from its CAM table. This table provides a mapping from core to group address. It contains core node ids of the multicast group. A receiver unicasts "Join Request" packet toward this core node [10]. This protocol assumes that there is an underlying unicast routing protocol. Due to node mobility, multicast mesh may become partitioned so the mesh maintenance is done by ensuring partition repair by means of a control packet (core node explicitly sends join request) sent by each active core node in the mesh partition to the active core nodes of other mesh partitions.

4 Comparing Points in the Protocols: Benefits and Limitations, Using the Simulation Model

The free space propagation model has been used as propagation model for simulation. This model shows a circular communication range around the sender. If a receiver is within the transmission range, it receives all data packets, else it discards

Table 1 Simulation parameters

Parameters	Values
Protocols compared	ODMRP, DCMP, CAMP
Area of simulation	1000 m * 1000 m
Count of nodes	50
Multicast group size	5–40
Mobility speed	1–20 m/s
Mobility model	Random way-point model
Propagation model	Free space propagation model
Node transmission range	150 m
Data packet size	225 bytes

the data packets. The simulation tool used was NS2 (Network Simulator 2). The simulation parameters are present in Table 1.

4.1 Analyzing ODMRP

- Source initiates mesh creation.
- It is unconstrained by any unicast routing protocol.
- It uses soft state for mesh maintenance, which means the source periodically floods "Join Request" control packets to refresh routes. This causes excessive generation of control packets [12].
- The same data gets forwarded to a single receiver via multiple paths. This leads to high amount of data forwarding.
- The main drawback of ODMRP is the lack of scalability with respect to number of senders that causes high control overhead due to path redundancy.

4.2 Analyzing DCMP

- It reduces control overhead and provides better packet delivery ratio as compared to ODMRP.
- As the number of sources increases, the performance of the routing algorithm improves [13].
- Source initiates mesh creation.
- The factor one (maximum number of passive sources allowed) and factor two (maximum hop distance allowed between core active node and passive node) depend upon variables such as network load, multicast group dimension, and total source tally.
- Collapse of core active node can lead to the entire mesh debacle.

4.3 Analyzing CAMP

- It eliminates flooding of control packets both for mesh creation and maintenance [14].
- Core node failure can lead to significant packet loss.
- It needs support of a unicast protocol.
- The mesh creation may be initiated by a receiver node.

5 Technical Requirements for Creating a New Multicasting Protocol: A Solution

First, build the topology: Fix one particular node to send out control packets to all other nodes in the mesh. Name every node which gets the control packet for the first time, with a label. If a node later gets other packets, maintain excess labels in the buffer. Secondly, whenever a transmitter receives a request, it might employ the name of the impetrating node to establish paths and send data to the target. When sending data, the initiator will verify whether the backup paths are required. And then, the source can verify the labeled names of the target nodes to know if there are identically labeled names in the same cluster. If not, then adopt the primordial route, and whenever the labels are identical, employ the backup paths.

6 Conclusion

This paper presents comparative review of three mesh-based multicasting protocols and proposes a solution that tries to overcome the challenges in the existing protocols in highly active MANETs. The proposed paradigm names nodes to create and sustain the mesh and multicast. This strategy avoids unnecessary transmission of control packets, but keeps up good packet delivery ratio. The efficiency of ad hoc multicast routing protocols is gauged by a number of variables like their data packet delivery ratio, data forwarding, or packet replication ability. That is decided by the count of data packets sent per original data packet and total control overhead. Mesh-based multicast routing helps to achieve this purpose. And, CAMP is most successful as far as avoiding unnecessary transmission of control packets is concerned. But ODMRP does not have any issues related to core node failure which affects both DCMP and CAMP.

The future work entails a design and development of a multicasting protocol which would be a hybrid of these methodologies, based on the proposed solution, which has the benefits of CAMP but eliminates its limitations, to be tested by making use of an appropriate model and a tool.

References

1. Hasti, A., Pandey, U.S.: Analysis of performance of multicasting routing protocol MAODV for QoS parameters using NS2. In: 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 845, 848. 11–13 Mar 2015
2. Garcia-Luna-Aceves, J.J., Spohn, M.: Source-tree routing in wireless networks. In: Proceedings of IEEE ICNP 1999, pp. 273–282, Oct 1999
3. Latake, S.P., Shinde, G.R., Kulkarni, R.J.: Tree, mesh structure based and stateless multicast routing protocols in wireless networks. Int. J. Comput. Sci. Inf. Technol. (IJCSIT) **4**(3), 485–488 (2013). ISSN:0975-9646
4. Nagaratna, M., Kamakshi Prasad, V., Rao, R.: Performance evaluation of mesh-based multicast routing protocols in MANET's. Int. J. Adv. Comput. Sci. Appl. **2**(7) (2011)
5. Tran, Q.-M., Dadej, A.: Optimizing cached route time-to-live in mobile ad-hoc networks. In: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications (AINA), pp. 193–200. IEEE (2015)
6. Biradar, R., Manvi, S.: Mesh based multicast routing in MANET: stable link based approach. Int. J. Comput. Electr. Eng. **2**(2), 1793–8163 (2010)
7. Farooq, M.U., Tapus, N.: CAMT: core assisted multicast tree for ad hoc networks. In: RoEduNet Conference 13th Edition: Networking in Education and Research Joint Event RENAM 8th Conference, pp. 1–5. IEEE (2014)
8. Yu, J., Kim, T., Na, W., Bae, H., Lee, Y., Lee, J., Vatandas, Z., Cho, S., Hur, J.: Fully-distributed multicast routing protocol for IEEE 802.15. 8 peer-aware communications. In: 2014 International Conference on Information Networking (ICOIN), pp. 64–69. IEEE (2014)
9. Usha, D.G., RSD, W.B.: Performance evaluation of multicast routing protocols in ad-hoc networks. In: 2012 2nd IEEE International Conference on Parallel Distributed and Grid Computing (2012)
10. Siva Ram Murthy, C., Manoj, B.S.: Ad Hoc Wireless Networks: Architectures and Protocols, pp. 320–322, 325–326, 328–330. Pearson Education Inc., New Delhi (2004)
11. Das, S.K., Manoj, B.S., Siva Ram Murthy, C.: A dynamic core based multicast routing protocol for ad hoc wireless networks. In: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & computing, pp. 24–35. ACM, New York
12. Moustafa, H., Labiod, H.: Multicast routing in mobile ad hoc networks. Telecommun. Syst. **25**(1–2), 65–88 (2004)
13. Badarneh, O.S., Kadoch, M.: Multicast routing protocols in mobile ad hoc networks: a comparative survey and taxonomy. EURASIP J. Wirel. Commun. Netw. **2009**, 26 (2009)
14. Garcia-Luna-Aceves, J.J., Madruga, E.: A multicast routing protocol for ad-hoc networks. In: Proceedings of IEEE INFOCOM'99, New York, NY, June 1999

SER Performance Improvement in OFDM System Over Generalized *K*-fading Channel

Keerti Tiwari, Bindu Bharti and Davinder S. Saini

Abstract In this paper, performance metric of orthogonal frequency division multiplexing (OFDM) system is analyzed over a composite fading channel, i.e., generalized *K*-fading channel. Here, OFDM system is considered which includes repetition code to enhance the wireless link performance with simplicity. Symbol error rate (SER) performance is evaluated using binary phase shift keying (BPSK) and 16-quadrature amplitude modulation (16-QAM) over generalized *K*-fading channel. This channel model considers Nakagami-*m* distribution to define multipath and gamma distribution to represent shadowing effects. Simulation results demonstrate that improved system performance can be achieved by using repetition code in severely faded environment. A comparative study of coded and uncoded system is also given in this paper. Consequently, SER performance is improved with the increase of shape parameters.

Keywords Orthogonal frequency division multiplexing (OFDM) · Generalized *K*-fading · Binary phase shift keying (BPSK) · 16-quadrature amplitude modulation (16-QAM) · Symbol error rate (SER)

1 Introduction

Next-generation wireless technologies have demanded efficient and reliable communication system in severe multipath fading environment. Therefore, orthogonal frequency division multiplexing (OFDM) is a competent and supporting technique

K. Tiwari (✉) · B. Bharti · D.S. Saini
Department of Electronics and Communication Engineering, Jaypee University of Information Technology, Waknaghat, Solan 173234, Himachal Pradesh, India
e-mail: krt.tiwari@gmail.com

B. Bharti
e-mail: bindu.bharti457@gmail.com

D.S. Saini
e-mail: davinder.saini@juit.ac.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_20

in severely fading environment [1, 2]. However, OFDM systems suffer from peak-to-average power ratio and peak interference-to-carrier-ratio problems. These problems can be overcome by using Galois field (GF) and complex field (CF) coding schemes [3, 4]. In [5], it has been reported that without the common phase error correction technique, OFDM degrades the performance of the communication system. Therefore, various codes such as convolution codes [6], Reed-Soloman (RS) codes [7], low-density parity-check (LDPC) codes [8] and Turbo codes [9] have been investigated to improve the system performance. OFDM with error correcting code yields better performance. Over the past decades, many researchers have reported different performance measures such as capacity limits, bit error rate (BER), throughput over different multipath fading channels [10, 11]. In [12], it has been discussed that the approximated repetitive coding yields reliable symbol regeneration and higher order modulation which improves spectral efficiency. Moreover, the decoding complexity of repetition code can be significantly reduced by QR decomposition with M-algorithm (QRM) maximum likelihood decoding (MLD) method [13]. In [14], a technique is recommended to achieve the frequency diversity gain in OFDM system using repetition code which is applicable in aerial acoustic communications. One another coding technique for OFDM called Hermite-symmetric subcarrier (HC) coding is also suggested which provides greater power efficiency than that of a simple repetition coding. Also, the effective performance of HC-OFDM is measured by considering variations in fading environment [15]. In [16], it has been illustrated that the maximal ratio combining (MRC) diversity technique gives better error performance than other diversity combining techniques such as equal gain combining (EGC), selection combining (SC). Hence, MRC is used for decoding in this paper. In [17], authors have been derived a mathematical expression to measure the BER of OFDM system with MRC under correlated Nakagami-*m* fading environment. It has been reported in [18] that sensitivity of OFDM system is affected insignificantly by the fractional change in the fading figure over frequency selective Nakagami-*m* fading channel. In [17, 18], the channel is analyzed over small-scale fading, but usually the received signal is obtained by the joint effect which is produced by the independent processes such as small-scale fading and large-scale fading. The combination of large-scale and small-scale fading effects introduce a composite distribution, i.e., generalized *K*-fading distribution [19]. The effects of fading and shadowing in the wireless channel are effectively approximated with generalized *K*-fading model. Moreover, in this distribution, multipath and shadowing effects can be represented by Nakagami-*m* and gamma distribution, respectively. It is also shown that this distribution is more familiar than the Nakagami-*m* lognormal model [20, 21]. Moreover, with the *K*-distribution model, mathematical analysis becomes simple in comparison to lognormal based models, e.g., the Nakagami-*m* or the R-L model [19]. In [22], the performance metrics of system are analyzed over *N**generalized**K*-fading channels. Moreover, the capacity of generalized *K*-fading channel with multiple-input multiple-output (MIMO) system is analyzed in [23].

In the existing literature, error performance of OFDM system has not been investigated using repetition code over generalized *K*-fading channel. MRC can be

used as the repetitive decoding which gives favorable performance. Here, binary phase shift keying (BPSK) and 16-quadrature phase shift keying (16-QAM) modulation techniques are used to evaluate the proposed system performance.

The rest of the paper is structured as follows. Section 2 describes OFDM system, generalized *K*-fading channel model and repetition codes. Section 3 illustrates the simulation results. Finally, paper is concluded in Sect. 4 and future scope of this work is also given in this section.

2 System and Channel Model

2.1 Received Signal of OFDM Model

It is considered that the message bits are mapped to the sequence of BPSK/16-QAM symbols in the OFDM transmitter. These symbols are subsequently converted into *N*-parallel streams carried out by different subcarrier [1]. Therefore, the transmitted signal of OFDM system is expressed as

$$x_l(n) = \frac{1}{N}\sum_{\mathcal{K}=0}^{N-1} X_l(\mathcal{K})\mathrm{e}^{\frac{j2\pi n\mathcal{K}}{N}}, \quad n = 0, 1 \ldots N-1, \;\; l = 0, 1 \ldots \infty \tag{1}$$

where $X_l(\mathcal{K})$ denote the lth transmit symbol at the $\mathcal{K}$th subcarrier and n is the index of $\mathcal{K}$th subcarrier. In our model, we have assumed that at the transmitter, cyclic prefix with significant length is added in the starting of OFDM symbol. At the receiver, added cyclic prefix is removed during demodulation process. Hence, inter-symbol interference (ISI) does not occur in OFDM symbol. Moreover, OFDM system performance is analyzed over generalized *K*-fading channel. This model is expressed as follows.

2.2 Model for Generalized K-fading Channel

The received OFDM symbol at the receiver is expressed as

$$Y_l(\mathcal{K}) = x_l(n)Z + w(n) \tag{2}$$

where Z is the generalized *K*-distributed signal envelop with the probability density function (PDF) given by [18]

$$f_Z(z) = \frac{4z^{m+k-1}}{\Gamma m \Gamma k}\left(\frac{m}{\Omega}\right)^{\frac{k+m}{2}} K_{k-m}\left[2\left(\frac{m}{\Omega}\right)^{\frac{1}{2}} z\right], \quad z > 0 \tag{3}$$

where m, k, $K_v(\cdot)$, $\Gamma(\cdot)$ [24, Eq. (8.310.1)] is the Nakagami-m fading, shadowing parameter, modified Bessel function of order $v(\cdot)$ [24, Eq. (8.432.1)] and the gamma function, respectively. $\Omega = E[Z^2]/k$ implies to mean power and $E[\cdot]$ signifies expectation operator. Different combination of shaping parameters k and m in generalized K-fading distribution describes variety of fading and shadowing model. For $k \to \infty, m \to \infty$ approximates additive white Gaussian noise (AWGN) channel, $k \to \infty$ approximates Nakagami-m distribution and $m \to 1$ approximates K-distribution. PDF of generalized K-fading distribution with reference to average signal-to-noise ratio (SNR) is expressed as [19]

$$f_\gamma(\gamma) = \frac{2\Xi^{\frac{(\alpha+1)}{2}}\gamma^{\frac{\alpha-1}{2}}}{\Gamma m \Gamma k}(\Xi)^{(\alpha+1)/2}K_\beta\left[2\sqrt{\Xi\gamma}\right] \quad \gamma \geq 0 \tag{4}$$

where, $\alpha = m + k - 1, \beta = k - m, \Xi = k\frac{m}{\bar{\gamma}}, \gamma = Z^2\frac{E_s}{N_0}$, $\bar{\gamma} = k\Omega E_s/N_0$, where E_s is energy per symbol, N_0 is noise power spectral density, and γ is SNR. There is different performance metrics of wireless channel, one of them is symbol error rate (SER). Symbol error rate for different modulation formats is expressed as [19]

$$SER(\gamma) = E\left[A_{\text{mod}}Q\left(\sqrt{2B_{\text{mod}}\gamma}\right)\right] \tag{5}$$

where $Q(\cdot)$ is the Gaussian Q-function. Moreover, modulation techniques are defined by constants A_{mod} and B_{mod}. Moreover, error correcting codes are significantly adopted to analyze the OFDM system performance in composite fading scenario. Hence, repetition code is discussed in Sect. 2.3.

2.3 OFDM with Repetition Codes

The performance of the OFDM system without coding scheme degrades due to the existence of nulls at subcarrier frequency [3]. Therefore, to recover this problem, error correcting codes are introduced for OFDM system [6–9]. In [25], it is discussed that repetition coding is a useful technique to reduce the probability of error, to improve SNR over the modulation and error correction mechanism. In addition, MRC diversity technique is advantageous to improve the reliability at the receiver, which helps to recover the corrupted symbol [12]. The error correction codes can be implemented before IFFT or after IFFT. In this paper, repetition coding is performed before IFFT as shown in Fig. 1. Here, $X_l(\mathcal{K})$ symbols are allotted at the transmitter. These symbols are then mapped as $p_{i,j}$ which is given as

$$X_l(\mathcal{K}) = p_{i,j}, \quad \mathcal{K} = F_m(i,j) \tag{6}$$

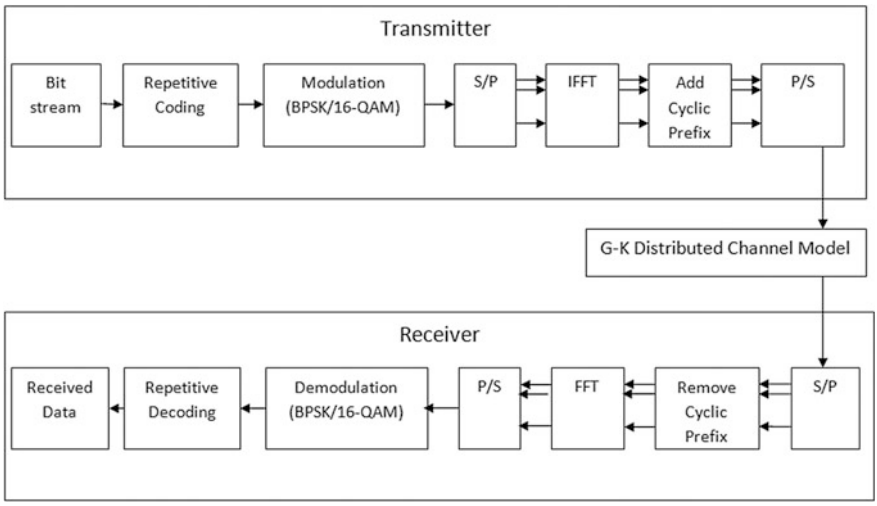


Fig. 1 Block diagram of OFDM system with repetition codes

$F_m(i,j)$ represents jth symbol in the ith group to the $\mathcal{K}$th subcarriers. Demapping is performed at the receiver. The received group symbol can be given as

$$q_{i,j} = p_{i,j}H_{i,j} + W_{i,j} \tag{7}$$

where $W_{i,j}$ denotes DFT of $w_{i,j}$.

Here, M_o groups are made after copying modulated symbols. The repetition decoded symbols are represented as

$$\begin{aligned} q_{i,j} &= \sum_{i=0}^{M_o-1} \mathcal{G}_{i,j} q_{i,j} \\ &= p_{i,j} \sum_{i=0}^{M_o-1} \mathcal{G}_{i,j} H_{i,j} + \sum_{i=0}^{M_o-1} \mathcal{G}_{i,j} W_{i,j} \\ &= p_{i,j} + \left(\frac{\sum_{i=0}^{M_o-1} H_{i,j}^* W_{i,j}}{\sum_{i=0}^{M_o-1} \left| H_{i,j} \right|^2} \right) \end{aligned} \tag{8}$$

where $\mathcal{G}_{i,j} = \frac{H_{i,j}^*}{\sum_{i=0}^{M_o-1} \left| H_{i,j} \right|^2}$ is the weight coefficients for repetition decoding. Here, the approximation of weight coefficient is done with the assumption that there is absence of inter-carrier interference (ICI) effects and the repeated symbols are taken adequately apart [12].

3 Simulation Results and Analysis

In this section, the simulation results of the proposed system model are illustrated. OFDM system with $N = 128$ subcarriers having cyclic prefix 32 is considered. Hence, one OFDM symbol includes total 160 samples. The bandwidth is 20 MHz which is taken into consideration and subcarrier frequency spacing is 20 MHz/128, i.e., 0.15625 MHz. The SER performance metric is analyzed for different values of m and k. In Figs. 2 and 3, SER is analyzed for uncoded OFDM system with BPSK and 16-QAM modulation techniques, respectively. It is illustrated that for low values of m and k, SER performance of the OFDM system is worst. However, as the values of m and k increase, system performance is improved. It is depicted that with high values of m and k, better performance can be achieved at low SNR as shown in Fig. 2. For $m = 2$, $k = 5.5$, less SER is achieved as compared to $m = 5.5$, $k = 2$. Thus, it can be analyzed that shadowing gives more impact on SER performance improvement. It is noted that the generalized K-fading channel is generated by the product of gamma random variables and channel matrix recommended for Nakagami-m fading with its independent and identically distributed (i.i.d.) entries. For all simulation, $\Omega = 1$ is considered. By comparing Figs. 2 and 3, it is depicted that with BPSK (low modulation order) better SER performance is achieved than 16-QAM (high modulation order).

Here, MRC is used for decoding to improve the system performance. It can be seen that the nature of SER curves for numerically chosen value of m and k for BPSK and 16-QAM modulation techniques is similar. Moreover, the bit error performance is improved at high SNR values with higher modulation order. Moreover, the analysis for coded OFDM (repetition code) system with BPSK and 16-QAM is depicted in Figs. 4 and 5, respectively. The code rate of employed repetition code is ¼. The illustration of SER performance for distinct values of m and k is similar as discussed for the uncoded OFDM system.

Nevertheless, the comparison of SER performance for coded and uncoded OFDM system with different modulation technique shows that the SER is improved

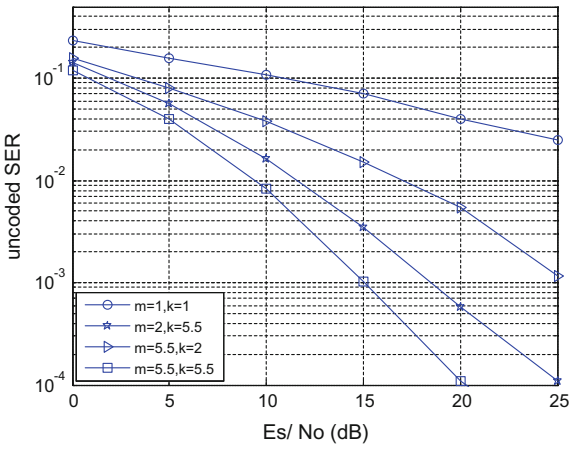


Fig. 2 SER of OFDM system for BPSK over generalized K-fading channel with arbitrary chosen numerical values of m and k

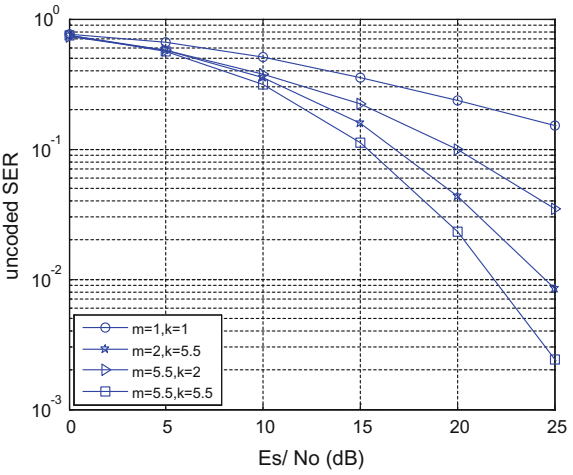


Fig. 3 SER of OFDM system for 16-QAM over generalized *K*-fading channel with arbitrary chosen numerical values of *m* and *k*

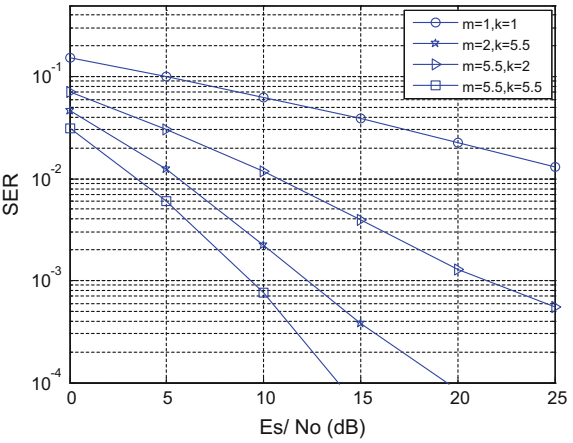


Fig. 4 SER of OFDM system using repetition code for BPSK over generalized *K*-fading channel with arbitrary chosen numerical values of *m* and *k*

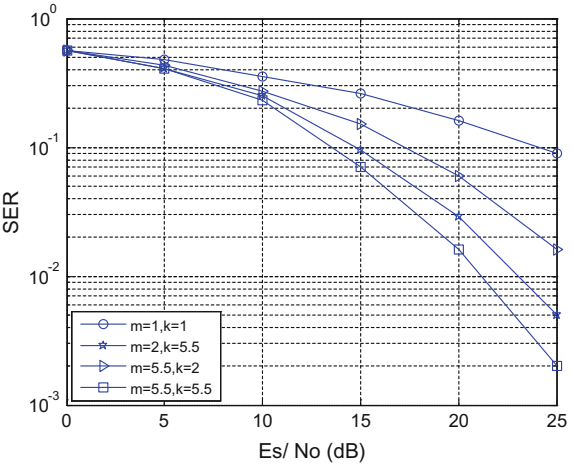


Fig. 5 SER of OFDM system using repetition code for 16-QAM over generalized *K*-fading channel with arbitrary chosen numerical values of *m* and *k*

Table 1 SER of uncoded and coded OFDM system for arbitrary values of k and m using BPSK and 16-QAM

SNR = 10 dB		SER			
		$m = 1$, $k = 1$	$m = 5.5$, $k = 2$	$m = 2$, $k = 5.5$	$m = 5.5$, $k = 5.5$
Uncoded OFDM	BPSK	0.1068	0.03825	0.01636	0.00829
	16-QAM	0.5075	0.3766	0.3655	0.3124
Coded OFDM	BPSK	0.0624	0.0118	0.00224	0.00076
	16-QAM	0.351	0.272	0.251	0.232

with coded OFDM system. Also, approximately 6 dB less SNR is required in coded OFDM at the SER of 10^{-2} for BPSK. Hence, the improved SER is achieved with the proposed coded OFDM system at low SNR as shown in Figs. 4 and 5. In addition, the comparison of uncoded and coded OFDM system with different values of m and k is presented in Table 1. It is illustrated that at 10 dB SNR, coded OFDM achieves less SER in coded OFDM, 0.444 and 0.1565 less SER at $m = 1$, $k = 1$ is achieved using BPSK and 16 QAM, respectively. Consequently, 0.00753 and 0.0804 less SER is achieved at high values of shape parameters ($m = 5.5$, $k = 5.5$) using BPSK and 16-QAM, respectively.

4 Conclusion

In this paper, SER performance is analyzed for repetition coded and uncoded OFDM system over generalized K-fading channel with BPSK and 16-QAM modulation techniques. A comparison is also made with arbitrary shape parameters. It is concluded that coded OFDM system yields better performance at low SNR in comparison to uncoded OFDM system. Moreover, it is also illustrated that the shadowing parameter has a significant effect on error rate performance. Furthermore, this work can be extended by using MIMO system with OFDM and system performance can be enhanced with various concatenated codes. The adaptive modulation techniques can be employed with MIMO-OFDM system over composite fading channel. Moreover, this analysis can be done in a noisy environment and effects of frequency and phase offsets can be seen in this scenario.

References

1. Li, Y., Stuber, G.: Orthogonal Frequency Division Multiplexing for Wireless Communications. Springer, New York (2006)
2. Samundiswary, P., Kuriakose, S.: BER analysis of MIMO-OFDM using V-BLAST system for different modulation schemes. In: Proceedings of IEEE Conference on Computing Communication and Networking Technologies at Coimbatore, pp. 1–6 (2012)
3. Wang, Z., Giannakis, G.B.: Complex-field coding for OFDM over fading wireless channels. IEEE Trans. Inf. Theory **49**(3), 707–720 (2003)

4. Sathananthan, K., Tellambura, C.: Coding to reduce both PAR and PICR of an OFDM signal. IEEE Commun. Lett. **6**(8), 316–318 (2002)
5. Shah, S.F.A., Tewfik, D.H.: Design and analysis of post-coded OFDM systems. IEEE Trans. Wirel. Commun. **7**(12), 4907–4918 (2008)
6. IEEE Standards Department, IEEE Press: ANSI/IEEE Standard 802.11-Wireless LAN (2001)
7. Pontarelli, S., Reviriego, P., Ottavi, M., Maestro, J.A.: Low delay single symbol error correction codes based on reed solomon codes. IEEE Trans. Comput. **64**(5), 1497–1501 (2015)
8. Muaini, S.A., Al-Dweik, A., Al-Qutayri, M.: BER performance of LDPC-coded nonlinear OFDM systems. In: Proceedings of IEEE Communications Signal Processing, and their Applications (ICCSPA), Shargah, pp. 1–5 (2013)
9. Sadjadpour, H.R.: Application of turbo codes for discrete multi-tone modulation schemes. In: Proceedings of IEEE ICC, Vancouver, BC, pp. 1022–1027 (1999)
10. Hwang, T., Yang, C., Wu, G., Li, S., Li, G.: OFDM and its wireless applications: a survey. IEEE Trans. Veh. Technol. **58**(4), 1673–1694 (2009)
11. Yih, C.-H.: BER analysis of OFDM systems impaired by phase noise in frequency-selective rayleigh fading channels. In: Proceedings of IEEE GLOBECOM, Neworleans, LO, pp. 1–5 (2008)
12. Seo, J.-W., Jang, S.-H., Jeon, W.-G., Paik, J.-H., Kang, M.-G., Kim, D.-K.: A time-domain ICI canceller using modulation order increasing and repetition coding in OFDM. In: Proceedings of IEEE Vehicular Technology Conference, Dublin, pp. 2320–2323 (2007)
13. Matsuoka, H., Doi Y., Yabe, T., Sanada, Y.: Performance of overloaded MIMO-OFDM system with repetition code. In: Proceedings of International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Kuching, pp. 239–244 (2014)
14. Toda, A., Sasamori, F., Takyu O., Handa, S.: Robustness against fading fluctuation in Hermite-symmetric subcarrier coding for OFDM systems. In: International Conference on Information and Communication Technology Convergence (ICTC), Busan, pp. 834–835 (2014)
15. Sasano, S., Sasamori, F., Takyu, O., Handa, S.: Performance evaluation of acoustic OFDM with repetition coding. In: International Conference on Information and Communication Technology Convergence (ICTC), Busan, pp. 798–799 (2014)
16. Rappaport, T.S: Wireless Communications: Principle and Practice, 2nd edn. Pearson Education Inc., Prentice Hall PTR (2001)
17. Dwivedi, V.K., Singh, G.: Improved BER analysis of OFDM communication system on correlated nakagami-m fading channel. In: IEEE Conference on Recent Advances in Microwave Theory and Applications, Jaipur, India, pp. 536–539 (2008)
18. Al-Dweik, A., Sharif, B., Tsimenidis, C.: Accurate BER analysis of OFDM systems over static frequency selective multipath fading channels. IEEE Trans. Broadcasting **57**(4), 895–901 (2011)
19. Bithas, P.S., Sagias, N.C., Mathiopolous, P.T., Karagiannidis, G.K., Rontogiannis, A.A.: On the performance analysis of digital communications over generalized-K fading channels. IEEE Commun. Lett. **10**(5), 353–355 (2006)
20. Shankar, P.M.: Error rates in generalized shadowed fading channels. Wireless Pers. Commun. **28**(3), 233–238 (2004)
21. Laourine, A., Alouini, M.-S., Affes, S., Stéphenne, A.: On the capacity of generalized-K fading channels. IEEE Trans. Wirel. Commun. **7**(7), 2441–2445 (2008)
22. Trigui, I., et al.: On the performance of cascaded Generalized K-fading channel. In: Proceedings of IEEE GLOBECOM, Honolulu, HI, pp. 1–5 (2009)
23. Matthaiou, M., et al.: On capacity of Generalized K-fading MIMO channel. IEEE Trans. Signal Process. **58**(11), 5939–5944 (2010)
24. Gradshteyn, I.S., Ryzhik, I.M.: Table of Integrals, Series, and Products, 7th edn. Academic, New York (2007)
25. IEEE Std 802.16e TM-2005: IEEE standard for local and metropolitan area networks-Part 16: air interface for fixed and mobile broadband wireless access systems, Feb 2006

Automatic Classification of WiMAX Physical Layer OFDM Signals Using Neural Network

Praveen S. Thakur, Sushila Madan and Mamta Madan

Abstract The multicarrier OFDM technology has been chosen by many recent networking standards as preferred modulation scheme at physical layer as it offers high robustness against multipath effects. Automatic modulation recognition of OFDM signal has been thus intensive research area in cognitive radios. Several algorithms have been proposed in past that carry out effective detection, parameter estimations, and automatic recognition of OFDM signals as part of radio sensing techniques. In this paper, we proposed neural network-based classification of WiMAX IEEE 802.19 physical layer OFDM signal which does not require any a priori information or depends on cooperative embedded information from transmitter. The proposed algorithm classifies WiMAX IEEE 802.16d OFDM signal in a heterogeneous network environment having other digital modulation signals. The proposed features are robust to channel noise and multipath fading effects on wireless channel.

Keywords WiMAX IEEE 802.16 · Multicarrier signals · Orthogonal frequency division multiplexing (OFDM) · Signal classification · Neural networks

1 Introduction

With the increasing demand for radio communications, the task of automatic modulation classification of transmitted signal in the RF spectrum has become a front-end processing stage and critical requirements in communication systems. Recent emergence of high-speed 4G wireless data communication standards like

P.S. Thakur (✉)
Banasthali University, Vanasthali, Rajasthan, India
e-mail: praveenprithvi705@gmail.com

S. Madan
Lady Shri Ram College for Women, Delhi University, Delhi, India

M. Madan
Vivekananda Institute of Professional Studies, Indraprastha University, Delhi, India

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_21

3GPP TS 36.211, WiMAX IEEE 802.16, DVB EN 302 583, WLAN IEEE 802.11, WRAN IEEE 802.22 employs multicarrier OFDM signals (orthogonal frequency division multiplexing) due to its robust protection characteristics against multipath fading effects. Software-defined Radio (SDR) and cognitive radio (CR) are finding strong applications in these networks as they enable the mechanism to use scarce communication spectrum effectively and efficiently. This is possible as they have capability to monitor radio spectrum, identify modulation scheme, and adapt its modulation to best suit the environment of operation. In this scenario, there is an immense requirement seen in these radios to classify multicarrier signal like OFDM, automatically from other single carrier modulation schemes, and to deduce further transmission parameters to proceed to the next stage. The automatic modulation classification stage forms the first step in these radios immediately after signal detection. For example, in case of cognitive radio, the radio continuously has to sense the spectrum around its vicinity and use an unused radio spectrum available to it. This means the radio scans and analyzes many signals available for modulation schemes to find out multicarrier class of signals. Once it finds out the presence of a OFDM signal, it has to next identify the modulation scheme used in each subcarrier. The modulation used on subcarrier of OFDM signal is kept adaptive and is changed based on channel conditions encountered to achieve best trade-off between transmission throughput and bit error rate (BER). When the channel conditions are favorable, the modulation type is increased to achieve best throughput, and in unfavorable channel conditions, modulation schemes having low BER are chosen on subcarrier of OFDM signal. The modulation information is transmitted to receiver on signaling channels so that at receiver side, correct demodulation can take place. However, this comes at extra cost of addition of overhead information and thus decreasing the overall throughput of transmission. The automatic modulation technique alleviates this problem by offering the advantage of classifying the modulation parameters at receiver side automatically and aids in demodulating the signal. If the classifying algorithm does not consume much receiver processor power or increase latency in network, then the net gain is bandwidth saving. ITU Recommendation SM.1600-1 suggests manual and automatic methods of classifying modulation in these networks. Under automatic methods, autocorrelation techniques are proposed to detect periodic sequences, such as preamble or mid-amble, synchronization word or pilot codes, and training sequences embedded in signal. Cyclic autocorrelation can identify OFDM and OFDMA standard signals by detecting the periodicity embedded in signal. Advanced methods like Haar wavelet transform can automatically identify if there is some a priori information available for transmission parameters. However, these techniques can identify standard signals only that comply to specifications. There have been many other techniques developed to classify OFDM signals. In this paper, we focus to evolve method to classify *Worldwide Interoperability for Microwave Access* (WiMAX) IEEE 802.16d OFDM signal used on air interface using neural network.

The paper is divided as follows: Sect. 2 briefly covers previous work done on automatically identifying OFDM signal, in Sect. 3, we present the signal model and signal construct, Sect. 4 describes the method employed and experimental results, and in Sect. 5, we conclude.

2 Related Work

The very first studies on OFDM classification are reported in [1] by Walter who used for the first time asymptotically gausianess characteristics of multicarrier signals. They estimated fourth-order cumulant of OFDM and single carrier signals and separate them since calculated cumulant of OFDM is zero. In [2], Leinonen and Juntti used decision theoretic approach methods mainly maximum likelihood, GLRT, and quasi-likelihood ratio test to identify between PSK modulation and QAM of OFDM subcarriers. Reddy et al. in [3] used the unique distribution of errors of various modulation schemes at given SNR. They generated the probability distribution function (pdf) of errors for given modulation scheme and SNR a priori and then compared it at receiver for estimated SNR value from noisy samples received. In other words, they boiled the blind demodulation problem to SNR estimation with a priori pdf model available for the system. They could identify with its subcarrier modulation BPSK, QPSK, QAM16, and QAM64. In [4], Tevfik et al. formulated a maximum likelihood classifier and a suboptimal classifier under noisy and ideal conditions. Huo in [5] exploited the fact that OFDM signals can be treated as collection of independently, identically distributed random variables and hence its amplitude distribution follows Gaussian distribution. They estimated fourth-order cumulant which is very small than a single carrier modulation scheme and used a radial basis function (RBF) neural network for classification. Han et al. in [6] used subcarrier spacing and guard interval information to classify different types of OFDM signal modes. In [7], Ulovec used fourth-order cumulant, normalized signal, and spectrum amplitude. Results are presented in confusion matrix as probability of correct recognition and probability of false alarms. Chen and Zhu in [8] used back propagation neural network and in cooperative environment classified OFDM signals based on higher-order moments as features. They could classify weaker SNR user also due to cooperative nature of their algorithm. Abdelaziz et al. in [9] tried to give solution to problem where detection of cyclic prefix or subcarrier spacing of OFDM signal is not possible due to smaller duration of cyclic prefix or where channel response is larger than the cyclic prefix or power of received signal is small. They used kurtosis minimization, maximum likelihood, matched filter, and cyclic frequency estimation principles in their method and claimed that this technique is successful in above situation. Haq et al. in [10] tried to use normalized signal spectrum amplitude to differentiate OFDM signal from other digital modulation schemes. Vladimír et al. in [11] estimated cyclic autocorrelation function using DFT under multipath fading and inexact frequency and timing parameters to identify OFDM signals. Their detector could classify 802.11g

WLAN OFDM signal even in negative SNR. Nouha et al. in [12] used cyclic cross-correlation function to detect energy of pilot tones on a 3gpp LTE OFDM signal. They also used Gaussian maximum likelihood approach which shows better accuracy over pilot-induced cyclostationarity but is more complex. In [13], Michael et al. exploited multiple cumulant for multiple-input–multiple-output (MIMO) systems, which extensively employs OFDM modulation schemes and showed that particularly eighth-order cumulant is most effective in identification of signals on MIMO systems. In [14], Rasha et al. used discrete Fourier transform, discrete cosine transform, and discrete sine transform to calculate mel frequency cepstral coefficients as features and employed neural network and support vector machines to classify OFDM signal in AWGN and multipath channel conditions. They presented results in negative SNR ranges as well. They extended their investigations to adaptive OFDM classification in [15] by utilizing fuzzy logic interface and used 13 features in back propagation-resilient multilayer perceptron neural network. Hassan et al. in [16] used higher-order statistical moments and cumulant features of the received signals in multilayer artificial neural network trained using the resilient back propagation learning algorithm to classify modulation scheme of MIMO systems in blind environment. Their method did not depend on any a priori information for classification. In [17], Al-Habashna et al. studied WiMAX and 3GPP LTE OFDM signals and accounted preamble, pilot- and reference signal-induced second-order cyclostationarity. They also presented computational load of the proposed algorithm and studied trade-off between number of samples and performance, and their method is independent of carrier, waveform, or symbol timing recovery. Michael et al. in [18] and [19] classified MIMO system modulation using fourth-order cumulant and higher-order cumulant in ideal condition assuming a priori state of channel information is known. They estimated channel blindly using independent component analysis. There proposed method performance achieves peak average likelihood ratio test (ALRT) performance when channel information is assumed to be known and reaches hybrid likelihood ratio test (HLRT) performance bounds when channel is blindly estimated. Gorcin and Arslan in [20] studied the effects of channel impairments, frequency phase offsets, and sampling mismatch on the well-recognized Gaussian characteristics of OFDM signal and classified OFDM signal from other digital modulation schemes like FSK, PSK, and QAM by formulating gaussianity test on complex data set. In [21], Sun derived analytical expression in time domain and frequency domain of second-order cyclic cumulant of OFDM signal by considering effects of time dispersion and consistent estimation errors. They only assumed that the OFDM signal has a cyclic prefix and does not require any other a priori information of signal. Liu et al. in [22] used independent component analysis to separate multiple streams in OFDM signal from a MIMO system. They detected the modulation of separated streams by maximum likelihood principle and support vector machine and established upper bound of performance. Guibene and Slock in [23] attempted to classify OFDM signal in a heterogeneous environment. They considered the presence of OFDM signal originated from digital video broadcast TV (DVB-T), 3GPP long-term evolution (LTE), and program making and special event (PMSE)

networks. They employed autocorrelation detector for DVB-T signals, cyclostationarity characteristic of 3GPP LTE signal, and Teager–Kaiser energy detector for PMSE signals in their parallel staged detector. Jantti in [24] presented a cepstrum-based energy detector and showed its superiority over energy-based detectors that are widely used for OFDM signal classification. They showed that cepstrum-based detectors are more robust than energy detectors. They also estimated the data lengths and the symbol lengths of the OFDM signal based on cepstral properties of the OFDM signal. Sun et al. in [25] tried cyclic cumulant and cyclic frequency method in both time and frequency domains to classify OFDM signals from single carrier, linear, digital modulation schemes.

The brief literature taken up above shows that there has been a very limited efforts invested in applying the artificial neural network techniques in classification of OFDM signal which has been applied otherwise very extensively in automatic classification of single carrier modulation scheme [26–30].

3 Signal Model

The WiMAX physical layer is based on OFDM. In case of OFDM, the available bandwidth (BW) is divided into number of equal bandwidth channels. If W is the available BW and if δ_f is single channel BW, then total number of subchannels created are as follows:

$$K = \frac{B}{\delta_f} \tag{1}$$

The OFDM transmitter converts serial data stream into parallel blocks of size K and modulates these blocks using inverse discrete Fourier transform (IDFT) to convert to OFDM symbols. Cyclic prefix is added to every block as per standard specification to maintain orthogonality between subcarriers. The individual subcarriers are modulated digitally before transmission on channel. At receiver end, the received signal in the kth subcarrier of OFDM signal can be represented by

$$r_k[n] = \sqrt{E_k}\, b_k|n|\, h_k|n| + \eta_k|n| \tag{2}$$

where E_k is the energy of the transmitted signal, $b_k|n|$ is the data symbols, $h_k|n|$ is channel coefficient, and $\eta_k|n|$ is noise on channel. The $b_k|n|$ is the independent identically distributed random complex symbols. The problem of OFDM signal classification is divided into two parts. The first part pertains to separation of a OFDM signal from other single carrier digital signals like PSK and QAM; second part consists of classification of OFDM signal from MFSK signals which belong to its own family of multicarrier signals. In our work, we have considered a IEEE 802.16 WiMAX OFDM signal classification from other digital modulation schemes like PSK, QAM, and multicarrier Mary (MFSK) signal. To achieve this goal, we

have used neural networks. We generated the set of various digital modulation signals like single carrier PSK2/8/16, quadrature amplitude QAM 8/16, and multicarrier MFSK 8/12/20 signals using MATLAB. We corrupted the signal sets with AWGN noise and then with Rayleigh-faded channel to get real channel conditions. The IEEE 802.16d WiMAX OFDM symbols were generated as per transmitter block diagram shown in Fig. 1. The wireless fixed IEEE 802.16 symbol is made up of 256 subcarriers, the number of which defines the FFT size. There are three different types of subcarriers: first, data carrier for data transmission; second, pilot subcarriers for channel estimation; third, null subcarriers used as guard bands. This is depicted in Fig. 2.

We generated a random data using *rand ()* MATLAB function and made payload data units (PDUs) of 36 bytes each. These PDUs were fed to error correction module which compromises of a Reed–Solomon block encoder, a convolutional encoder, and an interleaver. The FEC schemes depend on chosen modulation scheme as per Table 1, and in our case, we choose (40, 36, 2) RS scheme giving 40 bytes of data with 2 bytes of correction capability at receiver side. We used

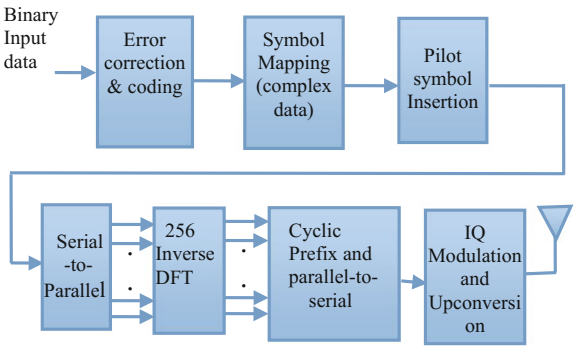


Fig. 1 WiMAX IEEE 802.16d transmitter

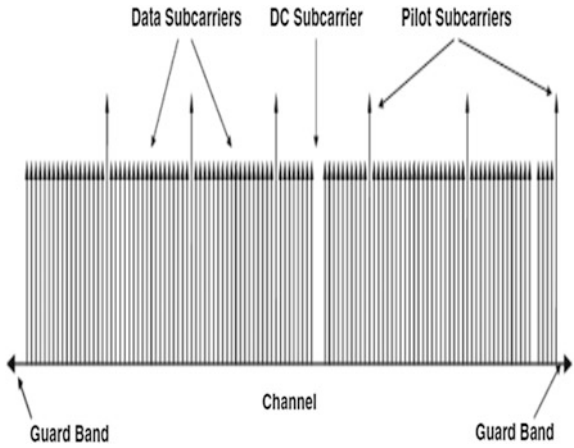


Fig. 2 IEEE 802.16d OFDM symbol

Table 1 WiMAX IEEE 802.16d modulation and coding scheme

Modulation	Uncoded block size (bytes)	Coded block size (bytes)	Overall coding rate	RS code	CC code
BPSK	12	24	1/2	(12, 12, 0)	1/2
QPSK	24	48	1/2	(32, 24, 4)	2/3
QPSK	36	48	3/4	(40, 36, 2)	5/6
QAM-16	48	96	1/2	(64, 48, 8)	2/3
QAM-16	72	96	3/4	(80, 72, 4)	5/6
QAM-64	96	144	2/3	(108, 96, 6)	3/4
QAM-64	108	144	3/4	(120, 108, 6)	5/6

MATLAB *rsenc(msg,n,k,genpoly)* function to encode data bytes as per RS encoding. The primitive polynomial used in the standard is $x^8 + x^4 + x^3 + x^2 + 1$. The convolutional encoding used is 1/2 which doubles the number of PDUs to 80 bytes. The standard specifies puncturing to allow RS code flexible for variable block size and variable correction capabilities. For QPSK scheme, puncturing is done as per the standard at rate of 5/6. The perforation vector for 5/6 puncturing scheme is [1 1 0 1 1 0 0 1 1 0], and we get total of 48 bytes. Both convolutional encoding and puncturing are realized using MATLAB function *convenc(msg,trellis, puncpat)*. WiMAX uses a 12-level interleaver to spread the errors occurring in burst. The interleaving is realized by storing the PDU bits row wise in a $N_{\text{row}} \times N_{\text{col}}$ matrix where $N_{\text{row}} = 12$ and $N_{\text{col}} =$ Total coded Bits/N_{row}.

Once the signal is encoded, we proceed to map the signal onto chosen digital modulation constellation. The IEEE 802.16d specification defines BPSK, QPSK, 16QAM, and 64QAM constellations. The support of 64QAM is optional for license-exempt bands. The 48 bytes (384 bits) is fed to a QPSK symbol mapper to produce 192 complex data which finally leading to 192 data carriers. Next, we have pilot carrier insertion stage in which eight pilot carriers are generated through a PRBS generator as per polynomial $X^{11} + X^9 + 1$ and placed permanently at eight fixed locations. The IEEE 802.16d specification defines frequency index between −127 and 128 index in which location of pilot carrier is fixed as below. These pilot carriers are BPSK modulated.

$$P_{-88},\ P_{-38},\ P_{63},\ P_{88} = 1 - 2d_k$$
$$P_{-63}, P_{-13}, P_{13}, P_{38} = 1 - 2d'_k$$

where d'_k is compliment bit of d_k PRBS generated bit.

The OFDM signal preparation steps are complete after placing 56 carriers that are zero carriers and are appended at the end as guard carriers. This allows natural decay of the signal so that emissions are decreased in adjacent bands. The OFDM symbol 256 data is fed next to IFFT module which produced a time-domain complex data. We add then cyclic prefix (CP) which helps in overcoming delay on

Table 2 Details of neuron model for MFSK classification

Network parameter	Detail
Type of ANN architecture	Multilayered perceptron
Input neurons	3
Hidden neurons	2 layers, 10 neurons
Output neurons	3
Activation function	Tan-sigmoid in hidden layer
	Log-sigmoid in output layer
Learning algorithm	Levenberg–Marquardt (LM)
MSE error for stopping learning	0.001
Target value for active output	0.9 and above
Target value for inactive output	0.1 or below

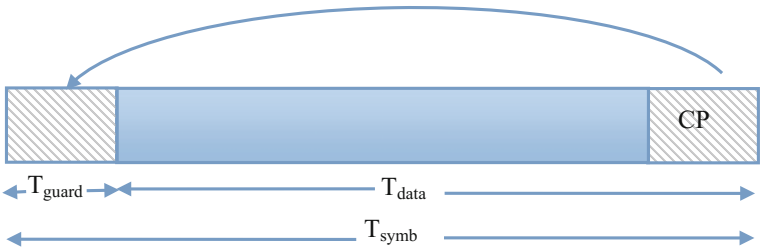


Fig. 3 Cyclic prefix addition in OFDM symbol

channel, which results into ISI effect. The CP is added in the end of the OFDM symbol as shown in Fig. 3 as copy of last portion of symbol itself.

After CP is added to each symbol, packet formation takes place. For the downlink subframe, preamble and FCH are appended to the downlink bursts after they have passed through all above physical layer modules. However, we have omitted this step as our signal is not actually transmitted in air. Other sets of the OFDM signal are prepared in same manner for other modulation schemes and each modulation with four CP lengths as per Tables 2 and 3.

4 Experiment and Results

The simulated signals were analyzed using a feed-forward neural network structure designed as per Table 2. Neural network has been extensively employed in identification of modulation schemes [27], but its use in classification of OFDM signals has been still very limited. Neural network techniques in automatic modulation classification mainly involve application of different architectures, trying different

Table 3 Key parameters of IEEE 802.16d WiMAX

WiMAX parameter	Value
Nominal channel bandwidth	3.5, 7, and 10 MHz
Number of subcarriers	256
Ratio of guard time to useful symbol time	1/4, 1/8, 1/16, 1/32
N_{FFT}	256
Subcarrier spacing	15.625, 31.25, 45 kHz
Modulation scheme	BPSK, QPSK, 16-QAM, and 64-QAM

learning techniques, and the identification of optimal parameters to train the network. There is a trade-off involved between getting accurate classification results and practical realizable network with minimum training time. Multilayer perceptron is by far the most widely network structure used for modulation classification. Generic steps involved in a neural network-based approach are depicted in Fig. 4. It consists of three stages. The first step is a preprocessing step which is a signal processing step to remove noise, unnecessary information to emphasis only discriminatory features from the raw communication signal. The second stage is called the feature extraction step which extracts useful information corresponding to exact feature from the processed data to map the information onto chosen feature space. The third is the pattern classifier stage which finds out membership of the extracted feature to a family of modulation class.

The performance of the neural network depends highly on the choice of the feature set used as input vector. A good feature set should yield limited training data, memory, and computation power. It should be insensitive to the transmission effects on the communication parameter and should remain sensitive to only the class of modulation to which it belongs. Some of the most popularly used feature sets that are tried out with different network architectures are time-domain parameters, spectral features, signal moments, and signal cumulant.

The neural network model used in our study is a multilayered perceptron (MLP) having three input layers, two hidden layers, and three output nodes. The three input nodes correspond to three features we have used, and the three output nodes correspond to three categories of signal the network classifies. The first output corresponds to single carrier digital signal that groups single carrier (SC) PSK modulation and QAM digital signals, second output corresponds to multicarrier MFSK class signal, and third output corresponds to multicarrier OFDM IEEE 802.16d signal. We have used two hidden layers because its error performance is better than single layer. There is trade-off in using number of hidden

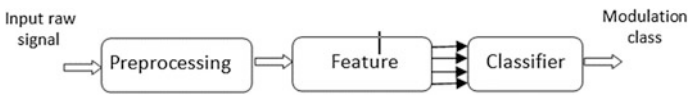


Fig. 4 Neural network-based modulation identification process

nodes and number of nodes. If the number of nodes is too few, the network performance may not be acceptable and it cannot classify to required accuracy while a too many nodes may require large training epochs. In our case, we have chosen 10 number of nodes in hidden layer. Nonlinear tan-sigmoid (hyperbolic tangent) activation function that ranges from −1 to +1 was used in hidden layer as it results better feature extraction. In output nodes, we used log-sigmoid activation function since it yields output in 0–1 range as output is supposed to be between 0 and 1. The details of used neural network structure are summarized in Table 2.

4.1 Key Features

The key features were derived for every available segment. The first parameter is derived from [10] for single carrier digital modulated signals. It is ϕ_{cnlp}, *absolute value of the centered nonlinear component of the instantaneous phase*, over nonweak intervals of a signal segment which was used first time by Nandi [28, 29]. The Hilbert transform converted input signal samples $x(i)$ into analytic signal which is a complex vector represented by $y(i)$. We have instantaneous amplitude $a(i)$ = ***abs*** $(y(i))$ and instantaneous phase $\phi(i)$ = ***angle*** $(y(i))$ where *abs* and *angle* are MATLAB standard functions, *abs* function calculates absolute value of input argument vector and *angle* function calculates the phase angle in radians of input complex vector.

We calculate our first feature ϕ_{cnlp} as below

$$\phi_{\text{cnlp}} = \text{unwrap}(\text{angle}(y(i))) - 2^{*}\pi^{*}F_{\text{c}}^{*}i/F_{\text{s}} \tag{3}$$

where F_{c} is center frequency and F_{s} is the sampling frequency.

The ***unwrap*** function in MATLAB smooths the phase in vector $y(i)$ by adding multiples of $\pm 2\pi$. This feature is used to identify digital modulated single carrier PSK and QAM family signal from the multicarrier signals. The plots for ϕ_{cnlp} of a QPSK signals are shown in Fig. 5 where the presence of phase changes is manifested in the form of maximum in histogram values of ϕ_{cnlp}. Similar plots are obtained for QAM signal also, which also have phase changes along with amplitude changes. Multicarrier signals do not have phase change characteristic, and thus single carrier digital modulated signal can be classified by this feature.

The second feature is *Ratio of Instantaneous bandwidth mean to global bandwidth.* We used this feature from [5], but instead of estimating the bandwidth (BW) from spectrogram, we used the power spectral density (psd) of signal. We calculate the mean of the psd spectral sequence as below

$$X(n)_{\text{mean}} = \frac{X(n)}{\text{length}(X(n))} \tag{4}$$

where $X(n)$ is the psd coefficients of the signal $x(n)$. The signals of MFSK class, which are also multicarrier signals, differ from OFDM in sense that the carrier

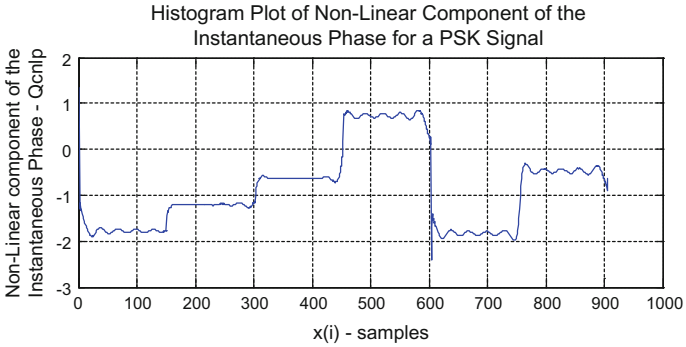


Fig. 5 Histogram plot of ϕ_{cnlp}

frequency used is not orthogonal. This allows them to be transmitted as narrow-band multicarrier signals. We exploited this difference and estimated the bandwidth occupancy in the signals by searching for the points $p1$ and $p2$ (Figs. 6 and 7) in the spectrum and store them in a bandwidth vector and use as a distinguishing feature between MFSK and OFDM signals. A maximum threshold of 1 kHz is chosen to mark the identified bandwidth as MFSK if less than threshold, or OFDM if greater than threshold.

The third feature we choose is *cyclic autocorrelation* peaks of OFDM signal [6]. The cyclic prefix inserted as guard band in the OFDM signal makes the OFDM signal a cyclostationary random process [11, 12]. A process, for instance, is said to be cyclostationary in wide sense if its mean and autocorrelation are periodic with some period. We calculate the autocorrelation of samples for various lags and search for a periodic peak in the result. A presence of periodic peaks is entered in an input vector to the neural network. In estimation of all the features, the observation time is more than one symbol period of OFDM signal.

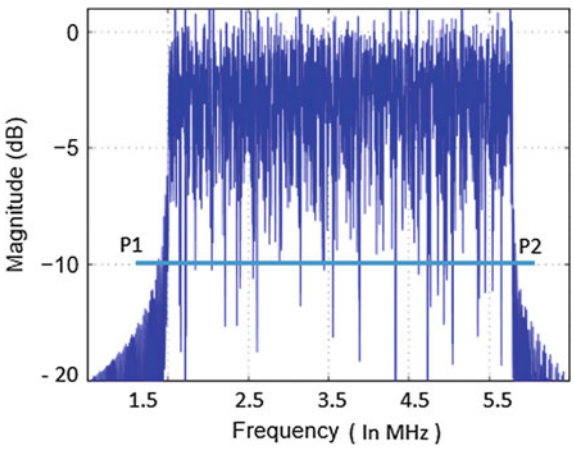


Fig. 6 Spectrum of OFDM signal

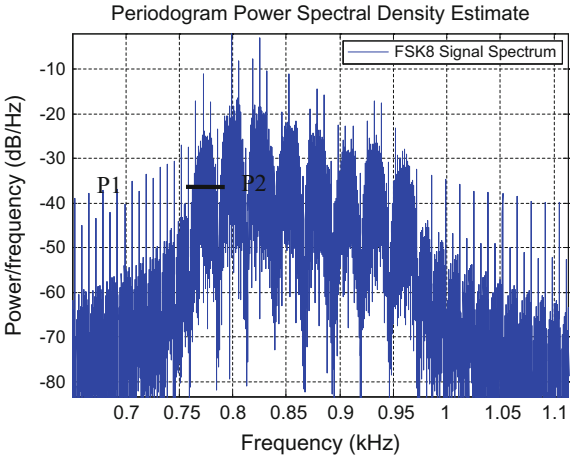


Fig. 7 Spectrum of MFSK signal

4.2 Training Phase

Training of neural network is an important step before the network is subjected to actual signal. We trained the network with training data set generated by matching with the validation set. Five hundred segments of signals from all three categories were generated in ideal and real channel conditions. We used a half of the generated data sets in training phase and remaining half for testing. During training, neural network biases were adjusted so as to match the neural network output as per training vector. The training data is fed to neural network in pairs as input and expected output pairs. The output of the neural network consisted of three neurons which correspond to one row of target vector. The identified modulation class is set as one in the row of target vector. There are many training algorithms available, but we used Levenberg–Marquardt (LM) algorithm since it is one of the fastest training algorithms and approaches second-order training speeds. The training results show good performance of the chosen network with selected features and network converged in less than 250 training epochs. The convergence is achieved when the mean-square error performance target reaches which was kept to 0.001.

4.3 Testing Phase

We tested the network structure with 250 test signals generated for each category at different SNRs and different guard intervals stored as test signals in a test set library. Test success was calculated for a given set as percentage of total number of signals identified correctly at the neural network output without adjusting the neuron biases. The compilation of test success measured as success percentage classification rate is shown in Tables 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, and 19. The results

Table 4 Success classification rate T_g = 1/4, SNR = −5 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	87%		
Multicarrier MFSK		77%	6%
IEEE 802.16d OFDM		2%	87%

Table 5 Success classification rate T_g = 1/4, SNR = 0 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	90%		
Multicarrier MFSK		85%	2%
IEEE 802.16d OFDM		0.2%	90%

Table 6 Success classification rate T_g = 1/4, SNR = 10 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	94%		
Multicarrier MFSK		90%	
IEEE 802.16d OFDM			93%

Table 7 Success classification rate T_g = 1/4, SNR = 20 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	99%		
Multicarrier MFSK		96%	
IEEE 802.16d OFDM			97%

Table 8 Success classification rate T_g = 1/8, SNR = −5 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	87%		
Multicarrier MFSK		76%	6%
IEEE 802.16d OFDM		2.2%	82%

Table 9 Success classification rate T_g = 1/8, SNR = 0 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	90%		
Multicarrier MFSK		87%	1.9%
IEEE 802.16d OFDM		0.15%	86%

Table 10 Success classification rate T_g = 1/8, SNR = 10 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	94%		
Multicarrier MFSK		90%	
IEEE 802.16d OFDM			90%

Table 11 Success classification rate T_g = 1/8, SNR = 20 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	99%		
Multicarrier MFSK		97%	
IEEE 802.16d OFDM			90%

Table 12 Success classification rate T_g = 1/16, SNR = −5 dB

Modulation type	Single Carrier	MFSK	OFDM
Single carrier	87%		
Multicarrier MFSK		78%	6.3%
IEEE 802.16d OFDM		1.7%	80%

Table 13 Success classification rate T_g = 1/16, SNR = 0 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	90%		
Multicarrier MFSK		85%	2%
IEEE 802.16d OFDM			84%

Table 14 Success classification rate T_g = 1/16, SNR = 10 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	94%		
Multicarrier MFSK		91%	
IEEE 802.16d OFDM			85%

Table 15 Success classification rate T_g = 1/16, SNR = 20 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	99%		
Multicarrier MFSK		97%	
IEEE 802.16d OFDM			88%

Table 16 Success classification rate T_g = 1/32, SNR = −5 dB

Modulation type	Single Carrier	MFSK	OFDM
Single carrier	87%		
Multicarrier MFSK		78%	7.2%
IEEE 802.16d OFDM		2.5%	78%

Table 17 Success classification rate T_g = 1/32, SNR = 0 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	90%		
Multicarrier MFSK		86%	2.2%
IEEE 802.16d OFDM			82%

Table 18 Success classification rate T_g = 1/32, SNR = 10 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	94%		
Multicarrier MFSK		90%	
IEEE 802.16d OFDM			80%

Table 19 Success classification rate T_g = 1/32, SNR = 20 dB

Modulation type	Single carrier	MFSK	OFDM
Single carrier	99%		
Multicarrier MFSK		99%	
IEEE 802.16d OFDM			80%

were taken on AWGN-corrupted and Rayleigh-faded signals as well as in idle channel conditions also. The results in idle conditions were found better than in depicted Tables 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, and 19 and have not been included due to space constraints. The classification of single carrier PSK, QAM against multicarrier MFSK, and OFDM signal is very good, and in better SNR conditions, almost 99% digital single carrier could be differentiated with multicarrier signals using selected feature ϕ_{cnlp}. The intra-class differentiation between MFSK and OFDM signal poses some challenge in lower SNR range where some MFSK signals are wrongly identified as OFDM signal and vice versa (Tables 4, 5, 8, 9, 12, 13, 16 and 17). This incorrect intra-class misclassification can be attributed due to inaccuracy in bandwidth processing and processing of cyclic autocorrelation vectors. This can be improved by adjusting to the set bandwidth threshold for classification between MFSK and OFDM. It can be noted that due to strong autocorrelation feature used for OFDM, the misclassification percentage is less for OFDM than MFSK case. The classification accuracy of the IEEE 802.16d OFDM symbol is seen also dependent on the guard interval time. The standard mentions four options due to the fact that the guard interval though aids in avoiding intersymbol interference effects but it actually increases energy requirement of the transmitter. Hence, the standard offers options to keep CP duration as minimum as 1/32 of the total useful symbol time. However with the decreasing guard period, the cyclic autocorrelation function also degrades, and in low SNR ranges, this results in lower classification rate. This is evident in the results for lower guard interval CP options, and classification rate falls to low values as compared to higher duration CP. However in a ideal channel conditions, the classification rate is better and more than 90% in worst case CP period is observed.

5 Conclusion

In this paper, we suggested classification of multicarrier OFDM signals for a WiMAX network which is competing with other 4G networking technologies like UMTS and 3GPP LTE. The OFDM multicarrier modulation of the WiMAX IEEE 802.16d network is classified with good accuracy in the presence of single carrier digital modulation and other class of multicarrier signals like MFSK. Distinguishing features were extracted for the three categories of signal, and a optimal neural network structure was designed to classify signals based on chosen features. It was observed that the cyclic prefix guard time period plays important role particularly when the SNR ranges are in lower ranges. The merit of the neural network-based classification however is that it does not depend on any cooperative environment like inclusion of symbols at transmitter side. Automatic modulation classification capability that does not require any additional information at transmitter side to aid modulation classification at receiver end greatly reduces transmission overheads and increases bandwidth efficiency of the system.

Further efforts are being invested to enhance proposed neural network capability to also include IEEE 802.16e mobile WiMAX OFDMA signal and 3GPP LTE 4G OFDM signal to make a more dynamic heterogeneous environment. Other possible research objectives can be to identify other neural structures like radial basis network and other robust features which are not sensitive to lower or negative SNR range. It is expected that a neural network-based modulation classification can be the best approach in today advanced data communication environment since it can be retrained quickly to adapt to new parameters of different networks which have to work in a highly heterogeneous network environment or quickly align to advancements in new air interface standards.

References

1. Akmouche, W.: Detection of multicarrier modulations using 4th-order cumulants. In: Military Communications Conference Proceedings, MILCOM (1999)
2. Lenonen, J., Juntti, M.: Modulation classification in adaptive OFDM. In: Vehicular Technology Conference, 2004, vol. 3, pp. 1554–2252 (2004)
3. Reddy, S.B., Yucek, T., Arslan, H.: An efficient blind modulation detection algorithm for adaptive OFDM systems. In: Proceedings of IEEE Vehicular Technology Conference, Orlando, FL, Oct 2003
4. Yucek, T., Arslan, H.: A novel sub-optimum maximum-likelihood modulation classification algorithm for adaptive OFDM systems. In: Wireless Communications and Networking Conference, 2004, vol. 2, pp. 739–745, March 2004
5. Huo, L., Duan, T., Fang, X.: A novel method of modulation classification for digital signals. In: International Joint Conference on Neural Networks, pp. 2435–2438, July 2006
6. Han, N., Zheng, G., Sohn, S.H., Kim, J.M.: Cyclic autocorrelation based blind OFDM detection and identification for cognitive radio. In: 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08, pp. 1–5 (2008)
7. Ulovec, K.: Noncoherent recognition of OFDM modulation. In: 18th International Conference Radioelektronika, pp. 50–55, April 2008
8. Chen, M., Zhu, Q.: Cooperative automatic modulation recognition in cognitive radio. J. China Univ. Posts Telecomm. **17**, 46–52 (2010)
9. Bouzegzi, A., Ciblat, P., Jallon, P.: New algorithms for blind recognition of OFDM based systems. Signal Process **90**, 900–913 (2010)
10. Haq, K.N., Mansour, A., Nordholm, S.: Recognition of digital modulated signals based on statistical parameters. In: 4th IEEE International Conference on Digital Ecosystems and Technologies, pp. 565–570 (2010)
11. Vladimír, S., Roman, M., Zbyněk, F.: OFDM signal detector based on cyclic autocorrelation function and its properties. Radio Eng. **20**(4), 927 (2011)
12. Nouha, A., Abdennaceur, K., Samet, M.: The fourth generation 3GPP LTE identification for cognitive radio. In: International Conference on Microelectronics (ICM), pp. 1–5, Dec 2011
13. Muhlhaus, .S., aus, Öner, M., Dobre, O.A., Jakel, H.U., Jondral, F.K.: Automatic modulation classification for MIMO systems using fourth-order cumulants. In: IEEE Conference Vehicular Technology, pp. 1–5 (2012)
14. Al-Makhlasawy, R.M., Elnaby, M.M.A., El-Khobby, H.A., El-Rabaie S., El-samie, F.E.A: Automatic modulation recognition in OFDM systems using cepstral analysis and support vector machines. J. Telecomm. Syst. Manag **1**(3), 1–7 (2012)

15. Al-Makhlasawy, R.M., Elnaby, M.M.A., El-Khobby, H.A., El-Rabaie S., El-samie, F.E.A.: Automatic modulation recognition in OFDM systems using cepstral analysis and a fuzzy logic interface. In: 8th International Conference on Informatics and Systems, pp. 56–61, May 2012
16. Hassan, K., Dayoub, I., Hamouda, W., Nzéza C.N., Berbineau, M.: Blind digital modulation identification for spatially-correlated MIMO systems. IEEE Trans Wirel. Commun. **11**(2), 683–693 (2012)
17. Al-Habashna, A., Dobre, O.A., Venkatesan, R., Popescu, D.C.: Second-order cyclostationarity of mobile WiMAX and LTE OFDM signals and application to spectrum awareness in cognitive radio systems. IEEE J. Sel. Top. Signal Process. **6**(1), 26–42 (2012)
18. Mühlhaus, M.S., Öner, M., Dobre, O.A., Jondral, F.K.: A low complexity modulation classification algorithm for MIMO systems. IEEE Commun. Lett. **17**(10), 1881–1884 (2013)
19. Mühlhaus, M.S., Öner, M., Dobre, O.A., Jondral, F.K., Jakel, H.U..: A novel algorithm for MIMO signal classification using higher-order cumulants. In: IEEE Radio and Wireless Symposium, pp. 7–9, Jan 2013
20. Gorcin A., Arslan, H.: Identification of OFDM signals under multipath fading channels. In: Military Communications Conference, pp. 1–7, Nov 2012
21. Sun, Z., Liu R., Wang, W.: Joint time-frequency domain cyclostationarity-based approach to blind estimation of OFDM transmission parameters. EURASIP J. Wirel. Commun. Netw, 1–8 (2013)
22. Liu, Y., Haimovich, A.M., Su, W., Dabin, J., Kanterakis, E.: Modulation classification of MIMO-OFDM, signals by independent component analysis and, support vector machines. In: 45th Asilomar Conference on Signals, Systems and Computers, pp. 1903–1907, Nov 2011
23. Guibene, W., Slock, D.: Signal classification in heterogeneous OFDM-based cognitive radio systems. In: 20th International Conference on Telecommunications, pp. 4284–4299 (2013)
24. Jantti, J., Chaudhari, S., Koivunen, V.: Cepstrum based detection and classification of OFDM waveforms. In: IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 8063–8067 (2014)
25. Sun, Z., Chen, Y., Liu S., Wang, W.: Cyclostationarity-based joint domain approach to blind recognition of SCLD and OFDM signals. EURASIP J. Adv. Signal Process. pp. 1–6 (2014)
26. Gorcin, A., Arslan, H.: An OFDM signal identification method for wireless communications systems. IEEE Trans. Veh. Technol. pp. 1–13 (2015)
27. Hazza, A. Shoaib, M. Alshebeili, S.A.; Fahad, A.: An overview of feature-based methods for digital modulation classification. In: 1st International Conference on Communications, Signal Processing, and their Applications (ICCSPA), pp. 1–6 (2013)
28. Nandi, A.K., Azzouz, E.E.: Modulation recognition using neural network. Signal Process. **56** (2), 165–175 (1997)
29. Nandi, A.K., Azzouz, E.E.: Automatic modulation recognition—II". J Franklin Inst **334B**(2), 241–273 (1997)
30. 802.16-2004—Standard for local and metropolitan area networks—part 16: air interface for fixed broadband wireless access systems

Routing Protocols in CRAHNs: A Review

Anukiran Jain, S. Umang and M.N. Hoda

Abstract Cognitive radio, CR is a promising technology to authorize the competent usage of restricted natural resource radio frequency spectrum for the wireless devices. The technology authorizes the secondary (unlicensed) users, SU to exploit underutilized spectrum allocated to primary (licensed) user, and PU by renovating the traditional static spectrum access approach to dynamic spectrum access without creating any/allowable interference for PU. Design and implement routing protocol in Cognitive Radio Ad Hoc Networks, is an upcoming challenge. Such protocols require addressing the issues like environmental awareness to identify the licensed spectrum which is comparatively underutilized by PUs and can be use by SUs respecting the privilege of PUs usage and avoidance any interference to them. This paper presents the revised analytical model using domain object model of Dynamic Spectrum Management Functions (DSMF) that also represents the concept of cognitive routing in Cognitive Radio Ad Hoc Networks (CRAHNs). The presented analytical model facilitates to enhance the understanding of the concept of routing protocol in CRAHNs. The paper designates suggested routing protocols in recent years. Based on the literature survey, the paper also provides the research gap in the area of cognitive routing protocol in CRAHNs and ends with concluding remarks.

Keywords Primary users · Secondary users · CRAHNs · Cognitive radio · DSMF · Cognitive routing protocols

A. Jain (✉) · M.N. Hoda
BVICAM, New Delhi, India
e-mail: anukiranjain@gmail.com

M.N. Hoda
e-mail: mca@bvicam.ac.in

S. Umang
ITS, Ghaziabad, UP, India
e-mail: Singh.umang@rediffmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_22

1 Introduction

Cognitive Radio Ad Hoc Networks (CRAHNs) is the network of cognitive radio(s) (the unlicensed radio devices comprise to cognitive technology) to utilize the spectrum allocated to licensed users in an opportunistic approach respecting the privileged policy for the action of licensed user within its allotted spectrum to maximize the spectrum utility in efficient manner [1, 2]. Routing in CRAHNs is similar to traditional Ad Hoc networks with additional complexities to address the issues like spectrum awareness, primary user activities awareness, route maintenance and lack of common control channel. These issues restrict the applicability of stable Ad Hoc networks routing protocols for CRAHNs. So there is a need to identify optimized cognitive routing protocol in terms of throughput end to end delay packet ratio. This paper helps to understand the routing protocol in CRAHNs through analytical model and review the various routing protocols in CRAHNs suggested by the researcher. Based on the literature survey, the paper also highlights the research gap with concluding remark. The paper is organized in five sections Sect. 1 provides the introduction; Sect. 2 introduces routing protocol in CRAHNS and discuss the analytical model for the same; Sect. 3 discusses the existing literature related to cognitive routing protocols; Sect. 4 discusses the research gap in the same domain, and Sect. 5 ends with the concluding remarks.

2 Routing Protocol in CRAHNs

Due to dynamic spectrum access, DSA, feature, CRAHNs need to face obscure topology and diverse QoS in comparison to Mobile Ad Hoc Networks which necessitate the proper routing protocol that also address the cognitive radios capabilities and reconfigure ability issues [1, 3, 4]. DSA exploits the spectrum utilization efficiently without interfering primary user activities. To realize the CRAHN, cognitive radio (CR) devices must have the capability to sense the white holes in licensed spectrum using spectrum sensing techniques that can result in multi-channel availability at a time for the secondary users. It makes the cognitive users to exploit the capability of spectrum decision to select the best available spectrum for the opportunistic use and vacant the spectrum or reconfigure the CR transmitter parameters (operating spectrum, modulation, transmission power, and communication technology) on detecting any primary user in the same spectrum to respect the PUs priority usage policy through spectrum sharing and spectrum mobility.

Analytical model [5] using domain object model can be used to enhance the understanding of Dynamic Spectrum Management Functions, DSMF, which includes cognitive capabilities and cognitive reconfigurability. Figure 1 represents the enhanced analytical model suggested in domain object model of CRAHNs functions [5], using domain object model to signify the involvement of DMSF

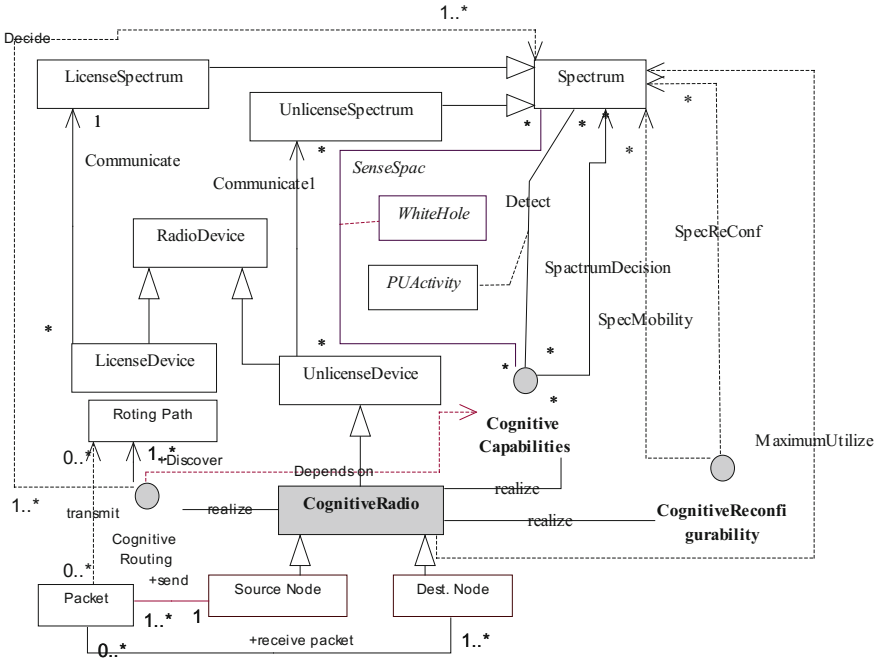


Fig. 1 Domain object model for cognitive routing in CRAHNs

to entail the appropriate routing protocols for CRAHNs. The model represents that each cognitive radio needs to implement the cognitive routing protocol which must be efficient to decide the finest available spectrum and transmit the data packets efficiently using its cognitive capabilities and reconfigurability for the competent usage of limited natural resource, i.e., spectrum. The model demonstrates the domain objects like spectrum which can be specialized as license spectrum and unlicensed spectrum; radio device which is specialized as license device or unlicense device; unlicense devise can be further specialized as cognitive radio which implements the cognitive capabilites and cognitive reconfigurability interface at the same time cognitive radio need to implement cognitive routing to maximize the spectrum usage and efficient data transmission.

3 Literature Survey

Cognitive routing protocols are required to deal with the changing spectrum of opportunities for cognitive radio(s); PUs privileged access for the licensed spectrum and no interference constraint by CR to any licensed PUs; for its action in its respective spectrum. Literature suggested several schemes to categorize the cognitive routing protocol based on full spectrum knowledge and local spectrum

knowledge [1, 6–8]. Cognitive routing protocols (more than twenty) discussed in paper are generally based on local spectrum knowledge.

AODV—Ad Hoc *On-Demand Distance Vector Routing* suggested in 2003 [9] is a novel routing protocol for Ad Hoc network in which routes are attain as per the requirement suitable for dynamic self-starting networks. AODV is a novel protocol as the basis for cognitive routing in Ad Hoc network.

SORP—Spectrum Aware Routing Protocol and *DORP; Joint On-demand Routing and Spectrum Assignment* suggested in 2007 [1, 3, 6, 7, 10, 11] are AODV-based routing protocol(s) consider cumulative switching and backoff delay suitable for delay sensitive application. Both protocol(s) provide the solution for whole path selection but does not emphasize on neighborhood discovery and avoid spectrum dynamics. *STOD-RP—Spectrum tree-based on-demand routing protocol* suggested in 2008 [1, 6, 7, 12] provides end to end linking using tree-based proactive routing. Suggested protocol provides spectrum decision along with route selection. The protocol comprises the features of statistical PUs' activities and considers CR users' QoS as route metric and introduces spectrum adaptive route discovery method. Metric used in this protocol includes channel overhead, protocol overhead, packet size, link rate, packet error rate band availability, and spectrum band switches.

Local Coordination-Based Routing and Spectrum Assignment suggested in 2008 [1, 7, 8, 13]. Protocol is suggested to achieve efficient routing for whole path selection and spectrum assignment in multi-hop CRNs with minimal end to end delay. Protocol describes two sections: joint on-demand routing algorithm with spectrum selection and local coordination scheme for load balancing among multiple frequency band at intersecting relay node.

SAMER—Spectrum Aware Mesh Routing suggested in 2008 [1, 6, 14]. Suggested protocol provides whole path selection process considering spectrum awareness dynamics based on long-term and short-term spectrum availability. It considers the hop count and spectrum availability to balance the long-term optimality and short-term opportunistic gain. Protocol used Path Spectrum Availability (PSA) metric based on local spectrum availability and spectrum block quality (bandwidth/loss rate). Protocol provides rank to the alternative path based on activities of PU and SU as well. SAMER avoids congested and occupied links.

SPEAR—A multi-hop distributed channel assignment and routing algorithm suggested in 2008 [1, 6–8, 15] to support high-throughput packet transmission. The protocol takes the flexibility of link-based approach for the end to end optimization of flow-based approach. Protocol consider three subsections: (i) integration of spectrum discovery with route discovery (ii) minimization of inter-flow interference through coordination of channel assignments per flow basis (iii) minimization of intra-flow interference through exploitation of local spectrum heterogeneity and assigning different channels to link. Suggested protocol selects the best path by allowing multi-path propagation toward destination by embedding channel assignment in RREP. The protocol provides channel reservation, and simulation result indicates significant improvement in throughput. Protocol uses traditional routing metric with manual parameter setting.

MSCRP—multi-hop single transceiver cognitive radio network routing protocol suggested in 2008 [7, 16] is based on AODV contribute to improve network throughput. Suggested protocol supports CR transceiver to function on one channel at a particular time. MSCRP is based on the approach of joint selection of the spectrum with the choice of neighborhood node. Protocol solves the deafness problem that constraints if two consecutive nodes are serving same flow; they must not be switching nodes. Protocol supports the local coordination to focus on load balancing. MSCRP applies three states to the node single channel state, switching state, and non-free state.

Improved Ant Routing Algorithm suggested in 2009 [6, 17]. Suggested approach is based on the principle of swarn intelligence which is inspired from the communal behavior of social insects. The protocol is based on on-demand routing protocol without CCC to crack large-scale optimization problem in a distributed way. Protocol also instigates the route repair procedure in case existing route get disable.

SARP—Spectrum Aware routing protocol for cognitive Ad Hoc network proposed in 2009 [3, 18] discusses about two functions of SARP intelligent multi-interface selection function (MISF) and intelligent multi-path selection function (MPSF). SARP assigns the interface to a route through MISF by using the delay of the RREQ packet as a metric. The suggested protocol selects a path to route packet through MPSF by using the throughput increment as metric. Protocol results in high throughput, low delay, and overhead.

Spectrum Aware Highly Reliable Routing in CRN suggested in 2009 [6, 19] exploits concept of multi-path routing. Metric used in this protocol includes channel stability time (CST), link stability time (LST) PU on/off period, switching time, and path effective time (PET). It also provides path maintenance mechanism.

RACON suggested in 2009 [20] designs data transportation in CRN using link modeling to maximize data delivery rate, minimize latency, and minimize aggregate system resource consumed in all. In this protocol, link cost metric of a node is computed dynamically based on history of spectrum usage instead of current state. The link cost increases if node is disconnected for long period or having history of frequently disconnected-to-connected transitions. Suggested protocol always route the data packet closer to the destination by supporting limited packet buffering for short period even when the destination is not physically connected to the source or its current network partition.

GYMKHANA Protocol introduced in 2010 [6–8, 21] is capable to discover most stable routes. It is described in three classes: (a) to collect key parameters support distributed AODV style protocol (b) the basis of mathematical structure is represented through a graph associated to a given path (c) the second smallest eigenvalue of the Laplacian associated to the graph is evaluated to compute closed formula. Mathematical model for Gymkhana is very complex.

SEARCH suggested in 2009 [6–8, 22] is a geographic forwarding-based Spectrum Aware Routing protocol for CRAHNs that jointly undertake path and channel selection to avoid the PU activities during route formation, during route operations can be adapted to the newly discovered and lost SOP, and to consider distributed environment with node mobility in various cases. SEARCH protocol

avoids the PU active region while routing. Author suggested that SEARCH can be extended to consider PU type with duty cycle and times of operation. More quality attributes may be added for next hop selection.

BCCCS—The Backup Channel and Cooperative Channel Switching Routing Algorithm suggested in 2010 [7, 8, 23] provides the concept of backup channel to focus on the route maintenance issue of CRAHNs. Each node periodically updates list of available channels with their priorities. Consider control packet channel request (CREQ), channel reply (CREP), and channel information (CINFO) required to maintain additional list and tables.

OSAB—Opportunistic Spectrum Access with Backup suggested in 2010 [24] discusses the CRAHNs challenge related to spectrum handoff that occurs when a channel occupied by SU and PU appears in the same channel. In this situation, SU needs to vacate the channel to respect the PU privileged usage of channel and results in degradation of performance of SU in terms of delay and link maintenance. OSAB offers the feature of reducing the number of spectrum handoffs. To evaluate the link maintenance probability and expected number of handoffs, a mathematical model is discussed by author. Results presented by author are positive for OSAB approach. Validation needs to be done through simulation for OSAB concept.

TACR—Traffic Aware Routing Protocol suggested in 2010 [6–8, 25] provides the combination of traffic aware routing and Q-learning algorithm based on on-demand routing protocol. It implements the cognitive packet to provide the current traffic information. Spectrum decision is based on the input parameters for traffic prediction and traffic perception. Q-learning technique helps to maintain route. The protocol results in reduced end to end delay, better throughput, and less packet loss in case of high traffic arrival rate.

WHAT based on weighted hop, spectrum awareness, and stability routing metric introduced in 2010 [8, 26] is able to capture overall quality of a path to have multiple consideration of metric calculation and enhance the network throughput. WHAT requires tuning of parameters to determine the metric value and path selection that can reduce the cognitive learning capabilities.

OSDRP—Opportunistic Service Differentiation Routing Protocol suggested in 2011 [27] addresses the cognitive routing issue where the average available communication time is shorter than the required communication time by cognitive radio(s). Author suggested a cross-layer cognitive routing protocol, for the dynamic CRNs. OSDRP emphasizes on minimum delay-maximum stable path for CRNs. OSDRP is a multi-metric routing that consider the availability of SOP with switching delay and queuing delay. Author identifies the possibility to explore implementation of geographical routing techniques to further reduce the overhead of proposed scheme.

CRP—A routing protocol for CRAHNs suggested in 2011 [6, 28]. CRP maximizes the bandwidth availability and provides explicit protection to PU receivers by considering the metrics for spectrum sensing, spectrum propagation characteristics, PU receiver protection, probability of bandwidth availability, and variance in the number of bits sent over the link. Suggested protocol works in two stages spectrum selection stage and next hop selection stage. CRP also considered route

maintenance by utilizing proactive and reactive components. CRP works on the assumption that PU transmitter with known location is stationary in nature with maximum coverage range.

SER—Spectrum and Energy Aware routing protocol for Cognitive Radio networks proposed in 2011 [3, 29] which includes the basic operations like route discovery, data transmission, and route maintenance that combine the spectrum and route discovery results in less delay in end to end linking, high throughput, and less overhead.

Routing Protocol with Route Closeness Metric suggested in 2011 [6, 30] exploits multi-path routing to attain reliability and throughput. This protocol introduced a routing metric route closeness. It represents a variation of the DSR protocol for the route discovery phase.

CAODV—Cognitive Ad Hoc On-demand Distance Vector Protocol presented in 2012 [8, 31] based on graph theory and mathematical analysis. CAODV proposed with two versions; one exploits inter-route spectrum diversity and another exploits intra-route spectrum diversity. CAODV is reactive routing protocol with three objectives: (i) interference avoidance to primary users during both route formation and data forwarding; (ii) perform a joint path and channel selection at each forwarder; (iii) take advantage of the availability of multiple channels to improve the overall performance. Introduce additional control packet PU-RERR. The protocol results in high resource consumption due to the feature of discovery of multi-path or multi-channel routes and additional control packet. This protocol can be extended by using more effective route metrics.

Cooperative routing protocol in multi-hop CRAHNs proposed in 2012 [32]. This on-demand routing protocol helps to get minimum cost path between source and destination pair having maximum throughput and minimum delay with control message in comparison to previous work. Suggested protocol used the cooperative communication (CC) technique to resist fading effect and improved channel capacity. Author implemented the cooperative routing protocol in ns-2 2.31 with cognitive radio cognitive network Simulator [33].

D^2CARP—Dual Diversity Cognitive Ad Hoc *Routing Protocol* suggested in 2012 [8, 34] is a variation of AODV. Protocol combines path and spectrum diversity. Route discovery process of the protocol offers multi-path and multi-channel routes. Suggested protocol offers improvement over CAODV in terms of packet delivery ratio, overhead, delay, and hop count. In D^2CARP protocol, RREP needs to be broadcast back to the source and need large routing table and more resource consumption.

RPCRAN—A Routing Protocol for Cognitive Radio Ad Hoc *Networks* suggested in 2013 [35] is sensitive to primary user activities and utilizes multiple channels to enhance performance. This protocol suggested the incorporation of channel selection mechanism in the routing layer instead of MAC layer. Simulation results are compared with AODV results.

LAUNCH—Location-based Cognitive Routing Protocol suggested in 2013 [6, 36] considers stochastic activities of PUs to select most stable route. The selection of next hop is based on greedy decision which satisfies the condition that

the next hop must be closer to the destination and result in minimum expected delay. LAUNCH studies the impact of changing SUs density, number of PUs, heterogeneity in PUs, mobility of SUs, data rate, and number of channels.

TIGHT—A geographic routing protocol suggested in 2014 [37] put forward three modes of routing to exploit spectrum opportunity by SU over the dedicated spectrum to PU without imposing interference on them. The *greedy mode* routes around the PU region using shortest trajectory circumventing method, without knowledge of primary user location. Greedy mode works best if the PU known to be rarely active [38]. The *optimal mode* works when the primary user location is known. In this mode, SU needs to compute the optimal trajectory to the destination SU [39]. The suboptimal mode further reduces the computational complexity of optimal mode at the cost of driving suboptimal trajectory from source SU to destination SU. The protocol is relatively less sensitive to node mobility and comparatively bear low overhead due to routing dependability based on location instead of next hop and doesn't favor route discovery and route maintenance.

4 Research Gap

Nowadays researchers are working extensively on the challenges related to opportunistic spectrum access and spectrum utilization. The networking concern needs to be addressed in Cognitive Radio Ad Hoc Networks (CRAHNs) [1, 4]. The methods for flexible spectrum use, distributes networks that wisely cooperate, low power, scalable implementation of cognitive radios are open challenges among researcher. Choosing the suitable path and choosing the suitable band at each path are the two major routing problems in CRAHNs [2]. There are many challenges that require attention of researchers related to cognitive routing in Ad Hoc networks includes: spectrum awareness, primary user activities, quality routes, and spectrum maintenance. Traditional routing protocols need to address the challenges of CRAHNs to provide the efficient cognitive routing protocol which can consider the spectrum decision with path selection based on spectrum awareness to provide the end to end communication. The cognitive routing protocols need to support routing with spectrum decision considering PUs' activities and sustain through reconfigurability to avoid unnecessary spectrum handoff. Instead of several suggested cognitive routing protocols by the researcher, it is strongly believed that research in this field needs major contribution [1, 6–8]. Minimizing the frequent change in CRN topology due to PUs' activities is an open research challenge in CRAHNs. Need to identify the techniques to predict PUs' activities in a spectrum so that the influence of these activities must be minimized on CRN topology. Researchers are working toward the direction to minimize the rerouting requirements for cognitive routing in case any PU unexpectedly appear in a give location that can result in degradation of network performance or unpredictable route failure. Coupling of quality metrics of end to end routes (nominal bandwidth, throughput, delay, energy efficiency, and fairness) with metrics on path stability, spectrum availability/PU

presence is an open research challenge. Effective signaling procedures are required to restore "broken" paths with minimal effect on the perceived quality. The neighbor discovery is an open issue of cognitive routing in Ad Hoc Networks, due to lack of CCC broadcasting.

5 Conclusion

The paper demonstrates cognitive routing in CRAHNs through domain object model and the importance of entire DSMF in cognitive routing. Through the discussed literature, it is known that the routing protocols suggested in recent years consider almost static CRNs with stable communication channel where the channel is available for longer time than required. PU activity can force the SU to vacant the available channel to maintain the precedence of PU for channel utilization. Cognitive routing algorithm need to be aware of spectrum availability, during CR in operation also, which is based on surrounding special environment. Researchers need to address the ways to couple routing algorithm with the entirely cognitive cycle of spectrum management. Dynamic self-organized, a well-known novel traditional Ad Hoc routing protocol, AODV, Ad Hoc on-Demand Distance Vector Routing protocol can be modified to propose a stable cognitive routing protocol in Ad Hoc networks.

References

1. Cesana, M., Cuomo, F., Ekici, E.: Routing in cognitive radio networks: challenges and solutions. Ad Hoc Netw. **9**, 228–248 (2011)
2. Bandyopadhyay, P.: Routing in cognitive radio ad-hoc networks. Cognitive networking and cross-layer interaction. University of Helsinki, Department of Computer Science, 15.01.2013–23.04.2013, pp. 134–138. www.hiit.fi/u/bayhan/uh/StudentReports/Payel_Bandyopadhyay_RA_finalreort.pdf
3. Walde, N., Barve, S.: A study: on routing schemes in cognitive radio network. Int. J. Adv. Res. Comput. Commun. Eng. **2**(8), 3262–3265 (2013)
4. Yu, F.R. (ed.): Cognitive Radio Mobile Ad Hoc Networks. Springer, New York, pp. 145–148
5. Jain, A., Umang, S., Hoda, M.N.: Conceptual understanding of cognitive radio adhoc networks. In: 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 2194–2198 (2015)
6. Abdelaziza, S., ElNainay, M.: Survey of routing protocols in cognitive radio networks. In: Preprint submitted to Elsevier, pp. 1–20 (2012)
7. Jain, S., Dhawan, A., Jha, C.K.: A survey: on routing protocols in cognitive radio ad hoc networks. Int. J. Comput. Sci. Inf. Technol. **5**(2), 2204–2206 (2014). ISSN: 0975-9646
8. Salim, S., Moh, S.: On-demand routing protocols for cognitive radio ad hoc networks. EURASIP, J. Wireless Commun. Netw. 24–29 (2013)
9. Perkins, C.E., Royer, E.M.: Ad hoc on-demand distance vector (Aodv) routing. Internet Engineering Task Force IETF, pp. 1–29, July 2003

10. Cheng, G., Liu, W., Li, Y., Cheng, W.: Spectrum aware on-demand routing in cognitive radio networks. In: Proceedings of 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, pp. 571–574 (2007)
11. Cheng, G., Liu, W., Li, Y.: Joint on-demand routing and spectrum assignment in cognitive radio networks. In: IEEE International Conference on Communications, pp. 6499–6503 (2007)
12. Zhu, G., Akyildiz, I., Kuo, G.: Stod-Rp: a spectrum-tree based on demand routing protocol for multi-hop cognitive radio networks. In: IEEE Global Telecommunications Conference, GLOBECOM, pp. 1–5 (2008)
13. Yang, Z., Cheng, G., Liu, W., Yuan, W., Cheng, W.: Local coordination based routing and spectrum assignment in multi-hop cognitive radio networks. Mobile Netw. Appl. 67–81 (2008)
14. Pefkianakis, I., Wong, S.H,Y., Lu, S.: Samer: spectrum aware mesh routing in cognitive radio net-works. In: 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN, pp. 1–5 (2008)
15. Sampath, A., Yang, L., Cao, L., Zheng, H., Zhao, B: High throughput spectrum-aware routing for cognitive radio based ad hoc networks. In: Proceedings of the International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM), pp. 113–117 (2008)
16. Ma, H., Zheng, L., Ma, X., Luo, Y.: Spectrum aware routing for multi-hop cognitive radio networks with a single transceiver. In: Proceednigs of 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, pp. 1–6 (2008)
17. Song, Z., Shen, B., Zhou, Z., Kwak, K.S.: Improved ant routing algorithm in cognitive radio networks. In: ISCIT 9th International Symposium Communications and Information Technology, pp. 110–114 (2009)
18. Ju, S., Evans, J.B.: Spectrum-aware routing protocol for cognitive ad-hoc networks. In: Proceedings of the IEEE Globecom, pp. 1–6, November 2009
19. Song, H., Lin, X.: Spectrum aware highly reliable routing in multihop cognitive radio networks. In: IEEE Wireless Communications and Signal Processing, pp. 1–5 (2009)
20. Talay, A.C., Altilar, D.T.: RACON: a routing protocol for mobile cognitive radio networks. In: CoRoNet '09 Proceedings of the 2009 ACM workshop on Cognitive radio networks, pp. 73–78 (2009)
21. Abbagnale, A., Cuomo, F.: Gymkhana: a connectivity-based routing scheme for cognitive radio ad hoc networks. In: IEEE Conference on Computer Communications, INFOCOM, pp. 1–5 (2010)
22. Chowdhary, K.R., Felice, M.D.: Search: a routing protocol for mobile cognitive radio ad-hoc networks. Comput. Commun. **32**, 1–6 (2009)
23. Zeeshan, M., Manzoor, M.F., Qadir, J.: Backup channel and cooperative channel switching on-demand routing protocol for multi-hop cognitive radio ad hoc networks (BCCCS). In: Proceedings of 6th International Conference on Emerging Technologies, pp. 394–399 (2010)
24. Kalil, M.A., Al-Mahdi, H., Mitschele-Thiel, A.: Spectrum handoff reduction for cognitive radio ad hoc networks. In: 7th International Symposium on Wireless Communication Systems Wireless Communication Systems (ISWCS), pp. 1036–1040 (2010)
25. Xu, Y., Sheng, M., Zhang, Y.: Traffic-aware routing protocol for cognitive network. In: Proceedings of IEEE 72nd Vehicular Technology Conference, pp. 1–5 (2010)
26. Chen, J., Li, H., Wu, J.: WHAT: a novel routing metric for multi-hop cognitive wireless networks. In: Proceedings of the 19th Annual Wireless and Optical Communications Conference Shanghai, pp. 1–6, 14–15 May 2010
27. How, K.C., Ma, M., Qin, Y.: Routing and QoS provisioning in cognitive radio networks. Comput. Netw. **55**, 330–342 (2011)
28. Chowdhury, K., Akyildiz, I.: CRP: a routing protocol for cognitive radio ad hoc networks. IEEE J. Sel. Areas Commun. 794–804 (2011)
29. Kamruzzarman, S.M., Kim, E., Jeong, D.G.: Spectrum and energy aware routing protocol for cognitive radio ad hoc networks. In: IEEE ICC proceeding, pp. 1–5 (2011)

30. Beltagy, I., Youssef, M., El-Derini, M.: A new routing metric and protocol for multipath routing in cognitive networks. In: IEEE Wireless Communication and Networking Conference (WCNC), pp. 974–979 (2011)
31. Cacciapuoti, A.S., Caleffi, M., Paura, L.: Reactive routing for mobile cognitive radio ad hoc networks. Ad Hoc Netw. 803–815 (2010)
32. Sheu, J.P., Lao, I.L.: Cooperative routing protocol in cognitive radio ad-hoc networks. In: IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks, pp. 2916–2921 (2012)
33. Cognitive Radio Cognitive Network Simulator. http://stuweb.ee.mtu.edu/∼ljialian
34. Rahman, M.A., Caleffi, M., Paura, L.: Joint path and spectrum diversity in cognitive radio ad-hoc networks. EURASIP J. Wireless Commun. Netw. 1–9 (2012)
35. Sieaj, M., Alshebeili, S.: RPCRAN: a routing protocol for cognitive radio ad hoc networks. Int. J. Innov. Comput. Info. Control Vol. **9**(11), 4583–4594 (2013)
36. Habak, K., Abdelatif, M., Hagrass, H., Rizc, K., Youssef, M.: A location-aided routing protocol for cognitive radio networks. ICNC, pp. 729–733 (2013)
37. Jin, X., Zhang, R., Zhang, Y.: TIGHT: a geographic routing protocol for cognitive radio mobile ad hoc networks. IEEE Trans. Wireless Commun. **13**(8), 4670–4681 (2014)
38. Walde, Nilima, Barve, Sunita: A study: on routing schemes in cognitive radio network. Int. J. Adv. Res. Comput. Commun. Eng. **2**(8), 3262–3265 (2013)
39. Jain, A., Umang, S., Hoda, M.N.: Exigency of cognitive radio network. IJCSI Mauritius IJCSI **12**(1) (2015)

Cluster-Tree-Based Routing—A Step Towards Increasing WSN Longevity

Shalini, Umang and M.N. Hoda

Abstract Network lifetime is a major factor in determining the efficacy of a wireless sensor network. There are several other issues involved, like management in case of link/node failure, node mobility. Since, the nodes in a WSN operate in unattended, battery operated mode, there is a constant need to minimize energy consumption and address topology changes so that the network lifetime may be maximized. Out of the basic tasks, i.e. sensing, local storage and processing and communicating, involved in a WSN, communication uses the largest fraction of the total energy consumed. Techniques like selective forwarding, clustering, data aggregation, are employed in order to reduce energy consumption during communication. It is basically the network topology that decides the scheme used for communicating the sensed data to the sink. Different topologies like flat, clustered, tree and cluster tree use evolving approaches to minimize the energy consumption during communication. This paper discusses and compares the approaches used and their contribution towards the desired behaviour of a prolonged network lifetime.

Keywords WSN · Cluster · Tree-based protocols · Cluster-tree-based protocols

1 Introduction

Sensor Networks are largely ***Distributed Systems*** that work on data generated by surroundings (and captured by sensors). These form a bridge between the virtual world and physical world [1]. Pervasive sensors may be woven into technological

Shalini (✉) · M.N. Hoda
BVICAM, New Delhi, India
e-mail: shalini.jaspal@gmail.com

M.N. Hoda
e-mail: mca@bvicam.ac.in

Umang
ITS, Ghaziabad, UP, India
e-mail: Singh.umang@rediffmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_23

fabric (like buildings and infrastructure) as well as natural environment (dense forests, huge water bodies, etc). Sensor networks have wide range of applications ranging from home automation for comfort and optimal usage of resources for military and defence. These may even be used for monitoring environment and predicting and protecting against natural disasters, thus resulting in unleashing of innumerable probabilities that would otherwise seem improbable and purely hypothetical.

WSNs face multitude of challenges because of their shear nature; some of these are listed as [1, 2]:

- Limited communication range, frequent errors and interference
- Ad hoc deployment
- Dynamic nature
- Unattended operation
- Need for energy conservation
- Robustness
- Scalability

Unlike traditional networks, where the focus is on maximizing channel throughput or minimizing node deployment, the major consideration in a sensor network is to **extend the system lifetime as well as the system robustness and scalability** [3]. Utilization of ***local processing*** **and** ***hierarchical collaboration*** would lead to reduction in the volume of transmitted data (by converting raw sensed data to a high-level representation of the target) and thus reduces the energy consumption and enhances the life of the network.

The data gathering methodology, i.e. the way nodes collaborate in order to collect and communicate data to the base station plays a major role in determining the energy consumption in the network, which in turn is dependent on the network topology [4]. Over the years, WSNs have witnessed evolution in data collection methodology, which range from flat communication to cluster-tree schemes. The first generation offers simplicity of operations whereas the latter offers various advantages like scalability, fault tolerance, addressing node mobility and many more [3].

2 Related Work

Flat Protocols: Flat protocols like flooding, directed diffusion involve direct communication between the sensor nodes and the base station. The process is simple and fault tolerant as failure of SNs does not impact a region, densely populated with sensor nodes. But the concept involves many drawbacks like implosion, overlap and resource blindness [2] thus suffering from a major drawback of high energy consumption. Also, transmitting sensed information over long distances between SN and BS causes rapid energy depletion in sensor nodes, thus leading to early death of the network [3].

Cluster-Based Protocols: Cluster-based protocols overcome the problems of redundant data transmission, long transmission distances, etc., [5] by dividing the sensed region into clusters. Each cluster contains a set of sensor nodes primarily involved in sensing the environmental information. The information gathered by these sensor nodes is collected by a special node termed as the cluster head (CH). The role of the CH is to aggregate the collected information, thus representing the current state of the sensed geographical region, and sending it to the base station. This mechanism limits the high energy demanding task of data communication to the CHs, hence although the energy of the member nodes of the cluster does not deplete quickly, the CHs are penalized for this gain. In order to enhance network longevity, the role of CH is circulated amongst different member nodes [6, 7]. Various factors like residual energy, connectivity with other cluster members, etc., are used to decide whether a member node may play the role of a CH or not. Cluster-based protocols like LEACH, TEEN [8], APTEEN [9], HEED [10], DEEC [11] that evolved over the years exhibit an increase in the network longevity [12, 13] but still do not offer much scalability since the communication between CH and BS is done in single hop. Chain-based protocols like PEGASIS [14] aim at reducing power consumption due to CH selection by eliminating the CH election through a chaining model. Though PEGASIS shows an improvement of 100–300% in terms of network life time, but the problem is high delay in case of long chains [12]. Advances in hardware saw attempts at leveraging capabilities of advanced nodes. SEP [15] harnessed the higher energy levels of advanced nodes for playing the role of CH.

A comparison of cluster-based protocols, TL-LEACH [16], DWECH [17], USC [18], PANEL [11] and HEER [19] is presented by the authors in [20].

Tree-Based Protocols: WSNs based on trees connect the sensor nodes to the BS using multilevel hierarchies. The BS serves as the root of the tree and the nodes farthest in the network act as leaves. The sensed data is transmitted from the leaves through upper levels to the root of the tree [21]. This approach suffers from a major problem of single path between any node and root; hence, any failure in the member nodes leads to partitioning in the network, hence requiring a change in the network structure. Protocols like EDGE and TREEPSI follow this approach.

EDGE—2005: Efficient data gathering is a tree-based protocol [22], which requires each node in the network to be a part of the tree structure, which in turn needs to be reconstructed whenever there is a change in the membership due to node failure or additions. Initial tree construction is based upon *child request (CRQ), child reply (CRP)* and *child acceptance (CAC)* packets. Tree construction is initiated by the base station by broadcasting CRQ. The non-members nodes which receive the CRQ within a predefined time period; send CRP back to the selected parent (the BS in first iteration) and the parent replies back with the CAC packet. The successful receipt of the CAC packet leads to addition of the child node to the tree structure. This process is repeated by the newly added nodes, thus augmenting the tree structure, after each iteration.

EDGE addresses change in tree structure due to node addition by using a parent request (PRQ) packet, which is sent by the added node. Prospective parent nodes reply by sending CRQ and the process of tree construction continues as before.

Node failures of internal nodes lead to orphaned nodes. Such orphaned nodes choose an alternate parent by selecting one of the nodes in a previously maintained parental candidate table (PC) or by sending a PRQ in case the PC has no entries.

TREEPSI—2006: Tree-based efficient protocol for sensor information (TREEPSI) [23]. It works by selecting a root node from all the sensor nodes, and the tree path is built thereafter. Building of the tree path is either done by the sink, centrally, using the location information, or in a distributed fashion on the individual nodes through a common algorithm.

Once the tree is built, data gathering is done in a bottom-up fashion, whence the leaf nodes collect the data and pass it on via the parent nodes to the root. The parent nodes also perform data aggregation in the process.

Cluster-Tree-Based Protocols: Cluster-tree approach links clusters in the network in a tree-like fashion [24]. The job of the CHs, as before, is to gather and aggregate the information sensed by the member nodes of the cluster. The aggregated information is forwarded to the BS, over a data collection tree (DCT). The members of the tree may either be CHs or, as in case of VELCT, special nodes that do not belong to any specific cluster. The advantage of maintaining a cluster tree rather than a node tree is that it leads to better fault tolerance, more scalability and decreased delay in transmission.

CTDGA—2012: Cluster-tree-based data gathering (CTDG) [25] works on certain assumptions like: nodes have ability to transmit, directly, to any other node as well as to the sink. It also requires that all sensor nodes have information regarding their location and are immobile in nature. As per the protocol, the base station has the responsibility to form the primal clusters, which, due to immobility of nodes, do not change during the network lifetime. The BS incrementally splits the entire network into smaller clusters and then goes on to select the cluster head using the stored information regarding the location of the nodes. The nodes located at the centre of the cluster are preferred to play the role of CHs. Once the formation of the primal network topology is over, the responsibility of cluster maintenance and choosing new CHs is shifted to member nodes; the choice is made independently within individual clusters.

Once the clusters are formed, the sink uses Prim's algorithm to form a minimum spanning tree in order to collect information from the entire set of interconnected clusters. The process of information transfer involves transmission of collected data, from child to parent nodes, with aggregation at each level, until the BS receives the final fused data.

CIDT—2014: Cluster independent data collection tree works on formation of data collection trees (DCT) [26] composed of data collection nodes (DCN), which in turn do not belong to a specific cluster. The responsibility of DCNs is to collect data from a cluster head and forward this collected data to the next DCN in the DCT. DCNs do not participate in the data collection process of a cluster and their sole responsibility is to communicate the collected information to the sink, through a tree that is independent of clusters in the network. The protocol ensures that DCNs are re-elected each time CHs are changed.

Table 1 Simulation result-based comparison of cluster and cluster-tree-based protocols [27]

	PDR (%)	Delay (ms)	Total energy consumed (mJ)
LEACH	79	10	250
HEED	84	9.5	230
CIDT	93	6.5	140
VELCT	98	3	80

VLECT—2015: is an enhanced version of CIDT that overcomes issues like node mobility [27], coverage, aims at selecting the cluster heads on various parameters like residual energy, coverage distance and least mobility, thus reducing the frequency of CH election and thereby increasing the cluster longevity.

Simulation on NS [26, 27] with 500 nodes in a region of 1000×1000 m^2 having data packets sized 512 bytes, cluster size $\sim$40 m, sensing range $\sim$20 m, yielded the following results (Table 1).

Thus supporting the claim that CIDT performs better that established cluster-based protocols like LEACH and HEED [28, 29] (Table 2).

Table 2 Features and issues in tree and cluster-tree-based protocols

Protocol	Year of introduction	Features	Issues
EDGE	2005	Tree-based protocol Offers shorter delay and higher PDR as compared to AODV, DD	Failure on any node leads to restructuring of the communication tree
TREEPSI	2006	Provides options for centralized (BS controlled) or decentralized tree building process 30% more energy efficiency as compared to PEGASIS and up to 300% better efficiency as compared to LEACH	Failure on any node leads to restructuring of the communication tree
CTDGA	2012	Cluster tree: more reliable than node tree, since failure of member nodes does not lead to restructuring of entire network	Does not address node mobility
CIDT	2014	Cluster tree. Works by building a data collection tree composed of nodes that do not belong to a specific cluster	Requires re-election of DCN every time CHs are changed due to failure or mobility
VELCT	2015	Enhanced version of CIDT. Aims at increasing cluster longevity by choosing stable links with maximum connection time and RSS	Requires re-election of DCN every time CHs are changed due to failure or mobility

3 Conclusion

It is observed that data collection scheme plays a major role in deciding energy consumption in a WSN. Out of the choices available, i.e. flat, clustered, tree and cluster-tree, the cluster-tree scheme combines the advantages of both cluster and tree schemes, namely reduction in volume of transmitted data (by means of aggregation in clustered networks) and multi-hop transmission (as in case of tree-based networks). At the same time, the need for frequent restructuring due to node failures as in case of tree-based schemes is eliminated. But the effectiveness of cluster tree is based on various factors like cluster dimension, tree intensity and mobility, and there is need for more intensive study related to factors that affect the efficiency of a cluster tree and their impact on the performance of the network as a whole. Also, CIDT and VELCT propose use of alternate DCT (separated from the CHs): the approach needs to be analyzed further, and its limitations/enhancements may be suggested.

References

1. Elson, J., Estrin, D.: Wireless Sensor Networks: A bridge to the Physical World. Center for Embedded Network Sensing. UCLA, Center for Embedded Network Sensing, Jan 2004
2. Heinzelman, W.R., Kulik, J., Balakrishnan, H.: Adaptive protocols for information dissemination in wireless sensor networks. In: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom '99 (1999)
3. Hedetniemi, S.M., Hedetniemi, S.T., Liestman, A.L.: A survey of gossiping and broadcasting in communication networks. Networks **18**, 319–349 (1988). doi: 10.1002/net.3230180406
4. Kulik, J., Heinzelman, W., Balakrishnan, H.: Negotiation-based protocols for disseminating information in wireless sensor networks. Wirel. Netw. (2002)
5. Liu, X.: A survey on clustering routing protocols in wireless sensor networks. Sensors **12**, 11113–11153 (2012). doi:10.3390/s120811113
6. Faheem, M., Ngadi, A.B., Ali, S., Shahid, M.A., Sakar, L.: Energy based efficiency evaluation of cluster based routing protocols for wireless sensor networks (WSNs). Int. J. Software Eng. Appl. **7**(6), 249–264 (2013)
7. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless sensor networks. In: The Proceeding of the Hawaii International Conference System Sciences, Hawaii, Jan 2000
8. Manjeshwar, A., Agrawal, D.P.: TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: Proceedings of IPDPS 2001 Workshops (2001)
9. Manjeshwar, A., Agrawal, D.P.: APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In: Proceedings of the International Parallel and Distributed Processing Symposium (IPDPSí02) (2002)
10. 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)
11. Qing, L., Zhu, Q., Wang, M.: Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. Comput. Commun. **29** (2006) (Elsevier)
12. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. Ad Hoc Netw. **3**, 325–349 (2005). Elsevier

13. Almazaydeh, L., Abdelfattah, E., Al- Bzoor, M., Al-Rahayfeh, A.: Performance evaluation of routing protocols in wireless sensor networks. Int. J. Comput. Sci. Inf. Technol. **2**(2) (2010)
14. Lindsey, S., Raghavendra, C.S.: PEGASIS: power efficient gathering in sensor information systems. In: Proceedings of the IEEE Aerospace Conference, Big Sky, Montana, Mar 2002
15. Smaragdakis, G., Matta, I., Bestavros, A.: SEP: a stable election protocol for clustered heterogeneous wireless sensor networks. In: Second International Workshop on Sensor and Actor Network Protocols and Applications (SANPA 2004)
16. Loscri, V., Morabito, G., Marano, S.: A two-level hierarchy for low-energy adaptive clustering hierarchy. In: Proceedings of the 2nd IEEE Semiannual Vehicular Technology Conference, Dallas, TX, USA, pp. 1809–1813, 25–28 Sept 2005
17. 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), Marina Del Rey, CA, USA, pp. 322–3398, 8–10 June 2005
18. Soro, S., Heinzelman, W.: Prolonging the lifetime of wireless sensor networks via unequal clustering. In: Proceedings of the 5th IEEE International Workshop on Algorithms for Wireless, Mobile, Ad Hoc and Sensor Networks (WMAN), Denver, CO, USA, pp. 236–243, 4–8 Apr 2005
19. Javaid, N., Mohammad, S.N., Latif, K., Qasim, U., Khan, Z.A., Khan, M.A.: HEER: Hybrid Energy Efficient Reactive Protocol for Wireless Sensor Networks (2013). arXiv:1304.0617
20. Jaspal, S.S., Umang, S., Hoda, M.N.: Evolution of routing protocols in wireless sensor networks. In: 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 2190–2193, 11–13 Mar 2015
21. Mamun, Q.: A qualitative comparison of different logical topologies for wireless sensor networks. Sensors **12**, 14887–14913 (2012). doi:10.3390/s121114887
22. Thepvilojanapong, N., Tobe, Y., Sezaki, K.: On the construction of efficient data gathering tree in wireless sensor networks. In: Proceeding of IEEE, ISCAS (2005)
23. Satapathy, S.S., Sarma, N.: TREEPSI: tree based energy efficient protocol for sensor information In: *2006 IFIP International Conference on Wireless and Optical Communications Networks,* p. 4
24. Cuomoa, F., Della Lunaa, S., Cipollonea, E., Todorovab, P., Suihko, T.: Topology formation in IEEE 802.15.4: cluster-tree characterization. In: Sixth Annual IEEE International Conference on Pervasive Computing and Communications (2008)
25. Chhabra, G.S., Sharma, D.: Cluster-tree based data gathering in wireless sensor network. Int. J. Soft Comput. Eng. (IJSCE) **1**(1) (2011). ISSN: 2231-2307
26. Velmani, R., Kaarthick, B.: An energy efficient data gathering in dense mobile wireless sensor networks. ISRN Sens. Netw. **2014**, 10 p. (Article ID 518268, Hindawi Publishing Corporation) (2014). http://dx.doi.org/10.1155/2014/518268
27. Velmani, R., Kaarthick, B.: An efficient cluster-tree based data collection scheme for large mobile wireless sensor networks. IEEE Sens. J. **15**(4) (2015)
28. Buttyan, L., Schaffer, P.: PANEL: position-based aggregator node election in wireless sensor networks. In: Proceedings of the 4th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems Conference (MASS), Pisa, Italy, pp. 1–9, 8–11 Oct 2007
29. Sharma, T., Kumar, B., Tomar, G.S.: Performance comparison of LEACH, SEP and DEEC protocol in wireless sensor network. In: Proceedings of the International Conference on Advances in Computer Science and Electronics Engineering (2012). doi:10.3850/978-981-07-1403-1_198

Performance Analysis of DTN Routing Protocol for Vehicular Sensor Networks

Ram Shringar Raw, Arushi Kadam and Loveleen

Abstract Vehicular sensor network (VSN) has become an active research topic in the field of networking. VSN is the application of vehicular ad hoc networks (VANETs). Vehicular delay-tolerant network (VDTN) has evolved from delay-tolerant network (DTN) and is formed by vehicular nodes with sensors embedded in it. Many routing protocols have been implemented in VDTN, each having its benefits and shortcomings in the implementation domain. In this paper, performance of two routing protocols, namely MaxProp and packet-oriented routing (POR), are analysed and compared on the basis of different parameters. Both the protocols are simulated on MATLAB.

Keywords Vehicular sensor network · Vehicular ad hoc networks · Delay-tolerant network · MaxProp · Packet-oriented routing

1 Introduction

Due to recent advances in inter-vehicular communications and decreasing cost of related equipment, VANETs have received much attention. It has been proved to be useful in road safety, pedestrian safety and many other commercial applications [1–4]. For instance, VANET can be used to make drivers aware of the forthcoming traffic jam. It can also be used to avoid accidents by alerting the driver about the speed and location of the nearby vehicles [5–7].

R.S. Raw (✉) · A. Kadam · Loveleen
Ambedkar Institute of Advanced Communication Technologies & Research, New Delhi, Delhi, India
e-mail: rsrao08@yahoo.in

A. Kadam
e-mail: arushi.kadam91@gmail.com

Loveleen
e-mail: loveleensingh27@yahoo.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_24

VSN is a kind of VANET in which vehicles are equipped with onboard sensors for monitoring the traffic and other services. Vehicles are generally not affected by major energy constraints and can be easily equipped with these sensing devices. VSN provides tremendous opportunity for many large-scale applications, one of which is delay-tolerant vehicular sensor networks (DTVSNs) which enable the transfer of data when the vehicular nodes are connected only intermittently. The main problem in VANET and VSN is the fast mobility of vehicular nodes which reduces the amount of time they are in communication range; this makes routing in DTVSN a challenging task [2, 8–10].

DTN is based on the concept of partially connected networks. It is best depicted as multi-graph, where edges are represented as the time required to transmit the packet with respect to the delay. The main objective of DTN is to maximize the probability of delivery whereas minimizing the delay [4, 11]. There are various strategies in DTN routing proposed. The first DTN routing protocol, Epidemic Routing protocol was proposed by Vahdat and Becker [12]. It follows the concept of flooding scheme routing, which means whenever the node receives a message, it will broadcast it to all its direct neighbours. It maximizes the performance of throughput, but it cannot be used in a large-scale urban resource constraint scenarios. In [13, 14], the authors propose a routing protocol called Probabilistic Routing Protocol using History of Encounters and Transitivity (PROPHET). PROPHET introduces a metric which estimates delivery predictability for every node for each known destination. When the two nodes meet, they compare their delivery predictability for each destination and send packets to the party that has higher probability of reaching the destination. On comparing the average cost per packet the value PROPHET found to be lower than the epidemic.

Work in [15] proposed Resource Allocation Protocol for Intentional DTN (RAPID) routing in which the packets are routed by the method of packet replication on estimating per-packet utilities. In [16], vehicle-assisted data delivery (VADD) model was proposed to reduce the delay vehicles find its next road to forward the packet on the basis of the traffic pattern. It is assumed that each vehicle is embedded with GPS receiver device. In [17], authors gave a DTN routing algorithm called GeOpps. It takes information from the satellite navigation system to route a data packet to a particular geographical location. This model requires cars equipped with GPS receiver. There are many protocols which are mentioned in [18–22]. MaxProp [23] and POR [24] protocols will be discussed in detail in the coming sections.

The organization of this paper is as follows: Sects. 1 and 2 presented the brief introduction of MaxProp and POR protocols, respectively. Section 3 gives the problem formulation about the work. In Sect. 4, simulation results and comparison analysis are discussed. Finally, Sect. 5 concluded the paper.

2 MaxProp Protocol

MaxProp [25] is a forwarding protocol which aims to increase the delivery rate and lower latency of delivered packets. It defines few methods to transmit and delete the packets for efficient buffer management. MaxProp uses acknowledgement sent to all peers to ensure them about packet deliveries. It also stores a list of previous transmission records so as to avoid redundant data to propagate to the same node. The packet is deleted from the buffer when either the acknowledgement of the packet is received or the buffer is full.

The protocol includes list of stored packets of ranked peers on a cost assigned to each destination. The lowest path cost among all possible paths will be considered for the particular destination. Packets with highest priority are transmitted first. Lowest priority packets are the ones which are deleted first to make space for new packets. When two peers discover each other, they exchange packets in an order as depicted in Fig. 1. It sets the priority by checking the hop count. If the hop count is less than a threshold hops, then the buffer is organized by hop count else it is done by the shortest possible distance.

Basically, this protocol addresses two resource limitations, i.e. transfer duration and storage difference between managing these two is that packets that are sent on transfer opportunity may be sent in the next opportunity. But if the packet is dropped from the buffer storage, then it may never be delivered.

2.1 Methods for Dropping the Packets

- When copy of message has been delivered to its destination. In this case, concept of acknowledgement is used.
- When no route with enough bandwidth exist between peers and message destination during the lifetime of message; cost estimation mechanism is used.
- When no copy of message has been transported but some copy of message will be delivered even if peer drops its copy. This is difficult to estimate and implement further. We use hop counts here as the packet that have transmitted further in the network is given the lower priority and is also dropped first.
- When the buffer is full, the packet with lowest priority is deleted first to make space for incoming packets.

Therefore, firstly the acknowledgement is deleted then the packets that have reached the threshold of hop counts with high cost followed by the packets with the hops below threshold.

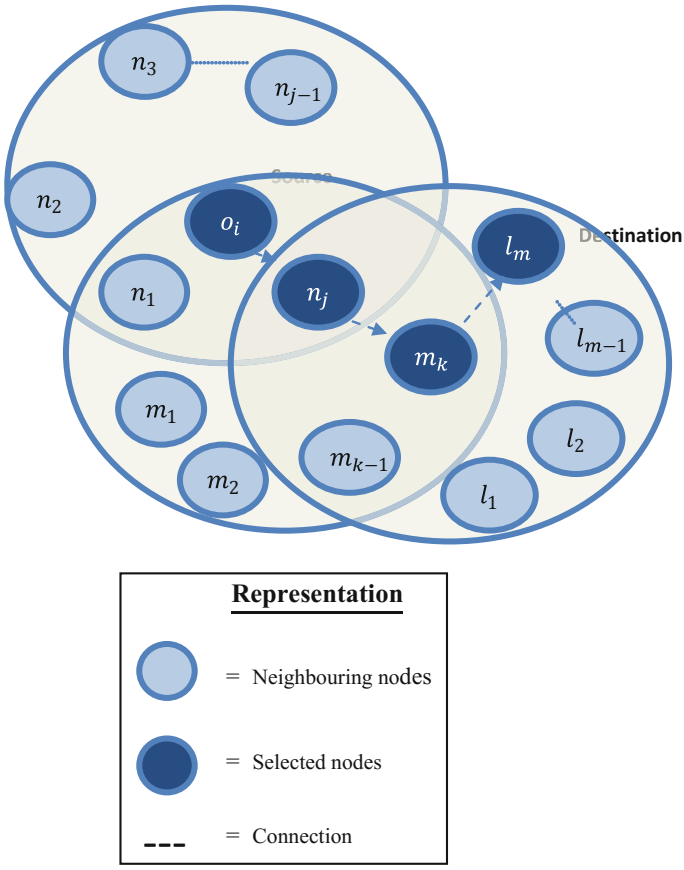


Fig. 1 POR scenario

3 Packet-Oriented Routing (POR) Protocol

This protocol also emphasizes on how to choose the best carrier for transmission of packets. This is done by utility-driven resource allocation problem, RAPID. Neighbour marginal utility (NMU) is calculated for idle neighbours within the communication range, one with the highest utility is selected and the connection is made. The status is changed from idle to busy.

After selecting the neighbour, source node exchanges the metadata which aids in removing the copies of packets which are been delivered and hence improving the overall network performance. Now, the marginal utility (MU) of the packets is calculated. The packets are delivered in the decreasing order of the MU. This process is followed at each node until the packets have reached the destination.

Figure 1 presents the scenario for POR routing protocol, where o_i is the source node which tries to forward the data packet to the destination node l_m. There are then n neighbouring nodes in the communication range of o_i. The packet is forwarded to the relay node n_j because of the highest utility as calculated. Similarly, the packet is transferred to the node m_k, and it forwards the packet further to l_m, the destination node.

4 Simulation Results and Compression Analysis

The main objective of this work is to compare and analyse the performance of the two DTN routing protocols, i.e. MaxProp and POR for VSNs. To analyse the performance of MaxProp and POR, we have taken buffer size as a key metric over adaptive threshold calculation. Comparison and analysis have been accomplished on the basis of their parameters such as throughput, packet delivery ratio (PDR) and end-to-end delay with respect to different scenarios. These parameters can be used to enhance the performance of DTN routing protocols for VSNs. Table 1 presents the parameters that were used for simulation for both packet-oriented routing protocol and MaxProp routing protocol.

4.1 Packet Delivery Ratio

Packet delivery ratio is a key parameter to evaluate the performance of routing protocol in any type of highly dynamic network. The packet delivery ratio can be determined from the total number of data packets received at the destinations divided by the total data packets sent from the sources. Generally, the network performance is better when packet delivery ratio is high. Mathematically, it can be represented as

$$\text{Packet Delivery Ratio} = \frac{\sum(\text{Total packets received by all destination node})}{\sum(\text{Total packets sent by all source node})} \quad (1)$$

Figure 2 shows a graph between packet delivery ratio and variation in number of nodes for both the protocols. As shown in the figure, packet delivery ratio variation

Table 1 Experimental parameters

Parameters	Value
Protocols	MaxProp, POR
Number of nodes	100
Simulator used	MATLAB
Simulation area	100 km^2
Average speed of vehicles	10 m/s

is from 0 to 3 for MaxProp protocol. But for POR protocol, it varies more and the highest packet delivery ratio can be obtained when the nodes are between the ranges of 50–60. It means it gives better performance as compared to MaxProp protocol.

4.2 End-to-End Delay

End-to-end delay is the amount of time taken by a packet to reach its destination through the wireless medium. End-to-end delay also depends on the packet delivery ratio. Probability of packet drop (due to collisions and interference) increases as the distance between the source and destination increases.

The expected end-to-end delay consists of all the possible delays, i.e. buffering route discovery delay, queuing delay, propagation delay and transmission and retransmission delays. Mathematically, it can be represented as in Eq. (2), where D, Tr_{id}, Ts_{id} are represented as end-to-end delay, packet reception and sent time, respectively.

$$D = (Tr_{\mathrm{id}} - Ts_{\mathrm{id}}) \tag{2}$$

As shown in Fig. 3, graphs are plotted for end-to-end delay with variation in communication range and different time loads. In Fig. 3a, an end-to-end delay is least between 50 and 100 of communication range and maximum at 40 m of communication range for POR while it ranges from 0 to 2 for MaxProp. Similarly, in Fig. 3b, an end-to-end delay for POR is lowest between 90 and 100 traffic loads, and it is maximum at 40. While for MaxProp, end-to-end delay ranges from 0 to 2. Therefore, end-to-end delay is more for POR protocol. It means MaxProp gives better performance as compared to POR protocol.

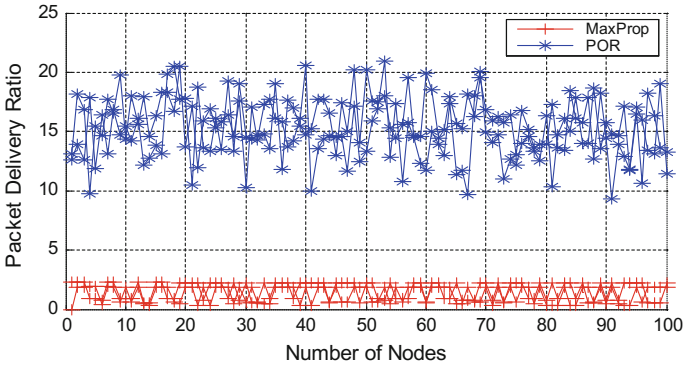


Fig. 2 Packet delivery ratio with different number of nodes

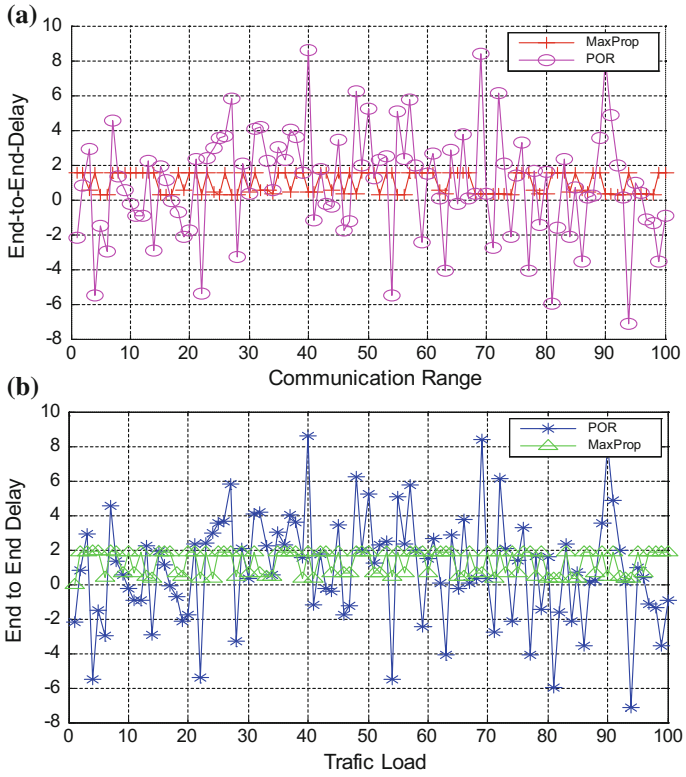


Fig. 3 **a** End-to-end delay with different communication range, **b** end-to-end delay with different time loads

4.3 Throughput

Throughput of the protocol can be described as the received packet size divided by the difference of the stop and start time of the packet between source and destination nodes.

$$\text{Throughput} = \frac{\text{RecvdSize}}{\text{StopTime} - \text{StartTime}} \tag{3}$$

In VSN, packets transfer between vehicles include large multimedia files, such as images of accidents, status of traffic on the road, traffic congestion, traffic signs, traffic efficiency. For getting fruitful results, all the data packets are sent at the beginning of the simulation. We also assumed that every vehicle may find the position of other vehicles at any time using GPS receiver and other centralized location services. Therefore, control overhead for calculating the position and the

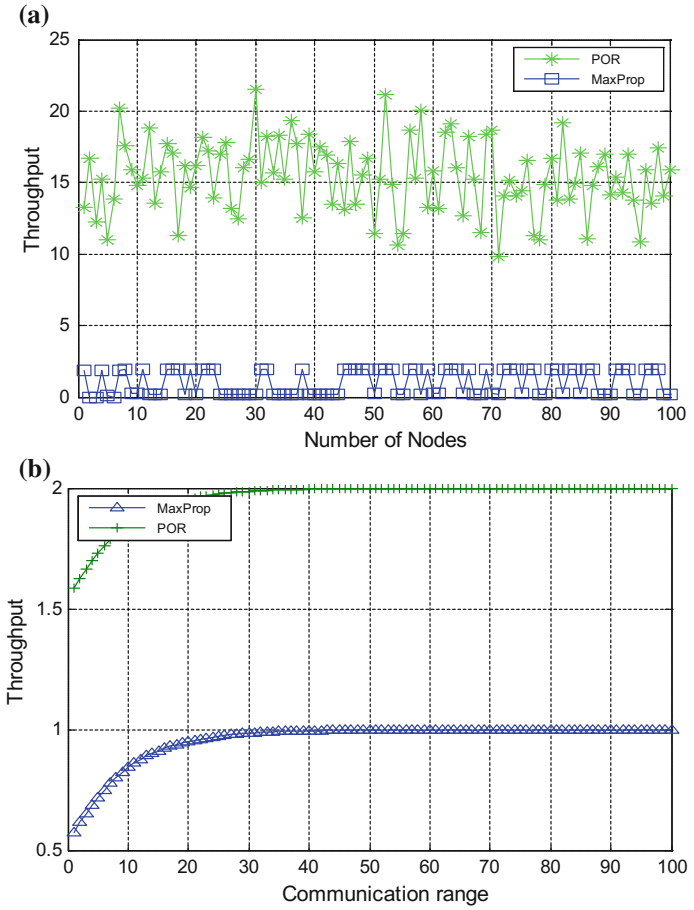


Fig. 4 **a** Throughput with different number of nodes and **b** with different communication range

distance between neighbouring vehicles of corresponding destinations can be ignored.

Performance of the protocols is also estimated by the above two graphs for throughput with different number of nodes and communication range. As shown in Fig. 4, in both the cases, POR gives better performance than MaxProp protocol.

5 Conclusion and Future Work

In this work, we have discussed the two position-based delay-tolerant network routing protocols for VCNs. These DTN routing protocols are MaxProp and POR. As per result analysis sections, POR protocol works according to the local

information of packets gained during neighbour selection method. It can support delay-tolerant applications in VCNs effectively. For the performance analysis, we have taken some key parameters such as packet delivery ratio, end-to-end delay and throughput. By comparison, POR protocol performs much better than MaxProp routing protocol. Further, POR adapts the DTNs and has an improved performance at scalability while predictably increases the networks delay. Therefore, these parameters could be used to maximize the performance of MaxProp routing protocol.

References

1. Fall, K.: A delay-tolerant network architecture for challenged internets. In: Proceedings of ACM SIGCOMM'03, Germany, pp. 27–34, Aug 2003
2. Rao, R.S., Soni, S.K., Singh, N., Kaiwartya, O.: A probabilistic analysis of path duration in VANETS using routing protocol. Int. J. Veh. Technol. (2014) (Hindawi Publication, United Kingdom)
3. Vahdat, A., Becker, D.: Epidemic routing for partially connected ad hoc networks. Technical Report CS-200006, Department of Computer Science, Duke University, Durham, NC (2000)
4. Raw, R.S., Lobiyal, D.K., Das, S.: A probabilistic analysis of border node based MFR routing protocol for vehicular ad-hoc networks. Int. J. Comput. Appl. Technol. Indersci. **51**(2), 87–96 (2015)
5. Lindgren, A., Doria, A., Scheln, O.: Probabilistic routing in intermittently connected networks. In: Proceedings of Workshop on Service Assurance with Partial and Intermittent Resources, Aug 2004
6. Jain, S., Fall, K., Patra, R.: Routing in a delay tolerant network. In: Proceeding of ACM SIGCOMM'04, 30 Aug–3 Sept, Portland, Oregon, USA (2004)
7. Rawand, R.S., Lobiyal, D.K.: E-DIR: a directional routing protocol for VANETs in a city traffic environment. Int. J. Inf. Commun. Technol. **3**(3), 242–257 (2011)
8. Karp, B., Kung, H.T.: GPSR: greedy perimeter stateless routing for wireless networks. In: Proceeding of ACM MobiCom'00, Aug 2000
9. Raw, R.S., Toor, V., Singh, N.: Comprehensive study of estimation of path duration in vehicular ad hoc networks. Adv. Comput. Inf. Technol. Adv. Intell. Syst. Comput. **177**, 309–317 (2013)
10. Zhao, J., Cao, G.: VADD: vehicle-assisted data delivery in vehicular ad hoc networks. IEEE Trans. Veh. Technol. **57**(3) (2008)
11. Leontiadis, I., Mascolo, C.: GeOpps: geographical opportunistic routing for vehicular networks. In: Proceedings of WoWMoM'07, Espoo, Finland, pp. 1–6 (2007)
12. Sede, M., Li, X.: BLER: routing in large-scale buses ad hoc networks. In: Proceedings of IEEE Wireless Communication and Networking Conference (WCNC'08), Las Vegas, NV, pp. 2711–2716, March 2008
13. Wu, H., Fujimoto, R.M., Guensler, R., Hunter, M.: MDDV: a mobility-centric data dissemination algorithm for vehicular networks. In: Proceeding of ACM VANET' 04, Philadelphia, Pennsylvania, USA, pp. 47–56, Oct 2004
14. Burgess, J., Gallagher, B., Jensen. D., Levine, B.: MaxProp: routing for vehicle-based disruption-tolerant networks. In: Proceedings of IEEE INFO COM 2006, Barcelona, Spain, Apr 2006
15. Li, X., Shu, W., Li, M., Huang, H., Wu, M.-Y.: DTN routing in vehicular sensor networks. In: Proceedings of IEEE Global Telecommunication Conference, pp. 1–5 (2008)

16. Burns, B., Brock, O., Levine, B.N.: MV routing and capacity building in disruption tolerant networks. In: Proceeding of IEEE INFOCOM, pp. 398–408, Mar 2005
17. Mahendrran, V., Praveen, T., Siva Ram Murthy, C.: Impact of persistent storage on the DTN routing performance. In: Distributed Computing and Networking, Lecture Notes in Computer Science, vol. 7129, pp. 513–524 (2012)
18. Han, S.D., Chung, Y.W.: An improved PRoPHET routing protocol in delay tolerant network. Sci. World J. (Hindawi) **2015**, 1–7 (2015). (Article ID 623090)
19. Xu, J., Li, J., You, L., Dai, C.: Dynamic groups based adaptive DTN routing algorithms in social networks. Int. J. Distrib. Sens. Netw. (Hindawi) **2014**, 1–13 (2014). (Article ID 623090)
20. Raw, R.S., Lobiyal, D.K., Das, S., Kumar, S.: Analytical evaluation of directional-location aided routing protocol for VANET. Int. J. Wirel. Pers. Commun. **82**(3), 1877–1891 (2015)
21. Paula, M.C.G., Rodrigues, J.J.P.C., Dias, J.A., Isento, J.N., Vinel, A.: Performance evaluation of a real vehicular delay-tolerant network test bed. Int. J. Distrib. Sens. Netw. **2015**, 1–11 (2015)
22. Johari, R., Gupta, N., Aneja, S.: POSOP routing algorithm: a DTN routing scheme for information connectivity of health centres in Hilly state of North India. Int. J. Distrib. Sens. Netw. **2015**, 1–9 (2015)
23. Wang, E., Jia, Y.Y.B., Guo, T.: The DTN routing algorithm based on markov meeting time span prediction model. Int. J. Distrib. Sens. Netw. **2013**, 1–7 (2013)
24. Zhang, L., Yu, C., Jin, H.: Dynamic spray and wait protocol for delay tolerant networks. Proc. Netw. Parallel Comput. Lect. Notes Comput. Sci. **7513**, 69–76 (2012)
25. Balasubramanian, A., Levine, B., Venkataramani, A.: DTN routing as a resource allocation problem. In: Proceeding of ACM SIGCOMM 2007

Analyzing Virtual Traffic Light Using State Machine in Vehicular Ad Hoc Network

Umang and Parul Choudhary

Abstract World is growing in urbanization which has escalated the growth of congestion and accidents on road. Due to increase in traffic, the commute time of people is becoming a huge problem in many cities. Traffic lights aid in smoothening traffic to some extent. To mitigate problem of congestion, safety and commute time of urban workers without leveraging huge expenses on new physical traffic lights a new approach known as virtual traffic lights (VTL) are proposed. Vehicles organize a VTL and help in reducing accidents at intersections. VTL improves the throughput of traffic at an intersection by updating itself to current traffic information and can also reduce carbon emissions and improve energy consumptions in a smart city. We propose a complete VTL algorithm through a finite state machine that will work and explore the horizons on larger environment in high and low mobility scenarios.

Keywords VTL · FSM · ILL · VTLL · DSRC

Nomenclature

VANET	Vehicular ad hoc networks
MANET	Mobile ad hoc networks
ITS	Intelligent transportation system
WAVE	Wireless access in vehicular environment
OBU	On-board unit
RSU	Roadside unit

Umang (✉)
ITS, Ghaziabad, UP, India
e-mail: singh.umang@rediffmail.com

P. Choudhary
BVICAM, New Delhi, Delhi, India
e-mail: paruldevsum@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_25

1 Introduction

World is heading toward urbanization which supports people in their economic growth and progress. This transit causes environmental pollution, resource, and energy consumption in urban cities. Since more than 50% of the world population lives in transportation convenient cities, the numbers of vehicles on the roads has increased than the capacity of the road network in these cities. As it incorporates huge investment in increasing road capacity, thus, it results in the acceleration of traffic safety and congestion in major capitals of the world. Many new scalable and cost-effective solutions are proposed to this daunting problem. Due to heavy traffic, the increase in commute time of people is becoming a huge problem in many cities. According to statics given by WHO more than 1 million human resources die out of road accidents. Traffic lights aid in smoothening traffic and accidents to some extent. But all intersections and road junctions are not provided with traffic light. A close study reveals that only a small percentage of road junctions are equipped with proper traffic lights and that too most of them are deployed where traffic density is high. The total number of traffic lights deployed actually is few as compared to the total number of intersections. More than 50% intersection accidents occur in road junctions without traffic light. Moreover, it incorporates a huge expenditure in installation and electric bill of traffic light at every intersection or road junction. Through VANETs Government and Enterprises are encouraged to integrate ICT into vehicle. To mitigate problem of congestion and commute time of urban workers without leveraging huge expenses on new physical traffic lights, a new approach known as virtual traffic lights (VTL) is proposed. Vehicles organize a VTL via VANETs and help in reducing accidents at intersections. In VANETs, vehicles operate at 5.9 GHz using technology of Dedicated Short Range Communications (DSRC). VTL improves the throughput of traffic at an intersection by updating itself to current traffic information and can also reduce carbon emissions and improve energy consumptions in a smart city. In VTL, scheme vehicles organize a leader at every road junction that takes care of controlling traffic at that junction for sometime. This responsibility is then handed over to another cluster leader in the orthogonal direction after sometime. This right-of-way decided by the elected leader is broadcast to all the vehicles in the same direction as well as the orthogonal direction. The man–machine interface used to inform each driver about the "right-of-way" is envisioned to be a display unit which can be on the windshield of every vehicle. This can make it convenient for each driver whether he should proceed or stop at that intersection. This paper is organized as follows. Section 2 focuses on VTL protocol. Section 3 covers an overview of the related work done on VTL and its simulations. Section 4 analyses the work done on VTL and describes it through a finite state machine. Conclusion and future scope are given in Sect. 5.

2 Virtual Traffic Light Protocol

The promising approach of virtual traffic lights (VTL) reduces congestion and cuts off the commute time of urban workers. This is implemented in the presence of vehicles running on vehicular ad hoc network (VANET).

Principle of Operation

In this protocol, conflicts are detected at road junctions and are sorted in an ad hoc manner using V2V communications. By using DSRC, each vehicle broadcasts its speed and position to check the presence of a conflict at the intersection. In case a conflict is determined, following protocol is executed by vehicles which are involved in the conflict:

1. **Leader Election Process**

At a road junction, when conflict has to be resolved vehicles in a same lane elect an individual lane leader (ILL). The vehicle close to intersection in individual lane is selected as ILL. All the individual lane leaders at the scenario must elect among themselves one which does the work of the virtual traffic light leader (VTLL) at the junction. VTLL announces its leadership to all individual lane leaders. This unanimously elected leader configures or installs temporary traffic light infrastructure. Leader or elected vehicle creates and broadcasts traffic light information. Other vehicles follow the traffic light infrastructure and follow the information of the traffic light which has been broadcast by the virtual traffic light leader. The elected vehicle stops itself by giving red light signal and coordinates with others in leading it.

2. **Generation of Traffic Light Information**

After being selected as a virtual traffic light leader, it decides the time duration of green light signal or right to move for each approaching direction. The timing of green light and red light could be static or dynamic depending upon different information received by the VTLL through VANET. The traffic behavior depends upon various parameters such as the volume of traffic at different time of the day in each direction, level of congestion at the junction, priority of different vehicles, number of vehicles waiting in each road, etc. Leader constantly detects the volume of traffic carried by road having green light, and when no additional vehicles are detected to move through the junction the green light is stopped and is placed to another connecting road [1].

3. **Leader Handover**

When the leader's lane shows green light, the leader will have the right to move and leave the junction. To maintain the flow of traffic light infrastructure, a new leader is elected by any of the following two processes

(i) The leader handover is done by current VTLL to any vehicle which is stopped due to red signal at the junction.
(ii) The leader handover is done when no vehicle is stopped due to red signal.

3 Literature Review

According to [2] in their paper [2] proposed concept of adaptive traffic light that changes the cycle of traffic lights dynamically depending on current traffic. Fixed traffic light decreases the throughput of traffic at intersections. Adaptive traffic light approaches improve traffic by dynamically changing the duration of traffic lights depending on current traffic. To maintain all physical traffic lights in a city is super expensive, and therefore virtual traffic light (VTL) VTL approaches may be a feasible solution to facilitate energy efficiency in a smart city. The proposed approach adapts the cycle of VTL according to current traffic, and results show that the proposed AVTL approach effectively improves the throughput of road junctions as compared to physical traffic light approach. The result of the adaptive approach improves average speed by 10.1% when compared with fixed cycle traffic lights.

Michel Ferreira and all in their paper [3] proposed a traffic light control system which is self-organizing, and work of the existing physical traffic lights is taken by vehicles themselves. They optimize the problem of congestion without using any roadside infrastructure by applying virtual traffic light protocol at road intersections. Through this protocol, they propose to replace physical traffic lights by in-vehicle signs which are possible with vehicle to vehicle V2V enabled vehicles. The protocol proposes to select a leader temporarily that broadcasts traffic light messages that are shown to drivers through in-vehicle displays. The vehicles elected and involved in this system themselves act as a traffic light and broadcasts the traffic signal messages to rest of the vehicles approaching toward the junction. Through simulation is done on large scale for Porto, they provide vital evidence to show that their system is not only scalable but it proves to be cost-effective to urban traffic control.

Nidhi and D.K. Lobiyal in their paper [4] propose to obtain results by simulating real-world scenario through VANET. Since the deployment cost is huge and implementation is a complex task, they believe research in VANET relies on simulation. In their work, they use tools such as Google Earth and GIS to generate a real-world map of their own university JNU. They analyzed and made traffic-related data from a limited area to capture the realistic vehicular mobility model. To accomplish their work they divided the entire region into various smaller routes. This model dynamically picks the driver's route and then analyzes its choice by simulating it with traffic lights on NS2 using AODV routing protocol and IEEE 802.11 standard. The impact of the virtual traffic light is estimated by taking various parameters such as rate at which packet is delivered, number of packets lost on way and chances of router failure. The proposed network regulates the flow of traffic in a

round robin fashion but for data transmission, it has become an obstacle since the packet forwarding nodes at the intersection drop the packets, due to the high number of transmission at the same time.

Ricardo Jorge Fernandes in his work [5] introduces an approach to enable in-vehicle traffic signs. The protocol creates virtual traffic light without a centralized control infrastructure. It is spontaneous in creating new traffic rules according to changing traffic situations. The use of VTL is described by using simulator DIVERT. Comparison between VTL and infrastructured-based pre-timed traffic lights is done, and VTL tends to show better results.

Suhail M. Odeh in his paper [6] estimates and calculates the possibility of congestion at four cross sections and also two highways. In this system, data is assembled at one place through imaging and transferred to the current system using genetic algorithm. Proposed system not only calculated the approximate time for green light but also keeps the count of traffic flow.

Florian Hagenauer, Patrick Baldemaier, Falko Dressler, and Christoph Sommer in their work [7] developed a few algorithms which worked on process of leader selection and calculate the timings of traffic lights. They are implementing the algorithm on a realistic platform giving service to support any abstract intersection in synthetic scenarios. They have given successful results in low to medium traffic load.

Samir A. Elsagheer Mohamed in his paper [8] has developed a system whose purpose is to save energy and increases the lifetime of traffic lights by decreasing its usage. This system turns down the lights automatically for the lanes which have zeroed the traffic and put up the lights for those lanes where the traffic is supposed to resume back. The system enlightens only that portion of road where there is any traffic or expectation of any vehicle movement [9] and thus working of maintenance of the lighting equipment for future.

4 State Machine of VTL

The virtual traffic light protocol gives an insight in which on the basis of leader election process the traffic light information is generated to other vehicles [10]. The VTL protocol is investigated in more depth by us, and we present a complete state machine of the entire VTL protocol concept [11, 12].

Overview of the state machine used to implement the VTL protocol is depicted in Fig. 1. A finite state machine $f(Q, \Sigma, \partial, q, F)$ comprises of five tuples. Q represents finite states [13]. The VTL state machine comprises of four states which are described as follows:

Idle

A state when there is no conflict or traffic is smooth or no approaching jam situation.

Individual Lane Leader

A state where vehicle is close to intersection as compared to other vehicles in the same lane and elected as a leader of individual lane.

Virtual Traffic Light Leader

A state where vehicle is closest to the intersection or road junction and is unanimously elected among all individual lane leaders.

Passive Vehicle

A vehicle not closes from the intersection and follows the VTL leader.

A finite state machine remains in any one state at one time, so VTL state machine can be in one of the four states. Σ represents the input mentioned upon the arrows in Fig. 1. ∂ represents the transition set of machine from one state to another. At any junction or cross-point, the vehicle first tries to determine the possibility of conflict between his vehicle and the approaching vehicles. It uses its location and also calculated the distance between own vehicle and approaching vehicles based on their locations. Now if in case, there is no conflict the machine remains in the same state of idle. In case of conflict, vehicle then calculates the distance between own vehicle and other vehicles to determine the closeness of vehicle with junction. If the vehicle calculates the smallest distance to the junction, then it declares himself as individual lane leader by election else, vehicle remains in passive motion and just obeys the traffic lights send by the leader. In case among the individual lane leaders, the one who is closest to crossover becomes a VTL leader or a vehicle it receives a handover from the current VTL leader becomes the new VTL leader. Vehicle on the road just obeys the traffic signals as initiated by VTL leader. Also, all these vehicles when passing the junction again come in idle state.

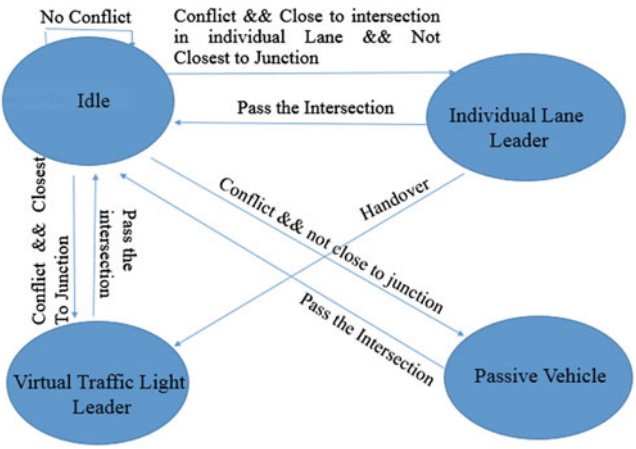


Fig. 1 Finite state machine implementing working model to VTL protocol

Q represents the initial state and F set of final states. In this state machine, Idle is the initial state and also final state.

5 Conclusion and Future Scope

The motivation of this paper comes from the main idea that the vehicle signs can be achieved through the collaboration of the local vehicles, creating virtual signs in a synchronized manner. Therefore, our main expected contributions of this work are to identify feasibility of VTL algorithm through a state machine. Investigation of the behavior of VTL protocols for traffic-congested environment will be the significant contribution of this work. Based on the outcome of investigation, design of efficient protocol for VTL protocol will be another vital contribution of this work.

References

1. Raya, M., Hubaux, J.: The security of vehicular ad hoc networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 1–11. Alexandria (2005)
2. Chou, L.-D., Tseng, J.-H., Yang, J.-Y.: Adaptive Virtual Traffic Light Based on Vanets for Mitigating Congestion in Smart City. ISBN: 978-0-9891305-0-9 2013 SDIWC
3. Ferreira, M., Fernandes, R., Conceição, H., Viriyasitavat, W., Tonguz, O.K.: Self-organized traffic control. In: 7th ACM International Workshop on Vehicular Internetworking (VANET 2010). Chicago, IL: ACM, Sept 2010, pp. 85–90 (2010)
4. Nidhi, Lobiyal, D.K.: Performance evaluation of realistic VANET using traffic light scenario. Int. J. Wirel. Mob. Netw. (IJWMN) **4**(1) (2012)
5. Fernandes, R.J.: VANET enabled in vehicle traffic signs (2009)
6. Odeh, S.M.: Management of an intelligent traffic light system by using genetic algorithm. J. Image Gr. **1**(2) (2013)
7. Hagenauer, F., Baldemaier, P., Dressler, F., Sommer, C.: Advanced leader election for virtual traffic lights. http://wwwen.zte.com.cn/endata/magazine/ztecommunications/2014/1/
8. Mohamed, S.A.E.: Smart street lighting control and monitoring system for electrical power saving by using VANET. Int. J. Commun. Netw. Syst. Sci. 351–360 (2013)
9. Singh, U., Reddy, B.V.R., Hoda, M.N.: GNDA: detecting good neighbor nodes in adhoc routing protocol. In: IEEE Second International Conference on Emerging Applications of Information Technology, pp. 235–238 (2011). doi:10.1109/EAIT.2011.62
10. Zeadally, S., Hunt, R., Chen, Y.-S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETS): status, results, and challenges. Springer Science Business Media, LLC (2010)
11. ETSI TR 102 638: Intelligent transport system (ITS); vehicular communications; basic set of applications; definition. ETSI TR 102 638 V1.1.1, pp. 1–81 (2009)
12. El Zarki, M., Mehrotra, S., Tsudik, G., Venkatasubramanian, N.: Security issues in a future vehicular network. In: Proceedings of European Wireless (2002)
13. Festag, A., Noecker, G., Strassberger, M., Lübke, A., Bochow, B., Torrent-Moreno, M., Schnaufer, S., Eigner, R., Catrinescu, C., Kunisch, J.: NoW—network on wheels: project objectives, technology and achievements. In: Proceedings of 6th International Workshop on Intelligent Transportation (WIT 2008), Hamburg, Germany, Mar 2008

Design and Analysis of QoS for Different Routing Protocol in Mobile Ad Hoc Networks

A. Ayyasamy and M. Archana

Abstract A mobile Ad Hoc Network (MANET) is an own and self structuring network of mobile devices, which are connected by wireless and Quality of Service (QoS) routing is a major challenge for research. In this paper, design and analysis of three major versions of QoS with support for effective routing schemes are being proposed. First scheme is improved-LABS, second scheme is context-aware adaptive QoS routing for mobile and wireless network using Fuzzy (COAAF) approach, and finally, context-aware adaptive service (COAAS)-based dynamic channel allocation approach for providing an optimal QoS over MANET, respectively. The proposed schemes are compared with other existing schemes like AODV, DSR, and FSR routing schemes.

Keywords Mobile ad hoc networks · QoS · COAAF · COAAS · I-LABS

1 Introduction

Mobile ad hoc networks (MANETs) [1] are self-organizing networks which operate without any infrastructure using 802.11-based wireless local area network (WLAN) technology. MANET has increased the attention [2] of node mobile services and different industry groups. The primary aim of quality of service (QoS) [3]-based research work focuses on multiple schemes or the approaches of providing adaptive QoS for topology dynamic high mobility [4, 5] MANET. Three approaches are discussed, based on an initial study, which stresses the need for QoS for MANET. In this paper, QoS-related services over MANET are proposed, some of the MANET protocols such as AODV [6], DSR [7] cannot be used due to their

A. Ayyasamy (✉) · M. Archana
Department of CSE, Faculty of Engineering and Technology, Annamalai University, Chidambaram, Tamil Nadu, India
e-mail: samy7771@yahoo.co.in

M. Archana
e-mail: archana.aucse@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_26

restricted mobility issues and the missing factor of dynamic update in node topology.

The proposed routing protocols are implemented as the ITU/IEEE condition and IEEE 802.11p MAC standards. This research proposes QoS-aware adaptive routing algorithm using fuzzy QoS metrics COAAF and middleware for delivering end-to-end QoS using dynamic channels COAAS. The three schemes primarily focus on session management using the selection and utilizing the update on transmission.

The rest of the paper is organized as follows: Sect. 2 elaborates about the literature survey on QoS-aware routing protocols and related issues. Section 3 discusses proposed QoS for three routing protocols, namely I-LABS, COAAF, and COAAS. The performance and test results are discussed in Sect. 4. Finally, Sect. 5 concludes the paper and also discusses the future direction.

2 Literature Survey

Three types of routing protocols are adapted in favor of ad hoc networks such as reactive [2], proactive [8], and hybrid [9]. These protocols have different criteria for designing and classifying routing protocols for wireless ad hoc network. Its use in the context of MANETs along with reactive and proactive is for all time an area under analysis. Routing protocols are difficult due to the fast moving nodes as their presentation degrades with speed. Such types of networks are complicated to manage as fast handoff deteriorates signal quality, maximizes interference and other reduction factors.

Chun and Baker [10] have discussed scheduling algorithm for packets sending and receiving by DSR and AODV protocols. Based on the routing protocol, the priority of packet control varies. In order to set the priority of data packets, the end-to-end packet delay is decreased [11].

The challenges focused on this research work include a consistent update on high speed, mobility, directional change, location update, lane/road change as well constraints on context update, where nodes do differ in size and space [12]. Even though high-quality research is being done on mobile ad hoc networking and related areas in highly developed countries, the concept of MANET is still in its immaturity in most of the efficiently slow developing countries, where mobile node services do not adopt any standards.

3 Proposed Routing Protocol Scheme

3.1 Improved-LABS

Time critical media services, defense applications, node position tracking, bandwidth hungry services between 'high mobile' nodes demand consistent QoS to be maintained over MANET. In this work, the QoS metrics and their performance over MANET using IEEE 802.11a/b/g/n standards are discussed. Radio propagation intensity of interconnecting links, end-to-end delay, and packet loss are QoS metrics adopted. The load or traffic intensity identified between source and receiver uses dynamic channel assignment to transmit the data over constrained intervals of time in order to achieve QoS. This scheme does not adapt well to a relatively large set of nodes in the domain. The standard ad hoc routing protocols such as AODV and DSR, uses QoS utilization in response to bandwidth demand over a variable type of services are analyzed.

A multi-route identifies several routing paths for effective data transmission over high-speed access by I-LABS. It works on the basis of traffic intensity as each router provides an optimal solution to handle large number of nodes in a domain and also yields high traffic intensity.

3.2 Context-Aware Adaptive Fuzzy (COAAF)

COAAF works on route identification, route binding, update, and deletion process based on the validation of adaptive QoS metrics, before the most favorable route selection process between the source and destination. The COAAF protocols also support applications which are not necessarily delay tolerant. COAAF routing protocols work on maintenance of an end-to-end path for streaming media data to make its goal. COAAF is modeled as a set of high-speed mobile nodes on varying lanes, where any mobile node can establish connectivity with other nodes traveling in the same direction or opposite direction of its motion.

COAAF transmits a QoS route request to discover an optimal route based upon a QoS parameter. COAAF includes each intermediate node determining whether the node can maintain the requested QoS parameter and, hence, update the QoS link metric with a fuzzy metric and forward the QoS route request, with temporarily reserving the required node resources. The objective node, upon getting the source QoS route request, generates a route reply including the flow identifier, updated QoS fuzzy metric, and QoS link metric for all discovered routes. The source node generates fuzzy QoS metrics based on the updated QoS link metrics along with the replies. The source node selects the optimal route to the destination node based on the fuzzy QoS route metrics and transmits route confirmations to intermediate nodes on the selected route.

3.3 Context-Aware Adaptive Service (COAAS)

Large variations of QoS latency, bandwidth, and jitter may occur in MANETs during media transfer. Applications need to adapt their functionality according to dynamic change of their QoS update. An enhanced service-based platform provides adaptive network services to higher level application layer components. COAAS is structured in such a way that it can provide QoS awareness to streaming applications as well as manage dynamic ad hoc network resources.

The COAAS architecture defines dynamic channel allocation [13, 14] for service, network, and the expected user's QoS by using well-defined policy sets. Services in use are defined at run time through objects space, which binds to event functionality for exhibiting their adaptive behavior along with network OS and related kernel components. The networking components and underlying infrastructure support heterogeneous OS, network, and sub-network domain setup are shown in Fig. 1.

COAAS middleware infrastructure defines a five-layered stack architecture, which functions on object monitoring, control, and query of device status with extended services toward session establishment. Network devices include various network components such as network adapter card, modem, access point, routers, and gateway.

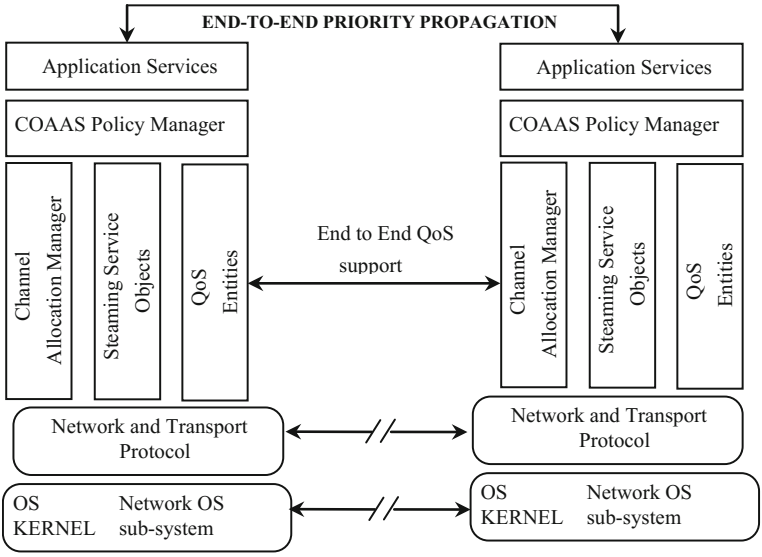


Fig. 1 COAAS: end-to-end QoS (runtime environment)

4 Results and Performance Analysis

In MANET, the test beds are generated using NS-2 [15] in order to measure the efficiency of protocols. Experiments were carried over 25 mobile nodes placed within a 1000 × 1000 m area randomly over a network.

The performance of first scheme (I-LABS) is compared with AODV and FSR as shown in Fig. 2. The QoS metric is maintained by I-LABS which are very low value compared with other existing QoS schemes. In this figure, when number of nodes increases, end-to-end Delay (EED) also increases in AOVD and FSR. But I-LABS approach performance is very less EED in terms of milliseconds.

Second scheme COAAF is analyzed in terms of round trip time (RTT). The RTT is called the time required for a single pulse or packet to take a trip from specific source to destination and back again. Figure 3 shows that the COAAF observed less RTT compared to FSR and AODV.

Third scheme COAAS performs better in terms of percentage of packet loss. Figure 4 shows that the COAAS scheme observed less packet loss compared to DSR and AODV.

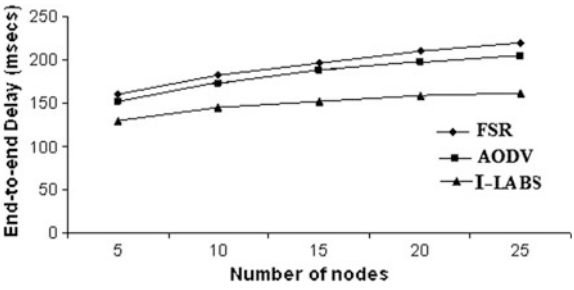


Fig. 2 Average end-to-end delay of I-LABS

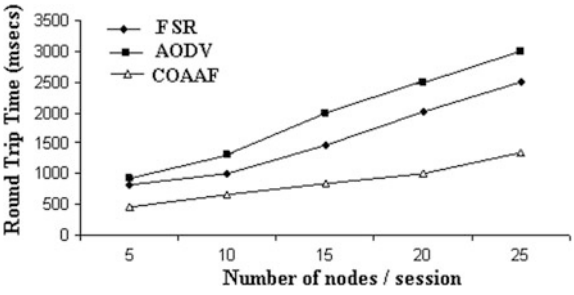


Fig. 3 Round trip time of COAAF

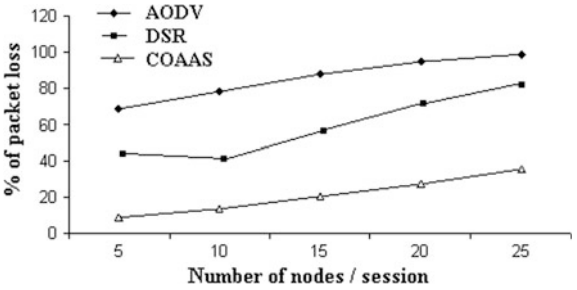


Fig. 4 Percentage of packet loss of COAAS

5 Conclusion

The main aim is to maintain a route that improves the quality for communication and data transmission. The three stable QoS schemes are used to select a route where all likely move at similar speed and toward similar directions are designed. The experiment results show that COAAF, COAAS, and I-LABS provide the best and adaptive routes for long time, when compared to AODV, FSR, and DSR. QoS invariable depends on issues such as node mobility, multi-session establishment, and service in use, which depend on node traffic prediction and service behavior at any node, which can be considered in future research.

References

1. Chlamtac, I., Conti, M., Liu, J.J.N.: Mobile ad hoc networking: imperatives and challenges. Ad Hoc Netw. **1**, 13–64 (2003)
2. Zheng, J., Simplot-Ryl, D., Mao, S., Zhang, B.: Advances in ad hoc networks. Ad Hoc Netw. **10**, 61–66 (2012)
3. Perkins, C., Royer, E.M.: Quality of service for ad hoc on-demand distance vector routing. http://people.nokia.net/charliep/txt/aodvid/qos.txt, Oct 2004
4. Ayyasamy, A., Venkatachalapathy, K.: Context aware adaptive fuzzy based QoS routing scheme for streaming services over MANETs. Wirel. Netw. **21**(2), 421–430 (2015)
5. Han, Q., Bai, Y., Gong, L., Wu, W.: Link availability prediction-based reliable routing for mobile ad hoc networks. IET Commun. **5**(16), 1291–1300 (2012)
6. Perkins, C., Belding-Royer, E., Das, S.: Ad hoc on-demand distance vector (AODV) Routing. RFC 3561 Network Working Group (2003)
7. Youssef, M., Ibrahim, M., Chen, L., Vasilakos, A.V.: Routing metrics of cognitive radio networks: a survey. IEEE Commun. Surv. Tutor. **16**(1), 92–109 (2014)
8. Alam, M., Prasad, R., Farserotu, J.R.: Quality of service among IP-based heterogeneous networks. IEEE Pers. Commun. **8**(6), 18–24 (2001)
9. Elizabeth, M., Belding-Royer.: Routing approaches in mobile ad hoc networks. In: Basagni, S. (ed.) Mobile Ad Hoc Networking, pp. 275–301. Wiley-IEEE Press (2004)
10. Chun, B.-G., Baker, M.: Evaluation of packet scheduling algorithms in mobile ad hoc networks. Mob. Comput. Commun. Rev. **6**(3), 36–49 (2002)

11. Ayyasamy, A., Venkatachalapathy, K.: An improved load balancing adaptive QoS buffer scheduler (I-LABS) for streaming services over MANET. Int. J. Comput. Sci. Eng. Technol. (IJCSET) **5**(05), 612–620 (2014)
12. Zeng, Y., Xiang, K., Li, D., Vasilakos, A.V.: Directional routing and scheduling for green vehicular delay tolerant networks. Wirel. Netw. **19**, 161–173 (2013)
13. Ayyasamy, A., Venkatachalapathy, K.: Context aware adaptive service based dynamic channel allocation approach for providing an optimal QoS over MANET. Int. J. Eng. Technol. (IJET) **6**(3), 1465–1479 (2014)
14. Abdul, Q.A., Premchand, S., Koyel, D.G.: Token based distributed dynamic channel allocation in wireless communication network. CSI Trans. ICT **2**, 109–116 (2014)
15. Information Sciences Institute: ns-2 network simulator Software Package. http://www.isi.edu/nsnam/ns/ (2003)

An Agent-Based Solution to Energy Sink-Hole Problem in Flat Wireless Sensor Networks

Mamta Yadav, Preeti Sethi, Dimple Juneja and Naresh Chauhan

Abstract Repeated and continuous transmission of data to the sink leads to energy loss in all the nodes in case of flat WSN. Especially, depletion of energy is highly acute in case of nodes that are near to the sink. Conventionally known as energy sink-hole problem, it causes early failure of the network even when there is a substantial amount of residual energy left in it. Though the research fraternity has been continuously addressing this problem and even has provided various solutions to deal with it, the use of mobile agents to meet the above-stated problem is still in its infancy. The paper proposes a mobile agent-based solution for solving energy sink-hole problem. The proposed solution aims to extend the network life by reducing redundant data being passed to the nodes near to the sink thereby reducing the load and saving battery life. The algorithm is implemented using aglets and the analytical results show significant improvement in the network lifetime.

Keywords Wireless sensor network · Energy sink-hole problem · Mobile agents Aglets

M. Yadav · P. Sethi (✉) · N. Chauhan
YMCA University of Science & Technology, Faridabad, India
e-mail: preetisethi22@gmail.com

M. Yadav
e-mail: mamtayadav5870@gmail.com

N. Chauhan
e-mail: nareshchauhan19@gmail.com

D. Juneja
Dronacharya Institute of Management & Technology, Kurukshetra, India
e-mail: dimplejunejagupta@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_27

1 Introduction

In the last two decades, advances in the micro-electromechanical systems (MEMSs) [1, 2] technology have amplified research in wireless sensor networks (WSNs). As defined by the research community, "A wireless sensor network is composed of tiny sensor nodes each capable of sensing some phenomenon, doing some limited data processing and communicating with each other [1, 3]." This wireless network of sensors is used in a myriad of applications like intrusion detection, object tracking, habitat, and other environmental monitoring, disaster recovery, traffic control, hazard and structural monitoring, and inventory management in factory environment to name a few. Despite the huge applicability of WSN, the network is however constrained by many operational and design challenges like low processing power, limited battery life, and short radio ranges of the sensing units. These challenges are thus key research areas, and so far many solutions for the same have also been proposed to meet them.

Among the above-listed challenges, one of the major issues is to look for ways and means to increase the lifetime of the network which is of prime importance in case of non-deterministic environments [3–5]. The current work thus deals with energy sink-hole problem which depletes the lifetime of the network. As the name suggests, energy sink-hole problem is the name given to the process of acute energy loss in the nodes of the network. The literature review [6–9] reveals that this energy depletion is found in nodes which are nearer to the sink as they are engaged in repeated and continuous transmission of data to the sink in addition to sensing. When the section nearer to the sink dies due to lack of energy, the network also fails since no data can be passed to sink anymore. The energy sink-hole problem thus causes early failure of the network even when there is a substantial amount of residual energy left in it.

2 Related Work

The problem of relaying the data to the sink which leads to energy loss of the intermediate nodes has been exhaustively explored, and various solutions have been proposed to meet it. Lian et al. [6] relate the data capacity of sensor nodes with their deployment pattern. The work emphasizes the fact that energy sink-hole problem in static model-based sensor networks serves as one of the major causes for this ineffective utility of energy and less lifetime of the network.

Lu et al. [9] have given an algorithm which enhances the network lifetime by reducing the data being forwarded around the sink node. The energy consumption required for isometric transmission is analyzed, and the tactics of small world are adopted to reduce the problem of energy hole.

Wu et al. [7] proposed a technique to avoid energy hole with non-uniform node distribution. It was concluded by the team that although unbalanced depletion of

energy found in WSN seems unavoidable as the network is based on multi-hop communication model and performs constant data reporting, but it is possible if nodes in the network are distributed in a manner such as number of nodes increases in geometric progression from the outer coronas to the inner ones except the outmost one. The solutions based on uneven distribution of nodes in a desired manner to solve energy hole can significantly improve the network life cycle, but the strategy is difficult to achieve in practice as in most cases the distribution of node density is difficult to control.

Song and Liu [8] suggested that searching optimal transmission range for the sensors in each corona and using it for transmission is the solution for energy hole problem and better lifetime of the network.

Luo along with his team [10] proposed a solution for enhancing the lifetime of the network by making use of mobile sink for collecting data. As the sink is mobile, the problem of energy hole is automatically corrected. However, in many applications, mobile sink is not found suitable.

The literature review [6–9, 11] done till the time of listing reveals that though the research community has put in a substantial efforts to solve the above-stated problem, it has been almost silent on the use of mobile agents for the same.

As the name suggests, mobile agents [4, 11–13] are a special class of software agents which are capable of carrying processing codes among the motes thereby allowing the computation and communication resources at the sensor nodes to be efficiently harnessed in an application-specific fashion. Owing to their inbuilt features, mobile agents adjust their behaviors depending on the quality of service needs (for example, data delivery, latency) and the network characteristics to increase network lifetime while still meeting those quality of service needs [3, 14].

The current work aims to exploit the power of mobile agents for dealing with the energy hole problem. The next section provides the detailed description of the approach adopted for increasing the lifetime of the flat static WSN.

3 Proposed Work

The work proposes an agent-based approach which becomes functional when the sink is notified by any node in its radio range that it has consumed one third of the total energy (i.e., 33.3%) and only two third is left in the node. Figure 1 shows an example of topology of sensor networks. In the given figure, sink is taken as level 0 node. The nodes in direct radio range of the sink (shown in white color) are termed as level 1 nodes, and those nodes that are in radio range of level 1 nodes except the sink are termed as level 2 nodes.

The subsection below describes the working algorithm for the proposed approach.

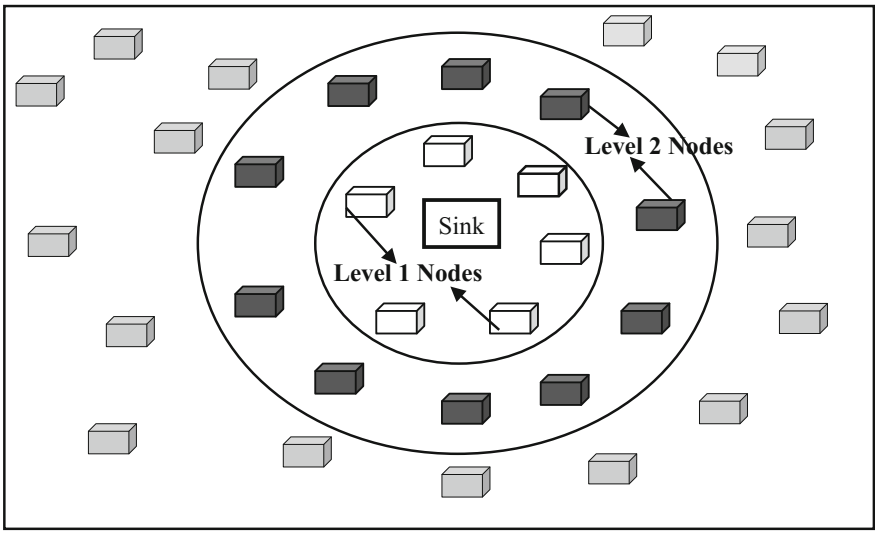


Fig. 1 Topology of sensor nodes

3.1 Working Algorithm

After the formation of itineraries, the data from the level 2 nodes go to the level 1 nodes in an efficient manner than before. As each level 1 node restricts itself to collect data only from pre-identified designated nodes, the amount of data forwarded is much less now. It can also be ensured that no data are lost as data from each level 2 node are accepted by one of the level one nodes; hence, all the data from level 2 region is passed to level 1 region. If the data received at level 1 region is compared to the data received at this level before applying the algorithm, it can be seen that overall redundancy is reduced in this region. Hence, the algorithm helps in reducing the network load near to the sink, thereby balancing the energy levels and reducing energy sink-hole problem. Itineraries only cover the part of network necessary to deal with the sink-hole problem. They are short and easy to build. Further, elongation of itineraries can also be done, but after level 2, it will not be for all the routes concurrently, only those nodes in the outer level whose energy level will get below a predefined threshold defined for that level, will dispatch the software agent in the radio range, and hence another node will be a part of itinerary, and the node with less energy left will now collect lesser data than before (Fig. 2).

Algorithm: Agent -based Energy Sink Hole Solution
Input :

- *a flat static dense WSN*
- *sensor nodes capable of hosting agents .*
- *a special node called sink with mobile agent embedded in it.*

Output : a network less affected by energy sink hole problem and with enhanced lifetime

1. *Generate mobile agent(MA) on the sink. MA runs and provides host with a "Itinerary sensor ID".*
2. *Sink dispatches MA to level 1 nodes .*
3. *MA arrives and runs on each of the level 1 nodes, provide each node with distinct "Itinerary sensor ID".*
4. *From each level 1 node MA is dispatched to the nodes in radio range of level 1 nodes i.e to level 2 nodes*
5. *After the arrival of agent on level 2 nodes, all the nodes run it (only once in case of multiple arrivals from more than one level 1 node) and the agent generates Itinerary sensor ID" for them.*
6. *Each level 2 node dispatches agent ,containing its own ID back to respected level 1 node from where agent arrived.*
7. *After agent arrival at level 1 node , node stores the Itinerary sensor ID of the level 2 node provided by the agent .*
8. *When any data packet arrives at level 1 node, data is accepted only if the source ID of data packet matches with the already stored itinerary ID's at that node.*
9. *The data is processed and passed to sink.*

Fig. 2 Algorithm for the proposed approach

4 Implementation and Results

The work has been implemented using Aglets [15–17]. Aglet API is an agent development kit.

It consists of a set of Java interface and classes that allow the creation of mobile Java agents. Mobile agents built using the tool will run on every machine that supports the Aglet API [18–21]. Aglet API is hosted by an Aglet Server, i.e., Tahiti Server. The implementation has been carried out on a single machine with three ports with port number 9000, 4434, and 434, respectively, (Fig. 3). However, the work is scalable to three different machines connected via LAN. As shown in the Fig. 3, port 4434 is acting as sink, port 9000 as level 1 node, and port 434 as level 2 node.

5 Analytical Results

The theoretical analysis of the proposed algorithm reflects that network load on the nodes near to the sink has reduced significantly after the application of the algorithm. Since sink-hole problem deals with the nodes that are nearer to sink, only partial sensor network is considered during analysis. Figure 4 illustrates the map of analysis.

As shown in Fig. 4 (left), there are four nodes (white colored) around the sink. These nodes are in direct radio range of sink. The radio range of level 1 nodes has been shown, and we can see some of their radio ranges overlap. Hence when some nodes at level 2 send data, they send it to more than one level 1 node.

Fig. 3 Output on command prompt for different ports

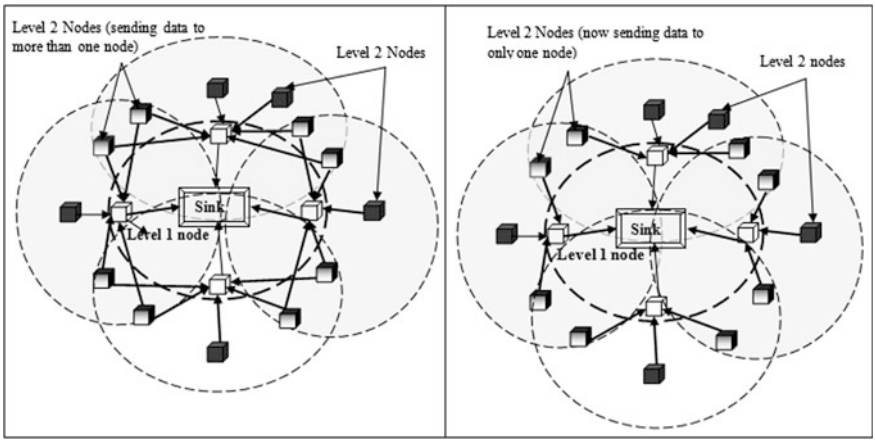


Fig. 4 Data transfer in traditional WSN (left), itinerary influence on data transfer procedure (right)

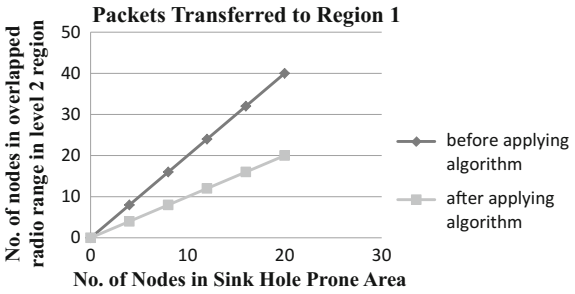


Fig. 5 Comparison of packets transferred to region 1

Double-shaded nodes are the nodes that are passing data to more than one node. Analyzing from Fig. 4 (left), total 20 units of data are coming from the level 2 nodes to the level 1 nodes out of which 7 units of data are being repeated as some of the level 2 nodes are passing data to more than one node, only 13 units of data are actually required to be passed to the level 1 nodes.

After applying the algorithm (Fig. 4 (right)), we form itineraries and each node at the level 1 only accepts data from predetermined level 2 nodes. Earlier, the level 2 nodes whose data were accepted by more than one level 1 node are now accepted by only one level 1 node. Thus, after applying the algorithm, we get exactly 13 pieces of data. Hence, we can say that the algorithm has reduced network load at the sink-hole-prone region by passing data in an efficient manner from level 2 region nodes to region 1 region nodes, which in turn has made the network load less by reducing the overall redundancy at level 1 region nodes.

Figure 5 shows comparison in number of packets transferred to region 1 before and after the application of algorithm. Sensor networks with different sizes are considered here. The x-axis represents the number of nodes in direct radio range of sink (level 1 nodes), and the y-axis shows the number of those nodes in the level 2 region, which is in overlapped radio ranges of two level 1 nodes. For simplicity, it is considered that whenever there is an overlap in radio ranges of region 1 nodes, it is due to two nodes placed closed to each other; however, there can also be an overlap in the radio ranges of more than two nodes also, itinerary effect in such a case is even more beneficial.

6 Concluding Remarks

The approach is well suited for a dense network where nodes are unevenly distributed in a given area. Though it adds the overhead of maintaining and dispatching mobile agents, but the advantage of removing redundant transmission in the nodes lying in close proximity of the sink compensates for the same. As the work proceeds by dividing the given area into concentric circles, the work can be extended to calculate the itineraries of nodes even far from the sink. However, it will involve selecting only those nodes whose energy level falls below the threshold.

References

1. Akyildiz Ian, F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Commun. Mag. 102–114 (2002)
2. Uddin, M.Y.S., Akbar, M.M.: Addressing techniques in wireless sensor networks: a short survey. In: 4th International Conference on Electrical and Computer Engineering Dhaka, Bangladesh (2006)
3. Chen, M., Gonzalez, S., Leung, Victor, C.M.: Applications and design issues for mobile agents in wireless in wireless sensor networks. IEEE Wirel. Commun. (2007)
4. Sethi, P., Juneja, D., Chauhan, N.: Exploring the feasibility of mobile agents in sensor networks in non-deterministic environments. Int. J. Adv. Technol. (IJoAT), **1**(2) (2010). ISSN 0976-4860
5. Ammari, H.M.: Investigating energy sink ole problem in connected k-covered wireless sensor networks. IEEE Trans. Comput. (2013)
6. Lian, J., Naik, K., Agnew, G.: Data capacity improvement of wireless sensor networks using non-uniform sensor distribution. Int. J. Distrib. Sens. Netw. **2**(2), 121–145 (2006)
7. Wu, X., Chen, G., Das, S.K.: Avoiding energy holes in wireless sensor networks with non uniform node distribution. IEEE Trans. Parallel Distrib. Syst. **19**(5) (2008)
8. Liu, M., Song, C.: Ant-based transmission range assignment scheme for energy hole problem in wireless sensor networks. Int. J. Distrib. Sens. Netw. (2012)
9. Yuting, L., Wang, W.: Energy hole solution algorithm in wireless sensor network. J. Netw. **9** (2014)
10. Luo, J., Panchard, J., Piorkowski, M., Grossglauser, M., Pierre, J.: MobiRoute: routing towards a mobile sink for improving lifetime in sensor networks. Hubaux School of Computer and Communication Sciences, Ecole Polytechnique Federale de Lausanne (EPFL), CH-1015 Lausanne, Switzerland
11. Chen, M., Kwon, T., Yuan, Y., Leung, V.C.M.: Mobile agent based wireless sensor networks. J. Netw. **1** (2006)
12. Gorton, I., Haack, J., McGee, D., Cowell, A., Kuchar, O.: Evaluating agent architectures: cougaar, aglets and AAA. Software Engineering for Multi-Agent Systems II, vol. 2940 (2004)
13. Lange, A.B., Oshima, M.: Seven good reasons for mobile agents. Commun. ACM **42**(3) (1999)
14. Outtagarts, A.: Mobile agent-based Applications: a survey. IJCSNS Int. J. Comput. Sci. Netw. Secur. **9**(11) (2009)
15. Ammari, H.M.: Energy sink-hole problem with always on sensors in two dimensional deployment fields. In: Challenges and Opportunities of Connected k-Covered Wireless Sensor Networks. Springer (2009)
16. Lange, D.B., Oshima, M.: Mobile agents with Java: the aglet API. World Wide Web **1**(3) (1998)
17. Horvat, D., Cvetkovic, D., Milutinovic, V., Kocovic, P., Kovacevic, V.: Mobile agents and Java mobile agents toolkits. Telecommun. Syst. **18**(1–3) (2001)
18. Pandey, R., Sharma, N., Rathore, R.: Aglets (A Java Based Mobile Agent) and its security issue. Int. J. Emerg. Trends Technol. Comput. Sci. **2**(4) (2013)
19. The Aglet-2.0.2 User's Manual Aglet Development group (2009)
20. http://sourceforge.net/projects/aglets
21. Yadav, M., Sethi, P., Juneja, D., Chauhan, N.: Development of Mobile agents with Aglets. Int. J. Innov. Adv. Comput. Sci. (2015)

Compact Low-Profile WiMAX-MIMO Antenna with Defected Ground Structure for Disaster Management

Madan Kumar Sharma, Mithilesh Kumar, J.P. Saini and Girish Parmar

Abstract This paper presents a novel, compact, and low-profile 2 × 2 multi-input multi-output (MIMO) antenna for WiMAX 802.16a applications which is very useful for disaster communication systems. Proposed WiMAX-MIMO antenna designed on low cost FR4 substrate with the compact size of 32 × 32 mm^2 with dielectric constant of 4.4. The defected ground structure perturbed in the form of L-shaped in the ground plane offer a good isolation up to −26 dB for the entire frequency band of 3–14 GHz. The two patches on the top of substrate perpendicular to each other introduced pattern diversity in the radiation pattern. The good impedance bandwidth of 0–14 GHz, high isolation and low correlation coefficient make the proposed design antenna suitable for WiMAX 802.16a applications.

Keywords WiMAX · MIMO · Diversity · Correlation

1 Introduction

To monitor various disaster situations of earthquake, catastrophes, and tsunamis, a real-time alarming systems or a reliable wireless communication system must be deployed [1]. Although different type of communication networks already exists such as cellular telephony system, wireless local area network(WLAN), wireless personal area network (WPAN), WiFi, but all these networks have low data

M.K. Sharma (✉) · M. Kumar · G. Parmar
Rajasthan Technical University, Kota, India
e-mail: madan.sharma.2015@ieee.org

M. Kumar
e-mail: mith_kr@yahoo.com

G. Parmar
e-mail: girish_parmar2002@yahoo.com

J.P. Saini
Bundelkhand Institute of Engineering & Technology, Jhansi, Uttar Pradesh, India
e-mail: jps_uptu@rediffmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_28

transmission rate, small coverage, and less reliable and therefore not useful for disaster management applications. WiMAX standard 802.16a is a key technology [2] that capable to provide the better coverage up to 5 miles with high-speed data transmission up to 75 Mbps with good quality of services (QOS), and hence WiMAX network can be used as a backup communication network. It can replace the damaged mobile base station-based network or other wireless network in case of different disaster situations. WiMAX works on worldwide interoperability for microwave access technique and having the ability to handle different disaster situations. The architecture or model of WiMAX can be modified for different applications at different convergence sub layers but at the physical layer there are two WiMAX topologies are used, i.e., point-to-point for backhauls and point-to-multipoint between base station and clients. In any of these situations multi-input multi-output (MIMO) antennas should be deployed [3] at transmitter or receiver section.

MIMO antenna can exploit the multipath to provide higher data rate and simultaneously increase range and reliability of communication network, all without consuming extra radio frequency. The channel spectral efficiency increases two times compare to single input and single output (SISO) network configuration [4]. Multiple antenna techniques are also effective techniques in mitigate the co-channel interference and multipath fading problems occurs in non-line-of-sight (NLOS) communication systems.

MIMO antenna may be implemented using two techniques [5]; i.e., first one is spatial multiplexing technique in which independent information sequences transmit simultaneously over multiple antennas, and ultimately, it offers higher data rate. Another is antenna diversity techniques (pattern, polarization, and beam forming) in which redundant data streams transfer on multiple antennas to reduce bit error rate and also increase range of transmission with the help of antenna diversity gain. But MIMO antenna efficiency limited by correlation coefficients because transmit signals from multiple antennas correlate some extant, and hence radiation efficiency of antenna decreases. If one antenna excited and another is terminated with matched load of 50 Ω, surface current induced in second antenna, reduced the radiation efficiency, and it termed as mutual coupling or isolation (S21). The researchers and academicians always make efforts toward the antenna miniaturization without degrade its performance in terms of pattern diversity, correlation coefficient, and mutual coupling in this race.

In [6] a Dual ISM Band MIMO Antenna for WiFi and WiMAX application designed on the FR4 substrate of size of 40×90 mm^2, and it covers frequency bands of 2.1–2.7 and 5.1–6.1 GHz only with isolation of ≤ 15 dB. A Tri-Band Printed Monopole Antenna for WLAN and WiMAX-MIMO systems presented in [7] which covers the multiband of 2.4, 3.8, and 5.2 GHz. with isolation of ≤ 12 dB only. Although a compact dual-band (5.8 GHz for WLAN and 5.5 GHz for WiMAX) antenna [8] offers a good port-to-port isolation of ≤ 20 dB with the size of 40×30 mm^2 but it is also not suitable for 802.16a version of WiMAX. A antenna [9] with substrate size of 45×45 mm^2 designed with the help of four micro-strip patch elements, but impedance bandwidth of antenna covers lower band

(2.3 and 2.5 GHz) of WiMAX. A Compact WiMAX-MIMO Antenna Design for laptop applications designed in [10] which has the total size of 70 × 8 mm^2, and impedance bandwidth also covers only lower frequency band of WiMAX, i.e., 2.3, 2.7, 3.4, and 3.7 GHz only with the isolation of below −15 dB for lower bands and up to −20 dB for higher bands. A self-shielding open slot antenna for WiMAX-MIMO application designed [11] on the ground plane size of 50 × 90 mm^2 which operates at the 2.6 GHz band of WiMAX and offered the isolation of $\leq$24 dB. A 2 × 2 MIMO antenna [12] designed for dongle application and frequency band of interest only 2.52 GHz only, although antenna size is very compact 25 × 8 mm^2 easily embedded in dongle card size of 90 × 25 mm^2 all parameters are fitted in the desired application. A compact dual-band multi-input multi-output (MIMO) antenna array with eight elements study carried out in [13] for the long-term evolution (LTE)/WiMAX mobile applications. The size of antenna is too large, dimensions of 140 × 70 mm^2 and it covers only lower bands (2.4–2.6 and 3.4–3.6 GHz) of WiMAX with the isolation of −20 dB only.

Mutual coupling is one of the important issue with MIMO antenna design, while thinking about miniaturization of antenna as discussed previously, if size of antenna reduced somehow a strongest mutual coupling occurs between the MIMO antenna elements. Although different techniques, such as inserting ground stubs, half wavelength slot etched in the ground plane, parasitic, connecting neutralization line, and Meta material inspired structures are used to minimize the size of antenna along with least mutual coupling between MIMO antenna elements. The nominal value of mutual coupling or isolation $\leq$15 dB is considered in most of the cases. With the best of our knowledge the all antennas studied from [6–13] does not cover the frequency band of interest of WiMAX 802.16a (3–11 GHz) with high isolation. The proposed design not only novel and compact in size but also fulfill all aspects of WiMAX 802.16a.

Rest of the paper organized in Sects. 2, 3, and 4. In Sect. 2 antenna design procedure and dimensions are given, in Sect. 3 study of all simulated results are carried out, and finally Sect. 4 concludes the paper with consideration of WiMAX-MIMO antenna used for disaster management, including future directions.

2 Antenna Design

The proposed antenna designed on the FR4 substrate with dielectric constant of 4.4 and thickness of 0.8 mm. The size of antenna is 32 × 32 mm^2, which is very compact and easy to embed in mobile transmitter and receiver of WiMAX. The two L-shaped slots cut in the ground plane denoted by GC_1 and GC_2. The two L-shaped ground plane slots perpendicular to each other offer good isolation between the two antenna elements. The two radiating patch perpendicular to each other provide good pattern diversity between the antennas elements and therefore yield low correlation coefficient. Antenna consists of two rectangular patches that are fed by 50 Ω micro-strip lines; ultimately, WiMAX range of frequency shifted from lower

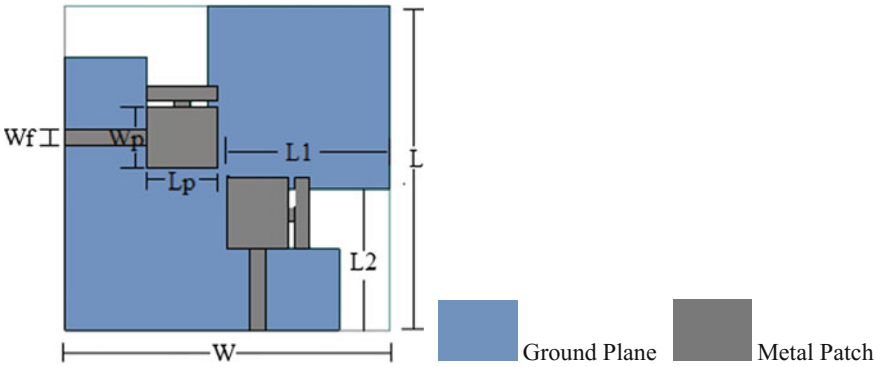


Fig. 1 WiMAX-MIMO antenna, $L = 32$, $W = 32$, $L_1 = 16$, $L_2 = 14$, $W_P = 6$, $L_P = 7$, $W_f = 1.53$

frequency band to ultra wideband with the help of T-shaped stub is attached to the rectangular patch which consists of a horizontal stub and a vertical stub. All dimensions of proposed antenna optimized with the help of CST Microwave studio simulation tool and designed structure as depicted in Fig. 1, all dimensions in mm, also listed with diagram.

3 Results and Discussion

Results of designed WiMAX-MIMO antenna studied and carried out with the help of CST Microwave studio simulation tool in the planer antenna design environment. Results are analyzed in terms of return loss, isolation or mutual coupling, correlation coefficient, radiation pattern, and diversity gain.

3.1 Return Loss and Isolation

Return loss is a measure of dissipated power across the antenna port due to impedance mismatch between micro-strip feed line and antenna itself. Antenna efficiency limited by this parameter, and it should be S11 ≤ 10 dB or low as possible. Figure 2 shows the simulated return loss of the proposed WiMAX-MIMO

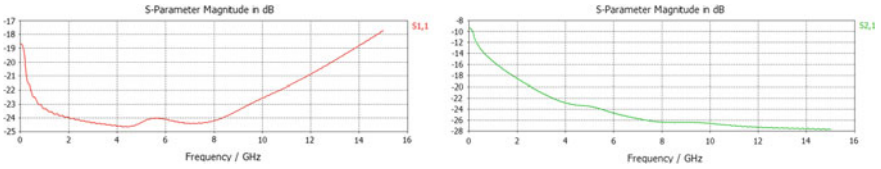


Fig. 2 Return loss and isolation

antenna. It can be observed that proposed antenna with defected ground structure of L-shaped not only offers return loss of S11 ≤ 10 dB for entire band of interest 3–11 GHz but also miniaturized size of propose antenna.

Port-to port-isolation can be determined by energized one port and other terminated with matched load of 50 Ω. Isolation represented in terms of S parameter, i.e., S21. High degree of isolation achieved in the proposed design as depicted in Fig. 2 and its noticeable value started from −21 dB at frequency of 3 GHz and increases more than −26 dB for the frequency up to 14 GHz.

3.2 Radiation Pattern

Radiation pattern is one of the most important figures of merit of antenna, which show the graphical representation of antenna field strength in the far-field mode. Multiple antenna radiation pattern differs from SISO configuration; they follow the diversity in their radiation pattern in multipath propagation of signals. The signal received in diversity systems can be correlated some extent, correlation of signal decreases antenna efficiency. Proposed WiMAX-MIMO antenna follows the pattern diversity in their pattern, and radiation patterns analyzed at the frequencies of 8, 10 GHz as depicted in Fig. 4. At these frequencies of 8 and 10 GHz, patterns of patch one and two are complemented each other. The proposed WiMAX-MIMO antenna offers good diversity in their radiation patterns with low correlation coefficient.

3.3 Correlation Coefficient

Correlation coefficient is a mathematical and statistical parameter and that have a great importance in multiple antenna design. Radiated signal from transmitting antenna propagated with multipath and arrived at receiver antenna with the diversity. Patterns at receiving antenna may or may not be correlated some extent due to degree of similarity among the received signals. The modulus of correlation coefficient varies from zero to one. Ideally, MIMO diversity system has its value is zero or low by default. The simulated results of correlation coefficient as depicted in Fig. 3. The proposed antenna has very low correlation coefficient with the value of

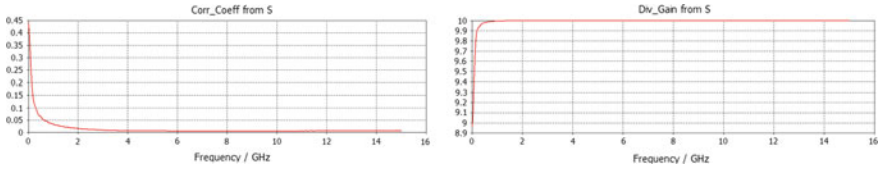


Fig. 3 Correlation coefficient and diversity gain

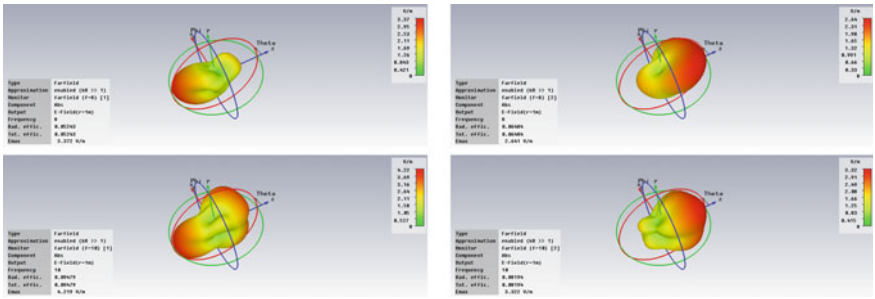


Fig. 4 Radiation patterns of patch 1 and 2 at the frequency of 8 and 10 GHz

less than 0.05 for the frequency of 0.6–15 GHz, which is very low and guaranteed the good diversity performance present in WiMAX-MIMO antenna. The result is depicted in Fig. 3.

3.4 Antenna Diversity Gain

Diversity gain of antenna is usually a measure of diversity performance of MIMO antenna with different diversity techniques, it simply describes a comparison with the received signal-to-noise ratio (SNR) from a single reference antenna and enhancement of combined SNR from multiple antenna systems. The diversity gain can also be calculated with help of correlation coefficient and given by Eq. (1), where ρ is denoted as correlation coefficient.

$$\mathrm{DG} = 10\sqrt{(1 - |\rho 2|)} \tag{1}$$

The proposed antenna diversity gain simulated with the help of computer and analyzed from *S* parameters, and it is to be notice from Fig. 3 that proposed WiMAX-MIMO antenna offers excellent diversity gain of 9.99 (Fig. 4).

4 Conclusion and Future Scope

In this paper, very compact and low-profile WiMAX-MIMO antenna designed and simulated with the help of CST. Proposed antenna is good candidate for disaster management. In future, 4 × 4 MIMO antenna can design which increases the diversity gain of antenna.

References

1. Bayrak, T.: Identifying requirements for a disaster-monitoring system. Disaster Prev. Manag. Int. J. **18**(2), 86–99 (2009)
2. Eklund, C., et al.: IEEE standard 802.16: a technical overview of the WirelessMAN™ air interface for broadband wireless access. IEEE Commun. Mag. **40**(6), 98–107 (2002)
3. Mohammad Ali, M.-A., Motahari, A.S., Khandani, A.K.: Communication over MIMO X channels: interference alignment, decomposition, and performance analysis. Inf. Theory IEEE Trans. **54**(8), 3457–3470 (2008)
4. Ngo, H.Q., Larsson, E.G., Marzetta, T.L.: Energy and spectral efficiency of very large multiuser MIMO systems. Commun. IEEE Trans. **61**(4), 1436–1449 (2013)
5. Mietzner, J., et al.: Multiple-antenna techniques for wireless communications-a comprehensive literature survey. Commun. Surv. Tutor. IEEE **11**(2), 87–105 (2009)
6. Roshan, R., Singh, R.K.: Dual ISM band MIMO antenna for WiFi and WiMax application. In: 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT), IEEE (2014)
7. Mallahzadeh, A.R., et al.: Tri-band printed monopole antenna for WLAN and WiMAX MIMO systems. In: Proceedings of the 5th European Conference on Antennas and Propagation (EUCAP), IEEE (2011)
8. Xiong, L., Gao, P.: Compact dual-band printed diversity antenna for WiMAX/WLAN applications. Prog. Electromagn. Res. C **32**, 151–165 (2012)
9. Wang, H., et al.: A compact wideband quad-element planar antenna for WiMAX MIMO Application. In: Antennas and Propagation Society International Symposium (APSURSI), 2014 IEEE, IEEE (2014)
10. Chen, W.-S., Chi, Y., Chang, F.-S.: Compact WiMAX MIMO antenna design for laptop applications. In: 2014 International Symposium on Antennas and Propagation (ISAP), IEEE (2014)
11. Pu, T.-C., et al.: A self-shielding open slot antenna for WiMAX MIMO application. In: Antennas and Propagation Society International Symposium, 2009, APSURSI'09, IEEE, IEEE (2009)
12. Chang, L.-C., et al.: A polarization diversity MIMO antenna design for WiMAX dongle application. Microwave Conference Proceedings (APMC), 2010 Asia-Pacific, IEEE (2010)
13. Li, G., Zhai, H., Ma, Z.: Isolation-improved dual-band MIMO antenna array for LTE/WiMAX mobile terminals. 10.1109/LAWP.2014.2330065, IEEE Antennas and Wireless Propagation Letters

A Comparative Study of Various Routing Classes and Their Key Goals in Wireless Sensor Networks

Yahya Kord Tamandani, Mohammad Ubaidullah Bokhari and Qahtan Makki

Abstract Regardless of the type of application and place of operation, one of the primary aims of wireless sensor networks (WSNs) is basically to achieve data communication while attempting to preserve the energy in order to function for a longer time and to avoid connectivity collapse by employing effective and robust power management strategies. There are various obstacles which need to be addressed and overcome so as to design suitable and efficient routing protocols for WSNs. The main issues are associated with the limitation of sensor nodes such as restricted power, processing power, and other constrained resources. In this paper, we have presented a comparative study of various routing classes and their key goals in WSNs. This paper aims to explore the most important routing protocols designed for WSNs along with their primary goals and compare them for a better understanding and further researches.

Keywords Wireless sensor networks · Routing protocols classes · Key goals Comparison

1 Introduction

Due to number of unique characteristics of wireless sensor networks (WSNs), the design of routing protocols for these types of networks is a very challenging task. Firstly, it is not practicable to design an overall addressing system for WSNs as in typical communication networks. Secondly, because of the significant redundancy of the generated data in WSNs, to preserve the energy and improve the bandwidth,

Y.K. Tamandani (✉) · M.U. Bokhari · Q. Makki
Department of Computer Science, Aligarh Muslim University, Aligarh, India
e-mail: Yahya.kord@gmail.com

M.U. Bokhari
e-mail: mubokhari.cs@amu.ac.in

Q. Makki
e-mail: qahtan.mekki@yahoo.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_29

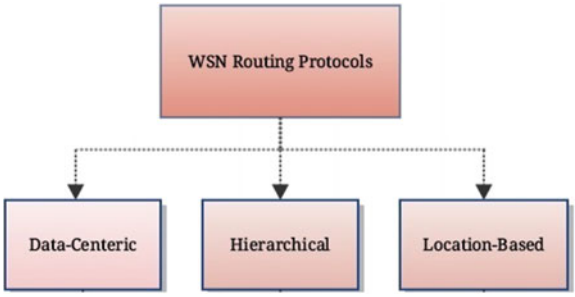


Fig. 1 Classification of routing protocols in WSNs

such redundancy has to be dealt with. Thirdly, sensor nodes are extremely constrained, regarding their energy, storage, and processing capabilities. More than a decade, many routing algorithms have been proposed and designed specifically for WSNs and most of them aim to prolong the life of the network [1–3]. These routing approaches typically can be categorized as data centric, location-based and hierarchical routing protocols (Fig. 1). Data centric routing protocols are typically based on query, hence capable of reducing the redundancy of the data significantly. In location-based approach, a message is forwarded from a source to the destination via the most efficient path discovered by the location of the neighboring sensor nodes of the sender. Hierarchical routing protocols divide the networks into number of clusters, and each cluster possesses a cluster head which is responsible for gathering data from other nodes (within the cluster), performing data aggregation and fusion then sending them to the sink. This paper aims to explore the most important protocols designed for WSNs along with their primary goals and comparing them with one another for a better understanding and investigation of open issues for further researches.

1.1 Routing Classes in WSNs

A routing algorithm could be thought of as a strategy by which a node comes to a decision about selection of a neighboring path to send a packet to a desired destination. The distinguished features of WSN make the routing a tough task. As there is an enormous number of nodes, distributed within the network, it will not be feasible to use a global addressing method [4]. In WSN, data are sent from several sources to a base station (sink). There are also some limitation related to sensor nodes which has to be considered carefully while designing of routing protocols such as energy, transmission, and processing power. Routing algorithms in WSNs can be classified as follows: data centric, location-based, and hierarchical routing algorithms as shown in Fig. 1.

2 Data Centric Routing Protocols

In WSNs, each single node is required to send out data to the sink which leads to a considerable redundancy, resulting in large wastage of energy waste. Thus, routing approaches have been introduced that are capable of selecting a range of nodes on query-based, known as data centric routing. Queries are sent by the base station (BS) to a particular region for the desired information. Considering that data are demanded via queries only a certain data from an interested region needs to be transmitted to and as a result this will reduce the redundancy of the data as well as the number of transmission which will improve the energy consumption and lifetime of the network significantly. One of the earliest routing protocols based on data centric approach is SPIN [5]. In SPIN protocol, data are named using meta-data or other high-level descriptors. With the help of an advertising mechanism, the data descriptors are exchanged before the transmission process. As soon as a node possesses a new data to be shared, it will generate an ADV message and send it to its neighboring nodes, and in return the neighboring nodes use a request message in order to obtain the desired data (provided they haven't possessed it already) through a REQ message. Finally, the source from where the ADV message has been generated and sent transmits the real data to finish up the process. The process is shown in Fig. 1 which is redrawn from [5]. Table 1 shows the most important routing protocols in this category along with their key characteristics and objectives (Fig. 2).

Table 1 Comparison of the main data centric routing protocols and their main objectives

Routing protocol	No. of possible BS	Data aggregation	Adaptive to mobility	Taking into account the battery lifetime	Key objectives of the protocol
SPIN [5]	Single	Yes	Yes	Yes	• Preserving energy to extend network lifetime • Reducing number of messages
Direct diffusion [6]	Multiple	Yes	Limited	No	• Fault tolerance • Improving on data diffusion
Rumor routing [7]	Single	Yes	Limited	No	• Reducing number of queries in network
Information-driven [8]	Single	Yes	Limited	Yes	• Extending network lifetime

(continued)

Table 1 (continued)

Routing protocol	No. of possible BS	Data aggregation	Adaptive to mobility	Taking into account the battery lifetime	Key objectives of the protocol
REAR [9]	Multiple	Yes	Limited	Yes	• Extension of network lifetime • Improving data delivery
MCFA [10]	Single	No	No	No	• Improving data delivery
ACQUIRE [11]	Multiple	Yes	Limited	No	• Query optimization • Extending network lifetime
Gradient-based routing [12]	Single	Yes	Limited	No	• Achieving data delivery via lowest number of hops
Link quality estimation-based [13]	Single	No	No	No	• Achieving data delivery with lowest number of retransmission
Energy-aware [14]	Multiple	Yes	Limited	Yes	• Extending network lifetime

3 Location-Based Routing Protocols

Location-based routing protocols utilize the geographical location of sensor nodes in order to form the optimal route and send packets from a source to the desired destination. A packet is sent from source to destination by considering the geographical position of the neighboring nodes of the forwarder. The information about sensor node's location is obtained via Global Positioning System (GPS) which is tiny and low consuming power devices embedded in the body of the sensor nodes. The following Table 2 depicts the main routing protocols in this class along with their key characteristics and objectives. GAF [15] is one of the location-based routing protocols which aims to prolong the network's life. A virtual grid id is formed, and all the nodes link themselves in it as it is depicted in Fig. 3. Nodes that are linked within the exact same location on the grid will be considered to have the same cost of routing. Hence to preserve energy in an attempt to prolong the network's life, nodes linked to the same point on the virtual grid could turn into the sleep mode. As we observe from Fig. 3, to reach node 5 from node 1 we could do it through the node 4 and turn the node 2 and 3 into the sleep mode. [4]. Table 2 displays the most important location-based routing protocols along with their main objectives and features.

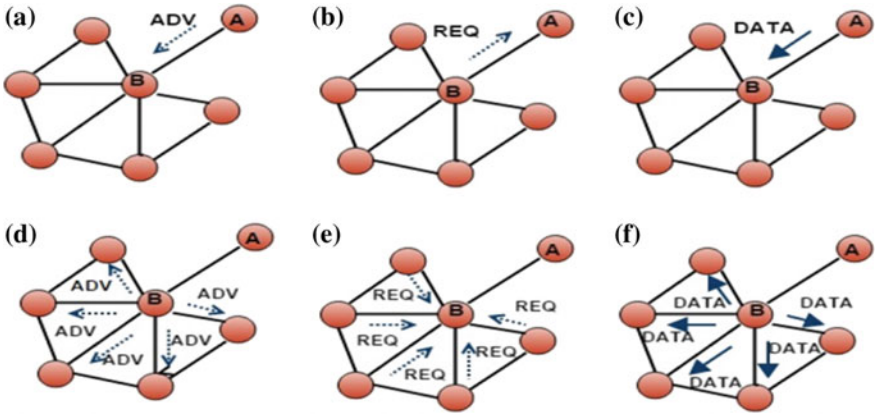


Fig. 2 Working procedure of SPIN protocol

Table 2 Comparison of the main location-based routing protocols and their main objectives

Routing protocol	No. of possible BS	Data aggregation	Adaptive to mobility	Taking into account the battery lifetime	Key objectives of the protocol
GAF [15]	Multiple	No	Limited	Yes	• Extending network lifetime
SPEED [16]	Multiple	No	No	Yes	• Extending network lifetime • Achieving real time
MMSPEED [17]	Multiple	No	No	Yes	• Extending network lifetime • Achieving real time • Enhancing SPEED protocol
GEAR [18]	Single	No	Limited	No	• Extending network lifetime
EAGR [19]	Multiple	No	Limited	Yes	• Enhancement of GAF protocol • Extending network lifetime

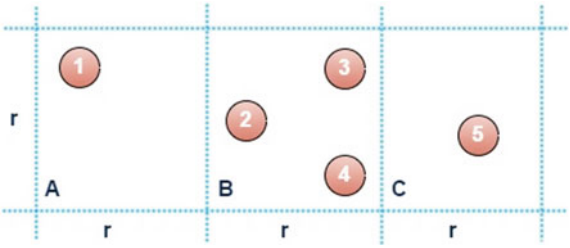


Fig. 3 Virtual grid in GAF

4 Hierarchical Routing Protocols

In this type of routing, the whole network is divided into number of clusters and in each cluster one node will act as the cluster head (CH) (Fig. 4). The CH is in charge of receiving the sensed data from other nodes within the cluster (cluster members) and performing data aggregation and/or data fusion, then sending the data to the base station. Different routing protocols have different techniques for selection of cluster heads. However, the residual energy of a node and its distance from the base stations are the main factors that are considered by the recent and modern routing protocols while election of CHs. The main objective of this category of routing protocol is to balance the energy among the sensor nodes in order to extend the lifetime of the network. The earliest and most well-known hierarchal routing protocol is LEACH [20] (Low-Energy Adaptive Clustering Hierarchy). It reduces the energy consumption of the network by choosing the CH nodes in a random fashion

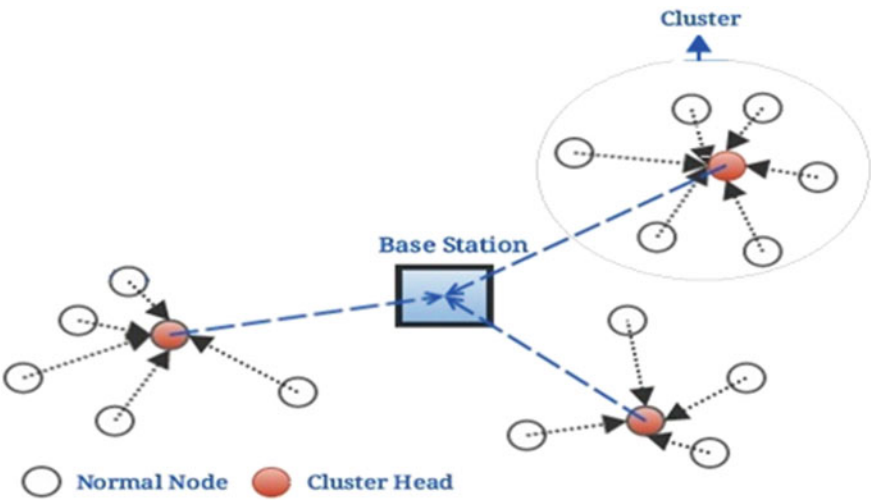


Fig. 4 Cluster formation in LEACH routing protocol

Table 3 Comparison of the main hierarchical routing protocols and their main objectives

Routing protocol	No. of possible BS	Data aggregation	Adaptive to mobility	Taking into account the battery lifetime	Key objectives of the protocol
LEACH [20]	Single	Yes	Fixed bs	Yes	• Extending network lifetime
PEGASIS [21]	Single	No	Fixed bs	Yes	• Extending network lifetime • Improving bandwidth of network
TEEN [22]	Single	Yes	Fixed bs	Yes	• Extending network lifetime • Achieving real time
APTEEN [23]	Single	Yes	Fixed bs	Yes	• Extending network lifetime • Achieving real time
EWC [24]	Single	Yes	Fixed bs	Yes	• Extending network lifetime • Guarantee the data delivery
Self-organized [25]	Single	No	Yes	No	• Achieving higher fault tolerance
Energy-aware cluster-based [26]	Single	No	No	Yes	• Extending network lifetime • Achieving real time

to distribute energy load evenly to each and every node. Figure 3 shows the cluster formation in LEACH routing protocol. Table 3 shows the main hierarchical routing protocols along with their main features and goals.

5 Conclusion

Mainly due to limitation of sensor nodes and other restrictions of WSNs, routing is significantly vital and plays an essential role in the efficiency of the network. In this paper, the characteristics and main objectives of main routing protocols in WSNs

have been given. Considering the main goals of these routing protocols, we realize that the energy efficiency and extension of network's life is the objective of most routing protocols. However, there is not a standard routing protocol for WSNs, and selecting the most efficient and suitable depends highly on the type of application. In this paper, main routing protocols in WSNs have been compared against one another in order to easily observe their strong and weak points. This helps to realize the open issues for further researches as well as for a precise selection of the most appropriate routing protocols to specific applications.

References

1. Ya, K.L., Pengjun, W., Rong, L., Huazhong, Y., Wei, L.: Reliable energy-aware routing protocol for heterogeneous WSN based on beaconing. In: 16th International Conference on Advanced Communication Technology (2014)
2. Tamandani, Y.K., Bokhari, M.U.: SEPFL routing protocol based on fuzzy logic control to extend the lifetime and throughput of the wireless sensor network. Wirel. Netw. (2015)
3. Zaman, N., Low, T., Alghamdi, T.: Energy efficient routing protocol for wireless sensor network. In: 16th International Conference on Advanced Communication Technology (2014)
4. Singh, S.: A survey on energy efficient routing in wireless sensor networks. Int. J. Adv. Res. Comput. Sci. Softw. Eng. Res. **3**(7), 184–189 (2013)
5. Heinzelman, W.R., Kulik, J., Balakrishnan, H.: Adaptive protocols for information dissemination in wireless sensor networks. In: Proceedings of 5th Annual ACM/IEEE International Conference Mobile Computing Networking—MobiCom'99, pp. 174–185 (1999)
6. Intanagonwiwat, C., Govindan, R., Estrin, D.: Directed diffusion: a scalable and robust communication paradigm for sensor networks. In: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking—MobiCom'00, pp. 56–67 (2000)
7. Braginsky, D., Estrin, D.: Rumor routing algorithm for sensor networks. In: First International Workshop on Sensor Networks and Applications, pp. 22–31 (2002)
8. Chu, M., Haussecker, H., Zhao, F.: Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks. Int. J. High Perform. Comput. Appl. **16**(3), 293–313 (2002)
9. Hassanein, H., Luo, J.: Reliable energy aware routing in wireless sensor networks. In: Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems 2006, DSSNS 2006, no. i, pp. 54–64 (2006)
10. Ye, F., Chen, A., Lu, S., Zhang, L.: A scalable solution to minimum cost forwarding in large sensor networks. In: Proceedings of Tenth International Conference on Computing Communication Networks (Cat. No. 01EX495) (2001)
11. Sadagopan, N., Krishnamachari, B., Helmy, A.: The ACQUIRE mechanism for efficient querying in sensor networks. In: Proceedings of First IEEE International Workshop on Sensor Network Protocols and Applications (2003)
12. Schurgers, C., Srivastava, M.B.: Energy efficient routing in wireless sensor networks. In: IEEE Military Communications Conference, 2001. MILCOM 2001, vol. 1, pp. 357–361 (2001)
13. Chen, J., Lin, R., Li, Y., Sun, Y.: LQER: a link quality estimation based routing for wireless sensor networks. Sensors **8**(2), 1025–1038 (2008)
14. Shah, R.C., Rabaey, J.M.: Energy aware routing for low energy ad hoc sensor networks. In: 2002 IEEE Wireless Communications Networking Conference, Rec. WCNC 2002 Cat No02TH8609, vol. 1, pp. 350–355 (2002)

15. Heidemann, J., Estrin, D., Xu, Y.: Geography-informed energy conservation for ad hoc routing. In: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, ACM, pp. 70–84 (2001)
16. He, T., Stankovic, J.A., Lu, C., Abdelzaher, T.: SPEED: a stateless protocol for real-time communication in sensor networks. In: Proceedings of 23rd International Conference on Distributed Computing Systems (2003)
17. Felemban, E., Lee, C.G., Ekici, E.: MMSPEED: multipath multi-SPEED protocol for QoS guarantee of reliability and timeliness in wireless sensor networks. IEEE Trans. Mob. Comput. **5**(6), 738–753 (2006)
18. Yu, Y., Govindan, R., Estrin, D.: Geographical and energy aware routing: a recursive data dissemination protocol for wireless sensor networks. Energy (2001)
19. Haider, R., Javed, M.Y., Khattak, N.S.: EAGR: energy aware greedy routing in sensor networks. Future Generation Communication and Networking (FGCN 2007), vol. 2 (2007)
20. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, 2000, vol. 2, p. 10 (2000)
21. Lindsey, S., Raghavendra, C.S.: PEGASIS: power-efficient gathering in sensor information systems. In: IEEE Aerospace Conference Proceedings, vol. 3, pp. 1125–1130 (2002)
22. Ghiasabadi, M., Sharifi, M., Osati, N., Beheshti, S., Sharifnejad, M.: TEEN: a routing protocol for enhanced efficiency in wireless sensor networks. In: 2008 Second International Conferrence on Future Generation Communication and Networking, vol. 1, pp. 2009–2015 (2001)
23. Manjeshwar, A., Agrawal, D.P.: APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In: Proceedings of 16th International Parallel and Distributed Processing Symposium (2002)
24. Cheng, L., Qian, D., Wu, W.: An energy efficient weight-clustering algorithm in wireless sensor networks. In: 2008 Japan-China Joint Workshop on Frontier of Computer Science and Technology, pp. 30–35 (2008)
25. Subramanian, L., Katz, R.H.: An architecture for building self-configurable systems. 2000 First Annual Workshop on Mobile Ad Hoc Networking and Computing, MobiHOC (Cat. No.00EX444) (2000)
26. Younis, M., Youssef, M., Arisha, K.: Energy-aware routing in cluster-based sensor networks. In: Proceedings of 10th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems (2002)

WLAN Channel Compatible Design Goal-Based Energy-Efficient Fibonacci Generator Design on FPGA

Sonam and Anuradha Panjeta

Abstract In this research paper, we have analyzed that life and reliability of an integrated circuit are affected when different frequencies have been used to perform the operation on the circuit, FPGA technologies, and design goals. Fibonacci generator has been taken as our target circuit. Our design is capable of working with operating frequency of different WLAN channels. The device operating frequencies of 802.11b/g/n, 802.11y, 802.11a/h/j/n/c, 802.11p, 802.11ad, and 802.11ah are 2.4 GHz, 3.6 GHz, 5 GHz, 5.9 GHz, 60 GHz, and 900 MHz. Along with the frequencies, the device is also operated at different FPGA technologies such as Virtex-6 (40 nm) and Artex-7 (28 nm) FPGA technology. Five different design goals have also been taken into consideration. It has been observed that large amount of power (96.75%) can be saved on operating the device at 28 nm technology instead of 40 nm technology along with area reduction design goal. Also, if the design is being operated at a frequency of 900 MHz instead of a high frequency of 60 GHz, 99.88% of power consumption can be saved by using the balanced design goal.

Keywords Design goals · Energy efficient · Virtex-6 · Artex-7 · WLAN channel · Fibonacci generator · FPGA

1 Introduction

A field programmable gate array consists a feature of matrix of gate array logic circuitry which is reconfigurable. By the use of FPGA, implementation of hardware for a software application can be performed. In the place of, one can use single

Sonam (✉) · A. Panjeta
Shree Sidhivinayak Group of Institutions, Kurukshetra University, Kurukshetra, Haryana, India
e-mail: Ed36464@gmail.com

A. Panjeta
e-mail: anupanjeta@rediffmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_30

FPGA by integrating millions of logic gates in a single IC chip then the role of many thousands of discrete elements get performed. The basic structure of FPGA is designed by the combinations of logic elements, programmable interconnect, and memory. FPGA does not have an operating system but for processing logic, a dedicated hardware is being used. The good thing in FPGA is that different processing logic will not compete to get same resources because they are parallel in nature, and therefore, even with the addition of any processing component in the circuit, there is no effect on the performance of the other processing part. Wireless networks are an integral part of day-to-day life for connectivity and communication. Reference [1] examines the problems relating to the topic of wireless security and the background literature. Characteristics of a new class of signal correcting Galois field codes are described, which provide error detection and correction at the physical level of computer networks without additionally generating and transmitting cyclic redundancy check (CRC) codes [2]. Wi-fi-enabled devices periodically broadcast in their unique identifier along with other sensitive information. Therefore, they are vulnerable to a range of privacy breaches such as the tracking of their movement and inference of private information [3]. The penetration of mobile phones and tablets to gain wireless access to the Internet has been accompanied by a similar growth in cyber-attacks over wireless links to steal session cookies and compromise private users' accounts [4]. Here, energy-efficient green Fibonacci generator is used to generate key for WLAN networks for secure green communication. Since power goes directly proportional to energy, so energy crises being faced by the whole universe can be overcome by making energy- and power-efficient devices [5–8]. In the following design, the power is being analyzed at different frequencies along with the change in design goals at 28 nm (Artex-7) and 40 nm (Virtex-6) FPGA technologies. After the comparison, the optimized technique is being suggested. There are many more energy-efficient techniques such as clock gating, capacitive scaling, and thermal scaling being used in order to make the device energy and power efficient [9–11].

2 Energy-Efficient Techniques

2.1 Design Goals

In this technique, the design is being tested at different design goals and the best goal is then selected out of all. There are total five goals which are defined as follows:

(i) Area Reduction: By applying such technique, less number of LUT's and registers are being used. So, less space is being utilized by the device, and hence, area will be reduced. So power is also affected by this.

(ii) Minimum Runtime: By applying this design goal, the execution time has been reduced. Number of cycles will be reduced and the program will execute in the minimum required time. Hence along with the time, the power has also affected.

(iii) Timing Performance: In this technique, timing is being reduced and along with it, power consumption is also decreased.
(iv) Balanced: It is the summation of all the above techniques. By applying such technique, we can get an optimized time, area, performance, and power also.
(v) Power Optimization: It is one of the design goals. This goal mainly affects the dynamic and static power as well. By applying such technique, we can get the optimized value of power (Fig. 1).

2.2 *Frequency Scaling*

In this technique, the range of frequencies has been changed from a lower range of MHz to higher range of GHz. Wireless local area network channel frequencies have been taken into consideration to make it WLAN compatible. The different frequencies are mentioned in Table 1.

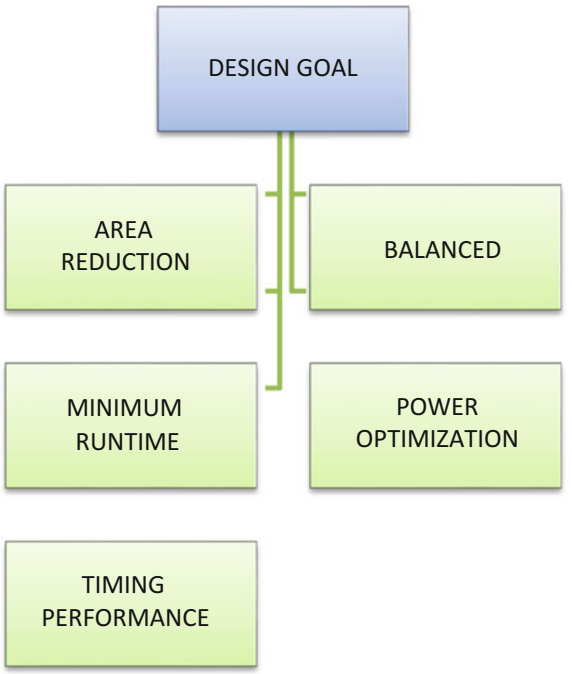


Fig. 1 Figure representing the different design goals

Table 1 Table representing the WLAN channel frequencies

900 MHz
2.4 GHz
3.6 GHz
5 GHz
5.9 GHz
60 GHz

Table 2 Table representing the different FPGA technologies

Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)

2.3 FPGA Technologies

With the advancement in the technology, the numbers of transistors fabrication on an IC have been increased from few thousands to millions and billions. In the following design, we are focusing on the four FPGA technologies which are 90 nm (Virtex-4), 65 nm (Virtex-5), 40 nm (Virtex-6), and latest 28 nm (Artex-7) technology. The 40 and 28 nm signifies the length of channel. By varying the four technologies, the power analysis has been done on all the technologies and afterward, the results of all the technologies have been compared and optimized technique has been chosen for the unicoder design (Table 2).

3 Static Power Analysis

3.1 Static Power Consumptions at Different FPGA's by Applying Area Reduction Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following static power consumptions are being observed as shown in Table 3.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **96.75%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **8.69%** of static power consumption can be reduced as shown in Fig. 2.

Table 3 Static power consumptions at different FPGA's by applying area reduction design goal

Freq.	Power			
	Static power consumptions at different FPGA's by applying *area reduction design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.042	1.294	0.321	0.167
2.4 GHz	0.043	1.296	0.322	0.167
3.6 GHz	0.043	1.299	0.323	0.167
5 GHz	0.043	1.301	0.329	0.167
5.9 GHz	0.043	1.302	0.335	0.167
60 GHz	0.046	1.396	0.491	0.167

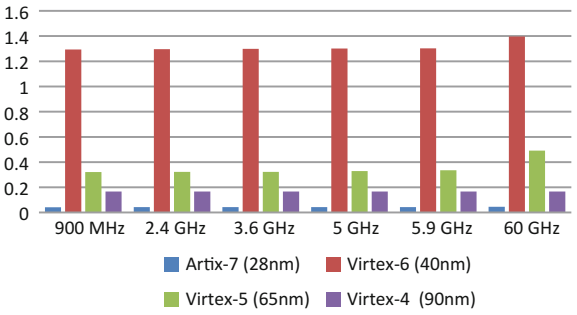


Fig. 2 Graph showing the static power consumptions at different FPGA's by applying area reduction design goal

3.2 *Static Power Consumptions at Different FPGA's by Applying* Balanced Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following static power consumptions are being observed as shown in Table 4.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **74.54%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **3.00%** of static power consumption can be reduced as shown in Fig. 3.

Table 4 Static power consumptions at different FPGA's by applying balanced design goal

Freq.	Power			
	Static power consumptions at different FPGA's by applying *balanced design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.042	1.298	0.323	0.170
2.4 GHz	0.043	1.307	0.328	0.178
3.6 GHz	0.043	1.314	0.333	0.186
5 GHz	0.043	1.322	0.343	0.196
5.9 GHz	0.044	1.327	0.352	0.203
60 GHz	0.060	1.607	0.491	0.219

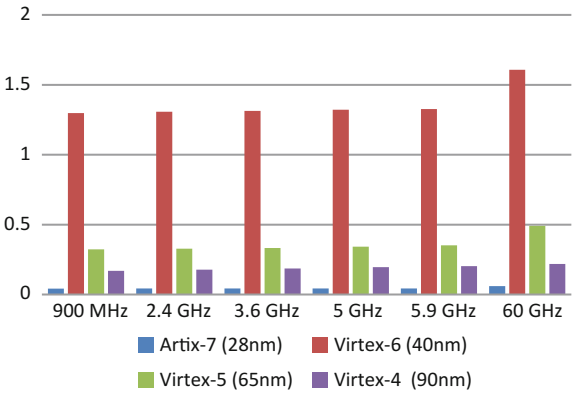


Fig. 3 Graph showing the static power consumptions at different FPGA's by applying balanced design goal

3.3 *Static Power Consumptions at Different FPGA's by Applying* Power Optimization Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following static power consumptions are being observed as shown in Table 5.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **96.68%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **28.33%** of static power consumption can be reduced as shown in Fig. 4.

Table 5 Static power consumptions at different FPGA's by applying power optimization design goal

Freq.	Power			
	Static power consumptions at different FPGA's by applying *power optimization design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.043	1.298	0.323	0.169
2.4 GHz	0.043	1.306	0.328	0.176
3.6 GHz	0.043	1.312	0.333	0.182
5 GHz	0.043	1.320	0.342	0.190
5.9 GHz	0.044	1.325	0.351	0.195
60 GHz	0.058	1.606	0.491	0.219

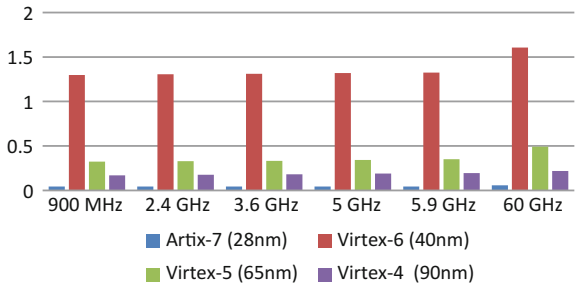


Fig. 4 Graph showing the static power consumptions at different FPGA's by applying power optimization design goal

3.4 *Static Power Consumptions at Different FPGA's by Applying* Minimum Runtime Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following static power consumptions are being observed as shown in Table 6.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **96.68%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **25.86%** of static power consumption can be reduced as shown in Fig. 5.

Table 6 Static power consumptions at different FPGA's by applying minimum runtime design goal

Freq.	Power			
	Static power consumptions at different FPGA's by applying *minimum runtime design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.043	1.298	0.328	0.172
2.4 GHz	0.043	1.307	0.328	0.181
3.6 GHz	0.043	1.314	0.333	0.189
5 GHz	0.043	1.322	0.343	0.199
5.9 GHz	0.044	1.327	0.352	0.206
60 GHz	0.060	1.607	0.491	0.222

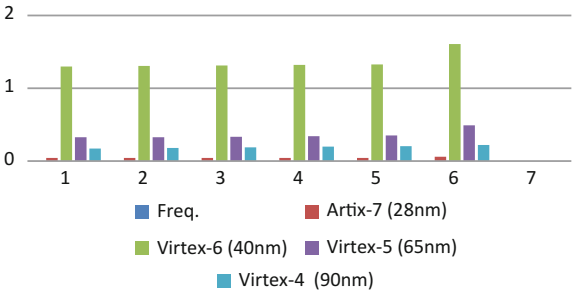


Fig. 5 Figure showing the static power consumptions at different FPGA's by applying minimum runtime design goal

3.5 *Static Power Consumptions at Different FPGA's by Applying* Timing Performance Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following static power consumptions are being observed as shown in Table 7.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **96.75%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **8.69%** of static power consumption can be reduced as shown in Fig. 6.

Table 7 Static power consumptions at different FPGA's by applying timing performance design goal

Freq.	Power			
	Static power consumptions at different FPGA's by applying *timing performance design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.042	1.294	0.321	0.167
2.4 GHz	0.043	1.297	0.322	0.168
3.6 GHz	0.043	1.299	0.324	0.169
5 GHz	0.043	1.301	0.329	0.171
5.9 GHz	0.046	1.303	0.335	0.171
60 GHz	0.046	1.401	0.491	0.216

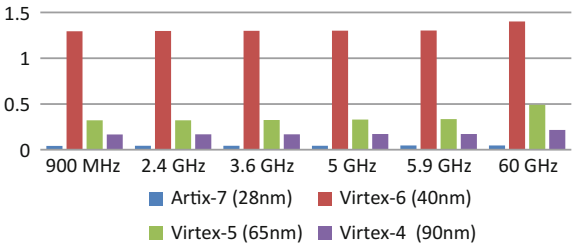


Fig. 6 Graph representing the static power consumptions at different FPGA's by applying timing performance design goal

4 Dynamic Power Analysis

4.1 Dynamic Power Consumptions at Different FPGA's by Applying Area Reduction Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following dynamic power consumptions are being observed as shown in Table 8.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **68.75%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **98.84%** of dynamic power consumption can be reduced as shown in Fig. 7.

Table 8 Dynamic power consumptions at different FPGA's by applying area reduction design goal

Freq.	Power			
	Dynamic power consumptions at different FPGA's by applying *area reduction design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.015	0.048	0.025	0.038
2.4 GHz	0.052	0.168	0.083	0.006
3.6 GHz	0.083	0.258	0.256	0.006
5 GHz	0.113	0.359	0.743	0.006
5.9 GHz	0.134	0.424	1.289	0.006
60 GHz	1.300	4.276	1979.146	0.008

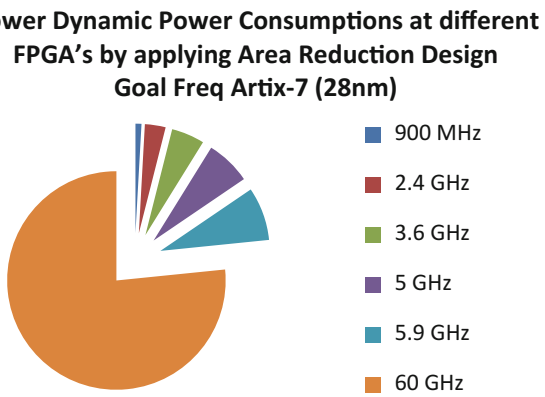


Fig. 7 Graph showing the dynamic power consumptions at different FPGA's by applying area reduction design goal

4.2 *Dynamic Power Consumptions at Different FPGA's by Applying* Balanced Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following dynamic power consumptions are being observed as shown in Table 9.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **7.877%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **99.88%** of dynamic power consumption can be reduced as shown in Fig. 8.

Table 9 Dynamic power consumptions at different FPGA's by applying balanced design goal

Freq.	Power			
	Dynamic power consumptions at different FPGA's by applying *balanced design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.006	0.284	0.253	0.252
2.4 GHz	0.203	0.615	0.688	0.666
3.6 GHz	0.302	0.920	1.164	0.996
5 GHz	0.420	1.28	2.002	1.381
5.9 GHz	0.494	1.51	2.773	1.627
60 GHz	5.025	15.287	1993.34	16.155

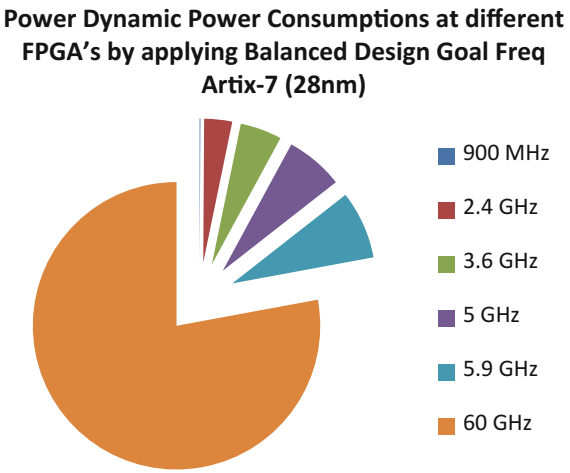


Fig. 8 Graph showing the dynamic power consumptions at different FPGA's by applying balanced design goal

4.3 *Dynamic Power Consumptions at Different FPGA's by Applying* Power Optimization Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following dynamic power consumptions are being observed as shown in Table 10.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **67.28%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **98.48%** of dynamic power consumption can be reduced as shown in Fig. 9.

Table 10 Dynamic power consumptions at different FPGA's by applying power optimization design goal

Freq.	Power			
	Dynamic power consumptions at different FPGA's by applying *power optimization design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.070	0.214	0.234	0.217
2.4 GHz	0.187	0.573	0.637	0.556
3.6 GHz	0.280	0.859	1.088	0.832
5 GHz	0.389	1.193	1.900	1.153
5.9 GHz	0.458	1.407	2.654	1.360
60 GHz	4.606	14.245	1993.055	13.501

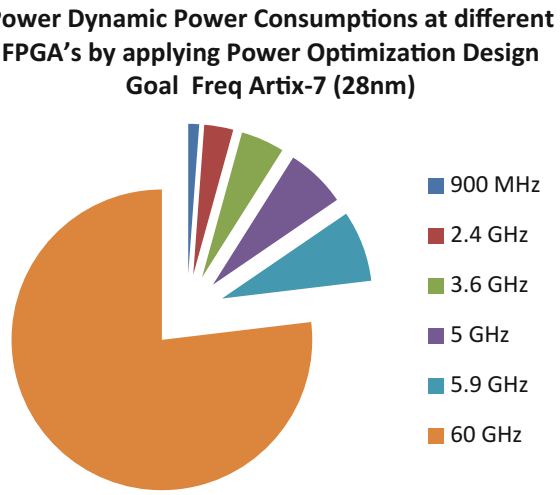


Fig. 9 Graph showing the dynamic power consumptions at different FPGA's by applying power optimization design goal

4.4 *Dynamic Power Consumptions at Different FPGA's by Applying* Minimum Runtime Design Goal

When the circuit is being operated at different frequencies and different FPGA technologies, following dynamic power consumptions are being observed as shown in Table 11.

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **64.01%** of power consumption can be saved if we will choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **98.48%** of dynamic power consumption can be reduced as shown in Fig. 10.

Table 11 Dynamic power consumptions at different FPGA's by applying minimum runtime design goal

Freq.	Power			
	Dynamic power consumptions at different FPGA's by applying *minimum runtime design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.070	0.231	0.688	0.257
2.4 GHz	0.203	0.614	0.688	0.668
3.6 GHz	0.302	0.920	1.163	1.000
5 GHz	0.420	1.280	2.002	1.387
5.9 GHz	0.494	1.511	2.773	1.635
60 GHz	5.029	15.287	1993.8	16.235

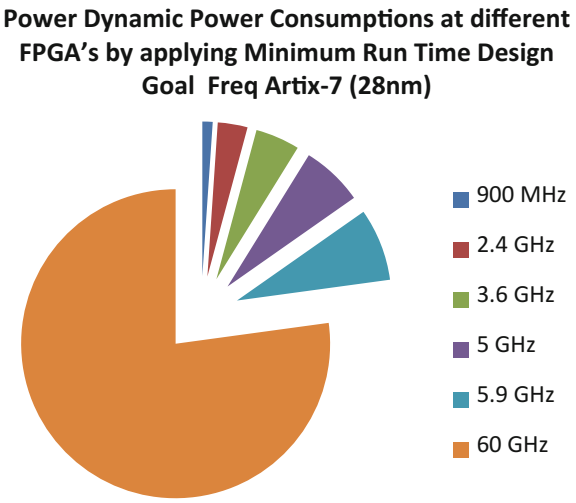


Fig. 10 Figure showing the dynamic power consumptions at different FPGA's by applying minimum runtime design goal

4.5 *Dynamic Power Consumptions at Different FPGA's by Applying* Timing Performance Design Goal

It has been observed that maximum power has been consumed in case of Virtex-6 (40 nm) FPGA technology and minimum power is being consumed at Artix-7 FPGA technology. Hence, **64.70%** of power consumption can be saved if we choose 28 nm FPGA technology instead of 40 nm technology at a frequency of 900 MHz as shown in the graph below. Furthermore, if we lower down our frequency from 60 GHz to 900 MHz, **98.71%** of dynamic power consumption can be reduced as shown in Fig. 11 (Table 12).

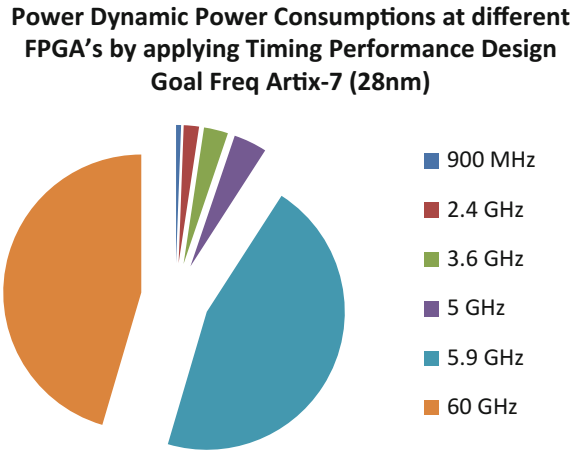


Fig. 11 Graph representing the dynamic power consumptions at different FPGA's by applying timing performance design goal

Table 12 Dynamic power consumptions at different FPGA's by applying timing performance design goal

Freq.	Power			
	Dynamic power consumptions at different FPGA's by applying *timing performance design goal*			
	Artix-7 (28 nm)	Virtex-6 (40 nm)	Virtex-5 (65 nm)	Virtex-4 (90 nm)
900 MHz	0.018	0.051	0.032	0.041
2.4 GHz	0.055	0.170	0.095	0.103
3.6 GHz	0.087	0.272	0.274	0.151
5 GHz	0.120	0.377	0.770	0.206
5.9 GHz	1.396	0.444	1.322	0.242
60 GHz	1.396	4.485	2517.604	1.992

5 Conclusion

In case of static power, if we move from 40 nm technology to 28 nm technology, then maximum power consumption savage of 96.75% is being done in the case of two design goals which are area reduction design goal and timing performance design goal. Wherein case of frequency, if we decrease lower range from 60 GHz to 900 MHz, then maximum power savage of 28.33% occurs in case of power optimization design goal.

In case of dynamic power, if we move from 40 nm technology to 28 nm technology, then maximum power consumption savage of 68.75% is being done in the case of area reduction design goal. Wherein case of frequency, if we decrease lower range from 60 GHz to 900 MHz, then maximum power savage of 99.88% occurs in case of balanced design goal.

6 Future Scope

As per the practical view, a 40 nm Virtex-6 and 28 nm Artix-7 FPGA used on Xilinx's 28 nm Artix-7, Altera's Stratix FPGA, ECP, XP, SCP/M series FPGA of Lattice, ABAX FPGA of Tabula, FPLIC series FPGA of Atmel, etc., can be used to redesign this Fibonacci generator. This approach can be extended to different hardware like router, gateway, and other devices which are especially required for communication purpose. Many other energy-efficient techniques like thermal scaling, heat sink, air flow can also be applied to make the device more energy and power efficient.

References

1. Liu, L., Stimpson, T., Antonopoulos, N., Ding, Z., Zhan, Y.: An investigation of security trends in personal wireless networks. Wireless Pers. Commun. **75**(3), 1669–1687 (2014)
2. Nykolaychuk, Y.M., Shevchyuk, B.M., Voronych, A.R., Zavediuk, T.O., Gladyuk, V.M.: Theory of reliable and secure data transmission in sensory and local area networks. Cybern. Syst. Anal. **50**(2), 304–315 (2014)
3. Cunche, M.: I know your MAC address: targeted tracking of individual using Wi-Fi. J. Comput. Virol. Hacking Tech. doi:10.1007/s11416-013-0196-1, ISSN: 2263-8733 [Springer Paris] (2013)
4. Alabrah, A., Cashion, J., Bassiouni, M.: Enhancing security of cookie-based sessions in mobile networks using sparse caching. Int. J. Inf. Secur. (2013). doi:10.1007/s10207-013-0223-8
5. Singh, S., Jain, A., Kaur, A., Pandey, B.: Thermal aware low power universal asynchronous receiver transmitter design on FPGA. In: IEEE 6th International Conference on Computational Intelligence and Communication Networks (CICN), Udaipur, 14–16 Nov 2014
6. Kaur, A., Singh, S., Pandey, B., Kaur, R.: Clock gating based low power efficienct Universal Gurmukhi Unicoder design on FPGA. International Symposium ICTT 2014, CHITKARA UNIVERSITY; 11/2014
7. Singh, S., Kaur, A., Pandey, B.: Energy efficient flip flop design using voltage scaling on FPGA. In: IEEE Sixth India International Conference on Power Electronics (IICPE), NIT Kurukshetra, 8–10 Dec 2014
8. Singla, A., Kaur, A., Pandey, B.: LVCMOS based energy efficient solar charge sensor design on FPGA. In: IEEE Sixth India International Conference on Power Electronics (IICPE), NIT Kurukshetra, 8–10 Dec 2014
9. Das, T., et al.: Low power Devnagari unicode checker design using CGVS approach. In: International Conference on Recent Advances in Mechanical Engineering and Interdisciplinary Developments (ICRAMID), Kanyakumari, India, 07–08 Mar 2014 (Upgraded to AMR Journal)
10. Kaur, A., et al.: Thermal aware energy efficient Gurmukhi unicode reader for natural language. In: IEEE Conference on 9th INDIACom, 11th–13th Mar 2015
11. Kaur, A., et al.: Capacitance scaling based Gurmukhi unicode reader design for natural language processing. In: IEEE Conference on 9th INDIACom, 11th–13th Mar

NS-2-Based Analysis of Stream Control and Datagram Congestion Control with Traditional Transmission Control Protocol

Rashmi Rajput and Gurpreet Singh

Abstract Internet applications like multimedia are comprised of a large amount of data traffic, and its transmission is increasing continuously due to the growth of Internet. The quality of different applications depends on network conditions and transport protocol. Quality of services needed by today's Internet applications cannot be fulfilled by the traditional transport protocol like transmission control protocol (TCP) therefore other transport protocols like SCTP and DCCP with advanced features were developed. This paper considered three transport layer protocols they are transport control protocol (TCP), datagram congestion control protocol (DCCP), and stream control transport protocol (SCTP). The analysis of these transport layer protocols is done on the basis of average throughput, number of packets sent, average jitter, delivery ratio, average delay, number of packets lost using NS-2. NS-2 provides virtual environment for simulation. Simulation result shows that DCCP achieves higher throughput with less jitter and less delay. However according to our simulation analysis, it is found that more number of packets is dropped in DCCP protocol than other two protocols. But DCCP overcomes its competitor protocols from all other parameters.

Keywords Congestion control · TCP · DCCP · SCTP · Multi-streaming Multi-homing

R. Rajput (✉)
Electronics & Communication Engineering, Yamuna Institute of Engineering & Technology, Gadholi, Yamunanagar, Haryana, India
e-mail: rashmirajput17@gmail.com

G. Singh
Computer Science & Engineering, Yamuna Institute of Engineering & Technology, Gadholi, Yamunanagar, Haryana, India
e-mail: gps_ynr@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_31

1 Introduction

With the introduction of new access technologies, the need for multimedia applications in the networks is rising day by day. During transportation, these multimedia applications are required to meet the quality of service requirements and better utilization of bandwidth [1]. Transport layer protocol is the most important factor which can affect the QoS of media applications [2]. The transport layer protocol TCP is mainly considered for the transportation of multimedia data, as it gives fast transmission of data and multimedia applications cannot tolerate any delay. TCP provides reliability and connection orientation with three-way hand-shaking. The only problem in TCP is it provides congestion control with more delay which is intolerant in multimedia applications. In order to overcome these problems, for the transportation of multimedia applications, DCCP is used. DCCP is an unreliable transport layer protocol which provides better congestion control in the network. It has support for explicit congestion notification (ECN) which provides notification of end-to-end network congestion [3]. SCTP is another transport layer protocol which provides reliability and congestion control in the network with many other features. It is connection-oriented protocol that provides ordered data delivery with no error in data. SCTP also provides features like multi-homing and multi-streaming. In multi-homing, to increase reliability of a network connection, additional alternative network interfaces or IP addresses are provided. SCTP also supports multi-streaming feature in which the data is sent in streams. Both multi-homing and multi-streaming are helpful for better transmission of data [3].

1.1 Transport Layer Protocols

Transmission Control Protocol (TCP):

Transmission control protocol (TCP) is a criterion used in Internet applications that defines procedure for establishment and maintenance of network conversation to exchange data.TCP gives information about the transmission of packets of data between two computers. TCP needs a connection to be established between source and destination and this connection is maintained until packets have been exchanged. TCP is stream-oriented protocol which allows sending process to deliver and receive data as stream of bytes. It provides error-free data transmission and congestion control with some delay. TCP also handles flow control by using sliding window on each connection. In the open systems interconnection model, TCP covers parts of transport layer and session layer [2]. There are a number of variants of TCP to control congestion which are given as below:

TCP Reno: TCP Reno will halve the congestion window if triple duplicate ACKs are received, perform a fast retransmission, and enter fast recovery [4].

TCP New Reno: TCP New Reno improves the TCP Reno's performance with modified fast recovery algorithm, when a burst of packets is lost [4].

TCP Sack: In this, when there is packet loss at receiver the receiver sends an ACK packet which includes the list of up to four ranges of sequence no. of packets. This sequence shows the no. of packets which have been successfully received, and the gap between two ranges is used by the transmitter to decide which packet is lost and should be retransmitted. TCP sack and TCP Reno differ by the ways through which multiple packets are dropped from window [4].

TCP Vegas: TCP Vegas detects congestion at an early stage unlike TCP Reno, New Reno, etc. It stress on packet delay, i.e., the rate at which the packets are sent and works on the basis of increasing round-trip time (RTT) values. The algorithm depends heavily on accurate calculation of the base RTT value [4].

Datagram Congestion Control Protocol (DCCP):

The datagram congestion control protocol (DCCP) is an unreliable transport protocol which is used for real-time applications in which delay is intolerable which is somewhat similar to UDP. DCCP is suitable for applications which demand timeliness to reliability, and also it provide unordered delivery of data as reordering leads to more delay [4]. DCCP is a new transport protocol that provides an unreliable transmission with congestion control and applicable to applications like streaming media [3]. DCCP has been designed with the best features of both UDP and TCP and additional feature of congestion control with less delay. DCCP is a congestion control protocol instead of flow control protocol. DCCP does not make use of flow control because flow control affects the transfer rate. The flow control is optional in DCCP, and if it is required to have flow control, then it is implemented on top of DCCP. DCCP has two types of congestion control mechanism like DCCP-TCP and DCCP-TFRC which are two such standard mechanisms.

DCCP-TCP-like congestion control mechanism (CCID 2) is similar to TCP as it has an algorithm that controls the congestion by tracking a transmission window. After tracking, it regulates the transmission rate [5]. DCCP-TFRC congestion control (CCID 3) has an algorithm which controls congestion by tracking packet loss rate and varying the transmission rate in a smoother manner using additive increase multiplicative decrease (AIMD). It is suitable for application which needs to transfer more data at a time [5].

Stream Control Transmission Protocol (SCTP):

SCTP is a reliable and connection-oriented transport protocol. It supports four-way hand-shaking during initialization and provides ordered delivery of data with flow control as well as congestion control. It also supports other features like full duplex data transfer, data fragmentation, multi-streaming, network-level fault tolerance through supporting of multi-homing at either or both ends of an association, check-summing, packet validation services to the user. It offers flow control similar

to TCP, and for acknowledgement, it uses selective acknowledgement mechanism. The design of SCTP includes appropriate congestion avoidance behavior and resistance to flooding and masquerade attacks [6].

SCTP also supports multi-homing. In multi-homing, to increase reliability of a network connection, additional alternative network interfaces or IP addresses are provided. During transmission, routing table of the host decides the source interface. Multi-homing is a salient feature of voice communication [7]. SCTP supports multi-streaming unlike TCP which support single data stream per connection. In multi-streaming, data are sent in streams, i.e., parallel transmission of data from source to destination. If a packet of particular stream is lost then the lost data are stored in buffer until it is retransmitted from transmitter. If one stream has error, entire transmission will not be delayed as multi-streaming gives error-free transmission [8].

2 Simulation Result and Analysis

In this section, we shall compare the performances of various transport layer protocols such as TCP, DCCP, SCTP using NS-2 [9–12]. There are many network simulators available in the market [13–16]. We choose NS-2 because this simulator is used by maximum researchers for their work. Moreover, NS-2 is an open source software, the code of which can be easily modified and can understand at any stage according to the needs and requirements of the researchers. It is also cost effective and consumes less time while changing the existing protocols in a controlled and reproducible manner. To estimate the performance of these protocols, a number of simulation experiments were run using NS-2 over a small network as shown in

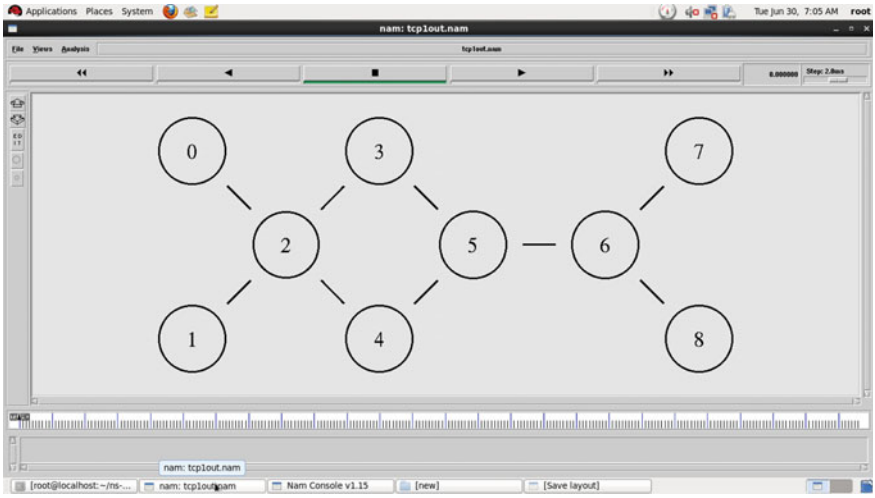


Fig. 1 Simulated topology

Table 1 Parameter comparison table

Parameters	Different transport layer protocols		
	TCP	DCCP	SCTP
Average throughput	7072.2035	9452.3567	3907.887
Number of packets sent	60,314	80,587	33,344
Number of packets dropped	27	126	72
Delivery ratio	99.95523	99.84364	99.78406
Average end-to-end delay	0.05952	0.03642	0.08693
Average jitter	0.064972	0.0148286	0.060727

Fig. 1 with a number of input nodes. The main parameters that are taken into consideration are average throughput, number of packets lost, number of packets sent, average end-to-end delay, delivery ratio, and average jitter. For all the three protocols, nine nodes were used and two-source two-destinations were taken into consideration first from source node 0 to sink node 7 and other from source node 1 to sink node 8.

In this paper, we considered the different parameters for comparing various protocols such as average throughput, number of packets lost, delivery ratio, delay, and jitter. We have conducted experiments on the given topology in this paper and analyzed the results on the basis of selected parameters. The values generated in the experiment are given below in the tabular form as shown in Table 1.

Average Throughput (bits per second): It is an output relative to input. It is also defined as an amount of data passing through a system from input to output over a period of time. A better congestion control algorithm results in the delivery of good number of packets with respect to time always. However, we have calculated it in packets per second.

$$\text{Average Throughput} = \text{Total number of packets received/Total Time}$$

The total time is the difference between last packet sent and first packet sent time.

Figure 2 shows that DCCP has higher output as compared to SCTP and TCP. SCTP gives least throughput.

(a) Number of packets sent: The total number of packets sent over a period of time helps in measuring the efficiency of the particular algorithm.

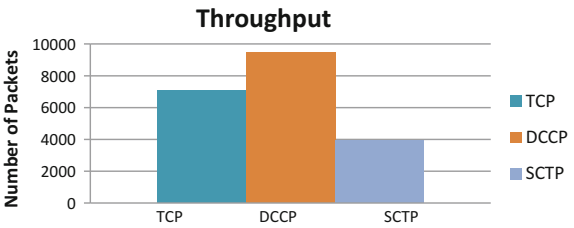


Fig. 2 Throughput

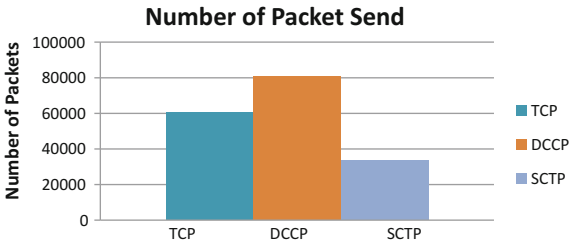


Fig. 3 Number of packets sent

Figure 3 shows the number of packets sent for communication of data. It shows that data rate of DCCP is better than others.

(b) Number of packets dropped: Packet drop is defined as the total number of packets lost during the transmission of packet from source to sink. It can be calculated by measuring the difference between total number of packets transmitted and received. Due to congestion, data packets are dropped during transmission. The amount of these packets dropped should be maintained low.

$$\text{Packet Dropped} = \text{Packets transmitted} - \text{Packets received}$$

Figure 4 shows the number of packets lost during the transmission. It shows that DCCP has maximum number of packets dropped and TCP has lowest loss.

(c) Delivery ratio: It is the ratio of total packets sent by the source to the total packets received by the destination. It is measured in percentage.

$$\text{Delivery Ratio} = \text{Total data packet delivered successfully} \times 100/\text{data packet generated}$$

Figure 5 shows that SCTP has minimum delivery ratio than both TCP and DCCP, whereas TCP has highest delivery ratio.

(d) Average Jitter: Time difference between two consecutive delays is called jitter. It is caused by network congestion, timing drift, or route changes. It must be as low as possible for an efficient protocol.

$$\text{Jitter} = \text{Delay}(A) - \text{Delay}(B)$$

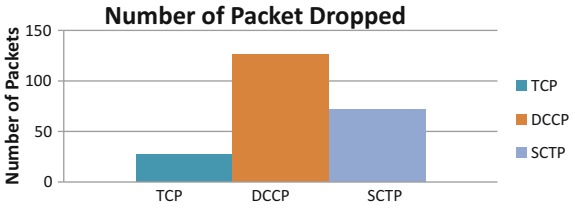


Fig. 4 Number of packets dropped

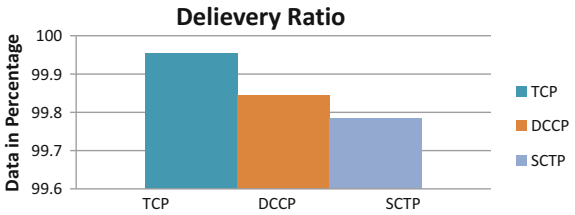


Fig. 5 Delivery ratio

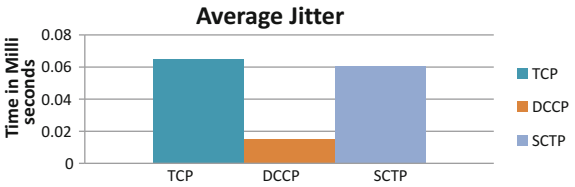


Fig. 6 Average jitter

where Delay (A) = delay of a current packet and Delay (B) = delay of a previous packet.

Figure 6 shows that DCCP has minimum jitter which is less than 0.02 ms and TCP has maximum. So DCCP is better than both SCTP and TCP on the basis of jitter.

(e) Average Delay: It is the total time taken by a packet to transmit from one node to other node. Minimum delay should be provided by any protocol. For measuring delay, the difference of sending time and receiving time of a packet is considered.

$$\text{Delay} = \text{Packet receive time} - \text{Packet send time}$$

Figure 7 shows that DCCP has minimum delay as compared to others therefore again on the basis of average delay DCCP is better than other two protocols.

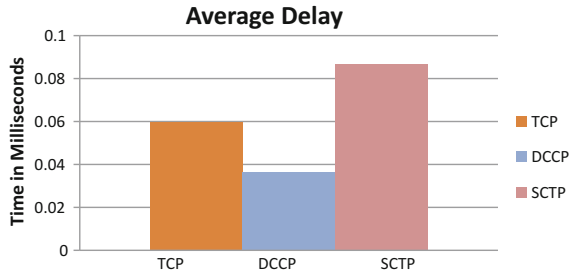


Fig. 7 Average delay

3 Conclusion

In this research paper, performance of TCP, DCCP, and SCTP is evaluated. Different performance metrics such as throughput, number of packets send, packet loss, delivery ratio, delay, and jitter are used for evaluating the performance of these protocols. Most of the times, DCCP works better than TCP and SCTP. On the basis of throughput, number of packets sent, average delay and average jitter, DCCP gives better performance. However TCP has least packet drop and so has highest delivery ratio. But, after comparing three protocols, TCP, DCCP, and SCTP on all the six parameters, it can be stated that DCCP can deliver better QoS in terms of the number of packets sent, jitter, delay, and throughput. Thus, it can be used for efficient transportation of data in different applications.

In future work, DCCP and SCTP protocols can be applied in many fields in which TCP is not much efficient such as heterogeneous network of wired and wireless networks while maintaining all the essential requirements like congestion control and reliability during the transmission.

References

1. Sharma, S., Singh, M., Singh, G.: Swarm intelligence based comparative scrutiny of different routing algorithms in MANETs. Int. J. Res. Eng. Appl. Sci. **2**(2), 1818–1831 (2012)
2. Postel, J.: Transmission Control Protocol:RFC 793 (1981)
3. Zikria: Video transport over heterogeneous networks using SCTP and DCCP. In: IEEE, vol. 20, pp. 180–190 (2009)
4. Rajput, R., Singh, G.: Comparing stream control and datagram congestion control with traditional transmission control protocol. Int. J. Comput. Sci. Mobile Comput. (IJCSMC) **4**(6), 570–577 (2015)
5. Floyd, S., Kohler, E.: Profile for datagram congestion control protocol (DCCP) congestion control ID 2: TCP-like congestion control, RFC 4341 (2006)
6. Khalid, M.N.: Simulation based comparison of SCTP, DCCP and UDP using MPEG-4 traffic (2010)
7. Boussen, S., Tabbane, N., Tabbane, S.: Performance analysis of SCTP protocol in WiFi network. In: 4th IEEE International Conference on Computer Sciences and Convergence Information Technology, pp. 178–182 (2009)
8. Brak, M.E.L., Brak, S.E.L.: Performance evaluation of SCTP protocol for smart grid environment. Int. J. Comput. Netw. Wireless Commun. (IJCNWC), 4(3). ISSN: 2250-3501 (2014)
9. Stevens, W.: TCP/IP Illustrated, vol. 1: The Protocols. Addison-Wesley (1994)
10. Afzal, M.K., Aman-Ullah-Khan, Pescape, A., Zikria, Y., Loreto, S.: SCTP vs. TCP delay and packet loss. In: IEEE International Multitopic Conference, pp. 1–5 (2007)
11. Bhatla, N., Kaur, A., Singh, G.: Relative inspection of Reno, New Reno, Sack, Vegas in AODV. Int. J. Res. Eng. Appl. Sci. (IJREAS) **4**(5) (2014)
12. Batla, N., Kaur, A., Singh, G.: Congestion control techniques in TCP: a critique. In: The Proceedings of 3rd National Conference of Advances and Research in Technology (ART-2014), pp. 45.1–45.5, 8–9 (2014)

13. Budzisz, Ł.: Stream control transmission protocol (SCTP): a proposal for seamless handover management at the transport layer in heterogeneous wireless network. PhD Thesis, Universitat Politècnica de Catalunya (2009)
14. Kamboj, R., Singh, G.: Various TCP options for congestion evasion. Int. J. Adv. Res. Comput. Eng. Technol. **4**(4), 1534–1539 (2015)
15. Chowdhury, I.S., Lahiry, J., Rahman, K.C., Hasan, S.F.: Performance analysis of datagram congestion control protocol (DCCP). Int. J. Comput. Theory Eng. **3**(5), 632–637 (2011)
16. Chellaprabha, B.: Performance of datagram congestion control protocol DCCP-TCP-like and DCCP-TFRC on sensor network. Int. J. Comput. Netw. Wireless Commun. (IJCNWC) **2**(2), 255–261 (2012)

Wireless Power Transfer Using Microwaves

Nitin Sharma, Tarun Bheda, Richa Chaudhary, Mohit and Shabana Urooj

Abstract In this paper, a model has been presented which transfers electric power without wires by using microwaves. A breadboard model of receiving antenna called rectenna is developed for preliminary experiments including wireless power transmission. The paper presents one to one MPT system in which electric power is transferred at radio frequencies ranging GHz so that the losses can be reduced which generally occurs during transmission and distribution of electrical power.

Keywords Wireless power transmission · Microwaves · Rectenna

1 Introduction

Transmission and distribution losses are always a key problem to power engineers. The main cause of this loss is resistance of wires. The power loss associated with transmission and distribution is approximated around 26%. According to the World Resources Institute (WRI), India's electricity grid has the highest transmission and distribution losses in the world [1]. Using high-graded conductors and cables can improve the transmission efficiency, but it would become costly too. Therefore, in this paper, we present a more effective, efficient, and low cost method of power

N. Sharma (✉) · T. Bheda · R. Chaudhary · Mohit · S. Urooj
School of Engineering, Gautam Buddha University, Greater Noida, India
e-mail: nitin.0361@gmail.com

T. Bheda
e-mail: tarunbheda@gmail.com

R. Chaudhary
e-mail: richachaudhary2106@gmail.com

Mohit
e-mail: mohit2661@gmail.com

S. Urooj
e-mail: shabanabilal@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_32

transfer. Transmission of electricity without wires has always been an attractive theme of interest from several past decades. Many prodigious researches have been practicing on this area to enhance the aspect of conventional transfer of electricity. Nikola Tesla was first to perform experiments in wireless power transmission and hence called "Father of Wireless." In early 90s, he has developed a spark-excited radio frequency resonant transformer now called Tesla coils by which he was able to transfer electricity without wires by inductive and capacitive coupling. Figure 1 shows Wardenclyffe tower designed by Tesla to transmit electricity over long distances wirelessly. The discovery of high power microwave emitters called magnetron has driven the idea of WPT technology to new dimensions. William C. Brown is known as the first person who achieved long distance wireless power transmission in 1960. In 1961, he published the first paper which proposes to use microwaves for transmission of power, and in 1964, he established a model of microwave-powered helicopter that gets power from microwave beam at 2.45 GHz [2].

At Goldstone in California in 1975 and at Grand Basin on Reunion Island in 1997, power ranging tens of kilowatts were transferred without wires [3]. Japan was the first to perform MPT experiment in ionosphere, a rocket named microwave

Fig. 1 Wardenclyffe tower

ionosphere non-linear interaction experiment (MINIX) is validated by experiment in 1983 [4]. Likewise, the Stationary High Altitude Relay Platform (SHARP) is the world's first fuel-free aircraft driven by microwave energy from ground which was testified in 1987 at Canada [5]. Also, Dryden Flight Research Centre of NASA recognized a laser-powered model airplane indoors in 2003. In 2004, Japan anticipated wireless charging of electric motor automobiles by microwave power transmission.

2 Materials and Method

It mainly involves a microwave source (magnetron 2.45 GHz), an antenna for transmission, and an antenna at the receiving end, also called rectenna. In this model, a 2.45 GHz magnetron is used as a microwave source, and the other choices are klystron, semiconductor microwave transmitters (GaAs MESFET, SiC MESFET, AlGaN/GaN HFET), microwave power module (MPM), and traveling wave tube (TWT). Rectangular microstrip patch antenna is used due to simplicity and low cost. According to recent researches, a slotted waveguide antenna is epitome to use for this purpose because of its high aperture efficiency approximated at 95% [6]. Ge 1N34 diodes are used to make rectenna model, these diodes have a very low forward voltage when connected in series and are able to convert RF power to DC [7]. Figure 2 shows the purposeful block diagram of wireless power transmission system.

Table 1 shows the efficiency of rectenna at different frequencies using various diodes one by one and calculating results according to observations obtained.

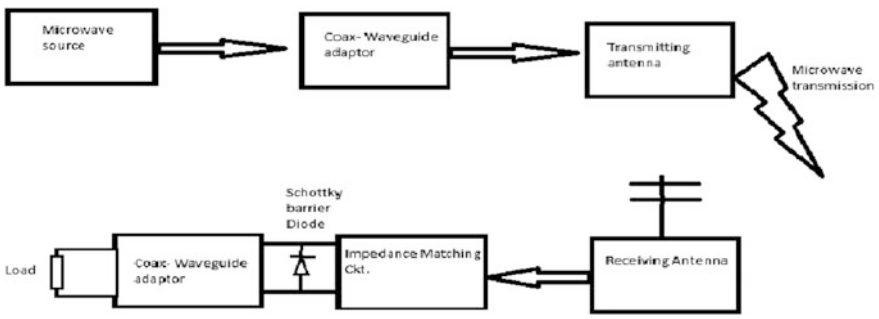


Fig. 2. Block diagram of wireless 58 power transmission system

Table 1 Efficiency of rectenna at different frequencies

Frequency (GHz)	Diode used	Measured efficiency (%)	Calculated efficiency (%)
2.45 [7]	GaAs-W	92.5	90.5
5.8 [8]	Si	82	78.3
8.51 [9]	GaAs	62.5	66.2

Table 2 Rectenna demonstration at operating frequency 2.4 GHz

Distance (m)	Output voltage, mV (DC)	Output rectenna current, mA (DC)
1	2.335	0.379
2	2.281	0.292
3	2.165	0.206
4	1.924	0.140

3 Results and Discussion

Five Ge 1N34 diodes are connected to build a demonstration model of rectenna. Table 2 shows the results obtained at operating frequency of 2.45 GHz.

The most scorching problem was to design a most efficient rectenna [8, 10, 11]. It was the most tedious target to achieve. The rectenna designed in this paper is made by using Ge 1N34 diodes. The amount of power transmitted using this rectenna was quite high and better than power transmitted by using any other method [12, 13]. Using this rectenna model, we succeeded to transmit electricity without wires up to four meters [9]. Earlier the use of microwave, for transmission electricity, was considered biologically hazardous, but now it has been proven that microwave have same amount of biological impact as much a household microwave oven [6].

4 Conclusion and Future Prospect

With the improvement in type of rectenna used and source of microwave, transmission of electricity, wirelessly and economically, has finally become a trance come true. The amount of power transmitted reported here in this paper could be enhanced by using more number of Ge 1N34 diodes and using additional circuit periphery like filters, amplifiers, and power electronic circuits. Using microwave to transmit power is the most efficient way than any other method used in present world. With the potential scope of such type of research can change the face of electrical engineering.

References

1. Tesla, N.: My inventions. In: Johnston, B. (ed.) Hart Brothers, Austin, p. 91 (1982). http://cleantechindia.wordpress.com/2008/07/16/indiaselectricity-transmission-and-distribution-losses
2. Brown, W.C., Mims, J.R., Heenan, N.I.: An experimental microwave-powered helicopter. 965 IEEE Int. Conv. Rec. **13**(5), 225–235
3. Lan Sun Luk, J.D., Celeste, A., Romanacce, P., Chane Kuang Sang, L., Gatina, J.C.: Point-to-point wireless power transportation in Reunion Island. In: 48th International Astronautical Congress, Turin, Italy, 6–10 Oct 1997, IAF-97-R.4.08, University of La Réunion, Faculty of Science and Technology
4. Matsumoto, H., Kaya, N., Kimura, I., Miyatake, S., Nagatomo, M., Obayashi, T.: MINIX project toward the solar power satellites—rocket experiment of microwave energy transmission and associated plasma physics in the ionosphere. In: ISAS Space Energy Symposium, pp. 69–76 (1986)
5. Schelesak, J.J., Alden, A., Ohno, T.: A microwave powered high altitude platform. IEEE MTT-S International Symposium Digest, pp. 283–286 (1988)
6. Venkateswara Reddy, M., Sai Hemanth, K., Venkat Mohan, C.H.: Microwave power transmission—a next generation power transmission system. IOSR J. Electr. Electron. Eng. (IOSRJEEE) **4**(5) 24–28. e-ISSN: 2278–1676 (2013)
7. Epp, L.W., Khan, A.R., Smith, H.K., Smith, R.P.: A compact dual-polarized 8.51-GHz rectenna for high-voltage (50 V) actuator applications. IEEE Trans. Microw. Theory Tech. **48**, 111–120 (2000)
8. Onda, M., Fujita, M., Fujino, Y., Kaya, N., Tomita, K., Yamada, M.: A stratospheric stationary LTA platform concept and ground-to-vehicle microwave power transmission tests. In: 37th AIAA Aerospace Sciences Meeting and Exhibit, Reno, NV, pp. 1–7 (1999)
9. Koert, P., Cha, J.T.: 35 GHz rectenna development. In: Proceedings of 1st Annual Wireless Power Transmission Conference, San Antonio, TX, pp. 457–466 (1993)
10. Satavekar, M.S.G.: Solar power satellites and microwave wireless power transmission technology. Adv. Electron. Electr. Eng. **4**(2), 193–200. ISSN 2231-1297 (2014)
11. Tesla, N.: The transmission of electrical energy without wires as a means for furthering peace. Electr. World Eng. **7**, 21 (1905)
12. "Good Bye Wires"… MIT News. 2007-06-07. http://web.mit.edu/newsoffice/2007/wireless-0607.html
13. Brown, W.C.: The history of power transmission by radio waves. IEEE Trans. Microw. Theory Tech. **32**(9), 1230–1242 (1984). ISSN: 0018-9480. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1132833

Performance Evaluation of AODV and DSR Routing Protocol on Varying Speed and Pause Time in Mobile Ad Hoc Networks

Anil Saini and Rajender Nath

Abstract MANET is an emerging approach to wireless communication with potential applications in random and dynamic environments. In MANET, there cannot be a central administrator due to mobile nodes and frequent breakage of links. Thus, routing in MANETs becomes a challenging job, and the motivation behind this paper is to discover and study the effect of pause time and mobility of nodes on Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector (AODV) routing protocols. Network Simulator version 2.35 has been used to perform the experiment.

Keywords AODV · DSR · End-to-end delay · MANET · PDR · Pause time Throughput

1 Introduction

Ad hoc wireless technology is an emerging approach to wireless communication with potential applications in random and dynamic environments. In contrast to cellular and infrastructure-based networks, it does not possess any fixed infrastructure or central administrator such as router. MANET is a set of independent system of mobile nodes that move freely and randomly. Its network topology is dynamic in nature and may change speedily and randomly. Due to this, the intercommunications among nodes keep on changing. MANET [1] depends on many other aspects including location of request initiator, topology of network, optimum selection of routers, and specific underlying features that could work on finding the path rapidly and efficiently. In MANETs, routing protocols are used to decide the

A. Saini (✉) · R. Nath
Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana, India
e-mail: saini.anil143@gmail.com

R. Nath
e-mail: rnath2k3@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_33

optimal route for packet transfer and make sure that the packets are reached to the desired destination. Several routing protocols for MANETs have been given, and their performance under different network situations and traffic constraints has been considered. Routing protocols are categorized as: proactive and reactive. Proactive-based routing protocols [2, 3] are also known as table-driven routing protocols. It maintains optimal routing information for each node in the network by spreading route update information at periodic intervals. Many proactive routing protocols have been proposed in the literature such as Wireless Routing Protocol (WRP), Destination-Sequenced Distance Vector (DSDV) routing protocol, Optimized Cluster-Head Gateway Routing (CGSR). Reactive-based routing [2, 4] protocols, also known as on-demand routing protocol, take a different method for routing as compared to proactive protocols. The advantage is that when a path is desired, it is immediately available which reduces the routing overheads. Various types of reactive-based routing protocols are as follows: Dynamic Source Routing (DSR) [5, 6], Ad hoc On-demand Distance Vector (AODV) [7, 8], and Temporally Ordered Routing Algorithm (TORA). Among these protocols, on-demand routing protocols are commonly used because they find routes in reactive fashion. AODV routing protocol uses are active approach to discover routes; it uses the destination sequence number to determine fresh path to the destination, which distinguishes it from other reactive-based routing protocols; it also uses a broadcast route discovery process to find a path to the target, and then, target node uses the unicast route reply massage to reply back to the source, whereas DSR is designed mainly to use in multi-hop mobile ad hoc networks.

This paper analyzes the AODV and DSR protocols for varying speed and pauses time by using performance evaluation metrics such as packet delivery ratio, throughput, and end-to-end delay.

The following sections are organized as follows: Sect. 2 discusses the related work. Section 3 presents the proposed work and simulation activity process for simulation scenarios. Section 4 discusses the simulation results. Section 5 presents the concluding remarks.

2 Related Work

There are numerous papers [6, 8–11] related to the performance evaluation of routing protocols in MANETs.

Lego et al. [6] compared the performance of DSR, DSDV, and AODV protocols on varying pause time. They found the value of PDR for AODV and DSR were almost equal when pause time was taken as 0, and it increased when pause time was increased.

Khattak et al. [8] analyzed various routing protocol by changing the mobility and density of nodes with TCP and UDP traffic. They show that all routing protocols did well under TCP traffic type, whereas PDR was less in case of UDP due to unreliable transmission.

Gupta et al. [9] compared the performance of AODV and DSR protocols considering three different scenarios by using network routing load, packet fraction rate, and end-to-end delay metrics. They found DSR started losing data packets when mobility of nodes and network resource were increased.

Lee [10] evaluated the performance of DSR and AODV routing protocols and found packet loss of DSR is more as compared to AODV for a less amount of time while it is almost equal to a greater amount of time. They further found DSR was more stable than AODV protocol due to absence of periodic packet broadcast and multiple paths.

Taksande et al. [11] studied DSR and AODV protocols by keeping network pause time and node speed as constant with changing network size. They concluded DSR protocol performs better for lesser no. of nodes as compared to AODV, whereas AODV protocol outperformed DSR protocol in terms of end-to-end delay.

3 Proposed Work

As discussed in the forgoing section, AODV and DSR protocols have not been studied for varying speed and pause time in MANETs [12–14]. Hence, this paper focuses on evaluating AODV and DSR protocols by changing both the speed and the pause time. For evaluation, following metrics are used: throughput, PDR, and end-to-end delay [15, 16]. Figure 1 shows the methodology of studying the performance of the protocols. A tcl script with wireless scenario and traffic pattern of mobile nodes is created, which is run on the network simulator. The outcomes of the simulation are trace file and the awk script, which are used for analysis.

The experiment is performed on NS2.35 by taking two scenarios, as shown in Tables 1 and 2. In Scenario 1, speed is kept constant and pause time is varied. In scenario 2, pause time is kept constant and speed is varied. The following three metrics are used to evaluate the performance of the proposed approach:

Throughput: Throughput is defined as the number of packets successfully transferred from one end to other per unit time [17].

$$\text{Throughput} = \frac{\text{No. of bytes recieved} \times 8}{\text{Simulation time} \times 1000}\text{Kbps} \tag{1}$$

Packet Delivery Ratio (PDR): It is the ratio of the received packets at the target node to the generated packets at the source node [18].

$$\text{PDR} = \frac{\text{No. of packet recieved}}{\text{No. of packet sent}} \times 100 \tag{2}$$

End-to-End Delay: It is average time required to transfer the data packets from source to destination [19].

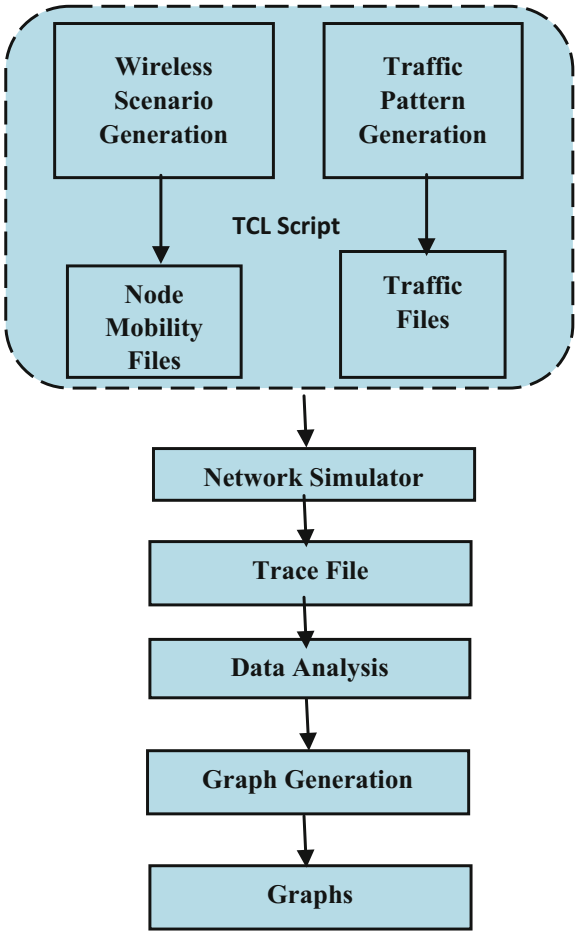


Fig. 1 Simulation activities

$$\text{End to End Delay} = \frac{\sum(\text{arrive time} - \text{send time})}{\sum \text{no. of connections}} \tag{3}$$

4 Simulation Results and Analysis

Tables 3 and 4 show the experimental values of end-to-end delay, throughput, and PDR for AODV and DSR protocols with varying speed of the nodes and constant pause time, i.e., 100 s. Tables 5 and 6 show the experimental values of end-to-end delay, throughput, and PDR for DSR and AODV protocols and varying pause time with constant speed, i.e., 2 m/s [20–22].

Table 1 Simulation scenario 1

Parameters	Values
Simulator	Ns 2.35
Media access control	802.11
Simulation period	500 s
Channel	Wireless channel
Protocols	AODV, DSR
Antenna model	Omnidirectional
Simulation range	670 m × 670 m
Traffic type	FTP
Radio propagation	TwoRay Ground
Interface queue type	DropTailPriQueue (AODV), CMUPriQueue (DSR)
No. of nodes	25
Speed	2 m/s
Pause time	0, 100, 200, 300, 400 (s)
No. of connections	8

Table 2 Simulation scenario 2

Parameters	Values
Simulator	Ns 2.35
Media access control	802.11
Simulation period	500 s
Channel	Wireless channel
Protocols	AODV, DSR
Antenna model	Omni
Simulation range	670 m × 670 m
Traffic type	FTP
Radio propagation	TwoRay Ground
Interface queue type	DropTailPriQueue (AODV), CMUPriQueue (DSR)
No. of nodes	25
Speed	1, 2, 5, 7, 10 (m/s)
Pause time	100 s
No. of connections	8

Table 3 AODV (TCP Agent) for 25 Nodes with 8 connections with constant pause time (100 s)

Pause time (s)	Speed (m/s)	End-to-end delay (s)	Throughput	PDR
100	1	0.52911	626543.65	99.12
	2	0.56479	614041.53	99.16
	5	0.49337	646147.81	98.99
	7	0.50525	628833.35	98.96
	10	0.48529	664151.94	98.61

Table 4 DSR (TCP agent) for 25 nodes with 8 connections with constant pause time (100 s)

Pause time (s)	Speed (m/s)	End-to-end delay (s)	Throughput	PDR
100	1	0.79886	642652.09	99.60
	2	0.77235	657537.17	99.64
	5	0.84206	641226.70	99.56
	7	0.93346	615488.76	99.52
	10	0.80645	642658.09	99.57

Table 5 AODV (TCP Agent) for 25 nodes with 8 connections with constant speed (2 m/s)

Speed (m/s)	Pause time (s)	End-to-end delay (s)	Throughput	PDR
2	0	0.58293	560884.56	99.31
	100	0.56479	614041.53	99.16
	200	0.46952	615804.76	99.11
	300	0.45677	632733.06	99.05
	400	0.50547	620460.62	98.74

Table 6 DSR (TCP Agent) for 25 nodes with 8 connections with constant speed (2 m/s)

Speed (m/s)	Pause time (s)	End-to-end delay (s)	Throughput	PDR
2	0	0.84075	652952.68	99.37
	100	0.77235	657537.17	99.64
	200	0.71514	650040.38	99.48
	300	0.75970	629148.62	99.69
	400	0.68679	628442.59	98.78

Figure 2 shows the throughput of DSR and AODV protocols with constant number of nodes, i.e., 25, constant pause time, i.e., 100 s, and varying speed (from 1 to 10 m/s), which is indicated on *x*-axis. The results show that in "low-speed"

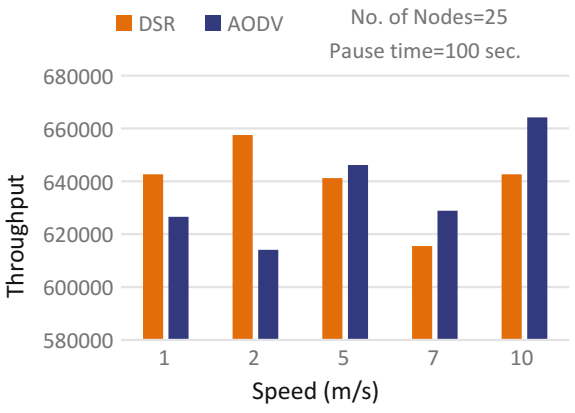


Fig. 2 Throughput versus speed (m/s) with constant pause time (100 s)

situation, DSR protocol outperforms AODV but in "high-speed" situation AODV outperforms DSR protocol.

Figure 3 shows the throughput of DSR and AODV protocols with constant number of nodes, i.e., 25, constant speed, i.e., 2 m/s, and varying pause time (from 0 to 400 s), which is indicated on x-axis. The results show that in the beginning and intermediate phase, DSR protocol outperforms AODV in "low-mobility" situation. On the other hand, in "high-mobility" situation, both AODV and DSR protocols give similar throughput value [23–25].

Figure 4 shows the PDR of DSR and AODV protocols with constant number of nodes, i.e., 25, constant pause time, i.e., 100 s, and varying speed (from 1 to 10 m/s), which is indicated on *x*-axis. The result shows that in both AODV and DSR Protocols when the speed of the node is increased, the PDR gets decreased. But in low-to-high mobility situation, DSR protocol gives better result as compared to AODV Protocol.

Figure 5 shows the PDR of DSR and AODV protocols with constant number of nodes, i.e., 25, constant speed, i.e., 2 m/s, and varying pause time (from 0 to 400 s), which is indicated on *x*-axis. In this scenario, it is observed that the DSR protocol gives better result than AODV in all situations.

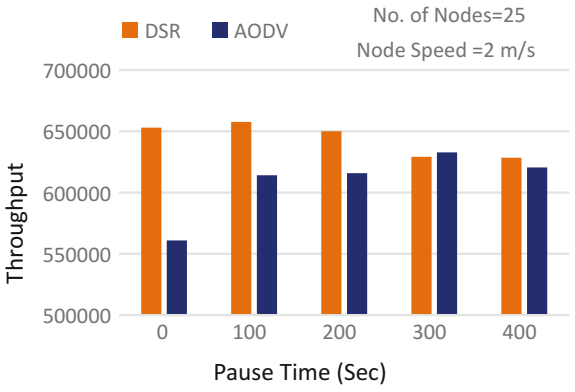


Fig. 3 Pause time (s) versus throughput with constant speed (2 m/s)

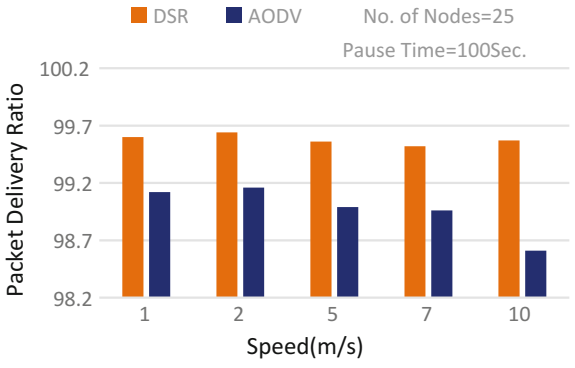


Fig. 4 Speed (m/s) versus PDR with constant pause time (100 s)

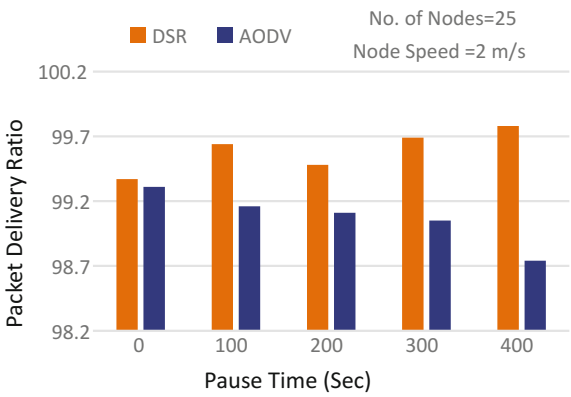


Fig. 5 Pause time (s) versus PDR with constant speed (2 m/s)

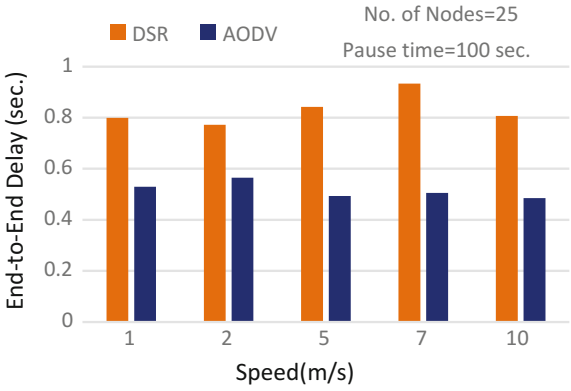


Fig. 6 Speed (m/s) versus end-to-end delay (s) with constant Pause Time (100 s)

Figure 6 shows the end-to-end delay of DSR and AODV protocols with constant number of nodes, i.e., 25, constant pause time, i.e., 100 s, and varying speed (from 1 to 10 m/s), which is indicated on *x*-axis. The result shows that in AODV protocol, when the speed of the node is increased the end-to-end delay gets decreased, but in DSR protocol, the delay is increased when the speed of the node is increased. So DSR has comparatively high delay than AODV in all situations.

Figure 7 shows the end-to-end delay of DSR and AODV protocols with constant number of nodes, i.e., 25, constant speed, i.e., 2 m/s, and varying pause time (from 0 to 400 s), which is indicated on *x*-axis. The result shows that in AODV protocol, when the pause time is increased the end-to-end delay gets decreased, but in DSR protocol, the delay is increased when the pause time is increased. So DSR has relatively high delay than AODV in all situations.

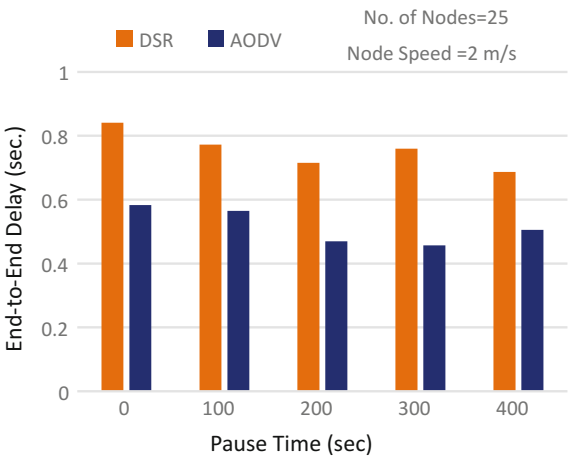


Fig. 7 Pause time (s) versus end-to-end delay with constant speed (2 m/s)

5 Conclusion

In this paper, performance of the two most widely used protocols—DSR and AODV—has been evaluated by varying speed and constant pause time. The experiment results have shown that AODV has outperformed DSR when speed of the node is low and pause time is kept constant. While AODV has performed well under high mobility of the nodes. It has also been found that the DSR has better results as compared to AODV in terms of throughput and end-to-end delay when pause time is kept constant. On the other side, AODV is performed better when pause time is varied.

References

1. Royer, E.M.: A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. University of California, Santa Barbara Chai-Keong Toh, Georgia Institute of Technology, vol. 2, pp. 1–22 (2004).
2. Johnson, D.B., Maltz, D.A., Hu, Y.-C.: The dynamic source routing protocol for mobile ad hoc networks. Internet-Draft, draft-ietf- manet-dsr-10.txt, July 2004
3. Raza, H.: Selection of cluster-head using PSO in CGSR protocol. In: International conference on digital Object identifier, vol. 3, Issue 4, pp. 91-94 (2010)
4. Perkins, C.E., Royer, E.M.: Ad hoc on-demand distance vector routing. In: Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 1999, pp. 90–100 (1999)
5. Hakak, S., et al.: Impact of packet size and node mobility pause time on average end to end delay and jitter in MANETs. In: IEEE International Conference on Computer and Communication Engineering (ICCCE), pp. 56–59 (2014)
6. Lego, K., Singh, P.K., Sutradhar, D.: Comparative study of adhoc routing protocol AODV, DSR and DSDV in mobile adhoc network. Indian J. Comput. Sci. Eng. (IJCSE) **I**(4), 364–371 (2011)

7. Kumar, P., et al.: Effect of pause time on performance of AODV and DSR routing protocols in wireless ad-hoc networks. Int. J. Modern Trends Eng. Res. **1**(5), 61–70 (2014)
8. Khattak, M.A.K., Iqbal, K., Khiyal, S.H.: Challenging ad-hoc networks under reliable & unreliable transport with variable node density. J. Theoret. Appl. Inf. Technol. (2008)
9. Gupta, S., Kumar, C., Rani, S., Bhushan, B.: Performance comparison of routing protocols using different mobility models. IJMECS **4**(8), 54–61 (2012)
10. Lee, J.-H.: Performance comparison of mobile ad-hoc multicast routing protocols. In: IEEE Journal Conference on Advanced Technologies for Communications, pp. 399–402, Oct 2008
11. Taksande, V.K., et al.: Performance comparison of DSDV, DSR and AODV protocol with IEEE 802.11 MAC for chain topology for MANET using NS-2. In: 2nd National Conference on Computing, Communication and Sensor Network, pp. 26–31, CCSN (2011)
12. Ahmed, A.: A comparative study of AODV & DSR with varying speed, pause time and node density over TCP connections in VANET. Int. J. Appl. Eng. Res. **2**(12), 3915–3955 (2014)
13. Jamalia, A., et al.: Scenario based pause time analysis of AODV, DSDV and DSR over CBR connections in MANET. Lect. Notes Softw. Eng. **1**(1), 57–60 (2013)
14. Park, V., Corson, S.: Temporally-ordered routing algorithm (TORA) version 1 functional specification. Internet Engineering Task Force (IETF) draft, July 2001
15. Rahman, A., Azad, S., Anwar, F., Abdalla, A.H.: A simulation based performance analysis of reactive routing protocols in wireless mesh networks. IEEE (2009). doi:10.1109/ICFN.2009
16. The Network simulator ns-allinone 2.35. http://www.isi.edu/nsnam/ns
17. Fall, K., Varadhan, K.: The ns Manual, University of Southern California, Information sciences Institute (ISI). http://www.isi.edu/nsnam/ns/ns-documentation.html
18. NS-2 with Wireless and Mobility Extensions. http://www.monarch.cs.cmu.edu
19. Dadhania, P., Patel, S.: Comparative performance analysis of AODV and DSR routing protocols in MANET. Int. J. Emerg. Trends Technol. Comput. Sci. (IJETTCS) **1**(3) (2012). ISSN: 2278–6856
20. Kaushik, S.S., Deshmukh, P.R.: Comparison of effectiveness of AODV, DSDV and DSR routing protocols in mobile ad hoc networks. Int. J. Inf. Technol. Knowl. Manag. **2**(2), 499–502 (2009)
21. Broch, J., et al.: A performance comparison of multi-hop wireless ad hoc network routing protocols. In: Proceedings of ACM, MOBICOM 98, Dallas, TX, Oct 1998
22. Upadhyaya, S., Joshi, P.: Comparison and performance analysis of reactive type DSR, AODV and proactive type DSDV routing protocol for wireless mobile ad-hoc network, using NS-2 simulator. J. Eng. Comput. Innov. **2**(10), 36–47 (2012)
23. http://www.isi.edu/nsnam/ns/ns
24. Mahdi, M.A., Wan, T.C.: Performance comparison of MANETS routing protocols for dense & sparse topology. In: International Conference on Information & Computer Networks (ICICN) (2012)
25. Gupta, A.K., Sadawarti, H., Verma, A.K.: Review of various routing protocols for MANETs. Int. J. Inf. Electr. Eng. **1**(3), 251–259 (2000)

TCP- and UDP-Based Performance Evaluation of AODV and DSR Routing Protocol on Varying Speed and Pause Time in Mobile Ad Hoc Networks

Arun Kumar Yadav and Ashwani Kush

Abstract Mobile Ad Hoc Networks are a self-configured, decentralized, and infrastructure-less network which can have different number of active links at any instants. Multihop wireless connectivity, frequently link breakage and mobility of nodes, gives this network a dynamic environment. Because of this dynamicity, it is quite difficult to propose a suitable routing protocol. Experimental analysis of working mechanism and functionality of available on-demand routing protocols (AODV and DSR) has been done using network simulator in this research paper. Results have been discussed using graphs, and analysis has been done.

Keywords AODV · DSR · MANET · PDR · TCP · UDP

1 Introduction

In this era of dynamicity, Ad hoc wireless network is a demanding an approach for the wireless communication [1], as it allows variable number of nodes with self-configuring behavior in the network. Ad hoc networks rely on infrastructure-less and decentralized administration which is polar opposite to the approach being used for cellular- and infrastructure-based networks such as routers. Since number of mobile nodes and active links for the communication are not fixed in this network, that's why it does not have a fixed topology. Randomly changing topology of mobile nodes for communication makes a perception that each node can act as host as well as router. In such a dynamic environment, to route packets

A.K. Yadav (✉)
Department of Computer Science & Applications, Kurukshetra University, Kurukshetra, Haryana, India
e-mail: arunkumar9429@gmail.com

A. Kush
Department of Computer Science, University College, Kurukshetra University, Kurukshetra, Haryana, India
e-mail: akush20@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_34

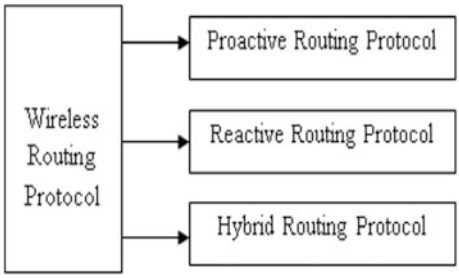


Fig. 1 Wireless routing protocol

efficiently by ensuring delivery to the correct node is a tedious task. Many other aspects like the selection of router and topology have to be considered while selecting a routing protocol for the MANET [2].

Depending upon the ability to find the efficient path, routing protocols can be categorized as proactive, reactive, and hybrid [2] as described in Fig. 1.

Proactive routing protocols [3, 4] maintain routing tables and have to periodically update it by means of sharing. Proactive routing protocols are also referred to as table-driven protocols. Some popular routing protocols are as follows: Destination-Sequenced Distance Vector (DSDV) [5] protocol, Wireless Routing Protocol (WRP) [6], and Optimized Cluster Head Gateway Routing (CGSR) [7].

Reactive routing [8, 9] protocols have the ability to find a path whenever required because of which these are also referred to as on-demand routing protocols. It finds an efficient path by flooding the route packets.

Reactive Routing Protocols [4] main under consideration are as follows: Dynamic Source Routing (DSR) [1, 10, 11] protocol, Ad hoc On-Demand Distance Vector (AODV) [3, 4, 12] routing protocol, and Temporally Ordered Routing Algorithm [13].

AODV [14, 15] is a type of reactive protocol which is sometimes referred to as On-Demand Distance Vector routing protocol. In AODV, links are established only when they are required for the efficient communication, and the communication is initiated by source node. It has the feature of both on demand as well as distance vector, and it uses a hop-to-hop methodology for packet exchange. To establish an efficient path for communication, source node is flooded with RREQ (Route Request) packets over the network. If there exists a valid and appropriate path from source to destination, then a RREP (Route Reply) packet is sent to the source node. If no valid path is there, then RERR (Route Error) packet is sent to the source node.

The Dynamic Source Routing (DSR) [2] is a reactive protocol which is based on two mechanisms, i.e., route discovery and route maintenance. A route discovery and route maintenance features of DSR allow the ad hoc network to be self-configuring and self-organizing and hence makes it infrastructure-less. Since it does not use beacon messages and hence saves battery power, reduces the network bandwidth, and avoids large routing updates.

This paper presents a TCP-/UDP-based performance of the two broadly used reactive protocols such as AODV [1, 4, 10] and DSR [1, 3, 4, 10]. The performance

of both AODV and DSR is calculated by varying speed and pause time and metrics used in PDR.

The remaining paper has following sections. Section 2 is about the literature. Section 3 has brief description of the research methodology. Section 4 describes the proposed work. Simulation results and analysis of protocols have been discussed in Sect. 5. Summary and conclusion have been given in the last section.

2 Related Work

There have been numerous work [1, 4, 10, 18] related to performance evaluation of mobile ad hoc protocols. Adlakha et al. [1] presented the overview on a comparison of AODV and DSR in constrained situation. Mishra et al. [10] evaluated performance of AODV and DSR using NRL (normalized routing load). Ahmed presented a comparative study of AODV and DSR in vehicular ad hoc network. Dhakal et al. [4] presented the performance comparison of reactive-based routing protocol. Upadhyaya and Joshi [16] presented the comparison of reactive- and proactive-based routing protocol using network simulator 2. Lee [17] presented the comparison of multicast routing protocol in MANET. Mahdi et al. [18] presented performance comparison of routing protocols in MANET for dense and sparse topology. In [10, 17], they have analyzed these protocols on the basis of packet delivery ratio and routing overhead. Analysis has been done by varying mobile speed only, but in another different paper [3, 14], it has shown different results by varying pause time and by keeping mobile nodes constant.

3 Research Methodology

Network simulator (NS2.34) [19–22] has been used to perform all the simulations by taking following parameters. Numbers of nodes are 20 with 6 TCP/UDP and 50 with 14 TCP/UDP connections; simulation time has been taken as 500 s. These scenarios have been considered in 670 m × 670 m area for 20 nodes and 1000 m × 1000 m area for 50 nodes. Random Way Point model [23] is used in which a mobile node has been initially placed at random location for the simulation. For simulation, environmental surrounding selected is pause time and speed. Pause time is changing between the ranges from 0 to 400 s. Work is performed by using reactive protocol (AODV, DSR) with varying pause time and speed of the node. Metrics being used for the evaluation of performance of proposed approach are as follows:

Throughput: The rate of successfully transmitted data per unit time in the network during the simulation is called throughput [6].

Packet Delivery Ratio (PDR): The fraction of successfully received packets, which survive while finding their destination, is called packet delivery ratio [24] (PDR). This performance also measures and determines the completeness and correctness of the routing protocol.
End-to-End Delay: The end-to-end delay [15] is the average time interval between the generation of a packet at a source node and the successfully delivery of the packet at the destination node. Less end-to-end delay gives better performance of the network.

4 Proposed Work

Figure 2 illustrates the simulation process activities of the proposed work, and the simulation parameters have been described in Table 1. Firstly, wireless scenarios and traffic patterns are defined in order to create a tcl script for the proposed system. Then, after tcl script is given as an input to the network simulator which executes it and generates a trace file. PDR is calculated. After PDR calculation graphs have been generated for different scenarios, the graphs have been cumulatively analyzed.

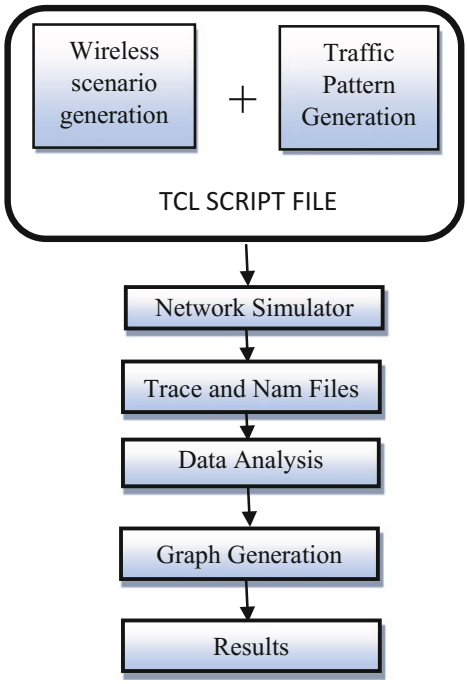


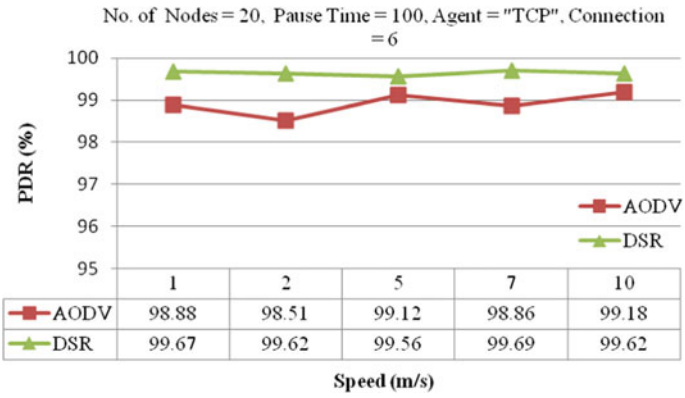
Fig. 2 Simulation process activities

Table 1 Simulation scenario

Simulation parameters	Parameter value
Simulator	NS-2.34
MAC type	802.11
Channel	Wireless channel
Antenna type	Omni
Radio propagation	TwoRay ground
Interface queue type	DropTailPriQueue (AODV) CMUPriqueue (DSR)
Simulation area	670 m × 670 m (for 20 nodes) 1000 m × 1000 m (for 50 nodes)
Mobile nodes	20 and 50
Pause time	0,100,200, 300,400
Speed	1.0, 2.0, 5.0, 7.0, 10.0 m/s
No. of connections	6 (for 20 nodes), 14 (for 50 nodes)
Routing protocols	AODV, DSR
Traffic sources	CBR(UDP)/TCP
Simulation time	500 s
Performance metrics	Packet delivery ratio

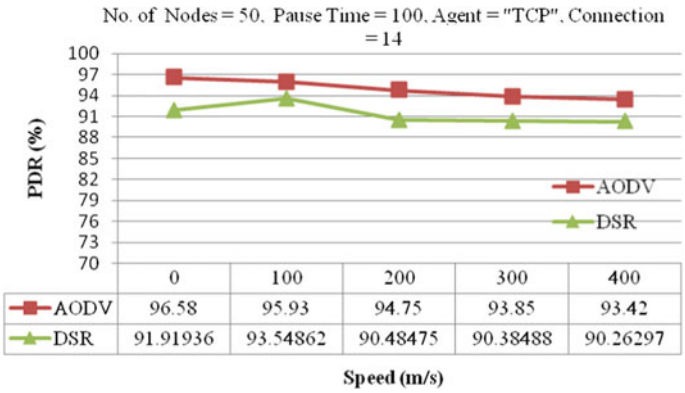
5 Experimental Results and Analysis

To analyze the performance of AODV and DSR, reading has taken by varying different parameters such as number of nodes, speed, pause time, and connection agent. For each scenario, PDR has been calculated. Graph 1 shows PDR for 20 nodes. Pause time is constant, i.e., 100 s, and speed varies from 1 to 10 m/s. Connection used here is TCP. It is observed that PDR for DSR is better than PDR for AODV for whole range of speed. It ranges from 98.5 to 99.2% in AODV and is



	1	2	5	7	10
AODV	98.88	98.51	99.12	98.86	99.18
DSR	99.67	99.62	99.56	99.69	99.62

Graph 1 PDR for 20 nodes versus speed (TCP agent)



	0	100	200	300	400
AODV	96.58	95.93	94.75	93.85	93.42
DSR	91.91936	93.54862	90.48475	90.38488	90.26297

Graph 2 PDR for 50 nodes versus speed (TCP agent)

approximately touching the same in DSR. In DSR, it outshines at many intervals in the range of 0.44–1.2% and so DSR outperforms AODV.

Graph 2 shows PDR for 50 nodes. Pause time is constant, i.e., 100 s, and speed varies from 1 to 10 m/s. Connection used here is TCP. It is observed that PDR decreases for DSR as well as for AODV as the mobility of nodes increases. It ranges from 93.4 to 96.6% in AODV and from 90.2 to 92% in DSR. In AODV, it outshines at all intervals in the range of 2.4–4.5% and so AODV outperforms DSR.

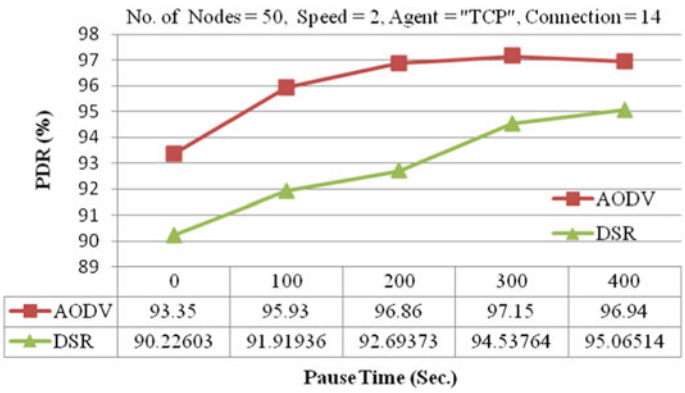
Graph 3 shows PDR for 50 nodes. Speed is constant, i.e., 2 m/s, and pause time varies from 0 to 400 s. Connection used here is TCP. It ranges from 93.3 to 97.2% in AODV and from 90.2 to 95.1% in DSR. In AODV, it outshines at all intervals in the range of 1.8–4% and so AODV outperforms DSR.

Graph 4 shows PDR for 20 nodes. Speed is constant, i.e., 2 m/s, and pause time varies from 0 to 400 s. Connection used here is TCP. It is observed in Graphs 3 and 4 that PDR increases for both DSR as well as AODV as the pause time increases. It ranges from 98.4 to 99.4% in AODV and is approximately touching the same in DSR. In DSR, it outshines at many intervals in the range of 0.4–1.3% and so DSR outperforms AODV.

Graph 5 shows PDR for 50 nodes. Pause time is constant, i.e., 100 s, and speed varies from 1 to 10 m/s. Connection used here is UDP. It is observed that PDR for AODV decreases while PDR for DSR increases as the speed increases. It ranges from 81.7 to 82.1% in AODV and from 82.5 to 83.2% in DSR. In DSR, it outshines at many intervals in range of 0.5–1.5% and so DSR outperforms AODV.

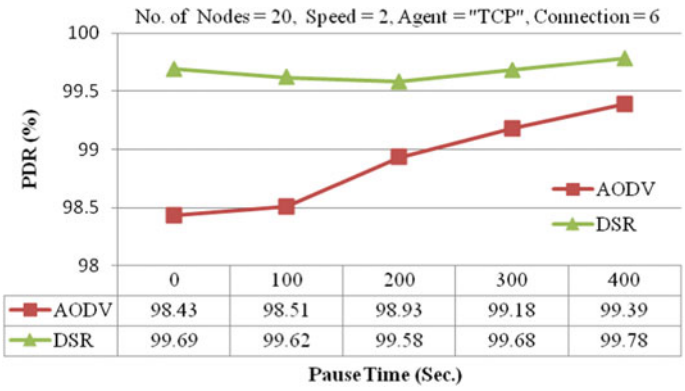
Graph 6 shows PDR for 20 nodes. Pause time is constant, i.e., 100 s, and speed varies from 1 to 10 m/s. Connection used here is UDP. Here, PDR for both DSR and AODV decreases as the speed increases. It ranges from 84.7 to 84.9% in AODV and is approximately touching the same in DSR. In DSR, it outshines at many intervals in the range of 0.1–0.3% and so DSR outperforms AODV.

Graph 7 shows PDR for 20 nodes. Speed is constant, i.e., 2 m/s, and pause time varies from 0 to 400 s. Connection used here is UDP. Here, PDR for both DSR and



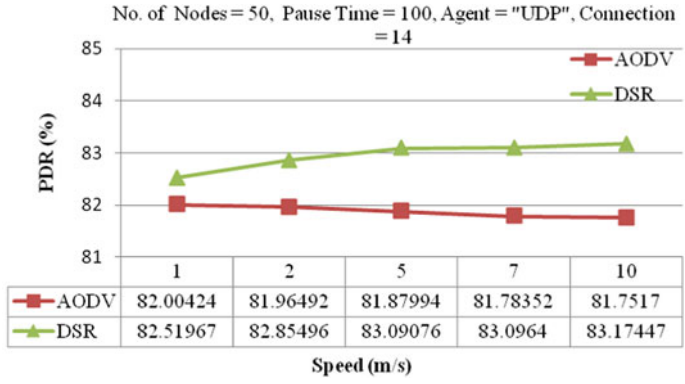
	0	100	200	300	400
AODV	93.35	95.93	96.86	97.15	96.94
DSR	90.22603	91.91936	92.69373	94.53764	95.06514

Graph 3 PDR for 50 nodes versus pause time (TCP agent)



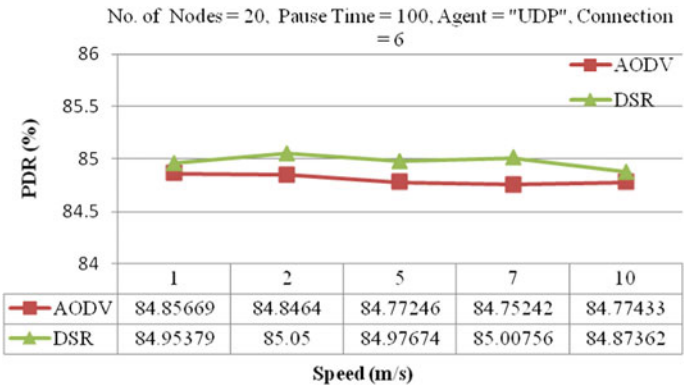
	0	100	200	300	400
AODV	98.43	98.51	98.93	99.18	99.39
DSR	99.69	99.62	99.58	99.68	99.78

Graph 4 PDR for 20 nodes versus pause time (TCP agent)



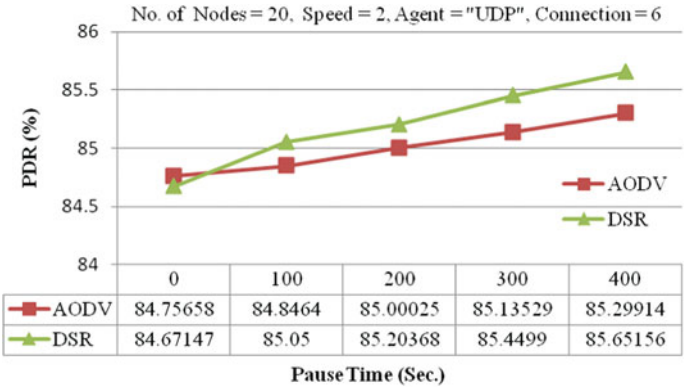
	1	2	5	7	10
AODV	82.00424	81.96492	81.87994	81.78352	81.7517
DSR	82.51967	82.85496	83.09076	83.0964	83.17447

Graph 5 PDR for 50 nodes versus speed (UDP agent)



	1	2	5	7	10
AODV	84.85669	84.8464	84.77246	84.75242	84.77433
DSR	84.95379	85.05	84.97674	85.00756	84.87362

Graph 6 PDR for 20 nodes versus speed (UDP agent)



	0	100	200	300	400
AODV	84.75658	84.8464	85.00025	85.13529	85.29914
DSR	84.67147	85.05	85.20368	85.4499	85.65156

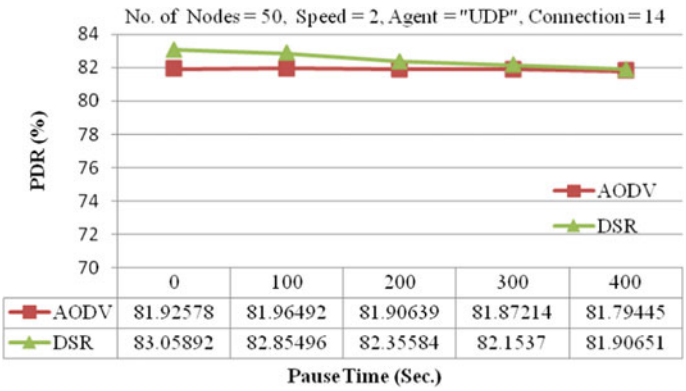
Graph 7 PDR for 20 nodes versus pause time (UDP agent)

AODV increases as the pause time increases. It ranges from 84.7 to 85.3% in AODV and is approximately touching the same in DSR. In DSR, it outshines at many intervals in the range of 0.2–0.4% and so DSR outperforms AODV.

Graph 8 shows PDR for 50 nodes. Speed is constant, i.e., 2 m/s, and pause time varies from 0 to 400 s. Connection used here is UDP. Here, PDR for both DSR and AODV decreases as the pause time increases. It ranges from 81.7 to 82% in AODV and is approximately touching the same in DSR. In DSR, it outshines at many intervals in the range of 0.1–1% and so DSR outperforms AODV.

After analysis of all the scenarios, it has been observed that

- For TCP-based network traffic, as the number of mobile nodes increases in ad hoc networks, AODV outperforms DSR.
- For UDP-based network traffic, DSR always performs better than AODV in mobile ad hoc networks.



	0	100	200	300	400
AODV	81.92578	81.96492	81.90639	81.87214	81.79445
DSR	83.05892	82.85496	82.35584	82.1537	81.90651

Graph 8 PDR for 50 nodes versus pause time (UDP agent)

6 Conclusion

In this work, an experiment has been performed to analyze the performance evaluation of AODV and DSR by using the network simulator for TCP-/UDP-based network traffic. On the basis of PDR, it has been found that for UDP traffic, DSR performs better than AODV in every scenario. While for TCP-based network traffic, AODV performs better than DSR in denser networks and DSR performs better in less dense network. It is concluded that for TCP-based traffic, PDR decreases with the increase in speed, whereas PDR increases with the increase in pause time. In future, more work will be carried out for throughput, delay as well. Also fading effect and other issues will be taken care of.

References

1. Adlakha, Alka, Arora, Vasudha: Performance evaluation of AODV and DSR routing protocols under constrained situation. Int. J. Adv. Res. Comput. Commun. Eng. **4**(7), 189–191 (2015)
2. Royer, E.M.: A review of current routing protocols for ad hoc mobile wireless networks. University of California, Santa Barbara Chai-Keong Toh, Georgia Institute of Technology, vol. 2, pp. 1–22 (2004)
3. Kumar, P., et al.: Effect of pause time on performance of AODV and DSR routing protocols in wireless ad-hoc networks. Veh. Commun. **1**(5), 61–70 (2014)
4. Dhakal, D., Gautam, K.: Performance comparison of AODV and DSR routing protocols in mobile ad-hoc networks: a survey. Int. J. Eng. Sci. Innov. Technol. **2**(3), 258–266 (2013)
5. Gupta, A.K., Sadawarti, H., Verma, A.K.: Review of various routing protocols for MANETs. Int. J. Inf. Electr. Eng. **1**(3), 251–259 (2000)
6. Azad, S., Rahman, A., Anwar, F.: A performance comparison of proactive and reactive routing protocols of mobile ad-hoc network (MANET). J. Eng. Appl. Sci. **2**(5), 891–896 (2007)

7. Raza, H.: Selection of cluster-head using PSO in CGSR protocol. In: International Conference on digital Object identifier, vol. 3, Issue 4, pp. 91–94 (2010)
8. Johnson, D.B., Maltz, D.A., Hu, Y.-C.: The dynamic source routing protocol for mobile ad hoc networks. Internet-Draft, draft-ietf-manet-dsr-10.txt, July 2004
9. Perkins, C.E., Belding-Royer, E.M., Das, S.: Ad-hoc on demand distance vector (AODV) routing. Mobile Ad Hoc Networking Working Group, July 2003, Internet-Draft
10. Mishra, P., Gupta, N.: Performance evaluation of AODV and DSR protocols in MANET. Perform. Eval. **4**(2), 10313–10320 (2015)
11. Valarmathi, A., Chandrasekaran, R.M.: Congestion aware and adaptive dynamic source routing algorithm with load balancing in MANETs. Int. J. Comput. Appl. **8**(5), 1–4 (2010)
12. Perkins, C.E., Belding-Royer, E.M., Das, S.R.: Ad hoc on-demand distance vector (AODV) routing. Internet Engineering Task Force (IETF) draft, Nov 2002. Available at http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-12.txt
13. Park, V., Corson, S.: Temporally-ordered routing algorithm (TORA) version 1 functional specification. Internet Engineering Task Force (IETF) draft, July 2001
14. Jamalia, A., et al.: Scenario based pause time analysis of AODV, DSDV and DSR over CBR connections in MANET. Lect. Notes Softw. Eng. **1**(1), 57–60 (2013)
15. Rahman, A., Azad, S., Anwar, F., Abdalla, A.H.: A simulation based performance analysis of reactive routing protocols in wireless mesh networks. 2009 IEEE, doi:10.1109/ICFN.2009
16. Upadhyaya, S., Joshi, P.: Comparison and performance analysis of reactive type DSR, AODV and proactive type DSDV routing protocol for wireless mobile ad-hoc network, using NS-2 simulator. J. Eng. Comput. Innov. **2**(10), 36–47 (2012)
17. Lee, J.-H.: Performance comparison of mobile ad-hoc multicast routing protocols. In: IEEE Journal Conference on Advanced Technologies for Communications, pp. 399–402, Oct 2008
18. Mahdi, M.A., Wan, T.C.: Performance comparison of MANETS routing protocols for dense & sparse topology. In: International Conference on Information & Computer Networks (ICICN 2012)
19. The Network simulator ns-allinone 2.35, http://www.isi.edu/nsnam/ns
20. Fall, K., Varadhan, K.: The ns Manual. University of Southern California, Information sciences Institute (ISI), http://www.isi.edu/nsnam/ns/ns-documentation.html
21. NS-2 with Wireless and Mobility Extensions, http://www.monarch.cs.cmu.edu
22. http://www.isi.edu/nsnam/ns/ns
23. Lin, G., Noubir, G., Rajaraman, R.: Models for ad hoc network simulation. College of Computer & Information Science. Mobility IEEE, vol. 7, pp. 4803–8356 (2004)
24. Broch, J., et al.: A performance comparison of multi-hop wireless ad hoc network routing protocols. In: Proceedings of ACM MOBICOM 98, Dallas, TX, Oct 1998

Hybrid Multi-commodity-Based Widest Disjoint Path Algorithm (HMBWDP)

Pallvi Garg and Shuchita Upadhyaya

Abstract The paper deals with the Traffic Engineering for online multi-path routing in MPLS networks. The algorithm presented is inspired from the concept of profile classes (in which the traffic demands are classified into various profile classes which are generated based on the SLAs signed by the Internet users). In the proposed algorithm, multi-commodity network flow formulation is used to prevent network bottlenecks and to ensure minimum rejected requests/traffic demands. In the proposed algorithm SLAs, Global and Local quasi-static knowledge about the network are used to generate multi-commodities based "profile classes" in the first phase and then these multi-commodities flows are distributed over Widest Disjoint Paths with respect to the bottleneck links in the second phase. The combination of multi-commodity-based flows and the disjoint paths w.r.t. bottlenecks prevents the network from saturation point which helps in minimizing the congestion, delays, rejected requests, and maximizing the throughput, i.e., improving the overall performance of the network.

Keywords Multi-protocol label switching · Equalizing blocking probability · Widest disjoint paths

1 Introduction

Multi-protocol label switching enables service providers to meet challenges accounted due to explosive growth of the Internet. Many traditional routing algorithms [1–3] and MPLS adaptive multi-path routing algorithms [4–8] have been presented by researchers in the past, but most of them suffered from shortcomings.

P. Garg (✉) · S. Upadhyaya
Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India
e-mail: pallvigarg@gmail.com

S. Upadhyaya
e-mail: supadhyaya@kuk.ac.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_35

In Profile-Based Routing [9] with many examples, researchers elaborated that if a bad path is selected for one flow; it may lead to generate bottleneck links for the upcoming future traffic flows. In the lack of additional network information about the traffic flows, any online routing algorithm can perform poor in the worst case. At the same time, it is not of much importance to gather all the knowledge about the network at once; instead, exploiting the network knowledge to its extreme is more important. The main objective of any multi-path routing algorithm is to fulfill the maximum traffic demands through the network by utilizing the network resources to its maximum and keeping the network congestion free by cleverly choosing the paths to avoid bottlenecks to enhance the overall performance.

The proposed algorithm is inspired by the concept of multi-commodity-based "profile classes" introduced in PBR [9]. With the help of multi-commodity flows, the traffic demands are classified into various profile classes which are generated based on the SLAs signed by the Internet users. "Commodity" could be represented as an entity that needs to be "shipped" from the source to the destination node by using MPLS on the underlying network. To select any path, information about the global network topology is always required. The presented work uses SLAs and infrequently exchanged global information to categorize the network traffic into various profile classes and then find the minimum cost in terms of bandwidth based on the globally exchanged information about the network in the multi-commodity-based preprocessing phase. In the Online Path Selection for Label Switch Paths request phase, Widest Disjoint Paths (WDPs) [10] using locally adaptive knowledge about the bottlenecks are used.

In the rest of the paper, in Sect. 2, Profile-Based Routing algorithm [9] and WDP including their key aspects and limitations are accounted. In Sect. 3, Hybrid multi-commodity-based Widest Disjoint Path is presented. In Sect. 3.2, the proposed algorithm is discussed. Finally, Sect. 4 concludes the paper.

2 Existing Algorithms

In the literature, on multi-path routing schemes, there are many proposed algorithms that use specific capabilities of an MPLS network. Dynamic Routing with Partial Information (DR-PI) [4], Dynamic Restorable Routing [5], Minimum Interference Routing Algorithm [7, 8], and Profile-Based Routing [9] used the MPLS technique extensively in multi-path routing. In DR-PI [4] and DORA [5], the number of rejected requests is not taken into consideration, considerable computation complexity is a major limitation for their online implementation, and no local/segment backups are considered in these algorithms. MIRA [7, 8] focuses extensively on the interference effect of a single ingress–egress pair at a time, so MIRA is computationally very expensive too. In PBR [9], the utilization of traffic profiles of data flows is proposed. PBR suffers from the limitation that there is no explicit fault recovery treatment. All these online multi-path routing algorithms have given important contribution to the exploitation of the MPLS topology (ingress–egress

nodes). A brief review and scope of improvement in PBR [9] and Widest Disjoint Path [10] algorithms is introduced next.

2.1 Profile Based Routing [9]

Profile-Based Routing algorithm [8] is the routing algorithm in which traffic going through network is measured, and the traffic flow is classified as per "profile classes." Each profile class includes Bi, which denotes the aggregate bandwidth requirement of the aggregated LSP setup requests between source s_i and destination d_i and is mapped to class ID. Each profile is symbolized by (class ID, s_i, d_i, B) called commodity ith. For approximately satisfying all the requests on future, the authors have proposed simultaneous equations to find amount of traffic of each ingress–egress pair distributed on every link (first step namely *multi-commodity Flow Preprocessing*). If the problem has solution, they applied the solution to the network. For each LSP demand, its class is determined, used the solution of the first step for each class to initialize the network topology and then used the shortest path algorithm (MHA) to find optimal solution (second step namely *Online Path Selection for LSP requests*). On general case, not all the profiles can be completely satisfied (Fig. 1).

2.2 Main Aspects and Limitations of Profile-Based Routing

1. The algorithm works in two phases—1. *Multi-commodity Flow Preprocessing phase and 2. Online Path Selection for LSP requests.*
2. The algorithm considers traffic in terms of classes or commodities as per SLA or from quasi-static information about network. It does not deal as per flows like MIRA [7, 8]. With the help of traffic routing based on commodities (classes), the optimized routing algorithm could be generated. Each profile class includes Bi

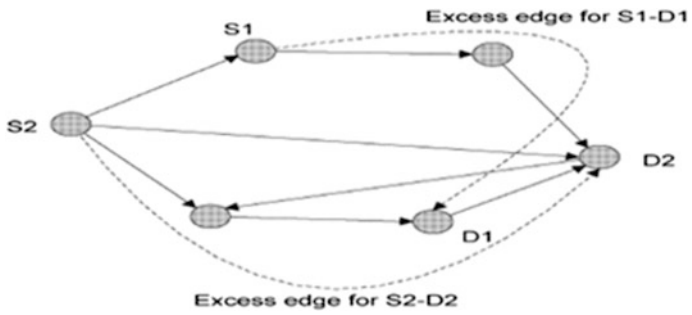


Fig. 1 Excess edges are added to the graph in the preprocessing phase to accept all the traffic demands in the preprocessing phase in PBR

which denotes aggregate bandwidth requirements of LSP setup requests between ingress–egress pairs required by the commodities for a group of source and destination pairs.
3. The "commodities profile classes" could be categorized and prioritized on various parameters based on types of traffic demand, packets, data, holding time, number of times the particular traffic demand is rejected, path failures, etc. So, one more parameter say P_i for each profile class C_i must be used. The value of P_i can be estimated by the globally exchanged information and SLAs to utilize the concept of multi-commodities with MPLS to the extreme.
4. The algorithm deals only with the splitting traffic as per profile class flow. For unsplittable traffic, the traffic has to go through a single path.
5. In PBR for Online Path Selection for LSP requests, minimum hop algorithm with the help of breadth first search is used, whereas **Hybrid multi-commodity Widest Disjoint Path algorithm** could be good choice to save the network from saturation point for any real-time network topology with the help of Widest Disjoint Paths w.r.t. the congestion points and bottlenecks.

2.3 Widest Disjoint Path [10] Algorithm

Most of the times, multiple paths perform good individually but when traffic is routed along them collectively, it may not perform so well and even quiet poor. The reason is sharing of the bottleneck links. The best way to reduce bottlenecks is to compute maximum disjoint paths, but this approach is static and overly conservative.

In Widest Disjoint Path algorithm, maximally disjoint paths are computed. If there are multiple such paths, then path with the highest width (w.r.t. bandwidth) is chosen for the network flow. But with this approach, overall network performance is degraded and majority of network resources are not utilized. Sharing of nodes or links does not matter, but the sharing of bottleneck links matters. To avoid congestion, sharing of bottlenecks must be avoided. Disjoint paths w.r.t. bottlenecks can enhance the performance of any network routing model. The knowledge about the bottlenecks is gained from the global link state updates. Proportioning the traffic to these disjoint paths can be done with the help of Equalizing Blocking Probability.

3 Hybrid Multi-commodity-Based Widest Disjoint Path Algorithm

In this paper, a Hybrid algorithm for dynamic multi-path routing using the advantages of two basic algorithms PBR and WDP using MPLS technique is presented. The quasi-static information is used about the network. The algorithm

works in two phases: preprocessing phase and path selection phase. Problem setup and basic routing requirements are mentioned next.

3.1 Problem Setup and Routing Requirements

The network can be modeled as a graph $G = (V, E)$; here, V denotes the set of nodes (i.e., routers) and E represents set of edges (i.e., links). The current residual capacity of each link $e \in E$ is denoted as $cap(e)$. Each Label Switch Path (LSP) can be set up as a subset of routers which are assumed to be ingress–egress routers. It is assumed that the network topology of all the ingress–egress routers (i.e., LIR and LER) is known and the information is changing very infrequently. Any appropriate time period θ can be predicted as a time duration after which network information is changed. Since many flow requests are inherently unsplittable, routing traffic flows along a single path without splitting is assumed and given high priority.

3.2 Hybrid Multi-commodity-Based Widest Disjoint Path Algorithm

Hybrid Multi-commodity-Based Widest Disjoint Path Algorithm

Step 1: Multi-commodity Flow Preprocessed Phase

- Predict optimized value of degree of multi-commodities i (where i is maximum number of commodity flows routed through edge e).
- Prioritize the commodities using globally exchanged link state metrics.
- Maximize the total carried traffic using global optimal proportioning.
- Minimize the Average Blocking Probability b_r.

Step 2: Path selection for LSP requests Phase

- Remove all edges e from graph G, for which blocking probability is more than b_r (for the whole network with the help of Localized Adaptive Proportioning). (These edges are critical edges having high blocking probability for any class C_{id}.)
- Find disjoint paths with widest residual bandwidth.

Step 3: Decrease the residual bandwidth b, in all the edges e for all paths P.

Step4: Route along label switch path P (s, d, b).

3.2.1 Multi-commodity Flow Preprocessing Phase

In this preprocessing phase, traffic profiles (C_{ID}, P_i, s_i, d_i, B_i) are generated, corresponding to a real-time network $G = (V, E)$, where C_{ID} is traffic class identity, s_i the finite set of sources, d_i is the finite set of destinations, and B_i is minimum aggregate bandwidth requirement for this traffic profile class C_{id} between set of sources s_i and set of destinations d_i. P_i is the priority assigned to this profile class based on the previous knowledge about the network. Each traffic class is treated as a separate commodity. The objective is to find widest disjoint routes w. r. t. the bottleneck links in the network to send maximum number of commodities along these disjoint routes, for the traffic flow demands between source nodes to the destination nodes. In the literature, global optimal proportioning has been extensively studied.

Since each source node (LER) knows real-time network topology information (which includes the maximum residual capacity cap(e) of every edge) and the traffic load to be routed between every ingress–egress pair. With the help of this globally exchanged knowledge gathered after every time period θ, offered traffic loads through the network and service level agreements (SLAs), the optimal proportions, for distributing multi-commodity-based flows to the LSPs for each ingress–egress pair, can be computed as described below.

$\sigma = (s, d)$ denotes a source–destination pair
λ_σ average arrival rate of flows arriving at the source node s destined for node d
μ_σ average holding time for the flows
v_σ offered load between source–destination pair σ

So, $v_\sigma = \lambda_\sigma / v_\sigma$

R_σ finite set of all the feasible paths for fulfilling traffic demands between pair σ
α_r optimal proportions of the path for each $r \in R_\sigma$ and $\sum_{r \in R_\sigma} \alpha_r = 1$
b_r is the average blocking probability
W is the total carried traffic

The objective in preprocessing phase is to maximize the total carried traffic W, with the help of global data exchange by updating the network information after every periodic time θ.

$$W = \sum_{\sigma} \sum_{r \in \widehat{R_\sigma}} \alpha_r v_\sigma (1 - b_r) \text{ is maximized} \tag{1}$$

The same objective can be achieved by minimizing the average blocking probability b_r, and to minimize b_r localized strategies are used in path selection phase. All such profile classes are generated by ensuring these objectives at the server side (i.e., router) before actual path selection, it seems highly complex but with the help of past data complexity can be reduced.

3.2.2 Path Selection Phase

Once the profile classes (class ID, P_i, s_i, d_i, B_i) are generated in the preprocessing phase, the traffic demand flows are now handled by grouping them as per profile class, between source–destination pairs through LSPs. In path selection phase, Widest Disjoint Paths w.r.t. bottleneck links are generated for the corresponding profile class flows generated and categorized in the preprocessing phase.

To find the bottleneck links, average blocking probability b_r is computed as below:

$$b_r = \sum_{i=1}^{k} \alpha_{r_i} b_{r_i} \tag{2}$$

The value of b_r must be minimized in preprocessing phase.

Since a set of multiple paths between any pair σ may perform well or near optimal individually but may lead to congestion and poor network utilization when performed collectively, it is wise to discard those links whose blocking probability is greater than b_r, since these links are bottleneck links. So to ensure that multi-commodity flows do not share bottleneck links, what can be done is to remove the traffic flows from one of the paths and then shifting the load to another candidate path by ensuring that there is no increment in the average blocking probability, b_r. Therefore, it is necessary to ensure that the candidate multiple paths are mutually disjoint with respect to the bottleneck links.

In Widest Disjoint Path algorithm w. r. t. bottlenecks, multiple disjoint paths are selected that do not share bottlenecks. If multiple such paths are found, then the path with the widest residual bandwidth is selected. With these widest residual bandwidth disjoint paths, both the objectives—minimizing the no of rejected requests and maximizing the traffic flow—are achieved with a balance.

4 Conclusions and Future Work

The main contribution of this paper is the development of Hybrid algorithm exploiting the concept of MPLS and profile classes generated using SLAs. The assumption is that the traffic demands are available, and all ingress–egress pairs are known. The key idea is to pre-compute the paths between any source–destination pair using the global and local knowledge about the network in the preprocessing phase before the actual path selection, with the objectives—minimizing the number of rejected requests and minimizing the average blocking probability. To minimize the blocking probability, disjoint paths w. r. t. bottlenecks are used with the help of which both the objectives can be fulfilled. The discarded paths which contain bottlenecks can be used for rerouting and as backup paths. In the near future,

experimentation of the algorithm in operational MPLS network and comparison of the simulation results of the present algorithm with those of the already existing algorithms are scheduled.

References

1. Awduche, D.O., Berger, L., Gain, D., Li, T., Swallow, G., Srinivasan, V.: Extensions to RSVP for LSP tunnels. IETF RFC 3209, Dec 2001
2. Guerin, R., Williams, D., Orda, A.: QOS routing mechanisms and OSPF extensions. In: Proceedings of Globecom (1997)
3. Steekiste, P., Ma, Q.: On path selection for traffic with bandwidth guarantees. In: Proceedings of the IEEE International Conference of Network Protocols, Oct 1997
4. Kodialam, M., Laksman, T.V.: Dynamic routing of bandwidth guaranteed tunnels with restoration. In: Proceedings of IEEE INFOCOM 2000, pp. 902–911, Mar 2000
5. Kodialam, M., Lakshman, T.V.: Restorable dynamic QoS routing. IEEE Commun. Mag. (2002)
6. Elwalid, A., et al.: MATE: MPLS adaptive traffic engineering. In: INFOCOM 2001, Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 3. IEEE (2001)
7. Kodialam, M.S., Lakshman, T.V.: Minimum interference routing with applications to MPLS traffic engineering. In: Proceedings of IEEE INFOCOM, vol. 2, pp. 884–893 (2000)
8. Kar, K., Kodialam, M., Lakshman, T.V.: Minimum interference routing of bandwidth guaranteed tunnels with MPLS traffic engineering applications. IEEE J. Sel. Areas Commun. **18**(12) (2000)
9. Suri, S., Waldvogel, M., Ramesh Warkhede, P.: Profile-based routing: a new framework for MPLS traffic engineering. In: Proceedings of QofIS, Sept 2001
10. Nelakuditi, S., Zhang, Z.-L.: On selection of paths for multipath routing. In: Proceedings of IWQoS'01 (2001)

A Perusal of Replication in Content Delivery Network

Meenakshi Gupta and Atul Garg

Abstract Content delivery network (CDN) is increasingly used to improve the network performance for end users. This helps to reduce the load on origin server by delivering the contents from the edge of the network in proximity to end users requesting for the contents. Content providers take the services of CDN service providers to improve the Quality of Service (QoS) requirements of their users, and in return, they have to pay for these services. Therefore, this demands optimal placement of contents on surrogate servers. This paper analyzes the existing strategies suggested for replication of contents on these servers to provide a foundation for devising a more efficient replication strategy in a CDN.

Keywords Content provider · Content delivery network · Origin server · Surrogate server · Content replication

1 Introduction

In recent years, the Web is gradually became part of our routine life. The servers of popular Web sites are finding it difficult to handle the Web requests of their users. Therefore, the trend is shifting from centralized to distributed architecture for Web content delivery. This has led to the development of content delivery network which is a large-scale distributed system of servers deployed at the edge of the Internet closer to end users. These servers are named as surrogate servers, replica servers, or CDN servers. The intent is to reduce the load on origin server network and as a result to improve the performance of Web content delivery at end users. The content providers take the services of CDN service providers to serve better Web requests from their clients. In return, they have to pay them for the storage

M. Gupta (✉) · A. Garg
MMICT & BM (MCA), Maharishi Markandeshwar University, Mullana, Haryana, India
e-mail: mnkshgupta@gmail.com

A. Garg
e-mail: atul.garg@mmumullana.org

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_36

space used for replicating the contents as well as for servicing the Web requests for these contents by them. Therefore, it is not efficient to replicate all the Web contents on every surrogate server [1]. The contents and surrogate servers for replication are selected in a way so that the cost of storing, maintaining, and delivering the contents is minimized and user-perceived Quality of Service is maximized. The strategy used for content replication is implemented during request redirection in the CDN system. Therefore, the replication and redirection policy has been considered jointly [2–4] earlier.

This paper focuses on the problems of assigning CDN resources for replication of contents, closer to end users to make their network experience better and reduce the cost as well. Various factors affecting the content replication strategies are discussed in Sect. 2. Section 3 presents a picture of existing strategies for content replication in CDNs, while their comparative analysis is presented in Sect. 4. Section 5 concludes the paper.

2 Factors Affecting Replication

The content replication in CDN requires consideration of various factors. These factors are taken as input for solving the replication issues. Some of these factors are controllable by the system such as the number of surrogate servers, their location, consistency protocols. However, the factors such as request rate, contents update rate, and available network bandwidth cannot be controlled by the system [5]. The various factors that are taken into account by different researchers and CDN service providers are as follows:

- ***Surrogate servers***—The decision about number and position of surrogate servers for content replication has to be taken into account. However, CDN service providers usually have pre-established infrastructure, so content providers have to only select the surrogate servers for replication out of existing ones.
- ***Storage capacity***—What amount of the storage capacity at each of the selected surrogate servers should be used for replication? As the servers have finite storage capacity for replicating the objects, therefore, the objects have to be replicated optimally on these servers keeping in view their limited storage space as well as storage cost.
- ***Content selection***—How much contents should be selected for replication on surrogate servers whether full or partial? Though the disks are becoming cheaper [6], the number and volume of contents is increasing as well. Therefore, the partial replication is preferred; further, it will reduce the storage and maintenance cost.
- ***Content outsourcing***—Which policy should be used to replicate and update the contents on surrogate servers? Different policies that have been suggested for the purpose are the following: cooperative push-based, uncooperative pull-based, cooperative pull-based [7].

- ***Contents granularity***—What should be the granularity of contents to be replicated, whether entire replication (coarsest grain), object replication (fine-grain), or per-group/cluster-based replication (coarse-grain) [8, 9]?
- ***Popularity of content***—Whether the decision about replication should be affected by the popularity of contents or not? It is cost effective to replicate the contents taking into account their popularity [9]. However, this information may not be always available or it is extremely volatile [6].
- ***Communication cost***—The cost of communicating the contents has to be considered. It largely affects the pricing in CDN. It comprises the cost of replicating contents from the origin server to surrogate servers, delivering the contents to end users according to their requests and updating the contents.
- ***Server load***—What should be the upper bound of load on a server? Whether the load balancing should be done to improve the performance of the servers?
- ***QoS requirement***—This is a mandatory factor, i.e., the performance requirement of Web content delivery expected by end users should be the main focus while deciding about the above-mentioned factors.

3 Existing Replication Strategies

With the development of CDNs, more and more surrogate servers are established. Replication of contents on as many surrogate servers as possible is not always a good strategy. This will increase the operational cost, i.e., storage and distribution cost. Moreover, when the number of replicas of contents exceeds a threshold, the performance starts decreasing [10]. Therefore, making the decision about the optimal number of surrogate servers, their location, and capacity is essential.

It has been proved in [11] that the problem of content replication in CDN is NP-complete. This means it is not feasible to solve this problem optimally for a larger number of objects and surrogate servers. Therefore, various heuristics have been suggested based on the information available for solving the problem. Here, some of these strategies are presented to have a better understanding of content replication process in CDN.

Random—A surrogate server and an object are selected randomly with uniform probability for replication subjected to the storage constraint of autonomous systems. However, an object can be assigned to several nodes but only once at a surrogate server [11].

Popularity—Firstly, the objects are arranged in decreasing order according to popularity among its clients. These then are replicated on surrogate servers starting with the most popular object subjected to storage constraints. The object popularities are assumed same across all the servers [11].

Greedy-Single—Each server i calculates cost C_{ij} for each object j, where $C_{ij} = p_j d_{ij}(x_o)$, p_j is popularity of object j, d_{ij} is the shortest distance to a copy of object j from server i. Then, the objects are sorted in decreasing order of C_{ij} and

stored as many objects, as the storage constraint allows in this order. The C_{ij}s are calculated only once under the initial placement x_o to store the objects subjected to storage constraints. These are not adjusted when the objects are replicated [11].

Greedy-Global—The server–object pair with highest C_{ij} is selected and object j is stored on server i, resulting in a new placement x_1. The C_{ij} is recalculated according to this new placement. This process is repeated until all the storage space is used [11].

Simple Replication Algorithm (SRA)—It is a greedy heuristic assuming that no replica exists and read/write frequencies are static and known in advance. The objective is the replication of objects on surrogate servers to minimize total data transfer cost. It improves quality of solution when read requests are considerably larger than write requests as it replicates objects based on local benefit value [1].

Genetic Replication Algorithm (GRA)—It is a genetic algorithm-based heuristic that performs better than SRA even when there is a change in size of network, capacities of sites, and update ratio [1]. However, it is slower than SRA.

Adaptive Genetic Replication Algorithm (AGRA)—It is an improvement over the GRA algorithm that takes current replica distribution as input and calculates new, using the changes in read/write requests for particular objects. It quickly adapts the replica distribution according to new demands [1].

Centralized Object Replication Algorithm (CORA)—The number and placement of replicas are decided by a centralized managing site and remain fixed until reallocation is done based on access pattern and load on surrogate servers. The objective is to improve latency of read transactions [12].

Distributed Object Replication Algorithm (DORA)—This algorithm is an improvement over CORA. In this algorithm, the decision of replication and migration of objects is taken by each site at local level based on the changing demand for objects [12].

Lat-cdn—This object placement algorithm is based on total network latency produced by objects and does not take into account the popularity of objects. Initially, all the objects are placed on an origin server. The objects are replicated based on the distance to a replica of object from surrogate server under placement. The surrogate servers are cooperative with one another and have the knowledge of objects replicated on other surrogate servers with in same CDN [6].

il2p—il2p stands for integration of load and latency object placement. This approach is an improvement over Lat-cdn that takes into consideration both latency and load of the object to replicate it on surrogate servers. The load of the object is measured by multiplying access rate and size of the object. The object with maximum utility value in terms of load and latency is replicated [13].

Constraint P-Median (CPM)—A three-phase algorithm in which the number of replicas for each file is computed proportional to visiting probability of the file and considering the storage capacity constraint of surrogate servers. The replicas are placed on the servers in a way to minimize the total network cost [14].

CDN Utility Replica Placement—This heuristic replication method is based on CDN utility metric to decide the placement of contents on surrogate servers.

The metric states the relation between the number of bytes served and pulled on a surrogate server [15].

Greedy Dropping—This is a local searching algorithm for content replication based on stochastic demands and M/M/1 servers. It assumes that all the objects have same size and all the servers have same storage capacity. Further, it supposes that initially every server holds all the objects irrespective of storage capacity constraint. Then, objects are removed one by one so that the number of travel demands for the origin server increases least. This process is repeated until one of the stopping conditions is met that may result in feasible or infeasible solution [16].

Tabu Search—This is a global searching algorithm based on tabu list to avoid repetitive search. Firstly, an initial solution is found using greedy dropping heuristic. If a feasible solution is not found, then greedy adding procedure is applied to find the initial solution. After that, tabu search procedure is implemented by swapping different objects between two servers to optimize the overall performance of CDN system under storage capacity and waiting time upper bound constraints [16].

4 Comparative Analysis

The various replication strategies discussed above have focused on diverse parameters. However, their main aim is to improve the performance of Web content delivery to end users, while minimizing the cost of replication and communication. Table 1 sums up the replication strategies discussed in previous section. The columns in the table are as follows: (1) storage constraint, (2) network latency/communication cost, (3) load balancing, (4) popularity of objects/request statistics, (5) granularity, (6) other considerations, (7) objective, and (8) algorithms compared.

The comparative analysis of these strategies portrays that the algorithm used for replication should be simple and fast. All of these strategies considered storage capacity constraint which is a certain percentage of total size of objects stored on the origin server. Network latency or communication cost plays an important role in deciding the replication of contents. However, very few strategies considered balancing of load on surrogate servers during the replication process. Popularity of objects, though volatile in nature, is also significant in taking the replication decision. It is inefficient to replicate objects that require frequent updates as this will not help much to reduce the network cost. The replication granularity applied in these strategies is fine-grain. However, this may be clustered in real network environment due to the problem in handling of a large number of objects. Additional assumptions and/or factors considered by these algorithms are also pointed up in the table. The objective of the algorithms is mainly to minimize the network cost and/or improve user-perceived performance of Web content delivery. The last column in the table shows the algorithms compared and the algorithm (in bold) that outperforms the others.

Table 1 Comparative analysis of various replication strategies

Replication strategies	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Random [11]	✓				Per object	Contents from several origin servers	To minimize the average number of ASs traversed to satisfy a request	Random, popularity, greedy-single, and **greedy-global**
Popularity [11]	✓			✓	Per object	Contents from several origin servers, homogeneous request patterns	Same as above	Same as above
Greedy-single [11]	✓	✓		✓	Per object	Contents from several origin servers, homogeneous request patterns, no cooperation between surrogate servers	Same as above	Same as above
Greedy-global [11]	✓	✓		✓	Per object	Contents from several origin servers, homogeneous request patterns, aggregate request rate of surrogate server, cooperation between surrogate servers	Same as above	Same as above
SRA [1]	✓	✓		✓	Per object	Based on Greedy method, contents from several origin servers, static read and write frequencies	To minimize network traffic	SRA and **GRA** (solution quality) **SRA** and GRA (running time)
GRA [1]	✓	✓		✓	Per object	Based on genetic algorithm, contents from several origin servers, static read and write frequencies	Same as above	Same as above
AGRA [1]	✓	✓		✓	Per object	Adaptive method based on genetic algorithm, contents from several origin servers, dynamic read and write frequencies	Same as above	GRA and **AGRA**
CORA [12]	✓	✓		✓	Per object	Centralized and static replication, considers only read queries	To improve request latency	CORA and **DORA**

(continued)

Table 1 (continued)

Replication strategies	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
DORA [12]	✓	✓	✓	✓	Per object	Distributed and dynamic replication, considers only read queries	Same as above	Same as above
Lat-cdn [6]	✓	✓			Per object	Cooperative push-based scheme	To minimize average response time	Random, Popularity, and **Lat-cdn**
il2p [13]	✓	✓		✓	Per object	Cooperative push-based scheme, object load (access rate * size of object), homogeneous request patterns	Same as above	Random, Popularity, Lat-cdn, and **il2p**
CPM [14]	✓	✓		✓	Per file	All files have equal size, number of replicas of each file is proportional to its visiting probability	To minimize total network delivery cost (transmitting + place cost)	Random and **CPM**
Utility approach [15]	✓	✓		✓	Per object	CDN utility metric	To maximize the utility of surrogate servers	**Utility**, il2p, and Lat-cdn
GD [16]	✓	✓			Per object	Local search algorithm, all objects and servers have same size	To minimize the average delay in the network	Random, GD, and **TB** (solution quality) Random, **GD,** and TB (running time)
TB [16]	✓	✓	✓		Per object	Global search algorithm, all objects and servers have same size	—do—	Same as above

5 Conclusion

A content replication strategy plays an important role in improving overall performance of any CDN. In this paper, various strategies that have been proposed for replication of contents are discussed. The main aim of these strategies is to reduce the network traffic and improve the response time of Web content delivery. An optimal replication policy will not only reduce the cost but will also improve the efficiency of request routing techniques to satisfy QoS requirements of end users. This comparative analysis of existing strategies for replication may help to devise a better approach for optimal replication of contents in CDNs.

References

1. Loukopoulos, T., Ahmad, I.: Static and adaptive distributed data replication using genetic algorithms. J. Parallel Distrib. Comput. **64**(11), 1270–1285 (2004)
2. Presti, F.L., Bartolini, N., Petrioli, C.: Dynamic replica placement and user request redirection in content delivery networks. In: IEEE International Conference Communications, ICC 2005, vol. 3, pp. 1495–1501 (2005)
3. Bektaş, T., Cordeau, J.F., Erkut, E., Laporte, G.: Exact algorithms for the joint object placement and request routing problem in content distribution networks. Comput. Oper. Res. **35**(12), 3860–3884 (2008)
4. Neves, T., Ochi, L.S., Albuquerque, C.: A new hybrid heuristic for replica placement and request distribution in content distribution networks. Optim. Lett. **9**(4), 676–692 (2014)
5. Sivasubramanian, S., Szymaniak, M., Pierre, G., Steen, M.V.: Replication for web hosting systems. ACM Comput. Surv. (CSUR) **36**(3), 291–334 (2004)
6. Pallis, G., Vakali, A., Stamos, K., Sidiropoulos, A., Katsaros, D., Manolopoulos, Y.: A latency-based object placement approach in content distribution networks. In: Proceedings of 3rd Latin American Web Congress, (LA-WEB 2005), IEEE, pp. 140–147, Oct 31–Nov 2 (2005)
7. Pallis, G., Vakali, A.: Insight and perspectives for content delivery networks. Commun. ACM **49**(1), 101–106 (2006)
8. Fujita, N., Ishikawa, Y., Iwata, A., Izmailov, R.: Coarse-grain replica management strategies for dynamic replication of web content. Comput. Netw. **45**(1), 19–34 (2004)
9. Chen, Y., Qiu, L., Chen, W., Nguyen, L., Katz, R.H.: Efficient and adaptive web replication using content clustering. IEEE J. Select. Areas Commun. **21**(6), 979–994 (2003)
10. Yang, M., Fei, Z.: A model for replica placement in content distribution networks for multimedia applications. In: Proceedings of IEEE International Conference on Communications (ICC'03), IEEE, vol. 1, pp. 557–561 (2003)
11. Kangasharju, J., Roberts, J., Ross, K.W.: Object replication strategies in content distribution networks. Comput. Commun. **25**(4), 376–383 (2002)
12. Tenzakhti, F., Day, K., Ould-Khaoua, M.: Replication algorithms for the world-wide web. J. Syst. Archit. **50**(10), 591–605 (2004)
13. Pallis, G., Stamos, K., Vakali, A., Katsaros, D., Sidiropoulos, A., Manolopoulos, Y.: Replication based on objects load under a content distribution network. In: Proceedings of 22nd International Conference on Data Engineering Workshops (ICDEW'06), IEEE, p. 53 (2006)
14. Sun, J., Gao, S., Yang, W., Jiang, Z.: Heuristic replica placement algorithms in content distribution networks. J. Netw. **6**(3), 416–423 (2011)

15. Pallis, G.: Improving content delivery by exploiting the utility of CDN servers. In: Proceedings of 5th International Conference Data Management in Cloud, Grid and P2P Systems (Globe). LNCS. Springer, Berlin, vol. 7450, pp. 88–99 (2012)
16. Yang, C., Huang, L., Leng, B., Xu, H., Wang, X.: Replica placement in content delivery networks with stochastic demands and M/M/1 servers. In: IEEE International Performance Computing and Communications Conference (IPCCC), pp. 1–8 (2014)

An Assessment of Reactive Routing Protocols in Cognitive Radio Ad Hoc Networks (CRAHNs)

Shiraz Khurana and Shuchita Upadhyaya

Abstract Cognitive radio ad hoc networks (CRAHNs) emerged to solve problems associated with wireless networking due to limited available spectrum. The problem of spectrum inadequacy can be removed by exploiting the usage of existing wireless spectrum intelligently. In a CRAHNs, secondary users SUs (unlicensed users) are able to exploit and utilize underused channel but should vacate the channels if any interference is caused to primary users PUs (licensed users) that own the channels. In this paper, various routing challenges in routing of CRAHNs are introduced. Then reactive routing schemes are discussed along with challenges it addresses. An analytic assessment is carried out in the end to identify the covered and uncovered challenges in reactive routing protocols and further concise of direction to be taken to improve upon the protocol.

1 Introduction

Cognitive radio ad hoc networks (CRAHNs) emerged to solve problems associated with wireless networking due to limited available spectrum. The problem of spectrum inadequacy can be removed by exploiting the usage of existing wireless spectrum intelligently. Earlier the spectrum is allocated using static spectrum allocation policies which have partitioned the radio spectrum into two parts: licensed and unlicensed bands. Licensed bands are given to licensed users which do not transmit all the times results into spectral resource waste. Examples of licensed bands are mobile carriers, television broadcasting.

Unlicensed users operate in unlicensed bands which supports variety of applications (e.g., sensor networks, personal area networks (PAN), mesh networks,

S. Khurana (✉) · S. Upadhyaya
Department of Computer Science and Applications (DCSA), Kurukshetra University, Kurukshetra, India
e-mail: shiraz.khurana@gmail.com

S. Upadhyaya
e-mail: shuchita_bhasin@yahoo.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_37

wireless local area networks (WLANs)), which has caused congestion in this category of band. To solve this problem of spectrum insufficiency in licensed band, the Federal Communication Commission (FCC) has recently approved the usage of unlicensed devices in licensed band. According to FCC [1] in static allocation scheme, the average utilization of licensed band varies from 15 to 85% and rest of the time spectrum goes unused. Henceforth, the concept of dynamic spectrum access (DSA) was introduced. DSA was proposed to solve these spectrum insufficiency problems. The software-defined radio (SDR) allows the development of such devices which can be adjusted to function in a wide spectrum band such devices are called cognitive radio (CR) devices. These devices can change their transmitting parameter like (operating spectrum, modulation, transmission power, and communication technology) on the basis of surrounding environment. These devices can identify spectrum blocks which are not getting used for communication and intelligently access this vacant spectrum blocks also known as spectrum holes. Devices that are capable of such properties can be collaborated to create a network called cognitive radio networks (CRNs) [2].

CRNs can be created with or without fixed network backbone. With fixed infrastructure support is called as centralized network, in which a base station provides single-hop connections to communicating nodes. Without any fixed infrastructure support it called as distributed network, in this nodes communicate with each other in an ad hoc manner [3], and this is called cognitive radio ad hoc networks (CRAHNs).

In CRAHNs, licensed users also known as primary users (PUs) will have priority in using spectrum; they have a license to operate in certain band. Unlicensed user or secondary user (SU) accesses these licensed bands in such a manner that is not reliable. SU have cognitive radio capability and they can use vacant spectrum band to carry on their activities without interrupting the transmission PU. At any instant, if PUs want to use its channel for transmission, it can do so. SUs must leave their current operating channels immediately. There should be no interference with PU transmission.

The remainder of this research paper is structured as follow: Sect. 2 discusses the need for new routing protocols in cognitive radio ad hoc networks and various challenges involved in this. Section 3 presents various types of routing protocols in CRAHNs. Section 4 discusses related work available in literature. Section 5 presents an analytical review on related work and challenge associated with routing in CRAHNs. Section 6 concludes the findings of this paper.

2 Need for Routing in CRAHNs

Routing in CRAHNs is quite different from traditional ad hoc networks routing due to various kinds of additional challenges involved in CRAHNs. The concept is depicted in Fig. 1.

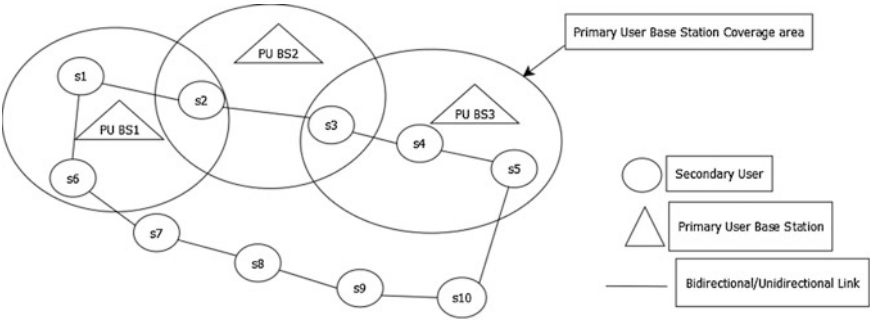


Fig. 1 Routing in CRAHNs

Figure 1 shows a CRN with three primary user base stations and various secondary users. Consider a case where SU (S1) wants to establish a route with SU (S5). Using a traditional mobile ad hoc routing protocol, it may provide a route with minimum number of hops with path (S1–S2–S3–S4–S5). However, this may provide poor network performance because the route passes through the three primary user base stations resulting in high interference to the primary users. While cognitive radio-based routing protocol may provide a route with larger number of hops (S1–S6–S8–S9–S10–S5) that generates less interference to the primary users and this increases end-to-end performance for SUs. So, it is clearly visible from the example given above that traditional routing protocols are not adequate for routing packets in CRAHNs.

2.1 Routing Challenges in CRAHNs

There are few key challenges in routing of packets in CRAHNs mentioned in literature [2–4]:

(1) **Variance in availability of channel**: The availability of the channel for data transmission is highly dependent on primary user's channel utilization and mobility of secondary user. A channel which is free from PU's activities will be preferred more rather than highly utilized one. Since chances of link failure are more as compared to traditional ad hoc networks so more channel switches are necessary.
(2) **Fusion of various operating environments**: Data can be exchanged between two secondary users if and only if they have at least one channel operating on same frequency. Every channel has different data rates and transmission range. A low power secondary user in routing path can be a bottleneck for data transmission. So, this parameter can also affect route selection.
(3) **Impractical scenario for control channel**: When nodes communicate in an ad hoc manner, they usually exchange control information in a fixed control

channel (CC). The availability of permanent and all time availability of CC cannot be guaranteed. So, chances of information loss of link failure are more in CRAHNs and selecting a route without channel information might not result into optimum paths. So, it is very important to consider this as a challenge.

(4) **Minimizing switching delay and back-off delay**: If a PU wants to access its licensed channel which is being used by a SU, it has only two choices of actions available. Either it can switch to new channel resulting into a switching delay or it can wait for the PU to finish its work resulting into back-off delay. Routing schemes should minimize both channel switch delay and back-off delay as these delays affect the routing performance.

(5) **Broadcasting on multiple channels**: Secondary users might be using any of the vacant channels available so a single broadcast on a single channel might not reach all the neighboring SUs. Henceforth, it is required to broadcast on multiple channels resulting into increased total number of transmissions on available bandwidth. So, it is suggested that proposed protocol must have some mechanism to minimize this traffic in CRAHNs.

(6) **Variety of SUs**: CRAHNs may have secondary users with different capability, e.g., transmission power and processing speed, for instance, an in-between SU with lower capacity may become hindrance in data flow due to its limited capacity and this can reduce performance. Therefore, routing protocols to be designed should consider variety of SUs as an important challenge.

(7) **Flexibility of secondary users**: This is another major challenge and also observed in mobile ad hoc networks. It is very difficult to maintain routes when secondary users are also mobile. It has considerable impact on the number of channel switches and energy consumption. Sudden movement of secondary users makes it more challenging to minimize interference with PUs.

(8) **Balance among number of hops and network-wide performance**: Selection of hops occurring in a route should be done carefully. A route with lower number of hops might have some advantages and disadvantages. Lower number of hops results into large propagation distance so as congestion. Since distance among nodes is quite large so chances of link failure and more energy consumption increases.

(9) **Energy preservation throughout network**: Multiple transmissions might be required in route discovery and route maintenance phase leads to more energy consumption, for example, flooding of RREQ control messages all over the networks incurs energy consumption and in route maintenance phase, to maintain routes lots of messages needs to be propelled on to the network that consumes lots of energy in network. Routing protocol should consider this energy preservation.

(10) **Primary user protection**: This is the main challenge which differentiates between ad hoc networks and CRAHNs. Primary users are the licensed users which have priority in using spectrum. The transmission of primary users

must be saved on all cost. If any SU is using spectrum of PU, the SU must abandon its transmission on that channel until or unless PU itself surrenders that channel.

Apart from these challenges mentioned in literature, challenge related to QoS has been anticipated in the context.

Quality of Service (QoS): This challenge can be seen as a collection of various challenges. QoS of a network can be measured by these metrics: network availability, bandwidth (throughput), Jitter, out of order delivery, dropped packet, latency.

3 Types of Routing Protocols in CRAHNs [5]

The routing protocols available in literature can be categorized into the following categories.

3.1 Proactive Protocols

Proactive routing protocol, every secondary user node in the network has one or more routing tables that are updated frequently. Each secondary user broadcast messages to other secondary users on regular intervals or to know if there is any modification in a network. This incurs additional cost to maintain up-to-date information, consequently, waste of bandwidth but it shows the real availability of the network. It also helps in reducing end-to-end delay. It includes following traditional routing protocols; fisheye state routing (FSR), destination sequenced distance vector (DSDV), etc.

3.2 Reactive Protocols

In contrast, reactive protocols, also identified as on-demand routing protocols, seek to set up the routes on demand. Every secondary user node in the network discovers or maintains a route based on-demand. Source starts the route discovery phase by broadcasting the route request packet, and the bandwidth is utilized only at the time the data is being transferred. The advantage is less overhead requires less routing information but produces substantial amount of control messages for route discovery and route maintenance. The examples of these traditional reactive protocols are ad hoc on demand routing (AODV) and dynamic source routing (DSR) protocols, etc.

3.3 Hybrid Protocols

Hybrid protocols have the advantage of both proactive and reactive routing protocols. It utilizes both proactive and reactive protocols to perform the routing. It provides a good balance of trade-off between communication overhead and delay. Example of traditional hybrid routing protocol is zone routing protocol (ZRP), etc.

In CRAHNs, we can use any of the routing protocols. Although research work has been done for all of these kinds of routing protocols, but according to the characteristics of cognitive radio networks, we found the reactive routing protocol most suitable one and an identification of the challenges they overcome.

Hence, the focus of Sect. 4 is on reactive routing protocols.

4 Reactive Routing Protocol Schemes in CRAHNs

Cheng et al. [6] suggested a flow-level channel selection method, which minimizes end-to-end delay of each flow by reducing two types of delays, channel switching delay for each flow along its path, and back-off delay for intersecting flows. It addresses routing challenges 1, 2, and 4. The channel selection method provides a suitable trade-off between these two delays. When a secondary user wants to switch between different flows, if it is switched to an unused available channel, it may create switching delay. If an assigned available channel is added to a new flow, it may create back-off delay. SU nodes share information (such as switching, queuing delays, back-off delays) among neighbor nodes in order to discover and choose better routes and re-routing decisions.

In [7], author targets challenge 1, 3, and 4. They proposed a joint framework of routing and channel assignment that exploits variance in channels to optimize routing performance and increase the network utilization. It works without central control channel (CCC). They suggested keeping a backup channel to satisfy for channel assignment to improve end-to-end performance by avoiding re-route procedures.

Kamruzzaman et al. [8] proposed a routing protocol which addresses spectrum and energy aware routing with channel time slot allocation for multi-hop CRAHNs which assign traffic over time slots of different channels along a route in order to maximize network throughput. It addresses challenges 8 and 9. The routing scheme with channel time slot assignment can reduce energy consumption and reduce traffic across multiple channels in various time slots. It also leads to a considerable increase in network efficiency and shortens end-to-end delay.

In [9], Wang et al. suggested a routing scheme that jointly undertakes the inter-flow intervention and cross-layer optimization for channel assignment and path selection for end-to-end route in order to enhance the performance of a network. The suitable transmission power is selected to reduce the interference. It deals with challenges 4 and 7. The interference between the flows is minimized by

selecting suitable transmission power. It allots weights to routes so as to select a route with minimal intervention and the least number of the channel switches. It chooses subsequent hops and channels by a cross-layer design, which includes the physical, data link layer, and network layer. The physical and data link layers control the transmission power and collect information about the channel, particularly inter-flow interference and network layer performs choice of route using this information.

The focus of [10] is on reducing the end-to-end delay. It addresses challenge 4. A maximum flow segment-based approach is added to channel selection in cognitive radio networks. It reduces the number of times channel is switched along a flow. The author has reported to reduce the end-to-end delay by 50%. In MFS-based approach search for a new chain is begin at the destination toward source node. Since every node can have different number of channels, so it starts looking for a path from destination to source, without changing its channel. When the search gets terminated on some intermediate node, the procedure is repeated from that node again. This metric is combined with AODV to get better result in routing of CRAHNs.

In [11], Qin et al. propose a routing protocol which handles the problem occurred due to emergence of primary user. It intelligently does spectrum selection and routing. It differentiates between spectrum holes or opportunities based on their duration of availability, so that unnecessary switch between different channels is avoided. The system selects channels with low PU usage and the less number of hops to the destination, to diminish the channel switches and interruption to PU transmission. After establishing a path, each SU monitors a set of backup channels continuously, and share that information with their respective neighbors of SU. Therefore, when the PU reappears in the current operating channel, groups switch SU for the backup channel and continue with their communications. It addresses challenges 1, 4, 8, and 10.

In [12], author discussed a distributed routing protocol named Spectrum Aware Routing protocol for Cognitive ad Hoc networks (SEARCH). Their approach is to mutually optimize the path and channel selection to avoid regions of PU activity during route formation so that the path latency is reduced. It adapts to the newly discovered and lost spectrum opportunity during route operation. Greedy geographic routing is applied on all the channels to reach the destination by identifying the primary user's activity region. Path information obtained from different channels is used by the destination node in a series of optimization measures to determine the optimal route in an effective manner. It addresses challenges 1 and 10.

Xi et al. proposed [13] a path-centric channel allocation algorithm for multi-hop ad hoc cognitive networks. They suggested a protocol that couples routing and channel allocation determining the channel assignments for each node to achieve global optimized performance. The proposed algorithm does not focus on dynamic channel allocation and PU activities. It only addresses the challenge 6.

Xie et al. [14] addressed the quality of services issue on routes for group communication in cognitive radio ad hoc networks. Since the nodes have different ambient environment in the CR network, the secondary users have different

available channels. This feature introduces additional complications for coordination and communication between nodes in a cognitive radio network. QoS is preserved in group communication by finding a multicast tree for each member in the group communication, which is rooted from a member and extends to all the other members, and each compound meets the trees QoS requirements. Due to the diversity in channel availability, it may require several broadcasts by the source, in order to obtain the messages received by all locations. Therefore, it is essential to construct a tree of routing communications and schedule the transmission along the tree such that the total bandwidth usage is minimized.

In Yang et al. [15] proposed an approach to reactively initiate route calculation and selection of frequency bands in a multi-hop cognitive radio networks. Availability channel nodes may change overtime, which is aimed at changing the network topology. Thus, channel availability information must be shared among secondary users. They also discussed the impact from multi-frequency flow and proposed a new scheduling scheme for intersecting nodes. Metric that evaluates the efficacy of routes, taking into account the spectrum of switching delays and back-off time is defined. It addresses challenges 1 and 4.

5 Analytic Overview

It has been observed that most of the protocols discussed here focused on minimizing switching delay and back-off delay. Lots of work has been done to cope up with diversity or variance in channel availability and solving problems associated with different kinds of operating environments [4, 9, 12]. To get full benefits of CRAHNs, all the challenges discussed here should be satisfied by the proposed routing protocol. But on the basis of literature discussed here, it is clearly visible that there is a need to combine the advantages of two or more protocols. For example, [11] satisfy challenges 1, 4, 8, and 10. It can be modified to support challenge 6 to solve issue related to mobility of secondary user. We should not only consider the primary issues related to CRAHNs but also secondary issues. For instance, very less work is available in literature in minimizing energy consumption in route discovery and maintenance; work can be extended in this direction for the protocol mentioned in Sect. 4. Above all the challenge of QoS provision is an issue that has attracted least attention in literature. Further work needs to be carried out in this direction also.

6 Conclusion

Cognitive radio networks (CRN) can be considered as next-generation wireless networks. It differs from traditional ad hoc networks due to some different criterion, e.g., primary user protection, variance in availability of channel, fusion of various

operating environments, impractical scenario for common control channel. This paper first discussed the challenges involved in CRAHNs and then various routing schemes for reactive routing protocols are discussed, and each scheme is identified with challenges it covers. It has been observed that none of the scheme covers all the challenges. Numerous challenges are still not addressed in routing schemes. Future work needs to complement the advantages of one protocol into another.

References

1. F.C. Commission, Spectrum policy task force, Technical report, Nov 2002
2. Cesana, M., Cuomo, F., Ekici, E.: Routing in cognitive radio networks: challenges and solutions. Elsevier Ad Hoc Netw. (2010)
3. Al-Rawi, H.A.A., Alvin Yau, K.-L.: Routing in distributed radio networks: a survey. Wireless Pers. Commun. **69**, 1983–2020 (2013)
4. Akyildiz, I.F., Lee, W.-Y., Chowdhury, K.R.: CRAHNs: cognitive radio ad hoc networks. Elsevier Ad Hoc Netw. (2009)
5. Kaur, H. et al. A survey of reactive, proactive and hybrid routing protocols in MANET: a review. IJCSIT **4**(3), 498–500 (2013)
6. Cheng, G., Liu, W., Li, Y., Cheng, W.: Spectrum aware on-demand routing in cognitive radio networks. In: New Frontiers in Dynamic Spectrum Access Networks, pp. 571–574 (2007)
7. Zeeshan, M., Fahad Manzor, M., Qadir, J.: Backup channel and cooperative channel switching on-demand routing protocol for multi-hop cognitive radio ad hoc networks (BCCCS). In: 6th International Conference on Emerging Technologies (ICET), pp. 394–399 (2010)
8. Kamruzzaman, S.M., Kim, E., Jeong, D.G.: Spectrum and energy aware routing protocol for cognitive radio ad hoc networks. In: Proceedings of IEEE ICC 2011, pp. 1–5 (2011)
9. Wang, J., Huang, Y.: A cross-layer design of channel assignment and routing in cognitive radio networks. In: 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), pp. 542–547 (2010)
10. Dutkiewicz, E., et al.: Maximum flow segment based channel assignment and routing in cognitive radio networks. In: Vehicular Technology Conference (VTC), pp. 1–6 (2011)
11. Qin, L., Wang, J., Li, S.: Stability-driven routing and spectrum selection protocol in cognitive radio networks. In: International Conference on Common Technology and Applications (ICCTA), pp. 269–273 (2009)
12. Chowdhury, K.R., Felice, M.D.: Search: a routing protocol for mobile cognitive radio ad-hoc networks. Comput. Commun. **32**, 1983–1997 (2009) (Elsevier)
13. Xin, C., Ma, L., Shen, C.-C.: Path-Centic channel assignment in cognitive radio wireless networks. Crown Com **2007**, 313–320 (2007)
14. Xie, L., Xi, J.: A QoS routing algorithm for group communication in cognitive radio ad hoc networks. In: International Conference on Mechatronic Science (2011)
15. Yang, Z., Cheng, G., Liu, W., Yuan, W., Cheng, W.: Local coordination based routing and spectrum assignment in multi-hop cognitive radio networks. Mobile Netw. Appl. **13**(1–2), 67–81 (2008)

Analysis and Simulation of Low-Energy Adaptive Clustering Hierarchy Protocol

Amita Yadav and Suresh Kumar

Abstract Wireless Sensor Network (WSNs) is a collection of small, self-powered devices with sensing capabilities. Sensor nodes are deployed for carrying out various applications such as disaster recovery, industrial control, health monitoring, environmental monitoring, etc. Battery is the main source of energy for sensor nodes. However, because of the limited storage capacity of batteries nodes remain operational for a limited amount of time. Energy efficiency or energy consumption plays a major role in the lifetime of WSN. It is very difficult or sometimes impossible to replace or recharge the battery in remote areas, e.g., deep forest. Hence, an energy saving of a sensor node is a major design issue. There has been a flourish of research efforts on prolonging the lifetime of WSN. Since environmental sensing and transmission of information to the base station are an important task in WSN that consumes energy. Therefore, routing plays a major role. Advancement in WSNs led to the development of various routing protocols. In this paper, we have simulated the LEACH protocol using MANNASIM framework. Network performance is analyzed in terms of total energy consumption, total number of live nodes in the network by varying the number of clusters using Network Simulator (NS-2).

Keywords Cluster head · Energy efficiency · LEACH · NS-2

1 Introduction

Every sensor node is equipped with one or more sensing units, a microcontroller, a radio transceiver for receiving and transmission of information, and a source of energy such as battery (Fig. 1). The sensor node in the sensor network senses the

A. Yadav (✉)
MSIT, New Delhi, India
e-mail: amitaay@gmail.com

S. Kumar
MRIU, Faridabad, India
e-mail: suresh.fet@mriu.edu.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_38

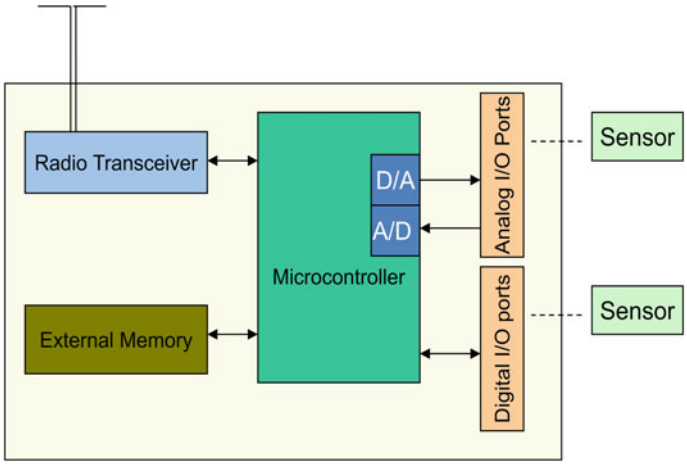


Fig. 1 Architecture of sensor node

interest region for some ambient condition and then converts it into electrical signals. Sensor node senses the temperature, humidity of constrained area. Depending upon the application requirement acoustic signals, seismographic data of the environment or maybe motion can also be sensed. The bearing of living creatures can, likewise, be observed [1]. Application areas of WSNs include battlefield monitoring, forest fire and traffic monitoring, etc. Based on application and capability, electrical signal processed for revealing some vicinity properties or compressed to reduce communication overhead. The sensor nodes form an ad hoc network, which refers as wireless sensor networks (WSNs). The communication unit wirelessly sends such data toward a central control directly or via other sensors. This central control is often referred as a sink or base station.

Generally, sensor nodes are energy constrained as they rely on finite sources of energy like battery. In some applications like disaster management, where human intervention is not possible, battery replacement is quite a difficult task. Energy harvesting from the environment is currently a promising research area. Due to limited source of energy, a lot of research work needs to be done from every possible aspect in gaining energy efficiency. Other key characteristics include limited computation and communication capability.

In Wireless Sensor Network, devices communicate wirelessly. If the sink is at distant place and because of limited transmission range of nodes, communication between nodes and sink requires intermediate nodes to forward the message. Therefore, devices have the responsibility of routing the messages as well as sensing the environment. Different routing protocols are required for such type of communication in wireless sensor networks. Inherent constraint and different characteristics from other wireless network pose great challenges to routing in WSN.

Various routing protocols for energy efficiency are already developed. Clustering is one of the techniques in routing. Nodes are grouped together to form clusters. In a network, there may be many clusters. In every cluster, there is a cluster head. Nodes communicate with the cluster head (CH), and CH sends data to the base station. Clusters are formed using different cluster formation algorithms [2]. Although formation and maintenance of clusters incur cost, the better performance of cluster-based protocols seeks attention of the researchers.

Among many hierarchal protocols, LEACH [3] (Low-energy adaptive clustering hierarchy protocol) is the most promising one. Lot of research work is still going on for the improvement of LEACH protocol.

This paper analyzes the cluster-based LEACH protocol for different performance metrics, e.g., total energy consumption in network. Very few papers have discussed the simulation of LEACH protocol using NS-2. We have discussed the LEACH protocol in brief, its limitations, and future scope.

2 LEACH Protocol

LEACH [3] is one of the most commonly used hierarchical routing protocols in wireless sensor networks [4], in which nodes in the network are divided into clusters. This is a single-hop communication protocol. Nodes closer to the cluster head join the cluster, only when they receive strong signals from the respective cluster head. Data transmits from sensor node to the base station via cluster head. Random selection of cluster heads reduces the energy consumption of the cluster head nodes. Cluster head aggregates, compresses the data using different techniques [5], and then transmits the information to the base station. LEACH uses distributed algorithm for the creation of cluster heads. Any node in the network can get a chance to become a cluster head, therefore, leads to efficient energy utilization and longer lifetime of the network.

Initially, the number of clusters or cluster heads is assumed. If CH node dies, all the nodes lose communication. Therefore, LEACH supports CH rotation.

In this protocol, there are two phases in a round.

(I) Setup phase and
(II) Steady-state phase.

In setup phase, each node decides to which cluster it belongs. CH broadcast the advertisement messages using CSMA-MAC protocol to nodes present in the network. The node which are not CHs, transmit the join request back to the CH to which cluster it belongs using the CSMA-MAC based on the received signal strength [6].

In setup phase, the CH sets the TDMA schedule for each node in the cluster [7]. The nodes send the sensed data based on their TDMA time slot to the CH. If one node is sending in their respective slot, other nodes will be in sleep state thus

minimizing the energy consumption. The setup phase comprises of allotment of cluster heads and the TDMA schedule to each sensor nodes. Steady-state phase is long as compared to setup phase, which minimizes the overhead of cluster formation in setup phase [7].

Steady-state phase deals with the transmission of sensed information from sensor nodes to the CH in their respective TDMA slot and then transmission of data from CH to the base station. Transmission of frames from nodes to the cluster head node is a low-energy transmission because of the join request initiated by the sensor nodes based on the strong signal received from CH during setup phase. The cluster head node is always in a receiving mode. Once the entire data received from nodes, CH performs the aggregation operations and sends the aggregated data to the base station [6]. This is a high-energy transmission because of the large data and distance between the base station and cluster head nodes.

3 Simulation Parameters

We have simulated the LEACH protocol using MANNASIM framework integrated with NS-2.35 on Ubuntu 13.04. We have investigated how the variation in a number of cluster heads affects the energy consumption of the wireless sensor network. Network performance is analyzed in terms of total number of live nodes and average energy consumption by changing the number of cluster heads and even the transmission range of common nodes. Set the parameters of simulation as given in Table 1.

For Figs. 2 and 3, transmission range is set as 50 m and for Figs. 4 and 5, transmission range is set as 30 m.

Table 1 Simulation parameters

S. No.	Parameters	Values
1	Numbers of nodes	100
2	Scenario size	500 × 500 (m^2)
3	Simulation time	500 s
4	Base station location	50 × 175
5	Transmission range	50 m
6	Percentage of cluster head	3, 4, 5, 6, 8, 10, 12
7	Initial energy	10 J
8	Node distribution	Grid
9	Min. packet in IFQ	50
10	Antenna model	Antenna/omni antenna

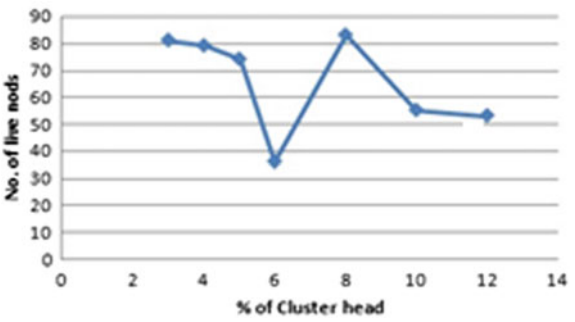


Fig. 2 Percentage of cluster head versus number of live nodes (transmission range = 50 m)

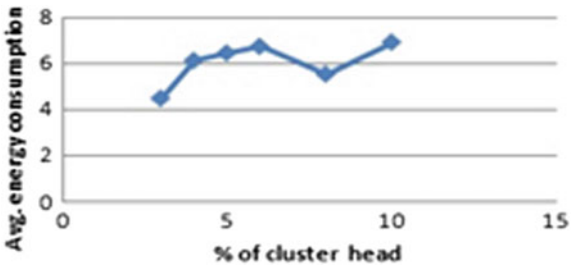


Fig. 3 Percentage of cluster head versus average energy consumption (transmission range = 50 m)

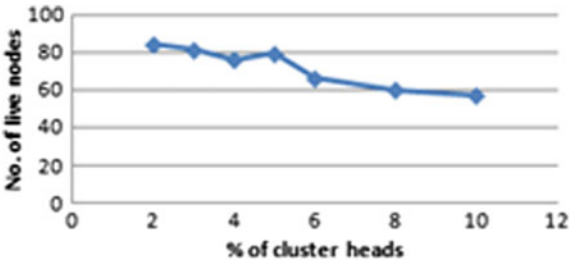


Fig. 4 Percentage of cluster head versus number of live nodes (transmission range = 30 m)

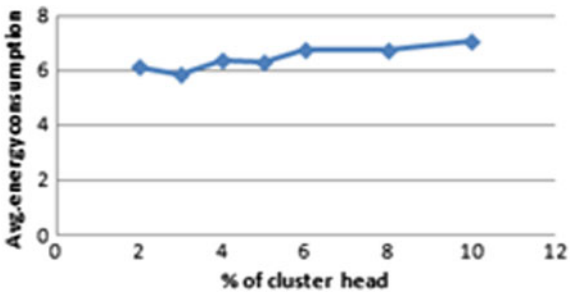


Fig. 5 Percentage of cluster head versus average energy consumption (transmission range = 30 m)

4 Results

First simulation result as shown in Fig. 2 shows that as the percentage of cluster head increases the total number of live nodes decreases but suddenly shows increment for 8% and after that again decreases.

Figure 3 shows the average energy consumption of the network versus percentage of cluster heads. As the number of cluster head increases, the average energy consumption increases. Energy consumption decreases again for 8% cluster head, but an overall increase in the energy consumption had been seen.

Figure 4 also shows the number of live nodes decreases, as the number of cluster head varies. Energy consumption also increases with the increases in number of cluster heads Fig. 5.

5 LEACH Limitations/Assumptions

1. LEACH supports random rotation of cluster heads and assumes that all nodes have similar residual energy after a round, which is not true.
2. There is no guarantee of even distribution of cluster heads in the entire network.
3. The number of cluster heads is predefined in the network, and there is no discussion on optimal cluster head selection.
4. Cluster sizes may vary in the network, as the number of nodes is not equal per cluster.
5. LEACH is well suited for small networks. Single-hop communications do not allow the large network.
6. LEACH assumes that nodes always have data to send in their respective TDMA slot, which is not true.

6 Conclusions

LEACH is a basic energy efficient routing protocol. Simulation results of NS-2 have shown that there is a decrease in number of live nodes and random energy consumption with the increase in the percentage of cluster heads because the time and energy are required in setting up of clusters. Optimal number of cluster head selection minimizes the energy consumption, which increases the number of live nodes in the network. By analyzing the simulations and limitations of LEACH protocol, the cluster formation algorithm of different routing protocols will be explored in future for better network performance.

References

1. Culler, D., Estrin, D., Srivastava, M.: Overview of sensor networks. Special Issue in Sensor Networks, IEEE Computer Society, pp. 41–49, Aug 2004
2. Brachman, A.: Simulation Comparison of LEACH-Based Routing Protocols for Wireless Sensor Networks. Springer-Verlag, Berlin, Heidelberg (2013)
3. Heinzelman, W.B., Chandrakasan, A.P., Balakrishnan, H.: Energy-efficient communication protocol for wireless micro sensor networks. In: Proceedings of 33rd Annual Hawaii International Conference on System Sciences, vol. 2, p. 10, Jan 2000
4. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. Ad Hoc Netw. **3**, 325–349 (2005)
5. Yao, K., Hudson, R., Reed, C., Chen, D., Lorenzelli, F.: Blind beam forming on a randomly distributed sensor array system. In: Proceedings of IEEE Workshop Signal Processing Systems (1998)
6. Tao, L., Qing-Xin, Z., Yu-Yu, Z.: An energy efficient adaptive clustering protocol for wireless sensor network. Sens. Transducers, 1726–5479 (2013)
7. Tyagi, S., Kumar, N.: A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks. J. Netw. Comput. Appl. (2013). doi:10.1016/j.jnca.2012.12.001

Packet Delay Prediction in MANET Using Artificial Neural Network

Harshita Tuli and Sanjay Kumar

Abstract MANETs are composed of sensing nodes which organize themselves into temporary topologies and forward data to each other. Delay prediction of packets in MANET depends on many variables; some of them are length of path from source to destination, hop count, mobility of nodes, interference from other neighbours, bandwidth and past values of delay, etc. In order to make data delivery more reliable, accurate prediction of delay is a necessary task. The goal of this paper is to predict the source to destination delay in MANETs in presence of all the factors affecting the delivery of packet. Simulation environment is NS3, and the prediction of delay involved is done by ANN techniques.

Keywords MANET · Delay · Artificial neural network · NS3 · MATLAB

1 Introduction

Mobile ad hoc networks (MANETs) are group of mutable nodes (communicating devices) coupled by wireless links. All nodes are self-governing in nature and dynamically organize into random and alternate network topologies. Traditionally, application areas of MANETs were tactical networks which improve battlefield communication where the network cannot rely on access to a fixed communication infrastructure. The network is ad hoc because of its special characteristics of each node's wish to pass on data to other nodes. This implies that every node performs the role of host and router simultaneously since it holds the information of routes between its neighbours and contributes and maintains network connectivity. For such an erratic network, routing is much more complex than in traditional wireless systems. Thus, in a MANET, quality of service is of prime concern. Quality of

H. Tuli (✉) · S. Kumar
Jaipur National University, Jaipur, India
e-mail: harshitatuli@gmail.com

S. Kumar
e-mail: sanjaysatyam786@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_39

service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. In order to provide quality delivery to real-time applications, it is imperative that ad hoc networks provide QoS support in terms of throughput, delay, jitter, reliability, etc. There are many researchers who have tried to address the issue of QoS many times through many ways. In this paper, we have tried to focus on delay which is an important QoS metric in ad hoc networks routing. Delay is defined as summation of transmission, propagation and processing delay. Estimation of end-to-end packet delay in MANET is complex because transmission, queuing and processing delays have to be considered, which in turn depends on many factors such as path length from source to sink, intermediate hops, link expiration time, mobility and interference. Because of nodes mobility, some of links may fail as soon as the path is established. This failure causes connection interruption and data loss. Many researchers have addressed this issue and tried to predict delay using many influential tools. Artificial neural networks are also one of them which provide the facility to classify any activity based on limited and incomplete data sources. Artificial intelligence/neural networks is an area which plays an important role in developing the knowledgeable system. There are several features of neural networks that make them beneficial for forecasting which are as follows:

(i) Neural networks are able to learn from limited available examples.
(ii) Neural networks can generalize after learning the data presented to them.

In this paper, we have tried to determine the total delay sum of packets from source to destination in presence of all the factors affecting delay. We have used ANN time series prediction model to predict the delay. The paper is categorized into different sections such as background work, data collection, ANN model, conclusion and future work and reference section.

2 Background

Delay prediction has been done by scientists in [1–4] papers in many ways. Singh et al. in [1] have used artificial neural network for prediction of end-to-end packet delay in MANET. For evaluation of delay path length, a number of neighbours between source and destination have been used as input parameters. In their study, they have applied radial basis function (RBF) network and generalized regression neural network (GRNN) for their analysis and evaluated that GRNN gives better prediction than RBF. [3]. In [5], Singh et al. have tried to predict the delay using fuzzy logic-based model and found that trapezoidal fuzzy-number-based model has stood at good position in prediction in terms of various criteria of performance of network. After the detailed study on this area of predicting delay, it has been observed that because of mobility of nodes, links on shortest path may fail as soon as the path is established. So, in papers [6–8], authors have focused on mobility prediction of nodes through different ways in order to ensure the packet delivery. In

[8], average E2E delay and throughput with restricted the mobility of nodes have been analysed. Authors proposed a model considering random access multihop wireless networks as open G/G/1 queuing networks and use the diffusion approximation in order to evaluate the average end-to-end delay. They have used mean service time of nodes to obtain the maximum achievable per-node throughput. Sheikhan and Hemmati, in [4], have presented multipath routing algorithm in MANETs and done a study on a transient chaotic neural network (TCNN) which chooses more reliable path for transferring packets. Also delay occurs due to packet dropping problem of nodes in order to conserve their battery which is selfishness of nodes. In [9] this property of nodes has been studied and protocol to control this behaviour is proposed which ensures safe delivery of packets. From the literature reviewed, it has been observed that delay is the most important metric of any network and it is aggressive too in case of MANETs, so prediction techniques are required to ensure safe and timely delivery of packets among source–destination pairs.

3 Data Collection

The data packet transmission and reception is simulated on NS3. The number of nodes is 30. Mobility model is taken to be of RandomWaypoint for movement of nodes with a speed of 20 m/s in an area of 300 $\times$ 1500 m. Friis loss model and ad hoc mode of Wi-fi with a 2 Mb/s rate (802.11b) have been considered for study. The power of transmission is set to 7.5 dBm. Routing protocol used is AODV protocol. By default, 10 source/sink data pairs for UDP traffic with rate of 2.048 Kb/s each are considered. NetAnim animator has been used to animate the flow of data packets. The data for analysis is taken after simulation which is saved in flow-monitor file. In flow-monitor file, the succeeding attributes can be obtained:

1. The time when the transmission of packets starts;
2. The time when the transmission of packets ends;
3. The time when destination starts receiving the packets;
4. The time when packet reception is ended;

Mean hop count is evaluated by understated expression.
Mean hop count = 1 + (no. of times a packet forwarded/received packets) [7].

4 ANN Model Development

For predictions to be accurate, the input variables are of supreme importance as they determine the structure of ANN. And moreover, time series prediction techniques can predict the values of future data set of the series based on past data observations

[10]. The number of input variables has implications on results too [10]. It may result in over fitting of data. For this paper, we have considered last delay and hop count as input variables. MATLAB has been used for implementation of neural network with hop count and last delay are the input parameters [11–14]. In this study, 70% of data set has been used for training, 15% for validation and 15% for testing process. For time series prediction, training of network is done using trainlm function. Figure 3 shows that error has decreased in testing phase, and it also shows the error histogram.

5 Results and Discussion

Results of simulation are shown in response graph in Fig. 1 which shows comparison of actual delay and predicted delay. It can be observed that predicted and actual outputs are close at some instances, and error has gone to zero for validation and testing sets. In other words, the computed error is low at instances which mean training done by the model is good, and also Fig. 2 shows best performance at epoch 2 but with very high mean square error (MSE) but finally at 8th epoch it has touched zero. In Fig. 3, the blue bars represent training data, the green bars

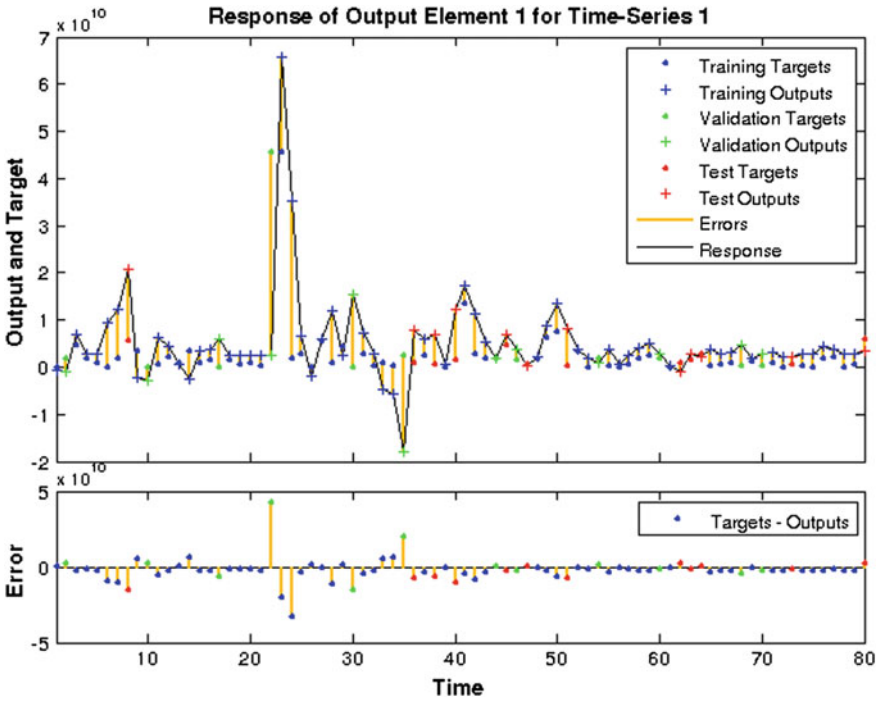


Fig. 1 Predicted versus actual delay

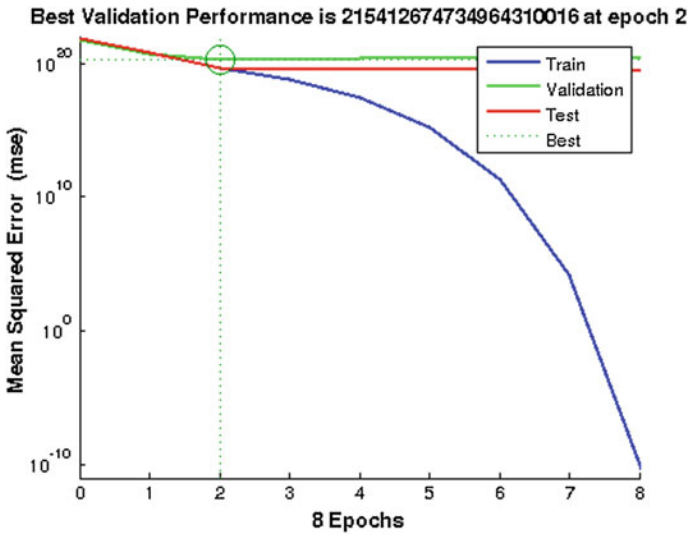


Fig. 2 Performance plot of simulated data

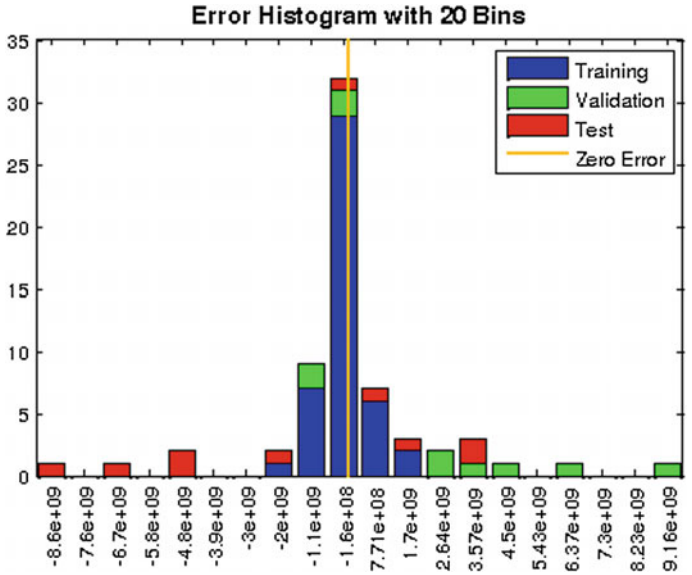


Fig. 3 Error histogram showing zero error

represent validation data, and the red bars represent testing data which shows that at −1.6e + 8 is the value where zero error has been achieved. Regression *R* Values measure the correlation between output and target the value for *R* in this is 0.886 which shows the prediction done by the model is close to actual values of delay.

6 Conclusion and Future Work

In above study, we have applied neural networks to model end-to-end delay of data packets in MANET. For modelling delay, we have used Levenberg–Marquardt back propagation algorithm for time series prediction. For our delay prediction, we have used hop count and last delay as input metric. Through literature reviewed under this study, it has been observed that fuzzy model can be combined with ANN techniques for better prediction of delay which can be the future study. Minimization of error that occurs during prediction can be another direction of future.

References

1. Singh, J.P., Dutta, P., Pal, A.: Delay prediction in mobile ad hoc network using artificial neural network. ScienceDirect, 201–206 (2012) (Elsevier)
2. Bisnik, N., Abouzeid, A.A.: Queuing network models for delay analysis of multihop wireless ad hoc networks. ScienceDirect, 79–97 (2007) (Elsevier)
3. Ghadimi, E., Khonsari, A., Diyanat, A., Farmani, M., Yazdani, N.: An Analytical Model of Delay in Multihop Wireless Ad Hoc Networks, pp. 1679–1697. Science + Business Media, Springer (2011)
4. Jun, T., Roy, N., Julie, C.: Modelling delivery delay for flooding in mobile ad hoc networks. In: 2010 IEEE International Conference on Communications (ICC) (2010). ISSN: 1550-360
5. Singh, J.P., Kumar, P., Singh, S.K.: Delay prediction in mobile ad hoc network using trapezoidal fuzzy numbers. In: 9th International Conference on Computer Science and Software Engineering, pp. 60–64. IEEE (2012)
6. Kaaniche, H., Kamoun, F.: Mobility prediction in wireless ad hoc networks using neural networks. J. Telecommun. (2010)
7. Carneiro, G., Fortuna, P., Ricardo, M.: FlowMonitor—a network monitoring framework for the network simulator 3 (NS-3). In: NSTOOLS 2009, Pisa, Italy, 19 Oct 2009
8. Bisnik, N., Abouzeid, A.A.: Queuing network models for delay analysis of multihop wireless ad hoc networks. ScienceDirect, 79–97 (2007)
9. Gonzalez, O.F., Howarth, M., Pavlou, G.: Detection of packet forwarding misbehavior in mobile ad-hoc networks. In: 2007 Center for Communications Systems Research, Springer
10. Pal, A., Singh, J.P., Dutta, P.: Path length prediction in MANET under AODV routing: comparative analysis of ARIMA and MLP model. Egypt. Inf. J. (2015) (Elsevier)
11. Chauhan, A., Kumar, S.: A pose based object recognition model for improving learning time and accuracy. Int. J. Comput. Appl. (2015)
12. Tuli, H., Kumar, S.: A review on delay prediction techniques in MANET. Int. J. Comput. Appl. **108**(14), (0975–8887) (2014)

13. Sheikhan, M., Hemmati, E.: Transient Chaotic Neural Network-Based Disjoint Multipath Routing for Mobile Ad-Hoc Networks, Springer (2011)
14. Noureddine, H., Ni, Q., Min, G., AlRaweshidy, H.: A new link lifetime prediction method for greedy and contention-based routing in mobile ad hoc networks. In: 10th International Conference on Computer and Information Technology, IEEE (2010)

Detection of Hello Flood Attack on LEACH in Wireless Sensor Networks

Reenkamal Kaur Gill and Monika Sachdeva

Abstract Wireless sensor networks are newer technology consisting of sensor nodes deployed in an unattended environment which collect environmental data by sensing and then forward it to the base station. The security of WSN in such an environment is very difficult. There are many routing protocols for WSN, but LEACH is the widely used energy proficient hierarchical routing protocol which saves nodes energy by forming clusters. In LEACH, cluster member forwards its data to the cluster head, which then aggregate and forward the entire data it received from member nodes to the base station. There are various types of attacks which threaten the services of LEACH are Sybil attack, black hole, selective forwarding, and Hello flooding attack. Hello flooding attack is a type of DoS attack which degrades the performance of LEACH by continuously sending large number of cluster head advertisement packets. Inside this text, firstly, we have discussed LEACH routing protocol and how it can be compromised by Hello flooding attackers. Once we threaten the services of LEACH by Hello flood attack, the impact of attacks on the performance metrics of LEACH is evaluated. In this paper, we have also proposed a detection strategy using coordinator nodes which detect the nodes causing Hello flood attack and then prevent it. The performance of algorithm is then tested using the NS-2 simulator.

Keywords Wireless sensor networks · LEACH · Hello flood · NS-2

R.K. Gill (✉) · M. Sachdeva
Department of Computer Science and Engineering, Shaheed
Bhagat Singh State Technical Campus, Ferozepur 152004, Punjab, India
e-mail: reenkamalgill@gmail.com

M. Sachdeva
e-mail: monasach1975@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_40

1 Introduction

Wireless sensor networks are the most modern research area which includes employment of sensors that exchange information with every other node only over an exacting environmental region to provide aggregate measurements. The fundamental working of sensor nodes is to sense and collect ecological data and send this to the base station after processing it [1]. Sensor node is a tiny device having low power and low cost and is proficient of communicating at short distances. WSN has a vast range of real-time applications such as military applications, environment applications, smart homes, monitoring of health issues.

WSN also faces various challenges like it does not include the security of the routing protocol at the design phase; restricted resources of WSN make it hard to employ complex security algorithms, and also WSN is open to everyone so it is more vulnerable to attacks.

For routing purposes of WSN, many routing protocols have been proposed which are categorized under location-based, data-centric, and hierarchical-based routing protocols. In data-centric routing protocol, base station sends query to the central region and waits for its data. For reducing data redundancy, it uses the concept of data naming [2]. Hierarchical routing protocols are the one in which member cluster forwards its data to the cluster head which then combine and reduce data to promote it to base station. These protocols are the energy efficient routing protocols since it saves lot of energy of sensor nodes by forming clusters. Last is the location-based routing protocol which uses the location information so that it can send data just to the particular location than sending it to the complete arrangement of nodes. Location routing protocols are not energy conscious; hence, these are not widely used.

The structuring of the rest of paper is as follows: In Sect. 2, we discuss LEACH routing protocol. In Sect. 3, attacks on LEACH are defined; Sect. 4 illustrates Hello flood attack simulation model; in Sect. 5, we talk about simulation model, and then in Sect. 6, simulation parameters are described along with performance metrics. Section 7 describes the simulation results by doing analysis of LEACH with and without attack; Sect. 8 defines the proposed detection technique and its results; in Section 9, we conclude the paper and define the future work.

2 LEACH and Its Phases

Low-energy adaptive clustering hierarchy is a protocol which improves lifetime of the network by forming the clusters. It is the most popular routing protocol in which sensor nodes form cluster by accepting the advertisement request from a cluster head on the base of received signal strength. It is then the task of cluster head to receive data from the cluster member nodes and send this data to the base station,

allowing nodes to save their energy. Only 5% of the total nodes from the network can become cluster head in each round.

Cluster head performs all the processing and aggregation of data before sending it to base station. The task of cluster head keeps on rotating; hence, LEACH is also known as dynamic routing protocol.

The working of LEACH protocol has several rounds, and each round can be viewed as follows: setup phase, which is the first step of LEACH functioning and steady phase, the next phase after cluster setup phase.

The basic steps of setup phase are:

1. Advertisement of cluster head
2. Cluster head setup
3. Transmission schedule formation

The first step of this phase is cluster head advertisement during which random number is chosen by each node that should be between 0 and 1, and its threshold value ($T(n)$) is computed (Fig. 1).

Here,

p node's cluster head becoming probability
r round in progress
G group of nodes that were not cluster head in initial round

If threshold value is less than the chosen random number, then node can become cluster head for current round. Once the node becomes a cluster head in first round, it is not then eligible for being a cluster head for the next $1/p$ rounds. Once $1/p - 1$ rounds are finished, the threshold is set to 1 and all the nodes are again eligible to become cluster head. Nodes that become cluster head then broadcast their advertisement using CSMA-MAC protocol [3].

During the second step, each node informs the cluster head about its choice of using CSMA-MAC protocol. During this step, the receiver of each head must be kept ON.

In third step, head node generates a transmission plan for each node during which it can send its data.

Next is the steady phase, it has following fundamental steps:

1. Each node sends out its data to cluster head
2. Data fusion by cluster head
3. Data communication to the base station.

$$T(n) = \frac{P}{1 - P \times \left(r \bmod \frac{1}{P} \right)} \qquad \forall n \in G$$

$$T(n) = 0 \qquad \forall n \notin G$$

Fig. 1 Formula to compute threshold value

During this phase, each sensor node forwards its data to the cluster head during the allocated TDMA schedule. Cluster head after performing data fusion transmits it to the base station. After a predefined time, the network then starts next round of LEACH by going back to the setup phase and steady phase.

3 Attacks on LEACH

There are various types of attack which threaten the services of LEACH protocol by degrading its performance. Attackers mainly drop, alter, spoof, or replay the packets. Following are the major attacks on LEACH [4].

A. *Sybil Attack*—It is generally made in peer to peer networks and is the complicated one to discover. It is the attack in which single adversary node takes the characteristics of several other legitimate nodes to access the data exchanged between them. Due to this attack, the fault-tolerant schemes of the network become inefficient [5].
B. *Selective Forwarding*—In this malicious node refuses to forward confident data to the network and simply drops those packets. The simplest version of selective forwarding is black hole attack in which adversary does not send any data to the neighboring nodes. This type of attack is easy to detect, but in case of selective forwarding the attacker is more intelligent and forwards data selectively. So it is difficult to notice.
C. *HELLO Flooding Attack*—Many routing protocols in WSN require transmitting hello packets to advertise itself to other nodes in the network. The nodes which receive these packets believe that it is in radio range of the transmitter. However, in case of attacker, it floods hello packets to waste nodes energy and increases network traffic and thus causes collisions.

4 Hello Flood Attack

LEACH is the commonly used clustering-based routing protocol of WSN. In LEACH, every non-cluster head node decides to join cluster head advertising node on the base of received hello packets, thus making LEACH vulnerable to a laptop-class attack known as Hello flood attack. Hello flood attack is a network layer attack [6].

An adversary node broadcasts hello packets with high transmitting power so that most of the nodes in the network select it as a cluster head. Nodes receiving these packets send join request to the adversary thinking that it is in their radio range but in actual nodes are far away from the enemy. As a result, the complete network is in the status of uncertainty as the sensor nodes have very small transmitting power so

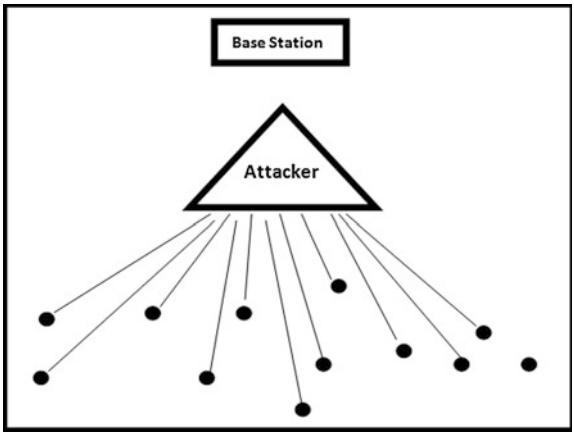


Fig. 2 Adversary transmits hello packets and routing information with enough power so that all the nodes in the network assume it as their neighbor

their packets will get lost in between without even reaching the adversary node (Fig. 2).

In Hello attack, adversary need not be able to construct genuine passage to launch Hello flood attack rather attacker just broadcast hello packets in order to cause collision in the network.

5 Simulation Model

The cost of setting real environment is much greater so various simulators are used to establish virtual environment. NS-2 has been used as a simulator for the purpose of simulation in our work. A square area of 1100 m * 1100 m is considered for research. The network of 50 immobile nodes is taken; out of these, 5% of the total nodes are taken as cluster head. We have used CBR traffic to create UDP packets. From the total nodes, only 1% of the nodes has high sensing and transmission power and is known as base station. Initial energy for the sensor nodes is 10 J.

5.1 Simulation Methodology

Initially, we have created LEACH routing protocol using TCL and awk scripts and then generated legitimate traffic in the network. After that, we have analyzed performance metrics such as packet delivery ratio, packet loss, and residual energy from the trace file of the network.

After that, we have implemented Hello flood attack on LEACH to analyze its effect by comparing the same performance metrics. The most important requirement for any network is security so for that detection strategy is proposed to identify adversary node in the network.

Table 1 Parameters for simulation

Parameter	Value
Number of nodes	50
Number of clusters	5
Network area	1100 m * 1100 m
Base station location	878 m * 586 m
Routing protocol	LEACH
Traffic type	CBR
Initial energy of nodes	10 J

5.2 Simulation Parameters

Performance metrics: Performance metrics considered for the network analysis with and without attack are as follows (Table 1):

Packet delivery ratio (PDR): It is the ratio of packets that are effectively reached the base station by the nodes. More the value of PDR better will be the performance of the network. It is defined as follow

$$\text{PDR} = (\text{packets received by the destination}/\text{packets generated by the source}) * 100$$

Packet loss: It defines the number of packets lost during the simulation.
Residual energy: After the entire simulation is over, the energy which is left is known as residual energy.

6 Simulation Results

For the simulation purpose, we first analyze the performance of LEACH by determining the value of performance metrics, and then we simulated LEACH with Hello attack and again analyze the metrics. At the end, we compare the results of both LEACH and LEACH with Hello attack

1. Packet delivery ratio

Figure 3 depicts the performance of LEACH with and without attack in terms of PDR. Figure 3 clearly depicts that the packet delivery ratio is better in LEACH than with Hello flood attack on LEACH.

The reason of decreased PDR with Hello flood attack is that malicious node increases the network traffic by sending advertisement packets with high

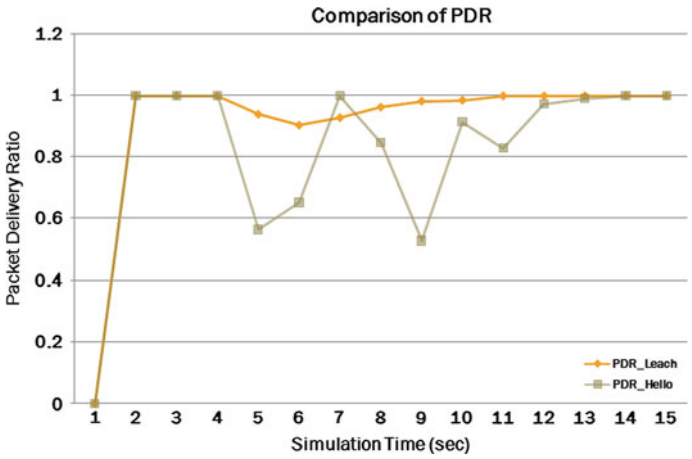


Fig. 3 Comparison of PDR with and without attack

transmission power, thus causing the sensor nodes data collision and some of the data is lost in between due to the distance between the malicious node and sensor nodes [7].

2. Packet loss

Figure 4 shows the number of packet loss in LEACH and with attack on LEACH. The number of lost packets in LEACH is much less than with attack [8]. The packet loss in attack increases abruptly due to the attacker node which allows nodes data to be lost in between. Packet loss in LEACH is due to the various other factors such as environmental issues, congestion, buffer overflow.

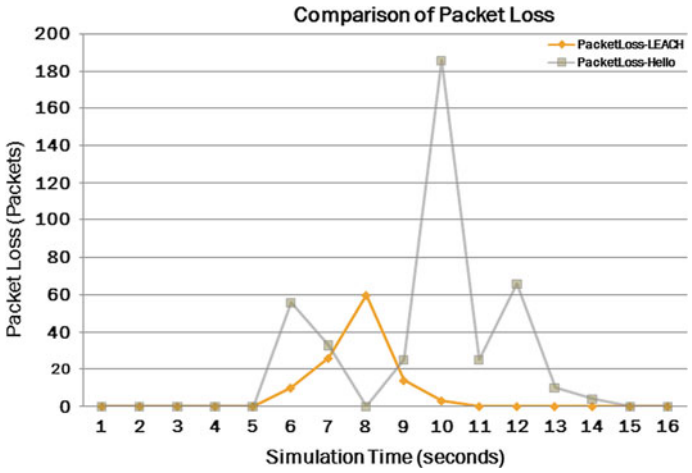


Fig. 4 Comparison of packet loss with and without attack

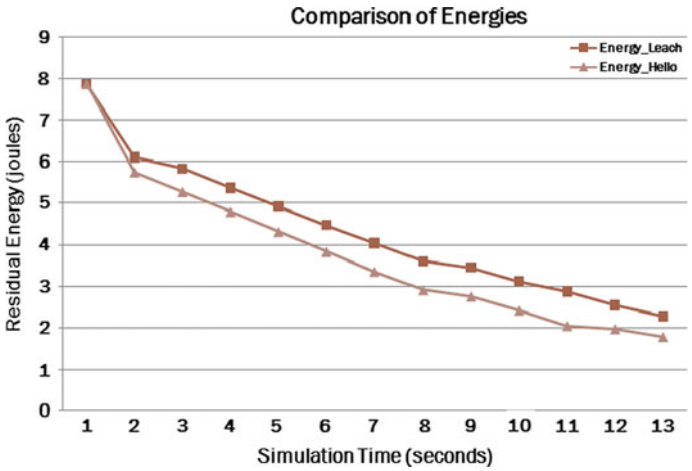


Fig. 5 Comparison of residual energy with and without attack

3. Residual energy

Figure 5 shows the remaining energy of the network with attack and without attack. Energy consumption in attack is more than in simple LEACH because Hello attack wastes lot of nodes energy by continuously transmitting hello packets [9, 10]. It leaves the node into the state of confusion as the far away nodes sending the packets into oblivion.

7 Detection Strategy and Results

The detection strategy proposed for the detection of Hello flood attack includes the deployment of coordinator nodes which are used to detect the malicious nodes in the network [11, 12]. Whenever any node receives a cluster head advertisement, it simply forwards this advertisement to coordinator node with the cluster head advertising node's ID. Coordinator node then sends this ID to the base station. The base station then computes degree of connectivity of each cluster head i.e., how many nodes have received advertisement request from a particular cluster head advertising node. The node whose degree of connectivity is greater than the threshold value will be marked as malicious, and this information is broadcasted in the network.

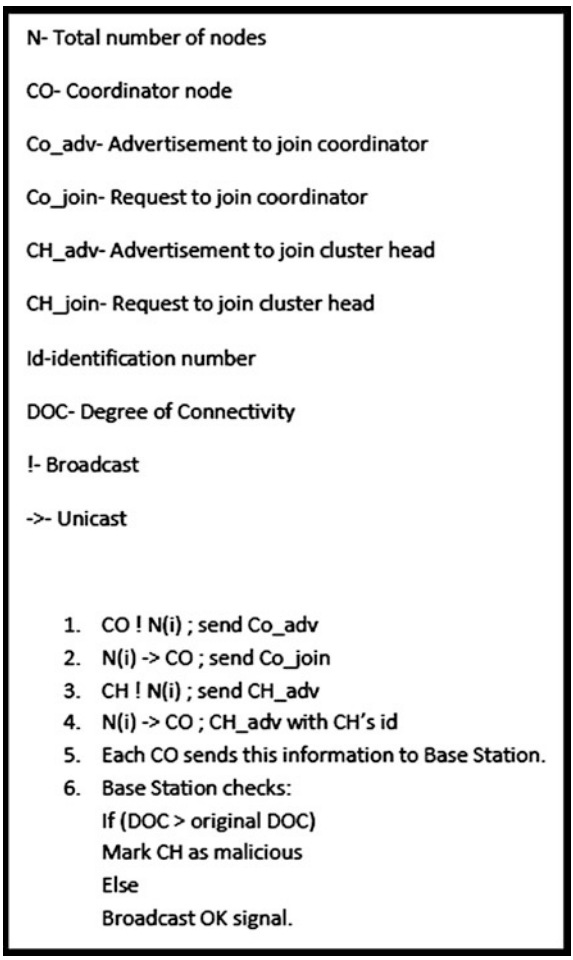


Fig. 6 Algorithm for detection strategy

The main task of coordinator node is just to take advertisement request from the sensing nodes and forward it to base station [13]. The count of coordinator nodes can be varied with increase in number of sensor nodes. Within our simulation, we have deployed five coordinator nodes.

Algorithm for this detection strategy is as follows (Fig. 6).

Figure 7 shows the improved results after applying detection strategy on LEACH with attack. The PDR is now above 80% which proves the efficiency of the detection strategy.

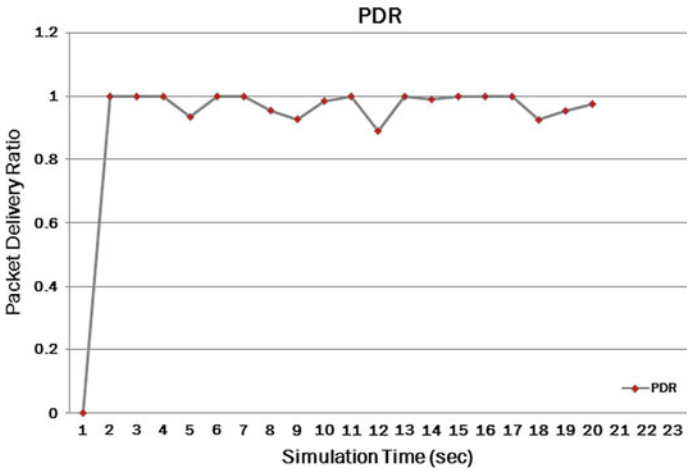


Fig. 7 Packet delivery ratio after detection

8 Conclusion and Future Scope

Security is the most fundamental feature of sensor networks. So, we have proposed a detection strategy to secure LEACH from Hello flood attack. This paper discusses LEACH and various types of attack on LEACH. We have simulated LEACH and then Hello attack on LEACH, compare their results and then implemented detection strategy.

In future, this approach can be enhanced by taking energy aspect in mind. Also, performance of LEACH can be analyzed with the presence of other type of active and passive attacks.

Acknowledgment Profound gratitude and indebtedness to Dr. Monika Sachdeva, Associate Professor, SBS State Technical Campus, Ferozepur, for her inspiring intellectual supervision as well as valuable suggestion throughout the research work.

References

1. Gill, R.K., Chawla, P., Sachdeva, M.: Wireless sensor network: threat models and security issues. In: International Conference on Communication, Computing & Systems (ICCCS-2014)
2. Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutorials **8**, 2–23 (2006)
3. Akkaya, K., Younis, M.: A survey on routing protocols for wireless sensor networks. Ad Hoc Netw. **3**(3), 325–349 (2005)

4. Almomani, I., Al-Kasasbeh, B.: Performance analysis of LEACH protocol under denial of service attacks. In: 2015 6th International Conference on Information and Communication Systems (ICICS). IEEE (2015)
5. Gill, R.K., Chawla, P., Sachdeva, M.: Study of LEACH routing protocol for wireless sensor networks. In: International Conference on Communication, Computing & Systems (ICCCS-2014)
6. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and counter measures. Ad Hoc Netw. **1**(2), 293–315 (2003)
7. Magotra, S., Kumar, K.: Detection of HELLO flood attack on LEACH protocol. In: 2014 IEEE International on Advance Computing Conference (IACC). IEEE (2014)
8. Singh, V.P., Jain, S., Singhai, J.: Hello flood attack and its countermeasures in wireless sensor networks. Int. J. Comput. Sci. **7.3**, 23 (2010)
9. Abhishek, J., Kant, K., Tripathy, M.R.: Security solutions for wireless sensor networks, Amity University, India. In: Second International Conference on Advanced Computing and Communication Technologies
10. Al-Sakib Khan, P., Lee, H.-W., Hong, C.S.: Security in Wireless Sensor Network: Issues and Challenges. Kyung Hee University Korea (2006)
11. Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., Jokerst, R.M., Analyzing interaction between distributed denial of service attacks and mitigation technologies. In: Proceedings of DARPA Information Survivability Conference and Exposition, vol. 1, pp. 26–36, 22–24 Apr 2003
12. Doddapaneni, K.C., Ghosh A. :Analysis of DoS attack on WSN using simulation. Middlesex University (2011)
13. Mohammad, S., Khosravi, F., Atefi, K., Barati, M.: Security analysis of routing protocols in WSN (2012)

Detection of Selective Forwarding (Gray Hole) Attack on LEACH in Wireless Sensor Networks

Priya Chawla and Monika Sachdeva

Abstract Wireless sensor networks (WSN) are mainly deployed in an unattended and hostile environment. So security is a major concern in these types of networks. Many routing protocols have been designed in WSN, which are responsible for maintaining the routes in the network. We mainly focused on LEACH, the most popular hierarchical routing protocol. But the services of LEACH are threatened by various kinds of attacks such as Black Hole, Selective Forwarding (Gray Hole), Sybil, and HELLO flood attacks. In this paper, firstly we have discussed LEACH and then how it can be compromised by Selective Forwarding Attack. The performance of LEACH without the existence of attack and with the attack has been evaluated in terms of various performance metrics such as packet delivery ratio, packet loss, and remaining energy of the network using Network Simulator (NS-2). We have also emphasized on how to secure the network if they have been threatened to Selective Forwarding Attack. To detect the malicious nodes in the network, we have proposed and implemented a detection strategy.

Keywords Wireless sensor networks · LEACH · NS-2

1 Introduction

Wireless sensor network (WSN) consists of a number of sensor nodes, which are deployed over a particular geographical area. The main purpose of the sensor nodes is to sense the information and, after proper processing and gathering the information, transmit it to the most powerful node having high energy resources as well as high computational and communication resources known as base station.

P. Chawla (✉) · M. Sachdeva
Department of Computer Science and Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur 152004, Punjab, India
e-mail: piyachawla12@gmail.com

M. Sachdeva
e-mail: monasach1975@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_41

WSN is used in various other areas like in military, medical applications, landslide detection [1].

According to [1], WSN is categorized into two types: unstructured and structured WSNs.

Unstructured WSN: It has a huge number of sensor nodes, and there is no proper way to deploy the nodes, i.e., nodes are deployed in an unplanned manner.

Structured WSN: It has a well-developed pre-planned criterion for the deployment of the sensor nodes in large area, i.e., at what specific locations, sensor nodes are to be deployed. As compared to unstructured WSN, it has a less number of sensor nodes. Maintenance and management cost is very less in structured WSN as compared to unstructured WSN.

As far as the concept of routing is concerned, routing protocols [2] in WSN are as follows:

(1) Data-centric protocols—In this type of routing protocols, queries are sent to specific regions by base station and then base station waits for its data. For example, SPIN protocol comes under this category.
(2) Hierarchical protocols—This type of routing protocol is based upon the clustering concept in which a network is divided into clusters and cluster head is chosen from each cluster, which is responsible for data transmission, e.g., LEACH, PEGASIS, TEEN, APTEEN.
(3) Location-based protocols—In this, the sensor node position is used to decide or determine the routing path, e.g., Geographical and Energy Aware Routing (GEAR), etc.

WSNs are becoming hottest research areas nowadays, but as it uses wireless medium as well as wireless channel is open and easily accessible to everyone, they are easily prone to attacks [2]. In this paper, we have discussed LEACH, the most popular clustered routing protocols, and the impact of the Selective Forwarding Attack on LEACH. Performance of LEACH with Selective Forwarding (Gray Hole) Attack has been evaluated with the help of the most well-known and popular simulator, i.e., Network Simulator (NS-2) [3, 4].

Our paper is arranged as follows: In Sect. 2, we have discussed LEACH protocol. Section 3 discusses the attacks on LEACH. Section 4 discusses the Selective Forwarding (Gray Hole) Attack on LEACH. Section 5 presents the objectives of the work. Section 6 gives the detailed description of simulation environment. Section 7 discusses results of performance analysis of LEACH with and without attack, Sect. 8 presents the detection strategy and its results, and then in Sect. 9, we have concluded our whole paper.

2 LEACH—A Hierarchical Routing Protocol

LEACH is the most popular hierarchical routing protocol. It increases the network lifetime as it uses the concept of clustering in which nodes are divided into clusters and from each cluster, cluster head is chosen, which is responsible for data aggregation and then data transmission to base station. Hence, it also saves energy of sensor nodes [5, 6].

The working of LEACH can be bifurcated into two steps, also known as phases:

(1) Setup Phase
(2) Steady Phase

In the first phase, i.e., setup phase, cluster formation takes place and then the election process of cluster heads is there, whereas in the second phase, i.e., steady phase, transmission of data takes place, i.e., firstly sensor nodes send data to their respective cluster heads and then after aggregating data, cluster head transmits it to the base station.

(1) Setup Phase—To choose a cluster head, threshold value $T(n)$ is computed and it is calculated by using the formula as follows:

$$T(n) = \begin{cases} \frac{P}{1-P*\left(r \bmod \frac{1}{P}\right)} & \text{if } n \in G \\ 0 & \text{otherwise} \end{cases}$$

where

p node's probability to become a cluster head
r present round, i.e., round which is current
G group of nodes that could not become cluster heads in the previous rounds

The node that wants to become cluster head selects a random number within the ranges 0 to 1. If the threshold value $T(n)$ is greater than the random number, the node is elected as the cluster head for that particular round. After that, elected cluster head broadcasts a message to all the nodes in the network in order to inform them that it is elected as the cluster head for this round. Based upon the signal strength of the message, the normal nodes reply back with an acknowledgment message to their respective cluster head to inform that they are ready to join their cluster. After receiving the acknowledgment message from the nodes, TDMA schedule is created by cluster heads in which each and every node in their cluster is assigned a particular time period in which nodes can send their data in order to avoid collisions in the network. And then, this TDMA schedule is sent to every node in the network.

(2) Steady Phase—During this phase, sensor nodes send data to their cluster heads. Before sending the data to base station, cluster heads perform its function, i.e., aggregation of data to eliminate redundancy in data.

3 Attacks Possible on LEACH

LEACH protocol is exposed to various kinds of attacks that degrade its performance to a large extent. Following are the major attacks on LEACH [7]:

(1) Sybil attack—The major possibility of this attack can be found in peer-to-peer networks. In this, a single malicious node uses the identities of various legitimate nodes in the network. For example, whenever two legitimate nodes want to communicate, malicious node comes in between the interaction and assures the sender node that it is the one to whom he wants to exchange the information. In this way, an adversary can take all the information.
(2) Selective Forwarding Attack—This attack mainly occurs at the network layer. It is also known as Gray Hole attack, in which a malicious node forwards some data to the base station and simply drops the rest of the data. This degrades the Quality-of-Service in WSNs. Detection of this attack is very difficult [8].
(3) HELLO Flood attack—Some routing protocols require to transmit HELLO messages to neighbor nodes to assure its presence. But when any malicious node comes in the network, it continuously sends HELLO messages to neighboring nodes just to waste the energy of the nodes for receiving these high signal strength messages. The major intention of the attacker node is to increase the traffic in the network that leads to collision also [9].

4 Selective Forwarding (Gray Hole) Attack

Now the thing is how LEACH is vulnerable to Selective Forwarding (Gray Hole) Attack. As we know, LEACH is a protocol which mainly relies on a cluster head for the aggregation of data and then sends it to the sink, also known as base station. So when any malicious node becomes the cluster head, it can launch this attack and selectively forwards data to the base station [10, 11]. This type of attack affects the network performance to a large extent. Its detection is very difficult.

5 Objectives of Work

The main objectives of our work are as follows:

(1) To analyze a LEACH protocol with various performance metrics.
(2) To analyze LEACH with the existence of a Selective Forwarding Attack under same performance metrics.
(3) To measure the impact of attack by comparing the results with LEACH.

(4) To propose and implement detection strategy for the identification of malicious nodes in the network.

6 Simulation Environment

To establish a realistic environment makes it so much cost expensive. Networking research community has provided us with various simulators, which is a replica of real environment, and simulators are mainly used to easily understand and demonstrate network-related queries. So we have chosen the most well-known simulator for our work, i.e., Network Simulator (NS-2), which has proved useful in studying the dynamic nature of communication networks. To create a network topology in NS-2, we have used 1100 m $*$ 1100 m area and 50 nodes have been taken. Out of 50 nodes, one node has much more computing power, communication as well as energy resources, which is known as base station. Constant bit rate (CBR) traffic has been used to create UDP packets.

6.1 Simulation Methodology

Now here is simulation methodology which means in what order we have done our work.

In the first step, we have created a network topology in NS-2 using Tcl and awk scripts and using LEACH as a protocol and then we have generated legitimate traffic in the network. After that, we have analyzed performance metrics of LEACH like packet delivery ratio, packet loss, and remaining energy of the network using trace (.tr) file which is the output file in NS-2.

In the next step, we have implemented Selective Forwarding Attack on LEACH and again we have analyzed same performance metrics and after that, we have measured the impact of attack on LEACH by comparing their results.

We have also emphasized on security factor that how to detect the attack, so we have proposed and implemented detection strategy for the identification of malicious nodes in the network.

Table 1 Simulation parameters

Parameter	Value
Total number of nodes	50
Number of clusters	5
Network field	1100 m $*$ 1100 m
Base station location	(884,590)
Routing protocol	LEACH
Traffic type	CBR
Initial energy of nodes	10 J
Simulation time	15 s

6.2 Simulation Parameters

See Table 1.

7 Simulation Results

7.1 Performance Metrics

The performance of LEACH with and without attack has been measured in terms of different performance metrics which are as follows:

(1) Packet Delivery Ratio (PDR)—It is the ratio of the number of packets successfully received by destination node to the number of packets forwarded by the source node. The performance of the network will be better if the value of packet delivery ratio is more.
(2) Packet Loss—The number of packets lost during the whole simulation is termed as packet loss.
The performance of the network will be better if the value of packet loss is less.
(3) Remaining Energy—It can be defined as the remaining energy of the network after the entire simulation is over.

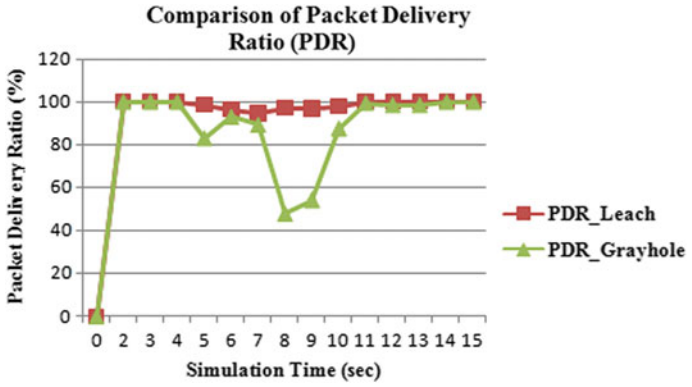


Fig. 1 Packet delivery ratio of normal LEACH and with the existence of Selective Forwarding (Gray Hole) Attack

7.2 Packet Delivery Ratio

Figure 1 shows the packet delivery ratio of LEACH with and without attack. It is cleared from the graph that without attack, approximately all the packets successfully received at the destination, PDR is very much better throughout the network. But PDR is greatly affected when attacker nodes come in the network. As the attacker nodes come, PDR goes on decreasing. Hence, this shows that how the performance of network starts declining when it is threatened to this attack.

7.3 Packet Loss

Figure 2 shows how many packets have been lost during the whole simulation in the case of LEACH without attack and with the attack. It is cleared from the graph that there is not much packet loss in case of LEACH without attack. Now, the thing is that in spite of not being attacked, still why some of the packets cannot reach its destination? Apart from malicious intent, there can be other reasons of dropping like collisions, buffer overflows, and traffic congestion in the network. But in Gray Hole attack, there is a huge amount of packet loss as the malicious node comes in the network. Hence, we can say that network performance is greatly affected when it is compromised by attacker nodes.

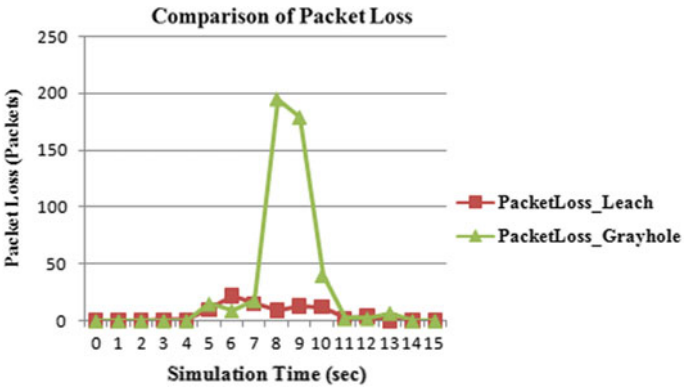


Fig. 2 Packet loss in normal LEACH and with the existence of Selective Forwarding (Gray Hole) Attack

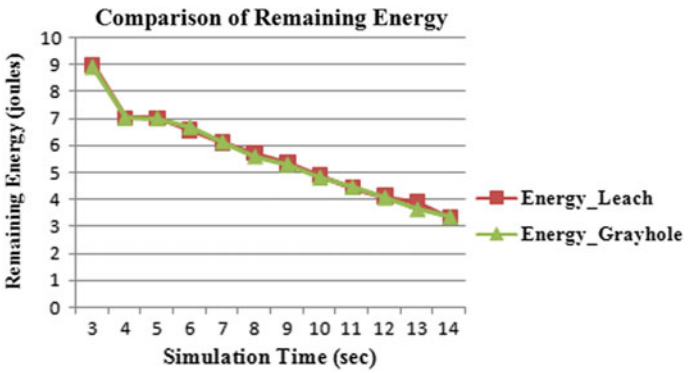


Fig. 3 Remaining energy of the network in normal LEACH and with the existence of Selective Forwarding (Gray Hole) Attack

Table 2 Algorithm of detection strategy

Step 1: Start the communication
Step 2: Sensor nodes start sensing data and send it to their respective cluster head
Step 3: Cluster head after aggregating data sends it to the base station
Step 4: Base station compares the data of each and every round
Step 5: If data received in the current round is approximately same or more as compared to previous rounds, then proceed with the normal communication
Step 6: Else if data received in the current round is very less, then the base station checks in that round which cluster head has sent very less data
Step 7: Mark that cluster head as malicious node and inform all the nodes not to forward data to that cluster head
Step 8: Continue the detection process

7.4 Remaining Energy of the Network

Figure 3 shows the overall average remaining energy of the network. It is cleared from the graph that energy consumption in both the cases is almost same. The question is why so? There is a logical reason behind this that although the attacker nodes are dropping packets but still they are participating in all other activities that consume energy.

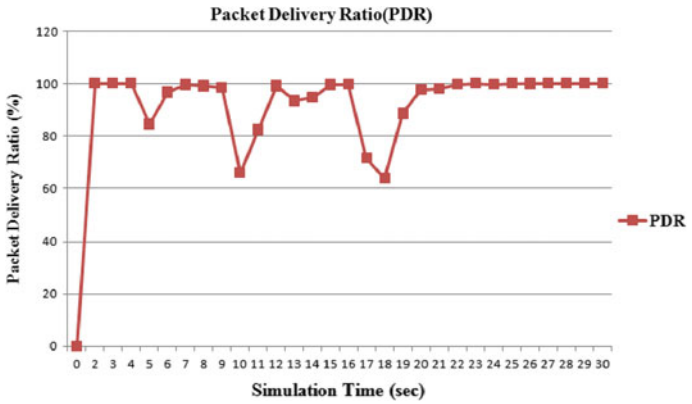


Fig. 4 Packet delivery ratio of the whole network on applying detection strategy

8 Detection Strategy

See Table 2.

8.1 Results of Detection

To implement the detection strategy, we have run the simulation up to 30 s; rest of all the simulation parameters are same as Table 1. As we know, LEACH is a protocol that works upon rounds. It is cleared from Fig. 4 that the point at which packet delivery ratio is very low, i.e., near about 60–85%, malicious nodes have been detected in those rounds on applying detection strategy and then removed from the network. After that, the packet delivery ratio starts increasing and reaches up to 95% or above. After 18 s, the packet delivery ratio is near about 100%, and up to 30 s, it remains 100%, which means that there are no malicious nodes left in the network. Hence, malicious nodes have been identified or detected and also removed from the network, which results in enhancing network performance. So this proves the efficiency of the detection algorithm.

9 Conclusion

This paper studied the impact of Selective Forwarding Attack on LEACH. The simulation results showed a huge drop in the packet delivery ratio. Also, it has been observed that the impact of attack in case of energy consumption is not very huge. We also proposed and implemented detection strategy and observed that how

network performance increases after the malicious nodes have been detected and removed from the network.

In future, performance analysis of LEACH can be done against various active and passive attacks and other detection techniques may be proposed and implemented.

Acknowledgements Profound gratitude and indebtedness to Dr. Monika Sachdeva, Associate Professor, Shaheed Bhagat Singh State Technical Campus, Ferozepur, for her inspiring intellectual guidance and valuable suggestion throughout the research work.

References

1. Gill, R.K., Chawla, P., Sachdeva, M.: Wireless Sensor Network: Threat Models and Security Issues
2. Prathap, U., et al.: Wireless sensor networks applications and routing protocols: survey and research challenges. In: 2012 International Symposium on Cloud and Services Computing (ISCOS). IEEE (2012)
3. Issariyakul, T., Hossain, E.: Introduction to Network Simulator NS2. Springer (2011)
4. The network simulator ns2. www.isi.edu/nsnam/ns
5. Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. IEEE (2000)
6. Gill, R.K., Chawla, P., Sachdeva, M.: Study of LEACH Routing Protocol for Wireless Sensor Networks
7. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Netw **1**(2), 293–315 (2003)
8. Tripathi, M., Gaur, M.S., Laxmi, V.: Comparing the impact of black hole and gray hole attack on LEACH in WSN. Procedia Comput. Sci. **19**, 1101–1107 (2013)
9. Magotra, S., Kumar, K.: Detection of HELLO flood attack on LEACH protocol. In: 2014 IEEE International on Advance Computing Conference (IACC). IEEE (2014)
10. Renold, A.P., Poongothai, R., Parthasarathy, R.: Performance analysis of LEACH with gray hole attack in wireless sensor networks. In: 2012 International Conference on Computer Communication and Informatics (2012)
11. Almomani, I., Al-Kasasbeh, B.: Performance analysis of LEACH protocol under denial of service attacks. In: 2015 6th International Conference on Information and Communication Systems (ICICS). IEEE (2015)

H-LEACH: Modified and Efficient LEACH Protocol for Hybrid Clustering Scenario in Wireless Sensor Networks

Vishal Gupta and M.N. Doja

Abstract Wireless sensor networks consist of independent sensors that sense and monitor the area of deployment and distributedly communicate this information to base station. The desirables of WSN are to have long longevity and high reliability along with maximized coverage. LEACH is one of the most discussed hierarchical, cluster-based routing protocols for sensor networks owing to its load-balancing characteristics. In this paper, we have presented a hybrid approach (H-LEACH) in which the clusters are fixed, but the cluster heads are chosen dynamically. The approach shows an improved performance that is duly supported by the simulation results using MATLAB. The paper concludes with the limitations and further scope for improvement in the proposed protocol.

Keywords Wireless sensor network/s · LEACH · H-LEACH · Cluster · Lifetime · Skewness · Base station (BS) · Cluster head (CH)

1 Introduction

In wireless sensor network (WSN), the sensor nodes mostly employ distributed algorithms to collect the information and wirelessly communicate this information to the base station, from where this information may be processed and analyzed.

Out of these responsibilities, the communication amongst nodes is considered to be the major energy consumption area in WSN [1]. The main approaches used in the literature to reduce this are either to limit the amount of data to be communicated or to minimize the distance between the source and sink of the data to be transported.

V. Gupta (✉) · M.N. Doja
Department of Computer Science, Faculty of Engineering & Technology, Jamia Millia Islamia, Jamia Nagar, New Delhi, India
e-mail: vishalg26@rediffmail.com

M.N. Doja
e-mail: mndoja@gmail.com; ndoja@yahoo.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_42

Different types of routing protocols and algorithms have been proposed by different researchers for WSN. The hierarchical protocols are the category of protocols that has got the most concern in this field. The characteristic of these protocols is to cluster the field nodes, thereby reducing the overhead for transmissions. In this approach, the nodes in the particular cluster talk to the cluster head of the respective cluster. The cluster head in turn communicates this received information to base station. Clustering significantly improves the network lifetime by minimizing the number of nodes participating in long-distance transmission to base station [2].

"Low-Energy Adaptive Clustering Hierarchy protocol" (LEACH) [3] is the widely discussed protocol with clustering hierarchy. However, the issues of the number of cluster heads and the cluster members cannot be controlled by LEACH [4].

In present day scenario, where we have very cheap and effective coordinate finding techniques like GPS, we can use this technological improvement to enhance the performance of basic LEACH protocol. In this paper, we have utilized this concept that if we have this information, we can modify the basic leach protocol to enhance its performance.

The paper organization is as follows: Section 2 presents the brief idea of the basic LEACH protocol. Section 3 summarizes some work done by different researchers to enhance the performance of the basic LEACH protocol. In Sect. 4, we have explained our proposed protocol H-LEACH with the simulation results supporting our claim. The paper lists the limitations and assumptions of this work in Sect. 5. Finally, the conclusion and future scope are presented in Sect. 6.

2 LEACH Protocol

LEACH [3] is the most popular clustering strategy for WSNs where the sensor nodes make autonomous decisions for dynamic cluster formation.

The protocol works in rounds, and the different rounds consist of two phases each: the set-up phase and the steady-state phase as shown in Fig. 1.

The cluster heads are chosen in the set-up phase on the basic of the following function (known as candidate/threshold function):

$$T(n) = \begin{cases} \frac{P}{1-P\left(r.\mathrm{mod}\frac{1}{P}\right)}, & \text{if } n \in G \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

where the meaning of symbols used is

P percentage of the cluster head nodes;
r number indicating the current round;
G set of nodes those were CH node in the previous $1/P$ rounds.

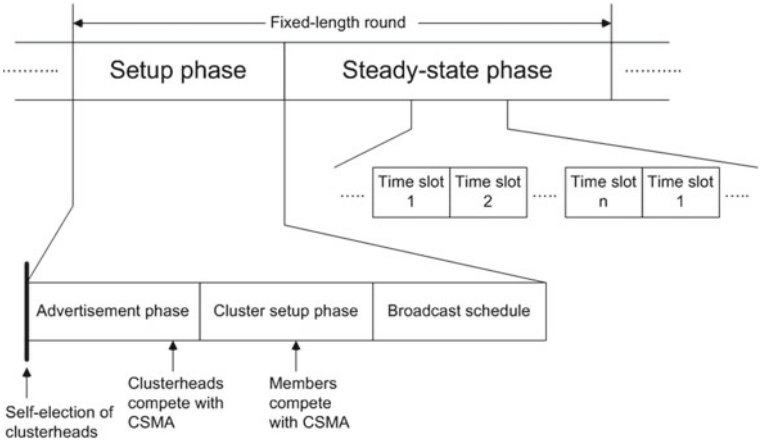


Fig. 1 LEACH protocol

The selected CH list is broadcast in the area, and the different member nodes pick the CH as one that is nearest to them and convey this to the selected CH with the join request. The CHs then create TDMA schedule for the different member nodes in the respective clusters for data transmission. In steady-state phase, the sensed data are transmitted by the different member nodes as per their time slot to the CH. The CH may aggregate this collected data (if desired) and then forwards this to the base station for further processing.

After this, the whole process is repeated over again marking the beginning of the next round.

3 Literature Survey

Much work has been done to enhance the performance of the basic LEACH protocol. In this section, we summarize some work by different researchers in this area.

LEACH-C [5] considers the residual energy when the clusters are formed. Muruganathan et al. in [6] have proposed a centralized protocol "Base station-controlled dynamic clustering protocol (BCDCP)" that claims to uniformly distribute the dissipation of energy amongst all the deployed sensor nodes.

In BN-LEACH [7], the author propose to select the CH using the Bayesian network (BN) model based on three factors distance to base station (BS), remaining energy and density. Wang and Zhu et al. in [8] have proposed LEACH-R routing scheme to improve the cluster head selection using the relaying node. WEEC [9] utilizes the location of each node for calculating the probability of CH-selection.

Kumar et al. [10] have proposed a heterogeneous model in which the selection of cluster head is based on weighted probability. Wang and Yong in [11] have proposed

cluster head selection using pseudo-cluster concept. Energy Efficient Extended LEACH (EEE-LEACH) proposed in [12] is a multilevel clustering approach to improve the energy efficiency. In [13], Farooq et al. have presented a "Multi-hop Routing with Low-Energy Adaptive Clustering Hierarchy (MR-LEACH)" protocol for WSN.

Liao [14] proposed a scheme to select CHs based on the residual energy along with the location information of nodes. They also presented an optimized threshold for selecting cluster head. In [15], Ma et al. have presented an "Adaptive Assistant-Aided Clustering Protocol using Niching Particle Swarm Optimization (AAAC-NPSO)" to increase the lifespan and data delivery rate by regulating the energy dissipation in the WSN. Mehra et al. [16] have proposed a LEASE protocol to control the energy dissipation rate of the different nodes in the network to enhance the efficiency. In [17], Abhishek and Sumedha have implemented node residual energy and node distance-based algorithm for clustering of nodes to minimize the average energy consumption in WSN.

Arumugam and Ponnuchamy [18] have proposed a protocol "EE-LEACH" claiming a better packet delivery ratio, lesser energy consumption and lesser E2E delay than the EBRP and LEACH protocols. Sheta and Solaiman [19] have presented two hybrid clustering algorithms called K-Means Particle Swarm Optimization (KPSO) and K-Means Genetic Algorithms (KGAs) showing improvements over traditional LEACH. An improvement over LEACH protocol is presented by Tohma et al. [20] on the basis of number of packets, number of living nodes, etc. using the OMNet++ as the simulation environment. Li and Changdong [21] proposed an improved LEACH algorithm that considers the current position and the current energy of the node.

The proposed work is presented in the next section.

4 H-LEACH: Proposed Protocol

We have proposed a modification in the basic LEACH protocol by utilizing the area and node location coordinates and then clustering the area on the basis of this information. In essence, we first partition the complete area in as many zones as the desired number of clusters. The protocol chooses one node from each zone as the CH of that area on the basis of LEACH criteria in each round. The role of the CH is rotated amongst the nodes of the respective zones in each round to balance the energy dissipation of the nodes. The member nodes of a particular zone talk to their respective zone cluster head.

Figure 2 shows the arbitrary deployment scenario for normal LEACH showing the base station, cluster heads (as picked by the current round of the protocol) and the member nodes in the given area of (100 * 100) units. The association of the member nodes to their respective cluster head for this round is shown by Fig. 3.

Figure 4 shows the arbitrary deployment scenario for H-LEACH showing the base station, cluster heads (as picked by the current round of the protocol) and the

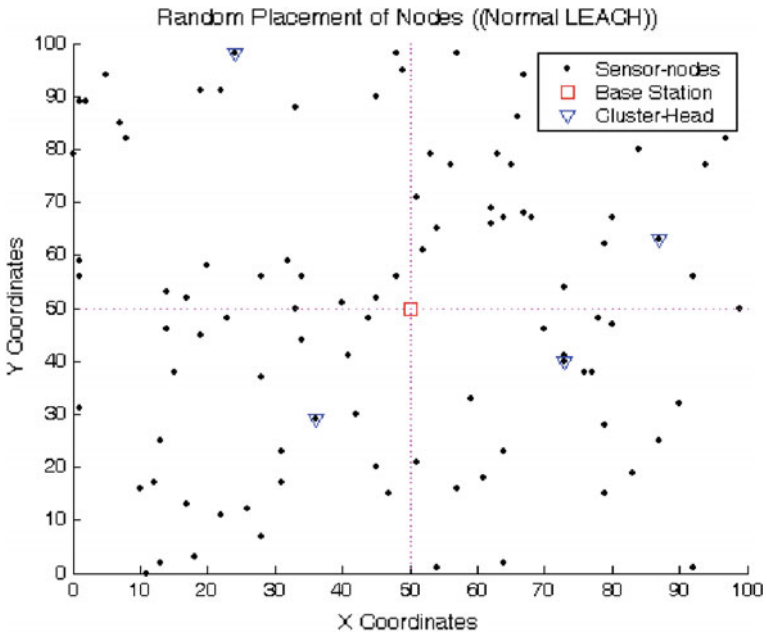


Fig. 2 Normal LEACH deployment scenario

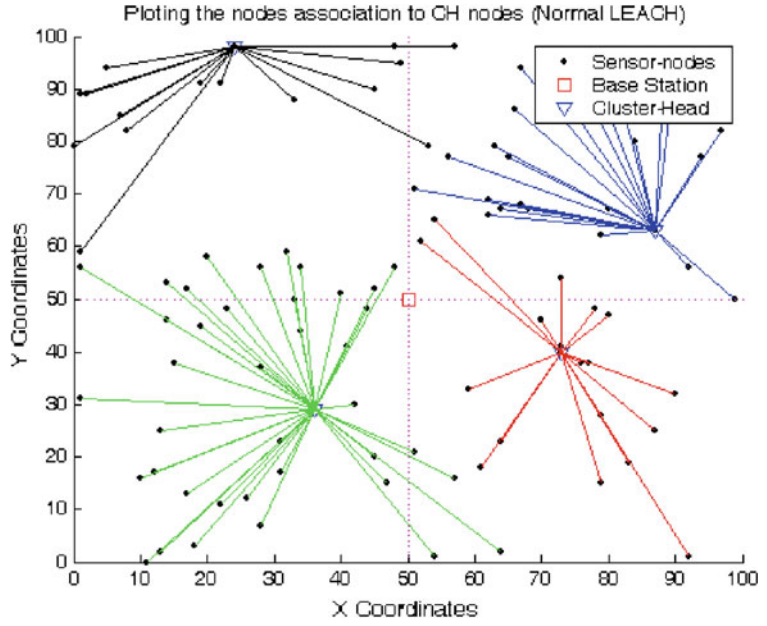


Fig. 3 Normal LEACH node association to CH

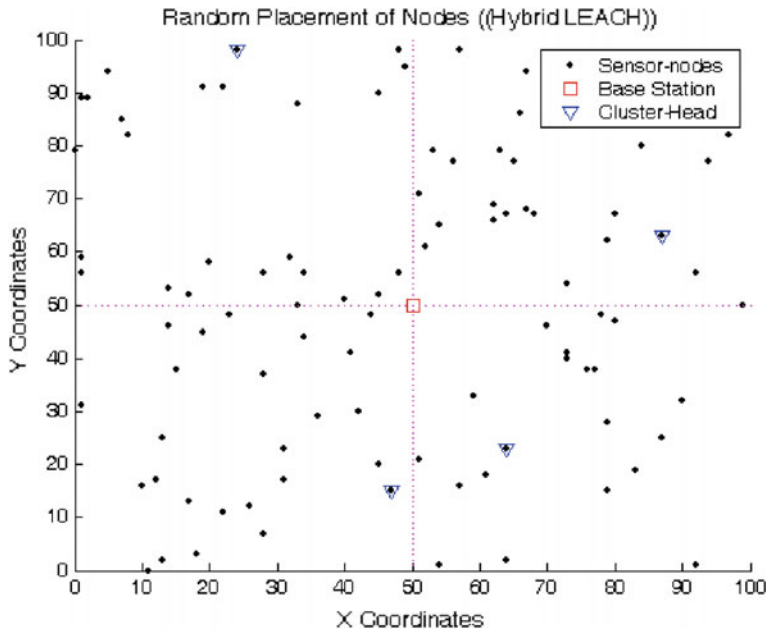


Fig. 4 H-LEACH deployment scenario

member nodes in the given area of (100 * 100) units. The association of the member nodes to their respective cluster head for this round is shown by Fig. 5.

Figure 6 presents the comparison of average energy consumed by all the member nodes in different rounds for some arbitrary deployment. Figure 7 shows the comparison of average energy consumed by all the member nodes in different deployment scenarios.

Figure 8 shows the energy gain corresponding to the difference of average energy spent by the member nodes in normal LEACH and H-LEACH protocol over different deployment scenarios.

5 Limitations and Assumptions

Comparing our protocol to the basic LEACH protocol, we have assumed that all the nodes deployed are well-aware of their location coordinates that are also shared by base station as well. Also, we have not considered the energy consumed by the CH nodes to transfer the gathered information to the base station because this will affect both the protocols roughly equally for a long run as the CH is chosen randomly in both the schemes.

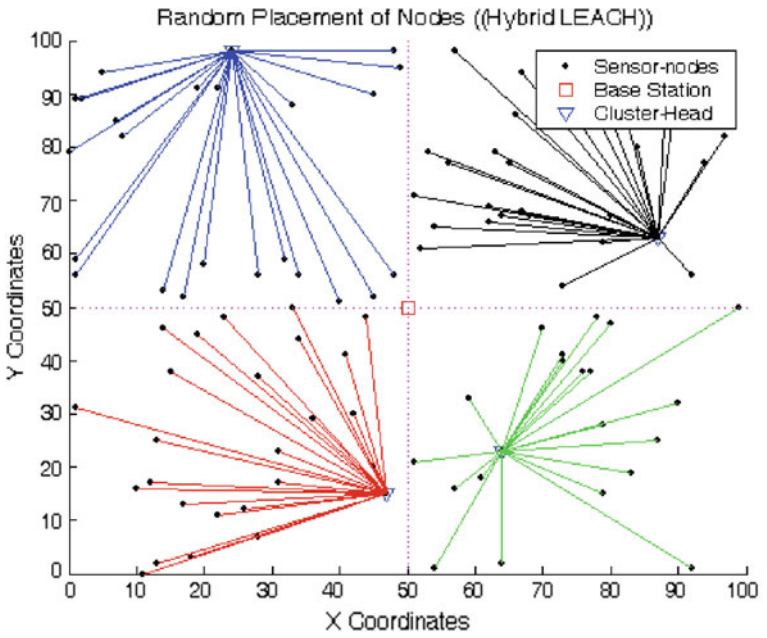


Fig. 5 H-LEACH node association to CH

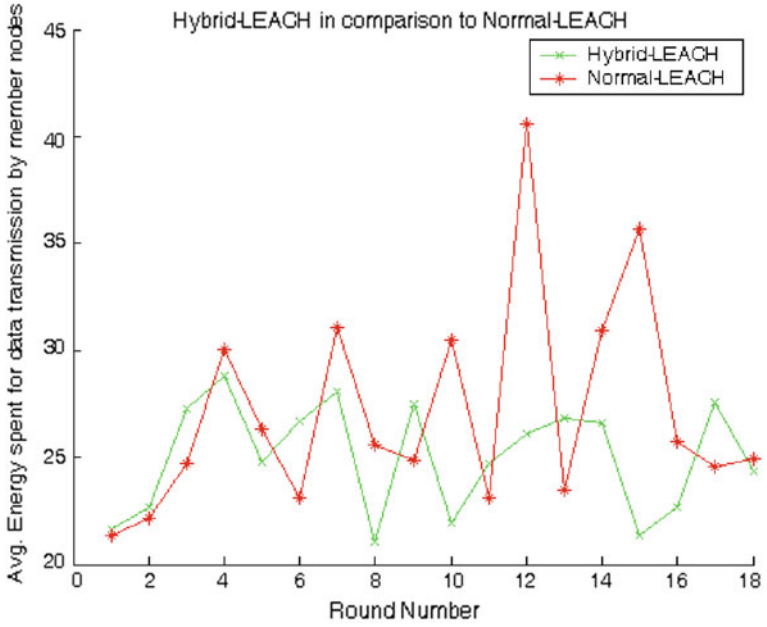


Fig. 6 H-LEACH versus normal LEACH (rounds)

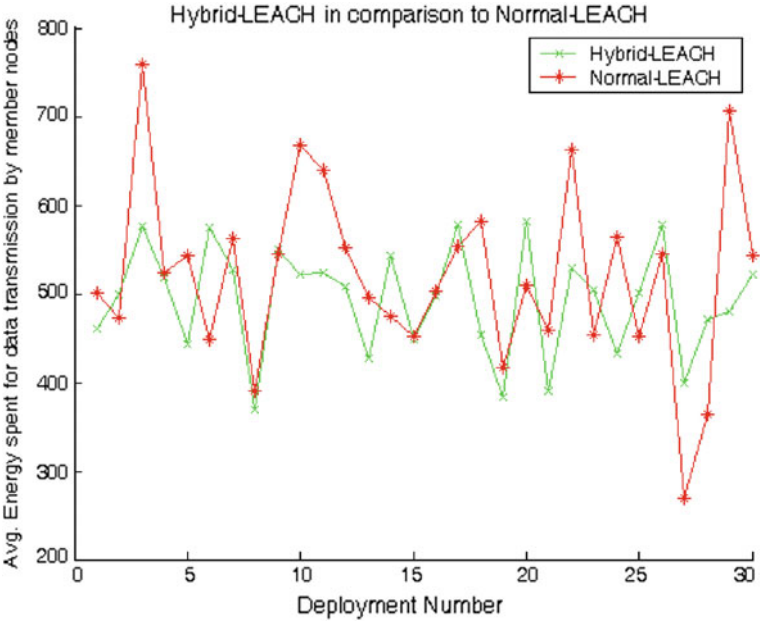


Fig. 7 H-LEACH versus normal LEACH (deployments)

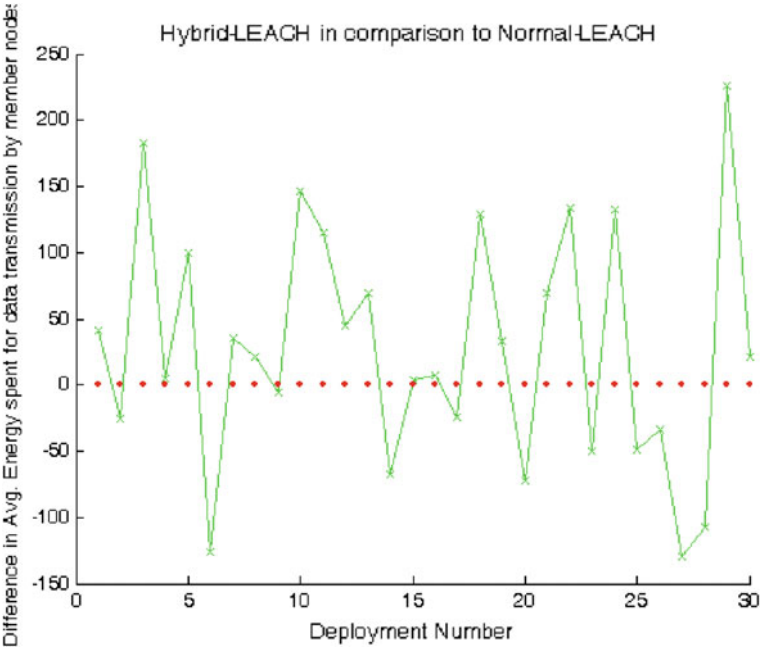


Fig. 8 Energy gain: H-LEACH versus normal LEACH (deployments)

There may be an extreme chance that some zone have very few or no nodes at all as the nodes are randomly deployed. In this case, the proposed protocol fails. But the probability of this case is negligible owing to the large scale, random but controlled deployment of the sensor nodes.

6 Conclusion and Future Scope

From the results obtained by the simulation clearly indicate that applying the available location information for nodes can result into an energy efficient design of a WSN. From Fig. 5, we conclude that the nodes in H-LEACH get associated with the CH node in the respective zone only, thereby guarding themselves to have long-distance CH association with CH nodes as shown by Fig. 3 in the case of normal LEACH.

From Fig. 6, we also observe that for some rounds, the results favour normal LEACH. These are the cases when the member nodes find this efficient to get associated with the CH nodes that are not in their zone but are nearer to them. But in long run, the Hybrid-LEACH protocol shows much energy gain as normal LEACH, thereby enhancing the lifetime of the network. Also, this is intuitive that this effect will keep on reducing as the number of zones/CHs is increased.

For future work, this will be interesting to see the effect of increasing the zones/CHs along with the number of deployed nodes on the energy gain of the given network.

References

1. Cheng, C.-T., Tse, C.K., Lau, F.C.M.: A Clustering Algorithm for Wireless Sensor Networks Based on Social Insect Colonies. Sens. J. IEEE **11**(3), 711–721 (March 2011)
2. Wei, D., Jin, Y., Vural, S., Moessner, K., Tafazolli, R.: An energy-efficient clustering solution for wireless sensor networks. IEEE Trans. Wirel. Commun. **10**(11), 3973–3983 (November 2011)
3. 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 (HICSS '2000), pp. 1–10. IEEE
4. Wang, Y., Xiong, M.: Monte Carlo simulation of LEACH protocol for wireless sensor networks. In: IEEE Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2005 (PDCAT 2005), pp. 85–88
5. Heinzelman, W., Chandrakasan, A., Balakrishnan, A.: An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. **1**(4), 660–670 (2002)
6. Muruganathan, S.D., Ma, D.C.F., Bhasin, R.I., Fapojuwo, A.O.: A centralized energy-efficient routing protocol for wireless sensor networks. IEEE Commun. Mag. **43**(3), 8–13 (2005)
7. Ghasemzadeh, H., Rezaeian, M., Dehghan, F., Mohsen, M.: BN-LEACH—an improvement on LEACH protocol using Bayesian networks for energy consumption reduction in wireless

sensor networks. In: 7th International Symposium on Telecommunications (IST'2014), pp. 1138–11143 (2014)
8. Wang, N., Zhu, H.: An energy efficient algorithm based on LEACH protocol. Proc. Int. Conf. Comput. Sci. Electron. Eng. **2**, 339–342 (2012)
9. Behboudi, N., Abhari, A.: A weighted energy efficient clustering (WEEC) for wireless sensor networks. In: Seventh International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), pp. 146–151 (2011)
10. Kumar, D., Aseri, T.C., Patel, R.B.: EEHC: energy efficient heterogeneous clustered scheme for wireless sensor networks. Comput. Commun. **32**(4), 662–667 (4 March 2009). ISSN 0140-3664
11. Wang, W., Peng, Y.: LEACH algorithm based on load balancing. TELKOMNIKA Indonesian J. Elect. Eng. **11**(9), 5329–5335 (2013)
12. Richard, W.G.: Extending LEACH routing algorithm for wireless sensor network. Data Communications Engineering (2009)
13. Farooq, M.O., Dogar, A.B., Shah G.A.: MR-LEACH: multi-hop routing with low energy adaptive clustering hierarchy. In: Proceedings of 4th International Conference on Sensor Technologies and Applications, pp. 262–268 (2010)
14. Liao, Q., Zhu, H.: An energy balanced clustering algorithm based on LEACH protocol. In: Proceedings of the 2nd International Conference on Systems Engineering and Modeling, pp. 72–77 (2013)
15. Ma, D., Ma, J., Xu, P.: An adaptive assistant-aided clustering protocol for WSNs using niching particle swarm optimization. In: Proceedings of 4th IEEE International Conference on Software Engineering and Service Science, pp. 648–651 (2013)
16. Mehra, P.S., Doja, M.N., Alam, B.: Low energy adaptive stable energy efficient (LEASE) protocol for wireless sensor network. In: Proceedings of 1st International Conference on Futuristic Trend in Computational Analysis and Knowledge Management (ABLAZE 2015), pp. 484–488. IEEE (2015)
17. Chunawale, A., Sirsikar, S.: Minimization of average energy consumption to prolong lifetime of wireless sensor network. In: Proceedings of IEEE Global Conference on Wireless Computing and Networking (GCWCN), pp. 244–248 (2014)
18. Arumugam, G.S., Ponnuchamy, T.: EE-LEACH: development of energy-efficient LEACH protocol for data gathering in WSN. EURASIP J. Wirel. Commun. Netw. (Springer Open Journal) (2015). doi:10.1186/s13638-015-0306-5
19. Sheta, A.F., Solaiman, B.: Evolving clustering algorithms for wireless sensor networks with various radiation patterns to reduce energy consumption. IEEE Sci. Inf. Conf. London UK 1037–1045 (28–30 July 2015). doi:10.1109/SAI.2015.7237270
20. Tohma, K., Aydin, M.N., Turgut, I.A.: Improving the LEACH protocol on wireless sensor network. In: IEEE 23th Signal Processing and Communications Applications Conference (SIU), 16–19 May 2015, pp. 240–243. doi:10.1109/SIU.2015.7129804
21. Li, L., Liu, C.: An improved algorithm of LEACH routing protocol in wireless sensor networks. In: IEEE 8th International Conference on Future Generation Communication and Networking (FGCN), 20–23 Dec 2014, Haikou, pp. 45–48. doi:10.1109/FGCN.2014.18

Implementing Chaotic and Synchronization Properties of Logistic Maps Using Artificial Neural Networks for Code Generation

Bijoy Kamal Bhattacharyya, Hemanta Kumar Sarmah and Kandarpa Kumar Sarma

Abstract Logistic maps, usually preferred for chaotic sequence generation, provide certain challenges while implementing for real applications. Specifically, while considered for applications as a coder or spread factor generators in wireless communication, certain modular and simplified approaches are necessary to mitigate effects of complex designs. The chaotic nature of logistic maps has been exploited for code generation and has been preferred for spread factor generation as part of spread spectrum modulation (SSM). In this paper, we describe an approach of using certain modular designs for reducing the complexities of a logic map coder and spread factor generator, specially the computational load, while implemented using artificial neural networks (ANNs). The learning ability of the ANN is used to track the chaotic and synchronization properties of logistic map and used as an aid to SSM in a wireless setup.

Keywords Logistic · Channel · Chaotic · Synchronization · Spread · Spectrum

1 Introduction

The dynamic nature of wireless channel makes voice and data communication through it a very tricky issue. One of the critical factors contributing to this dynamic and stochastic nature is fading of the signal which degrades the quality of service (QoS) [1, 2]. A range of tools and procedures has been developed to mitigate the

B.K. Bhattacharyya (✉)
Department of Mathematics, L C B College, Guwahati 781011, Assam, India
e-mail: bijoykamal@gmail.com

H.K. Sarmah
Department of Mathematics, Gauhati University, Guwahati 781014, Assam, India

K.K. Sarma
Department of Electronics and Communication Technology, Gauhati University, Guwahati 781014, Assam, India
e-mail: kandarpaks@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_43

effects of fading in wireless communication. Among them is certain communication techniques developed around the spread spectrum modulation (SSM). The QoS of a SSM-based communication method like code division multiple access (CDMA) is dependent on the generation of a spread factor (SF) which expands the spectrum much more than that normally required during transmission and identically shrinks the waveforms during recovery. The benefit derived is that due to the rapid expansion and shrinkage of the spectrum by a specially designed noise-like waveform, specific portions of the signal cannot be degraded by channel-related aberrations (natural and induced), much higher bandwidth is generated and collective lowering of the QoS is prevented. The spreading of the spectrum is done by using phase and frequency variations executed at rapid intervals in terms of variations in the waveform pattern of the SF. The SF is often obtained using a pseudo-noise (PN) sequence generated from multi-bit linear feedback shift registers (LFSRs). Gold codes are other preferred options. The PN sequence and Gold code generators are restricted by the physical size of the registers which at times places constraints in the designs while handling practical communication conditions. In many situations, the fading encountered in wireless channels require enhanced length SFs for better QoS [3]. Therefore, the chaotic properties demonstrated by logistic maps have been preferred for such cases [3, 4]. This is because of the fact that the generation of varying length of the chaos code is dependent on the iterations which the logistic map executes unlike the fixed register size-dependent behavior demonstrated by the other traditional SF methods. Deterministic chaos [5, 6] using iterative mechanism makes logistic maps ideal options for such situations. Further, logistic maps in synchronized states [7, 8] can also be effectively used to fight fading in wireless communication while being part of SSM systems [9]. However, such SF generation methods executed exploiting chaotic and synchronization properties of logistic maps provide certain challenges in terms of implementation. This is related to the fact that while the length of the chaotic sequences varies with fading conditions, the computation cycles fluctuate considerably. It puts constraints on the processing blocks. Therefore, certain solutions are required. The learning properties of artificial neural networks (ANNs) already used for innumerable applications [10, 11] can be effectively used to reduce the computational load involved in such frameworks.

In this paper, we describe an approach of using certain modular designs for reducing the complexities of a logic map coder and SF generator implemented using ANN. Initially, certain experiments are performed to configure logistic map generators of varying sequence lengths to improve QoS of transmissions in a faded wireless channel. The range of code generation mechanism is replicated by an ANN during training. After the ANN is trained, it effectively acts as a SF generator and demonstrates the deterministic chaotic behavior closely resembling that of an actual logistic map. The rest of the paper is organized as follows. Section 2 gives a description of the theoretical considerations involved with the work. Section 3 includes the experimental work. The experimental details and results obtained are included in Sect. 4. Section 5 concludes the discussion.

2 Theoretical Considerations

In this section, we discuss some of the theoretical aspects related to the work.

2.1 Logistic Map as Chaos Generator

A polynomial expression limited to second order is the basis of defining a logistic map executing complex and chaotic behavior and is governed by a mathematical expression [5, 6]

$$x_{n+1} = r * x_n(1 - x_n) \tag{1}$$

where x_n represents a number confined to binary zero and one and a zeroth year population with the parameter r taking values as shown in Table 1.

2.2 Synchronization in Logistic Maps

In many situations, multiple logistic maps can be used. Synchronization property is explicitly observed when multiple chaotic maps are coupled [5, 6]. Two logistic maps can be shown to be synchronized as given below:

$$y_{n+1} = x_n \tag{2}$$

$$x_{n+1} = y_n \tag{3}$$

Substituting respective logistic maps in the above expressions gives

$$y_n = rx_n(1 - x_n) \tag{4}$$

$$x_n = rq(1 - q) \tag{5}$$

with

$$q = ax_n + (1 - a)y_n \tag{9}$$

Putting $r = 4$ for x and y yields three solutions which subsequently gives $a = \frac{1}{2}$ and $a = \frac{5}{4}$ with the later not considered for realistic cases [5, 6]. For the case $= \frac{1}{4}$, a symmetrically coupled logistic map set is obtained.

Table 1 Behavior dependent on r

Range of r	Behavior of population
Between 0 and 1	Independent of the initial population
Between 1 and 2	Independent of the initial population
Between 2 and 3	Fluctuate around the value $r - 1/r$ for some time
Greater than 3	Dependent of the initial population

2.3 *Artificial Neural Network (ANN)*

ANNs are non-parametric, learning-based tools that capture the variations in the input data, retain the know-how and use it subsequently. Most commonly, ANNs are used for non-linear mapping of input to output in feed-forward form and trained with (error) backpropagation algorithm. In the feed-forward form, the ANN is formed by a number of layers of artificial neurons which are the basic processing units (Fig. 1). There is one input and one output layer and one or multiple hidden layers. The layers are connected with certain random weights which generate the parallel and connectionist nature of computing mimicking bio-inspired processing. During each cycle of execution, the output of the ANN is compared with a reference. The difference between the present output and the desired result is circulated back which triggers the modification of the connectionist weights. The different steps of the ANN training are as given below [12]:

1. Initialization of the weights and learning rate.
2. Perform steps 3–10 until the stopping condition is false.
3. Perform steps 4–9 for each training pair.
4. Each input unit receives the input signal x_i and sends it to hidden units.
5. Each hidden unit z_i sums its weighted input signals to calculate the net input.

$$z_{inj} = v_{oj} + \sum_i x_i v_{ij}$$

Output of the hidden unit is calculated by applying activation on z_{inj}

$$z_j = f(z_{inj})$$

The output signal from the hidden unit is sent to the output unit.

6. For each output unit y_k, calculate the net input

$$y_{ink} = w_{ok} + \sum_j z_j y_{jk}$$

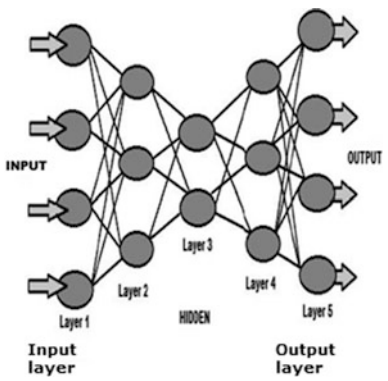


Fig. 1 Basic topology of an ANN in feed-forward configuration

Activation function gives the output signal which is given by

$$y_k = f(y_{ink})$$

7. Each output unit y_k receives a target pattern corresponding to the input training pattern and compute the error correction term

$$\delta_k = (t_k - y_k) f'(y_{ink})$$

On the basis of the error term, weight and bias are updated as:

$$\Delta w_{jk} = \alpha \, \delta_k z_j$$

$$\Delta w_{ok} = \alpha \, \delta_k$$

Also it sends δ_k to the hidden layer backward.

8. Each hidden unit z_j sums its delta input from the output unit.

$$\delta_{inj} = \sum_{k=1}^{\mathrm{m}} \delta_k w_{jk}$$

The term δ_{inj} gets multiplied with the derivative of $f(z_{inj})$ to calculate the error term $\delta_j = \delta_{inj} f'(z_{inj})$

9. Each output unit y_k updates the bias and weight

$$w_{jk}(\text{new}) = w_{jk}(\text{old}) + \Delta w_{jk}$$

$$w_{ok}(\text{new}) = w_{ok}(\text{old}) + \Delta w_{ok}$$

Each hidden unit updates its weight and bias

$$v_{ij}(\text{new}) = v_{ij}(\text{old}) + \Delta v_{ij}$$

$$v_{oj}(\text{new}) = v_{oj}(\text{old}) + \Delta v_{oj}$$

10. Check the stopping condition.

These steps constitute the training cycle of the ANN.

3 Proposed Method of Using ANN-Aided Chaotic Sequence Generation Using Synchronized Logistic Maps

Here, we discuss the proposed ANN-aided generation of chaos codes in binary form as varying SF for use in a SSM system. The work also describes the ANN-based approach of mimicking the synchronization achieved in coupled logistic maps during recovery of transmitted data bits.

The logistic map generates random binary bits which are obtained using thresholding and floating point to bit conversion-based binary sequence generation [5, 9]. For three different values of r, example sequences are shown in Table 2. The system model is shown in Fig. 2. Here, the logistic map generator is replaced by a trained ANN. This is shown in Fig. 3. First, constant length binary data blocks are obtained as summarized in Table 2 for feeding to the logistic map generator which acts as a reference to the ANN. For each input feed given by the data source, the ANN receives a sequence from the logistic map. This sequence length is varied between 4 and 32 representing a wide variety of patterns. Next, the ANN tracks varying length chaos codes which are used to fight fading effects. The chaos codes length is varying between 4 and 32 which are found to be suitable to fight fading observed in pedestrian and vehicular conditions of mobile communication. The training of the ANN is carried out using backpropagation algorithm as discussed in Sect. 2. The ANN-generated SFs are used in the SSM system. The most common SF codes are the PN sequences and Gold codes. As already discussed, these codes suffer from fixed register sizes hence are constrained to certain situations. Therefore, the logistic map generators serve as a ready replacement without having any fixed register length restriction. Instead, uses an iterative mechanism to generate varying sequence lengths. But this process since is computationally demanding, the proposed ANN-based approach reduces the computation considerably. Figure 4 shows an approach to use two coupled logistic maps based on

Table 2 Sequences generated by logistic map for r = 3.61, 3.65 and 3.69

Value of r	Binary sequence
3.61	00111000011010010100
3.65	01001001010010010101
3.69	01101001001110000110

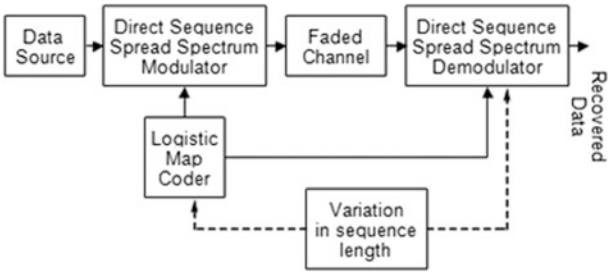


Fig. 2 System model

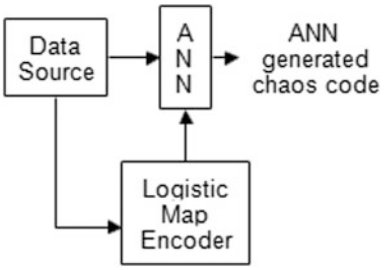


Fig. 3 ANN-based chaos code generator

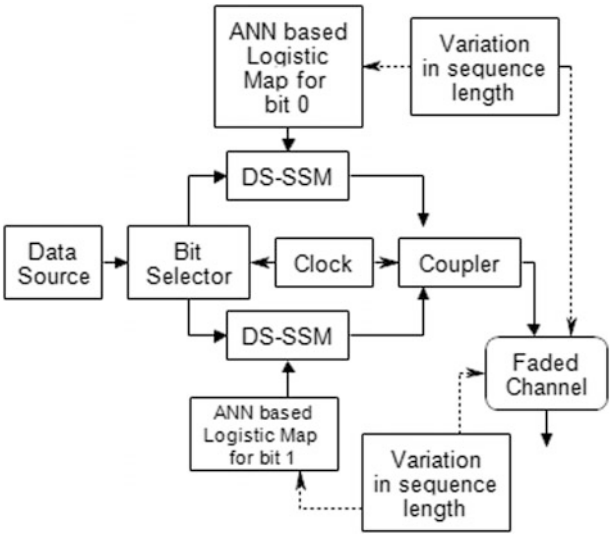


Fig. 4 Coupled ANN-based logistic map chaotic code generator

ANNs. Two ANNs are trained to handle chaos code generation for bifurcated streams of 1 and 0 bits working in a synchronized state with a clock. The two defined systems are trained and tested under a range of conditions.

4 Experimental Details and Results

A SSM system is constituted and several sets of trails are carried out using PN, Gold code, and chaos code sequences generated by ANNs in Rayleigh channel with communication involving pedestrian state and vehicular speeds in the range 10–100 Kmph. The ANN generates sequence lengths continuously between 4 and 32 under 0 and 10 dB signal to noise ratio (SNR). The QoS of the system is noted

Table 3 ANN parameters

Item	Description
Performance goal	0.001
Size of hidden layers	23
Training epoch	200
Validation cycle	10
Max. time during training	30 s
Activation functions	Input/output-log-sigmoid, hidden-tan-sigmoid
Cost function	Mean square error (MSE)

in terms of bit error rate (BER) versus SNR. The ANN parameters are shown in Table 3. The ANN is provided with a convergence goal of the mean square error (MSE) of 0.001. Maximum 200 epochs within 30 s time frame are used with multiple ANNs with log-sigmoid activation in the input and output layers and tan-sigmoid activation in the hidden layer. An example of the MSE convergence is shown in Fig. 5. The ANN-based chaos code generates satisfactory BER values.

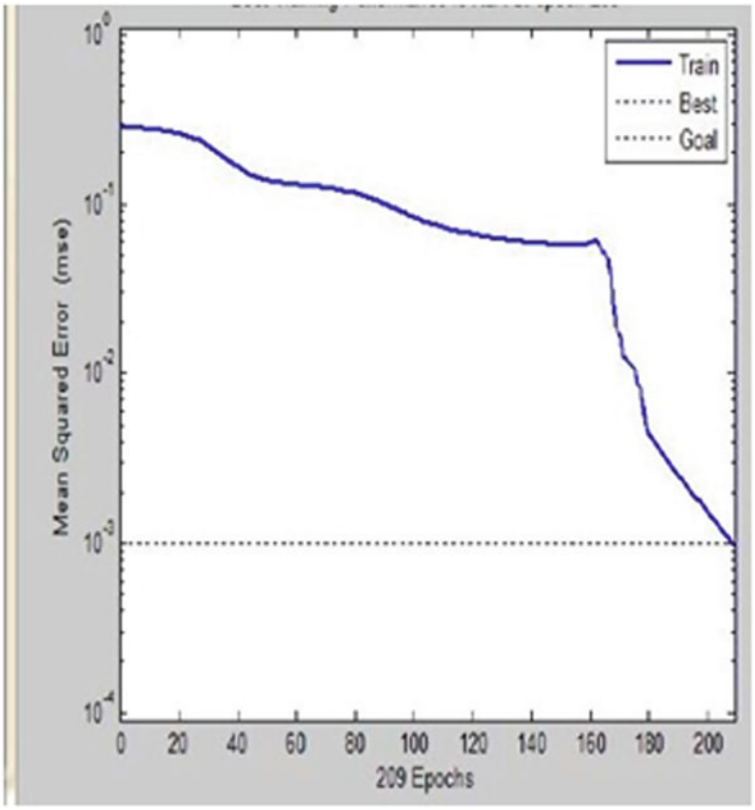


Fig. 5 MSE convergence plot of the ANN

Table 4 BER v/s SNR plot of varying sequence lengths of PN, Gold code, and chaos code

S. No.	Sequence length	SNR in dB	PN sequence	Gold code	Chaos code
1	4	0	0.1	0.1	0.1
		2	0.07	0.05	0.05
		4	0.06	0.04	0.034
		6	0.05	0.03	0.03
		8	0.04	0.018	0.015
		10	0.01	0.008	0.007
2	8	0	0.091	0.085	0.083
		2	0.0637	0.0425	0.0415
		4	0.0546	0.034	0.02822
		6	0.0455	0.0255	0.0249
		8	0.0364	0.0153	0.01245
		10	0.0091	0.0068	0.00581
3	16	0	0.078	0.0752	0.059926
		2	0.0546	0.0376	0.030005
		4	0.0468	0.03024	0.020347
		6	0.039	0.02259	0.017928
		8	0.0312	0.013536	0.008964
		10	0.0078	0.006016	0.004183
4	32	0	0.065	0.0623	0.061
		2	0.04585	0.0311	0.0305
		4	0.03924	0.02492	0.020808
		6	0.0326	0.0186	0.01839
		8	0.02608	0.01116	0.0093
		10	0.0063	0.00488	0.00434

Such a set of data for an average of ten trials under fading conditions is summarized in Table 4. Advantage of the chaos code is obvious. A few cycles are required to obtain the synchronization between the received bit streams and recover the data sequences. After the ANN is trained, the time required to perform the recovery of the data as part of the SSM is less compared to the PN sequence, Gold code, and conventional chaos code. This is seen from the data summarized in Table 5. The % saving in time is between 7 and 42 which are significant.

The chaos code generation involving logistics map and the use of coupled blocks improves QoS. It also adds to the computation. The ANN with its ability to learn the applied patterns and establish a mapping between input and output helps to generate the chaos codes nearly replicating the function of the logistic map. Experimental results show that the ANN, after it is trained properly, contributes toward saving of computing cycles while dealing with fading in a wireless channel acting as a chaos code generator.

Table 5 Average computational time due to varying sequence lengths

S. No.	Sequence length	Time is s (s)				% time saving w. r. t chaos code
		PN sequence (1)	Gold code (2)	Conventional chaos code (3)	ANN chaos code (4)	
1	4	1.35	1.42	1.4	1.25	11
2	8	2.13	2.3	3.1	2.56	17
3	16	2.52	2.55	3.6	2.1	42
4	32	3.1	3.3	4.4	4.1	7

5 Conclusion

Here, we have described the working of a trained ANN as a chaos code generator. The primary motivation has been to save computational cycles required by the logistic map while generating varying length chaos sequences as part of an SSM system to mitigate ill effects of fading. The trained ANN replacing the logistic map acts as a readily available chaos generator in a decoupled and synchronized form achieves the required QoS in a fading wireless channel.

References

1. Rappaport, T.S.: Wireless Communications: Principles and Practice, 2nd edn. Pearson Education, New Delhi (2004)
2. Turin, W., Jana, R., Martin C., Winters, J.: Modeling wireless channel fading. In: Proceedings of Vehicular Technology Conference, Atlantic City, NJ, October (2001)
3. Swami, D.S., Sarma, K.K.: A Chaos based PN sequence generator for direct-sequence spread spectrum communication system. Int. J. Circuits Syst. Sig. Process. **8**, 351–360 (2014)
4. Kashyap, K., Sarma, M.P., Sarma, K.K., Mastorakis, N.: Generation of orthogonal logistic map sequences for application in wireless channel and implementation using a multiplierless technique. In: Latest Trends in Circuits, Systems, Signal Processing and Automatic Control, pp. 292–296, June (2014)
5. Rasband, S.N.: Chaotic Dynamics of Nonlinear Systems. Wiley, New York (1990)
6. May, R.M., Oster, G.F.: Chaos from maps. J. Phys. Lett. A, **78**, 1–24 (1980)
7. Rasband, S.N.: Chaotic dynamics of nonlinear systems. Wiley, New York (1990)
8. Pikovsky, A., Rosenblum, M., Kurths, J.: Synchronization: A Universal Concept in Nonlinear Sciences, vol. 12. Cambridge University Press, Cambridge (2002)
9. Bhattacharyya, B.K., Sarmah, H.K., Sarma, K.K., Mastorakis, N.: Exploitation of Chaotic and synchronization properties of logistic maps for application in wireless communication. In: International Conference Applied Mathematics, Computational Science & Engineering (AMCSE 2015), Agios Nikolaos, Crete, Greece, 17–19 Oct 2015 (2015)
10. Bordoloi, H., Sarma, K.K.: Protein Structure Prediction Using Multiple Artificial Neural Network Classifier, Soft Computing Techniques in Vision Science. Studies in Computational Intelligence, vol. 395, pp. 137–146. Springer, Berlin (2012)
11. Devi, G., Sarma, K.K, Datta, P., Mahanta, A.K.: Indian J. Phy. **86**(1), 77–84 (2012)
12. Haykin, S.: Neural Networks: A Comprehensive Foundation. Macmillan Coll Div, New York (1994)

Enhancement of LAN Infrastructure Performance for Data Center in Presence of Network Security

Bhargavi Goswami and Seyed Saleh Asadollahi

Abstract Policy-based LAN infrastructure implementation has always been a challenge for the corporate bodies that has diversified networking situations to be handled in limited resources especially in presence of servers with firewall securities. This paper provides solution to many problems that are compromised by the corporate organizations so far, even when updated technology is present in today's world. Here, in this paper, we have improved the performance of existing LAN infrastructure by modifying certain corners of the networking scenario in presence of security considerations. Here, we have also implemented AAA and RADIUS security to overcome the remaining loopholes of the system. By proposing a novel approach toward network implementation, we obtained reports that brought overwhelming networking boost. Researchers, field workers at networking site, and all those who are part of the networking world must read this article before starting any implementation of networking scenario to get to know the do's and don'ts before the implementation phase is initiated.

Keywords Radius · MD5 · ACL · Distribution list · DMZ · LAN · AAA CAT-6

1 Introduction

In accordance with the specification provided in the research project, it is well thought-out that they have appointed me as Project Coordinator with a team of few research fellows, networking group for a huge data center company 'BG Networking Solutions' with three network managers assigned to me. We have

B. Goswami (✉)
MCA Department, Sunshine Group of Institutions, Rajkot, Gujarat, India
e-mail: bhargavigoswami@gmail.com

S.S. Asadollahi
MSc. IT and CA Department, Saurashtra University, Rajkot, Gujarat, India
e-mail: asadollahimcitp@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_44

provided particulars of the allocated task as follows. The registered headquarters of the corporation is in Bangalore, and this group is spread in due division workplace in Hong Kong and Sydney. Our main responsibility is to develop a blueprint, execute and experiment an innovative LAN infrastructure for all of the subdivisions. We must also put into practice novel protection measures for diversified subdivisions of the group and to permit far-off remote access to employees for definite task to be completed on time by these employees, being operational far-off from offices.

Major troubles in the existing network are:

- Managers of all section must get rights to use supplementary concealed resources which the staff is not permitted.
- The group has presently taken number of new IT maintenance personnel, but at present, the IT support department is packed so they have to take a seat in the HR section. IT support personnel require access to technological resources, but they are not provided. IT support team can barely access to the HR department resources as they are connecting to 'HR' switch.
- A few workers want to have right of entry to the network while operational away from the workplace.
- The network is sluggish since the group is developing and growing quantity of employees/customers.
- Managing director desires to put in a fresh advertising section to the corporation which necessitates that all spare equipment must be equipped for this purpose.

The group has provided us with Table 1, outlining how their employees are alienated in different level at different site and what safety measures and policy must be functional to them. The group has clearly mentioned how clustered strategies are put into action and is given as follows:

- Only HR division employees can have access to HR division network and no one else.
- Two senior managers are given rights to access finance division other than HR division employees and no one else.
- Manager of the division is not allowed to access network of another division but can access HR division.

Table 1 Branch-wise requirement and department-wise requirement of remote access and number of users

Department	Bangalore	Hong Kong	Sydney	Remote access
Human Resource	3	3	1	No
Finance	4	2	1	No
Managers	3	2	3	Yes
Electrical	2	3	1	No
Mechanical	2	2	3	No
IT support	6	3	2	Yes

- Electrical engineers are provided with access rights only to their own departmental subdivision network.
- Mechanical engineers can access only their own departmental subdivision network.
- IT support section employees are provided with the access to each and every network but no more than administrative and technical rights. They are not privileged to access or modify any files and folders of other section employees.

Now we desire to construct a trustworthy and proficient LAN infrastructure used for the specified circumstances in a model-based simulated environment prior to actually put into operation the network. All the simulations developed are provided in this article.

Section 2 describes analysis of LAN implementation, and Sect. 3 describes design of LAN with improvements. Section 4 has implementation of newly proposed design followed by Sect. 5 that shows the obtained results and its analysis, followed by Sect. 6 Conclusion and Sect. 7 Future Scope.

2 Analysis of LAN

We would like to have a helicopter view upon the available options for implementing and executing LAN infrastructure. Further, we would like to discuss the high-performing service provisions considering the concentration of traffic during office hours. Again, we would not come to the end before discussing about the performance, trustworthiness, and security measures to be considered during design of the LAN.

2.1 Assessment of Available LAN Technologies

It is a cardinal decision of selection of technology that is to be implemented during the building of LAN infrastructure, as it not only affects the capital of the working group but also the performance to a great extent. While looking into the most admired LAN technologies, top among the list will be Ethernet, Fast Ethernet, Gigabit Ethernet, Fiber Optics, etc. During the assignment of the research project, there was no limitation specified over the usage of the type of media whether guided or unguided. So taking into consideration the recognition, features, and expenditure, we would prefer usage of wired networks. Let us have a look upon available options.

In 1980, IEEE 802.3 was standardized and given a name Ethernet that became very well known later which is basically using technique called CSMA/CD for performing collision detection. This technology is widely implemented with hubs and switches by means of Cat-5 UTP twisted pair cables or coax thick cables using

STAR topology having the data rate of 10 mbps with 10 Base-T encoding techniques. But, the major disadvantage of Ethernet is its high collision domain. Again, the fact remains that in presence of this limitations, about 80% of the world prefers Ethernet over other available options.

Further, Ethernet evolved by adding to its data rate ten times making it to 100 mbps which was a major step ahead that got standardized and named Fast Ethernet in 1995. Two most popular among all the options available were 100 Base-T and 100 Base-FX where the only difference among them was the type of wires. UTP cable is used with 100 Base-T and uses fibers with 100 Base-Fx. The parameter to be considered while selecting among the options is the distance between the end hosts. Priority is given to fiber options when the distance is large and when the distance is small; we opt for UTP, unshielded twisted pair.

Moving ahead, Ethernet does not stop there, and within a short time of 3 years, superior technology was introduced that was Gigabit Ethernet also widely known as IEEE802.3ab/ah. Drastic boost of data rate was a major milestone for Ethernet that achieved data rate of 1000 mbps. Yes, we would like to mention that 802.3ab is using UTP Cat-7 cables, whereas 802.3ah is using fiber optics.

Still moving forward, Ethernet does not stop evolving and took a further step and brought 10 Gigabit Ethernet which was using both copper and fiber optics. The largest lifespan of the communication technology is of Ethernet, and still it is moving ahead with the support of researchers like us.

The question arises in the readers mind about the selection of Ethernet then we would like them to make a note that the feature with which it wins upon all other available technologies is the reliable data delivery at nominal expenditure.

2.2 Performance Analysis of Traffic Intensive Networks

As mentioned earlier in Sect. 1 of introduction that our network is having issues of delayed delivery and the network is behaving very sluggish because of the growing number of employees and customers of the BG Networking Group, especially in office hours network is suffering from drained throughput, huge delay inspiring the circumstances of high drop rate, and further worsen situation to multiple retransmission feeding congestion itself. We would propose Fast Ethernet and Gigabit Ethernet instead of Classic Ethernet as a solution to the problem solving also the issue of delay, throughput and control over drop rate and congestion.

2.3 Performance and Security Concerns

Network Security: For providing security to our BG networking group network, there are two options available, EAPOL and RADIUS [1, 2]. When remote access is to be provided, it is necessary to provide minimum EAPOL security and preferably

RADIUS server security that has advantage of AAA—authentication, authorization, and accounting. MD5 hash is the most trusted authentication algorithm that ensures security not over just the masquerading but also assures integrity. The requirement of distribution of data over the large distance covering multiple cities and multiple branches can be achieved using implementation of secure tunnel between the RADIUS servers additionally assisted with the facility of remote access. To avoid further intruders eavesdropping and unauthorized access to our networks, we would like to keep our servers on demoralized zone (DMZ).

Reliability: Reliability is directly proportional to the robustness of the network. And robustness assures that network is never going to fail whatsoever adversities it comes across. Again, it assures that network is available round the clock no matter what. To provide this service, we would invest upon backup data center along with main data center. Ether Channel is required to fulfill the requirement of backbone line between the two most busy heavily loaded routers that works over distributed layer. Usage of Ether Channel does protect us against traffic aggregation other than fault tolerance and heavy congestion control over backbone links between the routers. And, fault tolerance provides us the service of reliability over the network.

Performance: Usage of Ether Channel on backbone links over the network boosts the performance bringing it to almost double the one obtained before. If requirement exist, we would use fibers without hesitation. Reliable LAN technologies like Gigabit Ethernet and Fast Ethernet over the end host assure reliability to the networks. Ether Channel boosts the data rate over the traffic-studded routers. As a result, controlled congestion demotivates retransmission. As a result, once transmitted, packet gets delivered at first go with desired rate of transmission at the end providing expected network throughput.

3 Designing of LAN

This section describes the design requirements taken into consideration for the development of LAN infrastructure for BG networking group's data center networks. Further, we will also evaluate the criticality and suitability of the planned design and included components for doing the task.

Table 2 explains how the network that is developed will run in three branches and manage the departments of those branches critically. Table 2 carries the information about the number of users with their subnet range, which is clearly revealed in Fig. 1. Table 2 also describes the access rights and policy implementation very clearly to show which of the users are not permitted to remotely access the servers.

We would like to incorporate few laptops and computers, some routers and switches, dedicated servers with firewalls. There are two cardinal-linked routers that distribute data between the branches and working on the distributed layer that are most of the times crowded and congested. We would like to facilitate the link between these two routers with Ether Channel which once implemented so that,

Table 2 Indicating the number of staffs and remote access facility provision

Assigned network	Facilitated with remote access?	# Users	Networking departments
172.24.0.0	Yes	N	Remote access to staff
192.168.0.0	Yes	N + 47	Server zone (DMZ)
172.16.0.0	No	4	HR
172.20.0.0	Yes	8	Manager's
172.22.0.0	No	7	Finance
172.21.0.0	Yes	6	IT support
172.19.0.0	Yes	6	Mechanical
172.18.0.0	Yes	4	Electrical
172.17.0.0	Yes	N	Marketing

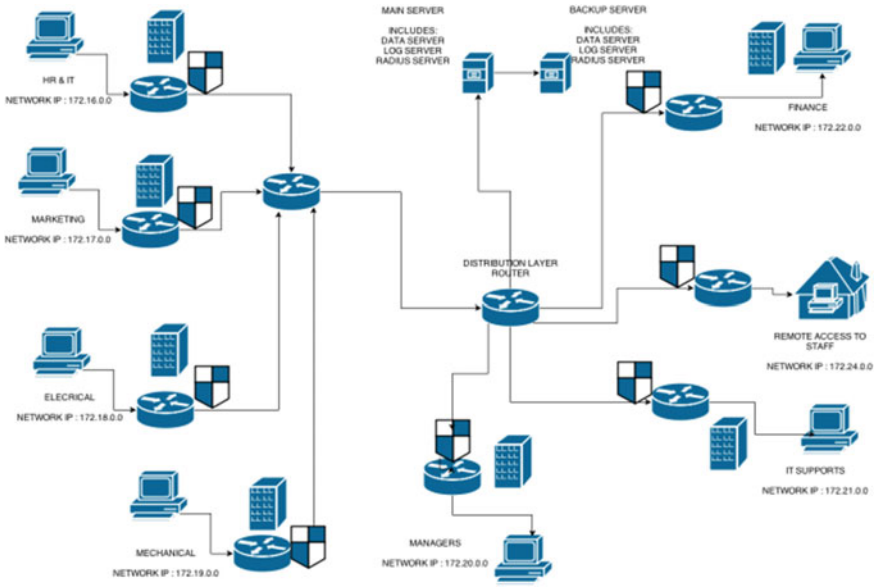


Fig. 1 BG networking group's infrastructure planning and development

congestion and jitter can be avoided over such a high-delay network links. There were two options, either use of a switch or a router over access layers. But, considering cost-effectiveness in accordance with future perspectives and flexibility needed over number of users, we would like to opt for L3 switches. Again, we would like the readers to note that we would make use of a RADIUS servers that provides authentication, authorization, and accounting facility in addition to EAPOL services with RADIUS servers giving the strong protection from intruders and opponents against the system. Addition of MD5 would be an added advantage over the implementation of security over the servers especially for remote servers.

We would like to provide distribution of network load between different departments so that there is no interference between the routing activities with the

independence of operational activities. We confine the subnet mask of 255.255.255.0, and IP address to every department will be provided separately to maintain control over access. Each server will be provided with different network address and its series so that unauthorized access is not permitted. We also need to provide fault tolerance along with uninterrupted availability, and for that we are facilitating our data center networks with backup servers [3]. Again, to provide strategic implementation of company policies, we will use access list in addition to distribution list. To keep control and monitor the smooth running of network activities, we will use Syslog Servers of Kiwi to keep logging the events of server, backup server, and routers connected to it [4].

There are some problems that BG networking group has come across over the years, and we suggest solution to the problems with less modification during the implementation stage.

(a) As the network seems to be behaving too slow because of increasing number of users and staff, we recommend the use of Ether Channel over backbone distribution layer routers that will use Layer 3 switches to support more number of end host with all the supporting features of a router with high data rate.
(b) Managers generally demand additional resources in comparison with other staff which was not permitted earlier. To have a control over each of the resources, we can implement access list and solve this issue without any compromise with the access rights.
(c) Now, as the group has hired few of the IT-supporting candidates before the department could arrange for their space, they are assigned the space of HR Department temporarily. But, their switch is different. To solve this issue, we have provided the solution by using access list that will allow IT Department employees to work comfortably while sitting in HR Department by using the same router.
(d) There is a requirement of additional Marketing Department that will be privileged with additional resources in comparison with other existing departments. We would recommend usage of Layer 3 switches connected with Fast Ethernet-wired connectivity that can be defined in the company policy for implementation of distributed list over the switches.
(e) There is a requirement by some of the staff members that they must be given the access to the network considering them not able to remain at the location of the work. The solution to this problem is provision of remote access in secure mode [3]. We will develop iterative tunnel mode for server access through remote connectivity. For implementing company policy, we will use access list with distribution list.

4 Implementation of LAN

Network simulator GNS-3 0.8.6 developed under GPL v2 license [5] has been used for implementation of the designing model for the task assigned. For implementing policy-based routing over remote access and other specified requirements, we have

used EIGRP [6, 7], as EIGRP being implemented widely for fulfilling enterprise requirements. For keeping track of the activity of users, further monitoring and profound management of log information, Kiwi Syslog server [4] is chosen. For the provision of availability service round the clock, development of actual and backup server both is done over RADIUS [1].

In this section, all the design specification is implemented by configuring the LAN of BG networking group's data center according to the requirements specified. Further, security implementation is done over infrastructure. As a final point, we would vitally evaluate and check our LAN. Few loopback for each network and subnets have been developed to examine the effectiveness of the policy implementation. It is understood that department-wise routers are different, and all the three branches are connected through single router.

(a) Other than HR staff and managers, there must be no access to anyone to the department of HR. This is achieved by implementing distribution list over access list applied over RADIUS server configurations. Successful implementation was tested where Marketing (172.17.10.1), Electrical (172.18.10.1) or Mechanical (172.19.10.1) Department tried to ping HR Department (172.16.0.0), but could not ping. However, Manager's department (172.20.10.1) has access to HR Department.

(b) All the managers have control over network of just their own department and over HR Department. Figure 5 shows the ping testing done over Marketing Department when tried to ping other departments, which reveled that it has access to only his department. Yes, remote access provision is made available securely through 172.24.10.1 over tunnel mode.

(c) The only department that has access to all other department is IT support team but only for technical assistance. To implement this policy where IT team can only provide technical solutions and cannot modify files and folders, we have used RADIUS servers. Resources are accessible by technical team but just for maintenance (Fig. 2).

(d) All the major economical transactions and decision of Finance Department is dealt with HR Departmental staff and due senior managers of the Management Department. In dealing with finance of the group, we have critically given access to this department only to the HR personals and managers. Figure 4 depicts the testing done over the manager's department loopback 172.20.10.1 over remote login from Electrical and Mechanical Department.

(e) Figure 7 shows how Mechanical Engineers were deprived access to other departments but just their own department using distribution list. Yes, again, remote access provision is made available for them through 172.24.10.1.

(f) Similarly, Fig. 6 shows that Electrical Engineers have access only to their own department. Electrical Department employees are allowed to work from home, and so there is a provision of remote access connectivity to its department only, i.e., Electrical Department 172.18.10.1 can make remote access through 172.24.10.1, but it cannot access Marketing Department 172.17.10.1 (Figs. 3, 4, 5, 6 and 7).

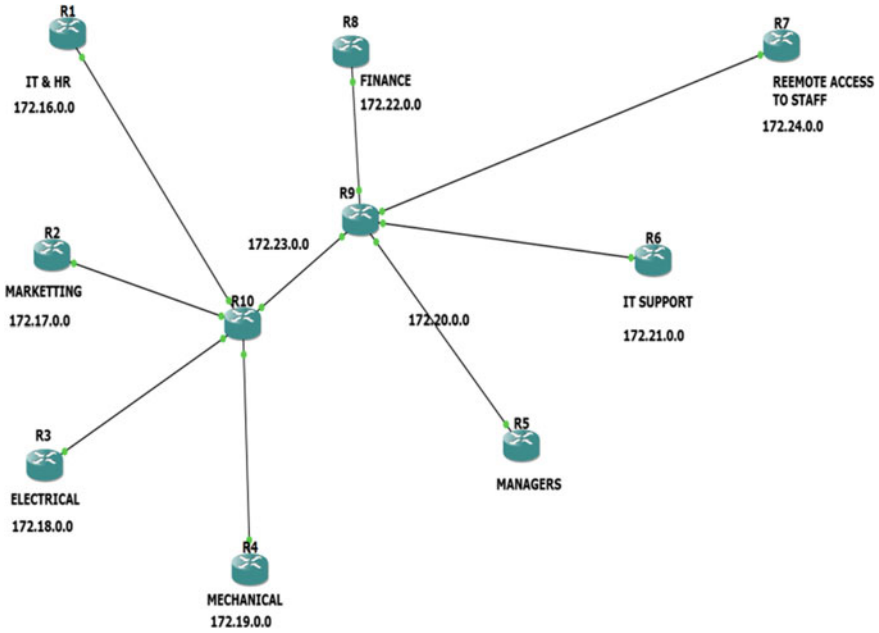


Fig. 2 Subnetting and implementing policy-based routing over the network of BG Networking Group

```
Connected to Dynamips VM "R1" (ID 0, type c3745) - Console port
Press ENTER to get the prompt.

HR#ping 172.18.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
HR#ping 172.19.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.19.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
HR#ping 172.20.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/98/152 ms
HR#
```

Fig. 3 Policy implementation and testing of access rights of HR Department

```
Connected to Dynamips VM "R8" (ID 7, type c3745) - Console port
Press ENTER to get the prompt.

R8#ping 172.20.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/128/304 ms
R8#ping 172.18.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R8#ping 172.24.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R8#
```

Fig. 4 Policy implementation and testing of access rights of Finance Department

```
Connected to Dynamips VM "R5" (ID 4, type c3745) - Console port
Press ENTER to get the prompt.

R5#ping 172.16.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 136/217/340 ms
R5#ping 172.17.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/170/212 ms
R5#ping 172.24.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/160/232 ms
R5#
```

Fig. 5 Policy implementation and testing of access rights of Manager's Department

```
Connected to Dynamips VM "R3" (ID 2, type c3745) - Console port
Press ENTER to get the prompt.

R3#ping 172.18.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R3#ping 172.24.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/116/216 ms
R3#ping 172.17.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.17.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R3#
```

Fig. 6 Policy implementation and testing of access rights of Electrical Department

```
Connected to Dynamips VM "R4" (ID 3, type c3745) - Console port
Press ENTER to get the prompt.

R4#ping 172.19.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.19.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
R4#ping 172.24.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.24.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/172/248 ms
R4#ping 172.18.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.18.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R4#
```

Fig. 7 Policy implementation and testing of access rights of Mechanical Department

5 Result Analysis of LAN

This section discusses the assistance provided for monitoring the activities and management of the system after the implementation phase is over to avoid issues post-implementation. Later, we evaluate the performance of the LAN infrastructure developed by checking its security and reliability aspects.

For maintaining the logs, analyzing the reports, and taking necessary actions, further, we maintained a standardized logging system called Syslog which not just has facility of logging the information but aid of checking severity of the messages by attaching labels like notice, warning, error which may be just an alert that is critical or of highest priority like emergency. Syslog server is set on 192.168.0.0.

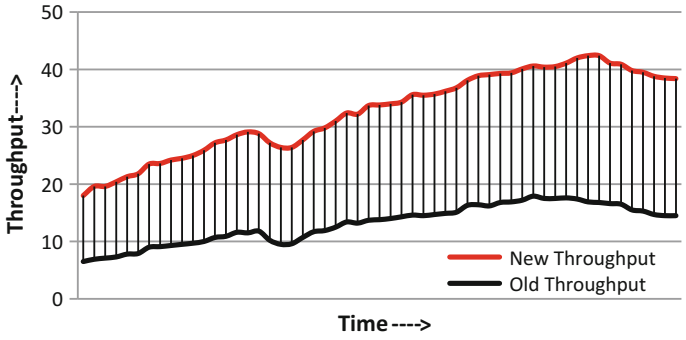
Usage of RADIUS server facilitates us with AAA that assures security and reliability [1]. Group-wise users are maintained for each department that provides access privileges to the users and put into operation business policy in addition to access rights. There is no difference in the rights whether the employee is working within the organization or making remote access. We have implemented actual and backup servers supporting data center networks to assist the entire network with the service of availability and sustainability to fault tolerance that at the end provides us the facility of reliability.

Performance evaluation of this network was observed by generating consecutive ping to multiple hosts of different networks from different networks for checking of different loopholes of the system. Ether Channel usage has overcome the limitations of network's sluggish behavior. Usage of advanced LAN technologies like Fast and Gigabit Ethernet over L3 switches has controlled congestion and data rate to great extend reducing the maintenance work of network administrators in addition to increased number of users and customers.

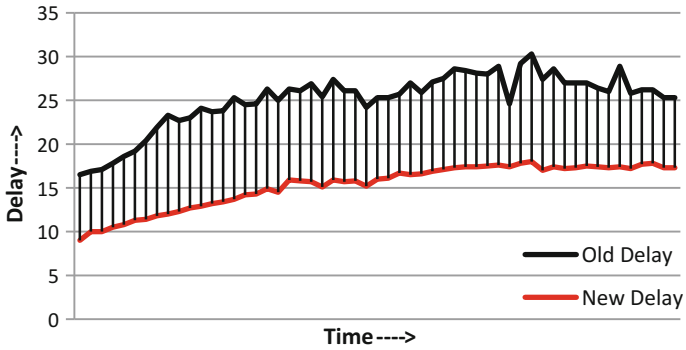
The following graphs are obtained in comparison to previously implemented scenario showing us the comparison between the network situation currently and earlier.

Graph 1 shows the throughput analysis of the LAN taken before the implementation of novel approach in comparison with the situation after the implementation of newly proposed approach. Red line indicates the values obtained after the modifications made. The graph clearly indicates that 31% of hike is observed in overall throughput of the LAN infrastructure. This is a remarkable enhancement of performance.

Graph 2 shows the delay observed in delivery of packets. Red line shows the delay observed after the implementation of newly proposed solution to resolve the



Graph 1 Throughput analysis of network in office hours



Graph 2 Delay analysis of network in office hours

issues of delayed instable network behavior. It was observed that 26% improvement is observed in the delay observed in previous situations. It was observed that the graph seems to be stable in comparison with earlier situation where the behavior was unpredictable and unstable. This small recommendation can make a remarkable performance boost in the network performance which was the aim of researchers and was achieved successfully.

6 Conclusion

The research project successfully reduced the congestion, increased the reliability over the network's behavior, enhanced the security, and improved sluggish behavior of the network to a great extend. The objectives indicated in section I have been achieved completely, and company policies have been implemented without addition to the complexity of handling data with minimum redundancy and more than expected performance. We could improve throughput by 31% and end-to-end delay by 26% which is a notable improvement in the performance of the network. The biggest advantage of this project is everything defined in the objectives have been achieved within the grant allocated to the project. Even, prospective customers and supplementary users have already been well thought-out at the time of design of the system which was major reason for the selection of L3 switches instead of routers.

7 Future Scope

In the assignment of research task, it was not clearly defined the number of staffs and users of the system in Marketing Department that are to be given access from office and remotely too which can be developed in future.

References

1. Cisco.: Configuring RADIUS and TACACS + Servers (Chapter 13). Available: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-4_10b_JA/configuration/guide/scg12410b/scg12410b-chap13-radius-tacacs.html. Last accessed 20th Oct 2014 (August 2015)
2. Cisco.: Implementation of RADIUS. Available: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html (September 2015)
3. GNS.: Network Simulator GNS3 v2. Available: http://www.gns3.com/. Last accessed 20th Oct 2014 (2014)
4. Cisco.: EIGRP Commands. Available: http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfeigrp.html. Last accessed 20th Oct 2014 (June 2015)
5. Cisco.: Cisco Nexus 5000 Series NX-OS Software Configuration Guide. Available: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/CLIConfigurationGuide/sm_syslog.html. Last accessed 20th Oct 2014 (Last updated: January 2012)
6. Hucaby, D.: Designing campus network. In: Keith Cline CCNP Switch 642-813, pp. 100–280. Cisco Press, Indianapolis, USA (February 2013)
7. Odom, W.: Path control. In: Plumbs, M., Swan, J. (eds.) CCNP Route 642-902, pp. 289–387. Cisco Press, Indianapolis, USA (January 2010)

High-Speed TCP Session Tracking Using Multiprocessor Environments

B.S. Bindhumadhava, Kanchan Bokil, Sankalp Bagaria and Praveen D. Ampatt

Abstract While protecting a target network for detecting a potential network attack, based on attack signature scanning methodology, stateful inspection plays a vital role to detect protocol-based scanning of sessions thus reducing false positives. We propose an architecture which comprises of session table management scheme to perform stateful packet inspection in real-time network scenarios. The architecture uses efficient data structure to store session information and a methodology to retrieve and modify the protocol state information. The state table also considers flow-based information for more accurately extracting attack signature parameters and thus enhancing accuracy of signature-based detection. A parallel thread for scanning the session table and for dealing with expired sessions is also incorporated to avoid memory overflow scenarios and supports higher number of valid sessions in real-time networks. A methodology to communicate with deep packet inspection engine and terminate those TCP sessions for which attack is detected which is incorporated using multithreading approach. We demonstrate two major architectures to enhance the performance of DPI with stateful inspection enabled in it using multi-processing techniques to achieve parallel processing and the experimental results.

Keywords Intrusion prevention systems · Stateful inspection · TCP state tracking · Session management · Multiprocessor environments

B.S. Bindhumadhava (✉) · K. Bokil · S. Bagaria · P.D. Ampatt
CNIE, Centre for Development of Advanced Computing, Bangalore, India
e-mail: Bindhu@cdac.in

K. Bokil
e-mail: kanchan@cdac.in

S. Bagaria
e-mail: sankalp@cdac.in

P.D. Ampatt
e-mail: apraveen@cdac.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_45

1 Introduction

An intrusion prevention system is a network security device which monitors a network for detecting and/or blocking any malicious activity occurring on the target network. The malicious activity can be infectious malware, computer virus, worm which actively transmits itself over the target network to infect other computers. There can be malicious and harmful programs like Trojan horses and backdoors which can cause loss of data, theft of sensitive data, system harm, data corruption, electronic money theft and misuse of the target system.

IPS Fig. 1 sits in the periphery of the network to be protected. It can work in various attack detection models two of which are well-known methods naming signature-based detection and statistical anomaly based detection.

There are predetermined attack patterns known as attack signatures. Signature-based IPS scans and compares the live network traffic against these known attack patterns. Once the signature-based IPS receives a network packet, it first decodes the packet as per standard TCP IP protocol stack RFC specifications and passes the decoded packet information for further inspection of packets.

Considering SNORT [1] (well known, comprehensive attack signature database, developed by Sourcefire) as a reference signature database, following is an example attack signature

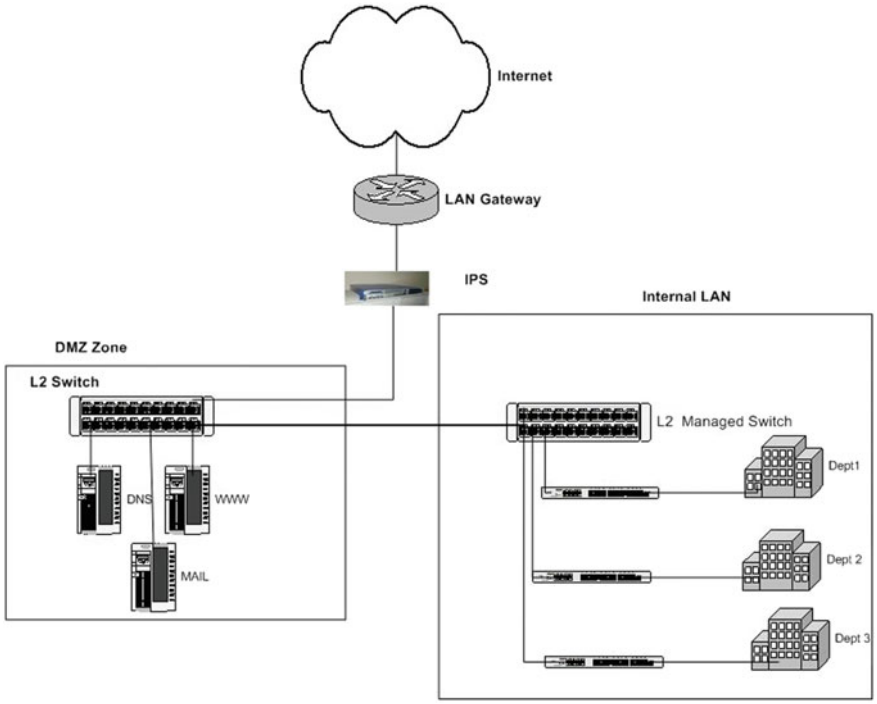


Fig. 1 IPS deployment diagram

alert tcp $EXTERNAL_NET ANY -> $HTTP_SERVERS $HTTP_PORTS (msg : "WEB - CGI FINGER ACCESS"; flow : to_server, established; uricontent :"/finger"; nocase; reference : arachnids , 221; classtype : attempted-recon; sid:839; rev:7;).

The signature says that an alert has to be generated for a packet if it is a TCP segment packet with packet flow from external network IP address to any IP address of predefined group of "HTTP SERVERS" IP addresses, from any TCP port number to any port of a predefined group of "HTTP PORTS" port numbers, with TCP flow from TCP client to TCP server, if the TCP connection is established and the current packet is part of established TCP connection transacted payload data, if the uri content of HTTP is "/finger", which is not case sensitive content, with signature ID 839.

Considering the part of above signature-flow—to the server over an established connection, it is necessary to keep track of the state of network connection (like TCP stream and even UDP communication) [2]. It is necessary to identify legitimate packets for different types of connections. Only those packets matching a known active connection have to be analysed for such signatures while other has to be separated for not matching for these particular signatures.

This is called as "stateful inspection" of network traffic [3] and is different from stateless detection in the sense that no memory of previous packets is maintained in later one, which can make the network to be protected vulnerable to spoofing attacks. This makes it imperative to know whether the current packet is part of a valid active established connection or part of new connection establishment process or an invalid packet vaguely claiming to be part of existing connection.

Our work talks about a method comprising of architecture and data flow of packets for maintaining the TCP connection states for existing valid active TCP connections and any new valid connections getting processed. We also maintain the flow information to know whether the current packet is generated from server or from client. We then present different architectures for multi-core implementation [4] of the IPS engine with stateful inspection capability integrated [5]. We demonstrate our work with test results performed for different packet sizes at specific packet rates [6] and present performance statistics.

2 Related Work

Previous works related to TCP state management schemes [5, 7] and packet processing engines [8] including stateful inspection have addressed storage of TCP connection state information such as TCP state, packet flow direction information, TCP flags information, TCP connection termination, classifying signatures valid for current TCP state and packet processing for appropriate content matching. IPS architecture using GPGPU [9] have various packet processing engines running code for extracting TCP information through incoming packets and storing the data in a single memory layout, various engines sharing common TCP state table. IPS

architecture using network processors [10] have TCP offload engines which store TCP state information and work on packets offline by extracting TCP-related information and performing packet processing. The related work is observed to have memory overflow because of not inspecting invalid TCP connections and erase the timed out TCP connections and terminating the sessions for which attack is detected. With multiple packet processing engines running at high performance have been slowing down [11] because of sharing of large memory layouts for accessing TCP state table thus tampering the performances.

3 Proposed System Architecture

The system architecture Fig. 2 comprises of multi-core approach [4] in which each core runs an application for TCP connection management and deep packet inspection in co-ordination with TCP processing engine. As described in the diagram above, considering scalability compatibility, in the four-core machine, there are packet processing engines PE1, PE2, PE3 and PE "N", where the solution is scalable and expandable meeting current network speeds and operational functionalities. The load balancing application distributes [12] incoming network traffic equally within multiple queues pertaining to each core, and it is made sure that traffic pertaining to single TCP connection enters single queue thus allowing discrete TCP connection tables for respective engines. Multiple threads within an application in a core allow scanning the packet for TCP information, updating the TCP connection table, scanning packet for any potential attack signatures, performing complete signature match only for shortlisted signature IDs for a particular TCP session packets, scanning the TCP table for timeout TCP sessions, terminating invalid connections for timeout sessions as well as part of prevention of attack to save the victim from harmful network attacks [13, 14].

3.1 Maintaining Connection Records and Packet Flow

The packets are received to the system from a load balancer which distributes the traffic according to number of processing cores available [15]. Each processing core runs the connection management and deep packet inspection application individually. Each processing core is accompanied with a packet capturing queue [16]. It is made sure by the load balancer that traffic pertaining to single TCP connection enters a single queue corresponding to a processor core. Once a packet is received by a core, it is decoded further for the protocol field [17]. If it is a packet pertaining to a TCP connection, first the four tuple values are considered for operation—named source IP, destination IP, source port, destination port. As demonstrated in Fig. 3, the hash value is calculated based on the 4 tuples. The information about the

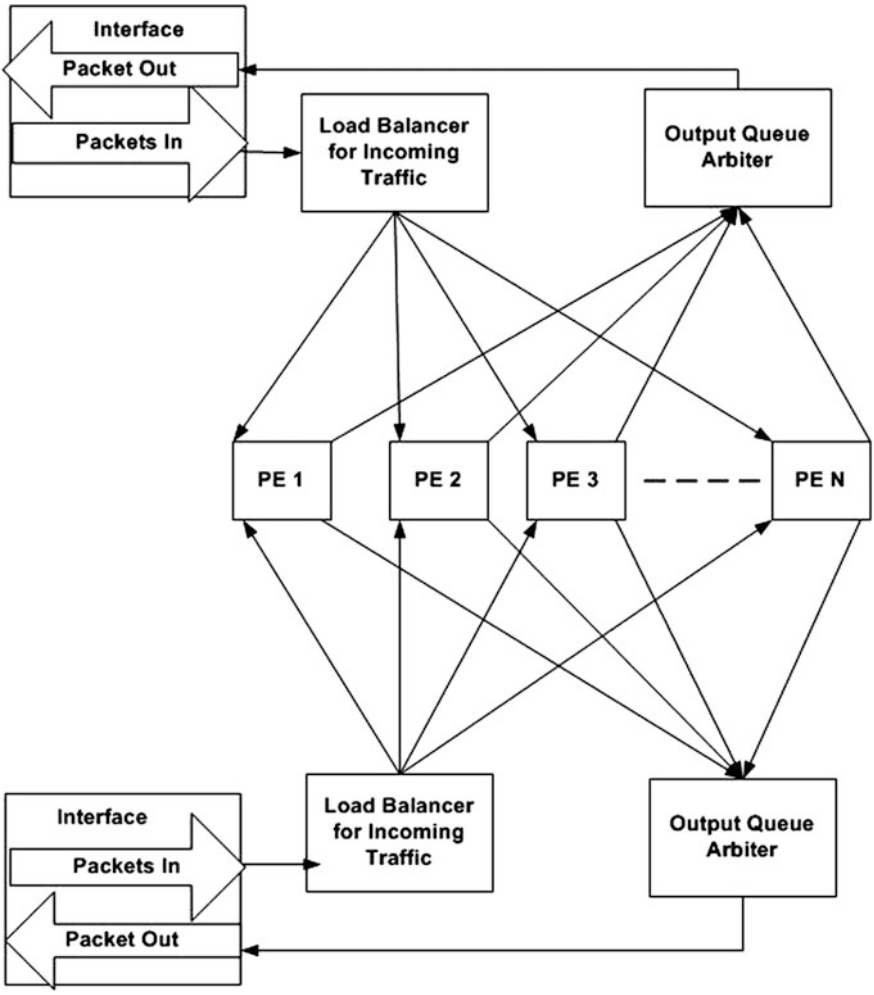


Fig. 2 System architecture with multi-core approach

incoming packet (tuple values) are stored in the data structure along with hash key (needed for collision resolution) and protocol state.

According to the TCP protocol standard, the connection state for incoming TCP session is calculated by the system and stored in the same data structure element [18, 19]. Flow information such as flow from server/client to server/client is also stored per flow. The packet is then passed to deep packet inspection (DPI) engine where it is scanned against a set of attack signatures [20]. As required by DPI engine, TCP session information such as state of connection (SYN received/connection established/connection terminated), flag present in current packet (ACK), flow information (from client/from Server) is retrieved from connection management database and passed to DPI [5, 7]. Based on this information, attack signatures valid for current packet

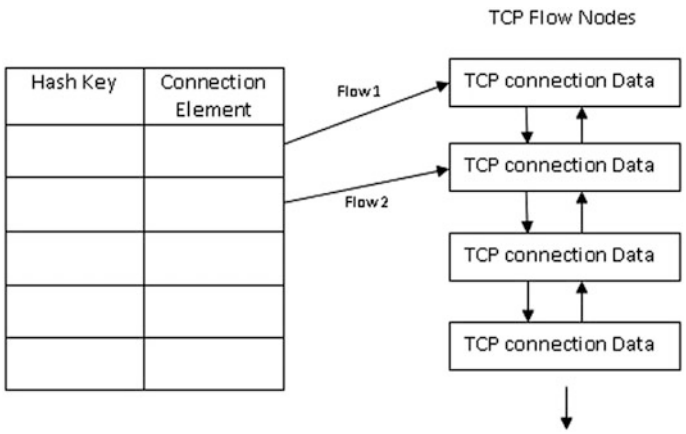


Fig. 3 Connection table

and for current session are identified and then taken into consideration for performing matching operation. Upon reception of packets pertaining to existing connections, the connection management database is updated according to IEEE TCP protocol standards. If the connection is terminated in valid standard, the entry is removed from database. A parallel thread runs through the database, to identify such connections which cross TCP timeout specified by standards and are terminated. Such connections for which packets are found to be malicious by DPI are also terminated and logged in attack database.

3.2 Data Flow

Figure 4 indicates data flow within a processing element which mainly comprises of two components—deep packet inspection and TCP connection management.

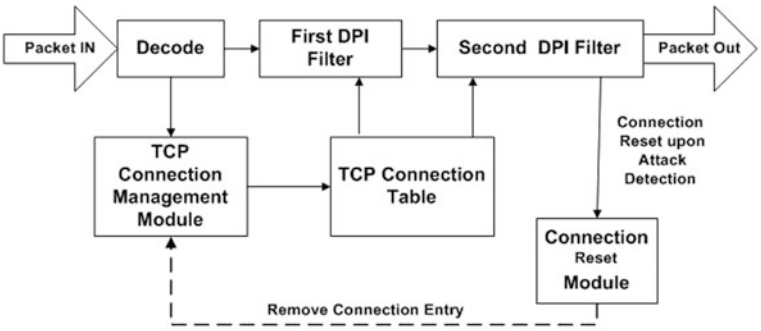


Fig. 4 Processing element

Upon reception of a packet, decode block decodes the packet for inspection of specific protocols against protocols specified in attack signatures to be matched for. Attack signatures are matched against incoming packet in two major steps where potential signature IDs are generated in first filter by partially matching the attack signatures, and all those potential signatures are matched completely in second filter. Deep packet inspection module consists of filters which analyse the packet for various aspects covering attack signatures like content part, keywords, case sensitivity, port number ranges and IP address ranges. The decoded packet is also sent to TCP connection management module where it follows path to update TCP connection table for maintaining connection records as explained before.

DPI filters query TCP connection table for particular connection tuple, and API is developed for the same. Upon performing signature detection, if attack is detected for whom an action of DROP has to be performed, the respective packet is dropped and the information is logged into a log file. In addition to this, if this packet is part of an existing TCP connection, a TCP reset packet is sent to both the TCP ends and the concerned entry is deleted from TCP connection table. All clean packets are sent to another interface with TCP connection entries maintained in the connection table.

4 Parallelism

Two main approaches for achieving parallelism in packet processing were explored.

1. Passing all incoming packet data to the available processing engines which run the DPI and connection management applications. As demonstrated in Fig. 5, the available signature set is divided into chunks of signature subsets according

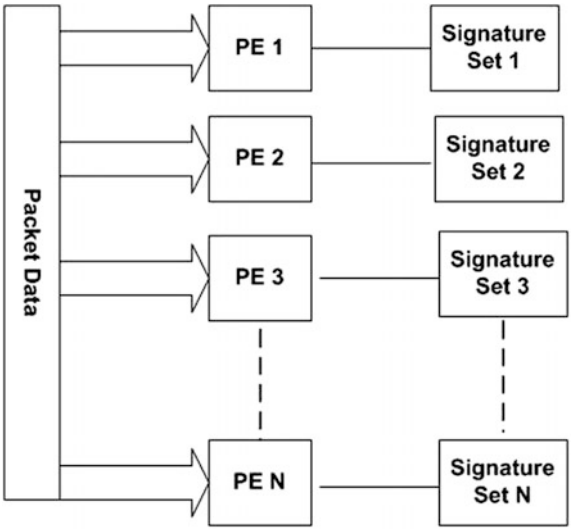


Fig. 5 Distribution of all traffic to all processing engines with division of signature sets

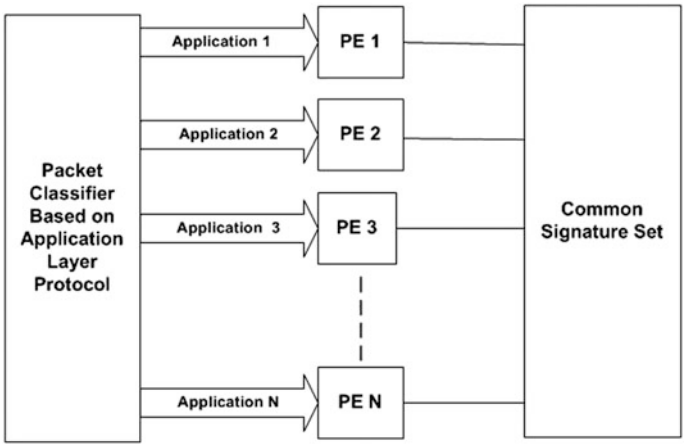


Fig. 6 Common signature set with packet classification

to protocol specified in the attack signatures. Each processing engine is dedicated to specific protocol and handles signature subset pertaining to that protocol.

2. Entire signature set is shared between all processing engines, refer Fig. 6, perform DPI and connection management. But incoming packets are classified according to application layer protocols and passed to appropriate processing engine.

5 Experimental Results

Various test cases were formed to test the false positive responses of deep packet inspection engine alone, without incorporating the stateful inspection. The same test cases were performed for comparison with integrated TCP stateful inspection engine.

The test cases included varied percentage of malicious traffic from 0 to 100%. The tests were performed on Spirent packet generation equipment for packet rates up to 1 Gbps. ThreatEx add-on software was used to generate the malicious traffic of desired percentage in the generated traffic.

Percentage False Positives

The test cases included generation of malicious traffic from 0 to 100%, refer to Fig. 7. The tests were performed on single processing engine with packet rates of 1 Gbps and packet size of 1514 bytes. The false positive performance was improved from DPI alone to DPI integrated with stateful inspection engine as we can see in Fig. 7.

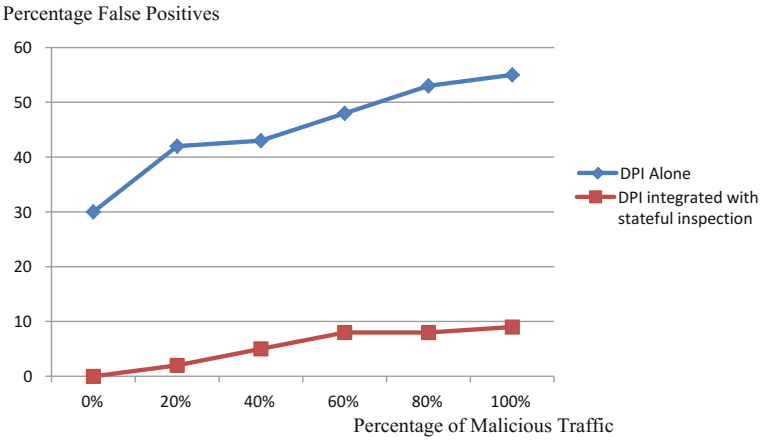


Fig. 7 Graph for percentage of false positives

Further, experiments were performed for multi-processing engines running instances of DPI with stateful inspection capability.

Figure 8 gives glimpse of test cases performed for packet rates up to 10 Gbps with packet size of 1514 bytes and increase in number of processing engines. Each engine ran an instance of DPI, with stateful inspection, individually with a common signature set shared between them. The packets were classified according to application layer protocol with all the packets pertaining to single connection entering single queue associated with each engine, as demonstrated in Fig. 6.

It was observed that performance decreased when TCP connection management database was shared among all processing engines, whereas each processing engine accompanying its own TCP connection database boosts up the traffic speeds it can handle. It was also observed boost in performance as a number of processing engines were increased from two to four. Considering that there is limitation on number of engines supported in a machine and the operating system for

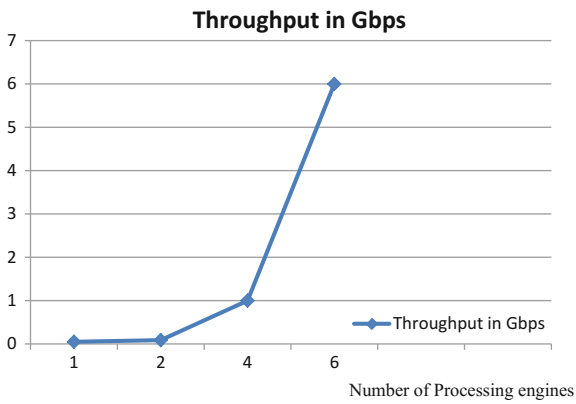


Fig. 8 Graph for throughput performance with increase in number of processing engines

management of engines, we could perform testing on packet speeds of about 6 Gbps successful packet processing speed on an interface of 10 Gbps with six engines processing in parallel.

6 Conclusion and Future Work

With high contemporary network speeds, it is necessary to support high-performance network devices for applications such as application switches, intrusion prevention systems, routing and security applications. Managing TCP connection information plays important role to handle TCP sessions as whole for stateful handling of data traffic. It is further extended for TCP reassembly and handling the TCP segments for these applications. Parallelism plays important role in building high-speed networking applications. It is thus necessary to identify components within the target application, which can be performed in parallel. By integrating the sequential components and parallel components into appropriate processing engines and data flow, it is possible to design scalable solutions to achieve higher performances meeting contemporary requirement of network processing power as well as higher speeds with accurate results. GPGPU (general purpose graphics processing units) is an extension to multi-processing approach to achieve this processing power as well as high-speed performances. Experiments are getting carried out to further incorporate parallelism by effective use of GPGPU architecture and enhancing the functionalities of existing solution towards more secure and robust intrusion prevention mechanism.

References

1. Snort—The Open Source Network Intrusion Detection System. http://www.snort.org
2. Necker, M., Contis, D., Schimmel, D.: TCP stream reassembly and state tracking in hardware. In: Proceedings of the 10th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (2002)
3. Attig, M., Lockwood, J.W.: SIFT: SNORT intrusion filter for TCP. In: 13th Annual Proceedings of Hot Interconnects (2005)
4. Wan, Z,. Liang, G., Li, T.: Multi-core processors based network intrusion detection method. J. Netw. **7**(9) (2012)
5. Dharmapurikar, S.: Robust TCP stream reassembly in the presence of adversaries. In: 14th USENIX Security Symposium (2005)
6. Deri, L.: Wire speed packet capture and transmission. In: E2EMON (2005)
7. Agarwal, P.: TCP Stream Reassembly and Web Based GUI for Sachet IDS, thesis, IIT Kanpur, Feb 2007
8. Houghton, N.: Single Threaded Data Processing Pipelines and Intel Architectures. VRT, Vulnerability Research Team (2010)
9. Jamshed, M.A., Lee, J., Moon, S., Yun, I., Kim, D., Lee, S., Yi, Y., Park, K.: Kargus: a highly scalable software based intrusion detection system. In: Conference on Computer and Communications Security (2012)

10. Vallentin, M., Sommer, R., Lee, J., Leres, C., Paxson, V., Tierney, B.: The NIDS cluster: scalable, stateful network intrusion detection on commodity hardware. In: Recent Advances on Intrusion Detection, pp. 107–126. Springer (2007)
11. Day, D.J., Burns, B.M.: A performance analysis of SNORT and suricata network intrusion detection and prevention engines. In: ICDS 2011 Fifth International Conference on Digital Society (2011)
12. Song, H., Lockwood, J.W.: Efficient packet classification for network intrusion detection using FPGA. In: International Symposium on Field Programmable Gate Arrays (2005)
13. Novak, J., Sturges, S.: Target Based TCP Stream Reassembly. Sourcefire, Aug 2007
14. TCP Congestion Control. RFC 2581, IETF, Apr 1999
15. Cabera, J.B.D., Gosar, J., Mehra, R.K.: On the statistical distribution of processing times in network intrusion detection. In: 43rd IEEE Conference on Decision and Control, vol. 1, pp. 75–80. IEEE Press (2004)
16. Aho, A., Corasick, M.: Efficient string matching: an aid to bibliographic search. Commun. ACM **18**(6), 333–340 (1975)
17. Bos, H., Huang, K.: Towards software based signature detection for intrusion prevention on the network card. In: Recent Advances in Intrusion Detection, pp. 102–123. Springer (2006)
18. Baboescu, F., Varghese, G.: Scalable Packet Classification. ACM Sigcomm (2001)
19. Alserhani, F., Akhlaq, M., Awan, I.U., Cullen, A.J., Mellor, J., Mirchandani, P.: SNORT Performance Evaluation. Informatics Research Institute (2011)
20. Deri, L., Martinelli, M., Cardigliano, A.: Realtime high speed network traffic monitoring using ntopng. LISA, 70–80 (2014)

Integrated Next-Generation Network Security Model

Rajesh Kumar Meena, Harnidh Kaur, Kirti Sharma, Simran Kaur and Smriti Sharma

Abstract In today's scenario, cyber threats are becoming labyrinth and difficult to manage. The traditional security management systems are not capable to handle upcoming novel threats resulting in performance deterioration. In this paper, various next-generation technologies have been integrated together that provide an efficient, manageable, robust, and flexible system that not only effectively tackles all the existing attacks but can mutate itself to fight against zero-day attacks. The proposed system includes intelligent techniques that are required for the future cyber world like next-generation intrusion prevention system (NGIPS), network breach exposure system (NBES), cloud-based antivirus, anti-spam, personalized censor-ware, SPARTA (access control service), MONICAN (control and management technique). It will result in a reliable, efficient, and quick responsive system to obtain remarkable results in the network security.

Keywords Cavernous packet examination · NBES · APG · PHGE · Bayesian filter · General management

1 Introduction

Network security as a specialized field in computer networking that involves securing a computer network infrastructure [1, 2]. With the increase in dependence on the computer systems, network security is one of the major concerns. Losses of private information and access by unwarranted sources are problems that scrape the

R.K. Meena (✉)
Laser Science and Technology Centre, Defence Research and Development Organisation, Metcalfe House, Delhi, India
e-mail: rkmeena@lastec.drdo.in

H. Kaur · K. Sharma · S. Kaur · S. Sharma
Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India
e-mail: smritisharma111193@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_46

surface only. Despite of the existing technologies, there is no panacea to the network security problem as it is fast transmuting into rampant hazard. Presented integrated security system is another effort to deal with this peril situation [2, 3].

This system is an amalgamation of mechanisms that are not only flexible and robust but also adept enough to tackle any next-generation upcoming threats. This system is highly optimum and is determined to provide best services in securing the network. Its major components are next-generation intrusion prevention system (NGIPS), network breach exposure system (NBES), cloud-based antivirus, anti-spam, personalized censor-ware, SPARTA (access control service), MONICAN (control and management technique) [1–3].

The continuously evolving and increasing intrusion by worms or viruses is leading to a major loss of data. In the present scenario, where major emphasis is being laid on data warehousing and big data, even a slight discrepancy or loss of data can lead to inefficient working. The proposed system is not just a conventional UTM (unified threat management) that simply combines the security system but is responsible for thwarting any attacks by sensing the network itself.

The network CPE-based integrated security system which can effectively cope with the various security threats by indentifying and authenticating seven layers of Internet traffic that can be applied without overloading the network traffic. It can also be regarded as the optimum solution to cope with unknown network-based threats in the future (Fig. 1).

2 Next-Generation Intrusion Prevention System

Intrusion prevention system is a network security technology that inspects the stream of traffic to detect and prevent any malicious activity. It maintains a log about all such activities and attempts to block/prevent it. IPS can take such

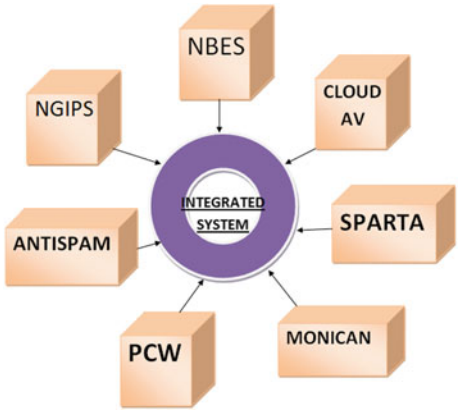


Fig. 1 Components of integrated security system

measures as reporting any intrusion, discarding the malicious packets, and it can even block the offending IP addresses.

Next-Generation Intrusion Prevention System is an unconventional and innovative system that secures the network from emerging threats and risks. NGIPS is built on the top of traditional IPS and has additional capabilities like user awareness and application awareness. These features assist NGIPS to provide fast, reliable, and accurate solutions in an economical manner.

2.1 Need for NGIPS

IPS deals with traditional threats. As new attacks are developed for breaching the safety of the network, it becomes necessary to evolve our security systems in order to cope with and survive such attacks. To enhance the accuracy of responses, we need additional knowledge like behavior of the network, user identity, and the devices connected to the network. This data is easily made available through this improved system.

Moreover, we need to secure the client-side applications in addition to providing safety for server-side applications.

2.2 Characteristics of NGIPS

Examination of encrypted traffic: Security and consistency are prominent concerns for certain industries like finance, banking. As a result, most of the network traffic is coded in a form that cannot be used to provide any information to the hackers. These encrypted packets can sometimes breach the security of the system.

Application knowledge and full stack reflectivity: The NGIPS should have knowledge of all the applications running on the network. It should have full stack visibility which includes not only applications, but also operating systems, versions, devices, networks, and even files. It not only reduces the surface of attack by restricting access to suspicious applications but also imposes certain policies and preserves bandwidth. Moreover, by restraining certain features of operating system, it can improve the productivity, thereby decreasing the extent of network area exposed to risk.

Content awareness: The main objective of any IPS system is the ability to identify and counteract various threats. The threats cannot be only of conventional type but, with emerging technologies, can also be embedded in content such as MS Word, PDF files. The NGIPS system is capable of carving files for analysis out of many protocols, encodings, and several compression methods. The system blocks any file which is found to be suspicious.

Contextual understanding: Context refers to the group of conditions that exist where and when an attack takes place. This context is a significant measure to determine the priority of response. This context can be based upon several factors like

(i) **Network Sense**—The NGIPS system should be fully aware of network including various hosts connected to the network and their conformity with IT policies. If certain devices or applications are currently disconnected on a particular network, then security for such devices can be turned off so as to increase productivity, decrease load, and to avoid unneeded checks.
(ii) **Behavior Sense**—This type of sensing includes determining the amount and type of traffic that should be considered harmless. Thereafter, it is the job of NGIPS to monitor and report any abnormal or unfamiliar traffic. Anomalous network traffic may indicate a threat trying to attack the server so identifying it prevents system breaches and data loss. In addition to this, behavior awareness also monitors amount of data transferring order to identify any decrease in efficiency.
(iii) **Identity Sense**—The NGIPS system must have complete knowledge of the identity of each and every user connected to the network either directly or indirectly. This data is available from both Microsoft Active Directory systems and a variety of open standards-based LDAP directory servers. Using this information, the attackers can be identified easily.

Adaptable engine: NGIPS system has the ability to adapt to the changing needs in order to maintain significance against varying security demands. A key component to make NGIPS system agile is Snort. The NGIPS is adaptable in the following ways:

(i) **Standard Discovery**—In order to save time and effort required to configure the system, following three options are provided:
    (a) *Protection Over Accessibility*—It is the topmost level of security with greatest number of validations enabled. It is used when network security is preferable relative to user's convenience.
    (b) *Accessibility Over Protection*—It is the least restrictive security level and is used when access to network resources is at highest priority.
    (c) *Balanced Protection and Security*—It provides optimal solution to organizations with typical security needs.

(ii) **Custom Modifications**—In addition to the above mentioned basic policies, NGIPS provides users with the option to customize the detection rules and set various other policies to accommodate their requirements.

3 Network Breach Exposure System

Network breach exposure system (NBES) monitors the traffic crossing the network and detect the intrusion which after being compared with the previously known set of malicious activities. Network security aims to protect the system from unauthorized insecure activities. Intrusion detection senses the unusual activity and alerts the administrator. Generally, inbuilt firewalls are not enough to provide security to a network completely because the attacks committed from outside are stopped, whereas inside attacks are not. It causes breach detection systems to become active. BES helps a system to stop attacks and recover from them with the minimum loss. It analyzes the security problems so that they are not repeated. Cavernous packet examination (CPE) is a very common method of network breach exposure system. Signature-based network breach exposure system (NBES) requires to match a predefined pattern that is already identified as harmful to the network. NBES should have the feature of dynamic reprogramming, fault tolerant, susceptible to attacks, easy to install, and should detect different types of attacks. There are two types of intrusion detection system:

(i) **Exploitation Detection**—Exploitation-based Breach exposure system (BES) aims to distinguish events that violate system protocols. It can only detect known attacks.
(ii) **Glitch Detection**—Glitch-based BESs try to analyze abnormal activities and flag these activities as attacks. It can also detect new attacks.

Exploitation detection have very low false positive rate. Since they depend on comparing the incoming traffic with known strings, they are unable to identify novel attacks. Hence, a high false negative rate is observed.

To detect intrusions, there are two techniques namely hybrid NBES and Honeypots. Snort is the chosen system as exploitation-based BES while packet header glitch exposure (PHGE) and network traffic glitch exposure (NETGE) are chosen as glitch-based BES. Glitch detection-based breach exposure systems are divided into many sub-categories that are statistical methodologies, data mining, genetic algorithms, and immune systems, etc. Among these sub-categories, statistical methods are the most commonly used ones in order to detect breaches by analyzing strange activities occurring in the network. PHGE and NETGE statistical methods are chosen as the glitch-based breach exposure systems in this paper. We have implemented a hybrid BES by mounting glitch-based BESs, PHGE and NETGE to Snort as a preprocessor. PHGE models protocols. Also, it takes care of dynamic reprogramming of network. PHGE tags only the first anomaly it detected as an alert even if there is a series of the same glitch recurring. This feature reduces the number of fake alerts. NETGE, models single packets like PHGE, uses dynamic-conditioned protocols and models values that are known (Fig. 2).

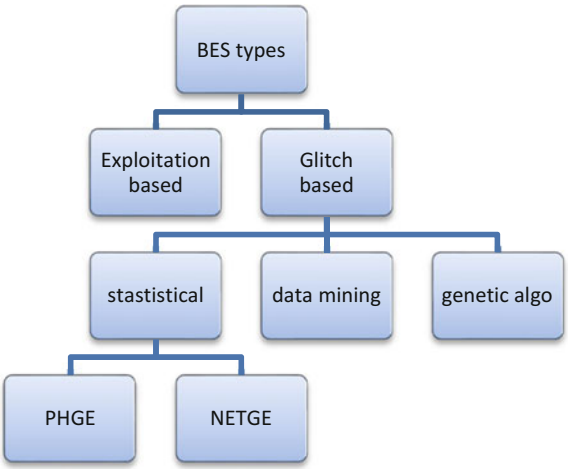


Fig. 2 Hierarchy of BES

Snort is an open source and rule-based network breach exposure system. Snort combines new functionalities during compilation. Snort is a network breach exposure system. It runs over IP networks and analyzes real-time traffic for detection of misuses.

(A) **Approach**

(i) *Using PHGE and NETGE*

PHGE calculates glitch scores for every packet and makes no difference between incoming and outgoing traffic. Network traffic glitch exposure (NETGE) is the second glitch-based approach added to Snort as a preprocessor in this paper. NETGE models packets, and it operates in two stages: The first stage is the filtering of incoming packets. The second stage is the modeling stage. Filtering stage eliminates the traffic up to 98–99%. This exclusion simplifies the traffic for the next modeling stage. Only the traffic data, which provide indication of attacks, is passed to the modeling stage. After surveying many papers and techniques, we have concluded that final system is called the hybrid BES (Snort + PHGE + NETGE), and it is tested on a dataset containing approximately 200 attacks. It is observed that number of attacks detected increases much more with the hybrid BES. Snort is able to detect $\sim$25 attacks. After PHGE is added as a preprocessor, this number increases to 50, and finally after NETGE, the number of attacks detected increases up to 140. As a result, the hybrid BES is said to be more powerful than the signature-based because it uses the advantages of glitch-based approach for detecting unknown attacks.

(ii) *Using Honeypots*

Another technique to detect intrusions is called Honeypots. Honeypots are incorporated in network with firewall and breach exposure systems to provide concrete secure platform to an organization. The disadvantage of above discussed system is

that it detects those malicious activities that are blocked by firewall and may also generate large number of false positives. Honeypots then introduced in the network to utilize the network's unused IPs, and the attacker's behavior is analyzed on these Honeypots. Honeypots improve BES too by decreasing the numbers of false positives and accurate. Honeypots is an individual security resource that provides features such as early warning system, and capturing novel exploits to gathering intelligence on rising threats. There are two types of Honeypots: First is research Honeypots, and other one is production Honeypots. Research Honeypots are basically used to achieve information about the new ways of attacks, viruses, worms which are not detected by BES. These Honeypots are used for research purposes. Its primary function is to trace the path of attacker and gain knowledge about the new ways of attacks performed threats. Production Honeypots are easy to organize and are primarily used by companies or corporations. These Honeypots are assembled with server inside the network of the organization to improve overall security. It provides instant security to production resources. Honeypots assume that the traffic sent is unauthorized that means there is no false positives and no false negatives. One more advantage of using Honeypots is that it can work in any IP environment including IPv6. IPv6 is the new version of IPv4 (Fig. 3).

Nowadays, the demand for a secure network is increasing. Network security can be maintained by making use of various authentication techniques. One crucial challenge with computer and network security is the determination of the difference between normal and unsafe activity. The ultimate design goal for a breach exposure system is the development of automated and adaptive design tool for network security. Honeypots is an exhilarating new technology with huge prospective for security communities.

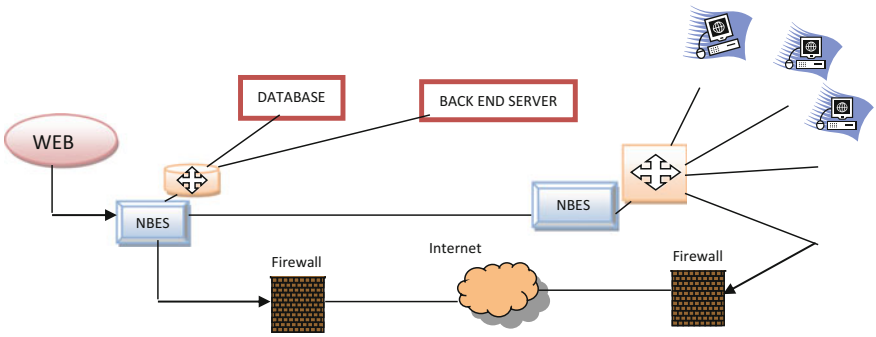


Fig. 3 NBES in internal mode deployment

4 Cloud Antivirus

Antivirus software is one of the most widely used tools which detects and protects our workstation from the infected and unwanted files. It is installed on almost every computer or workstation in the organizations or home users across the world. However, the traditional host-based antivirus is ineffective against zero-day attacks or next-generation malware. Therefore, the malware detection capabilities are shifted to the cloud by implementing the antivirus as an in-cloud network service, extolling the speed of cloud computing to deliver real-time protection. Since most of the analyzing capabilities have been shifted to the cloud computing, it does not impact on the system's performance and resources compared to the host-based antivirus.

(A) **Host-Based Antivirus Software**

Traditional antivirus software relies upon signatures to identify malwares. When a malware arrives, it is scrutinized by the dynamic analysis system. Proper signatures of the malware are extracted from the file and added in the signatures database of the antivirus [4]. When a particular file has to be scanned, it is matched with the signatures stored in the database, and if it matches the signature, then the antivirus knows which malware it is and takes the appropriate procedure against it.

However, this approach is not effective against new malwares, which are not yet analyzed, due to two reasons. First, many of the malwares remain undetected by the antivirus. There is a considerable chance of susceptibility between when the threat is discovered and when the malware researchers generate the signature and update the software to detect it. Second, the malwares exploit the vulnerabilities of the ever-increasing complexity of the antivirus software.

(B) **Antivirus as an In-Cloud Network Service**

Cloud antivirus is a technology that deploys lightweight software on workstations, while performing the majority of data analysis on the provider's cloud infrastructure [5]. One of the benefits of offloading analysis to the cloud is that the decision engine's logic is not directly accessible by the attackers. Oberheide [6] proposed in his thesis "N-Version Antivirus in the Network Cloud" a new model for detection functionality currently performed by antivirus. The key changes are as follows:

(i) **Malware Analysis by Cloud Engine**—Instead of performing the complicated analysis on each and every end-host, the lightweight software captures the significant information about the files and provides them to the analysis engine. The report returned by the cloud engine determines whether to permit/deny access to the file [7].
(ii) **Multiple Scanning Engines**—The analysis should be performed by deploying multiple, heterogeneous detection engines in parallel for detecting malicious and unwanted files (Fig. 4).

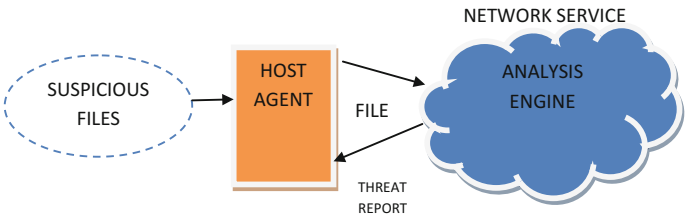


Fig. 4 Flow of process for cloud AV

(C) Approach

In this, we use cloud as software as a service (SaaS), where users are provided access to application software and databases, referred to as on-demand software. We combine the traditional signature-based detection technique with dynamic detection method based on heuristics and behavior.

(i) Optimized Signature-Based Matching

This method depends on the signature database and string matching algorithm (for similar DNA sequences) to find variants of virus efficiently. Based on the self-replicating characteristic of the virus, many replicas of the virus coexist in the system. Viruses scan the files and target them by inserting the malicious code in them. When a virus is found, its signature is stored temporarily in the cache so that the replicas need not be matched with huge amount of signatures in database. So, signature matching time is greatly reduced.

(ii) Dynamic Analysis Using Heuristic and Behavioral Methods

This method analyses the suspicious file's characteristics and behavior to declare it affected. Heuristic analyzer looks for suspicious commands indicative of a class or family of viruses. If a file contains matching code patterns, then it is declared as infected. For depth analysis, behavioral analyzers can also be used. Behavioral analyzers execute the suspicious file or program in a virtual environment logging what actions it performs. Depending on the actions, analyzer declares the file infected (Fig. 5).

The report is then submitted to the user for him to take necessary actions if the file is infected. We combined the optimized signature-based matching and heuristic technique to detect known as well as unknown viruses. This approach provides 35% better detection against recent threats compared to a single antivirus engine and a 98% detection rate across the cloud environment.

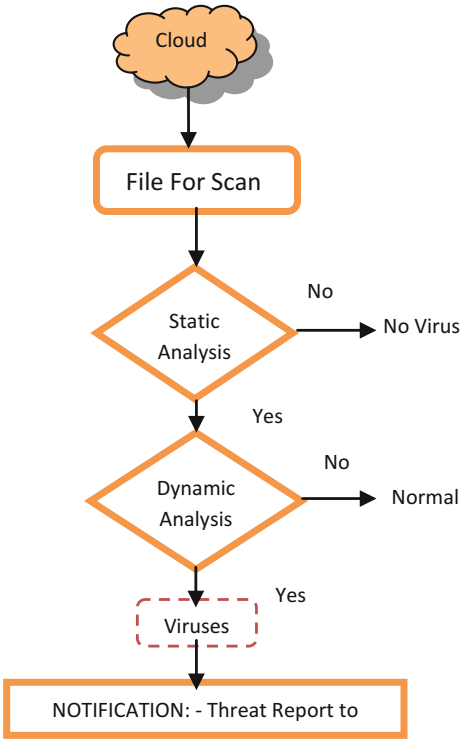


Fig. 5 Flowchart for malware detection

5 Anti-spam

'Spam' is defined as flooding the Internet with multiple copies of a single message in order to impose the message on people who would not otherwise choose to receive it. They are mainly used for commercial advertising, often for dubious products. Sometimes, clicking on links in spam e-mail may send users to phishing Web sites or sites that are hosting malware.

There are two main types of spams—Usenet spam and e-mail spam. Cancellable Usenet spam is a single message sent to 20 or more newsgroups. These types of spam generally deprive the users from useful content by overwhelming them with a stream of advertising posts. e-mail spam targets individual users with direct mail messages

Spam detection techniques can be broadly classified into (1) Based on machine learning (2) Not based on machine learning. Machine learning is a technique that discovers and studies the algorithms that can draw inference from and make predictions on data (Fig. 6).

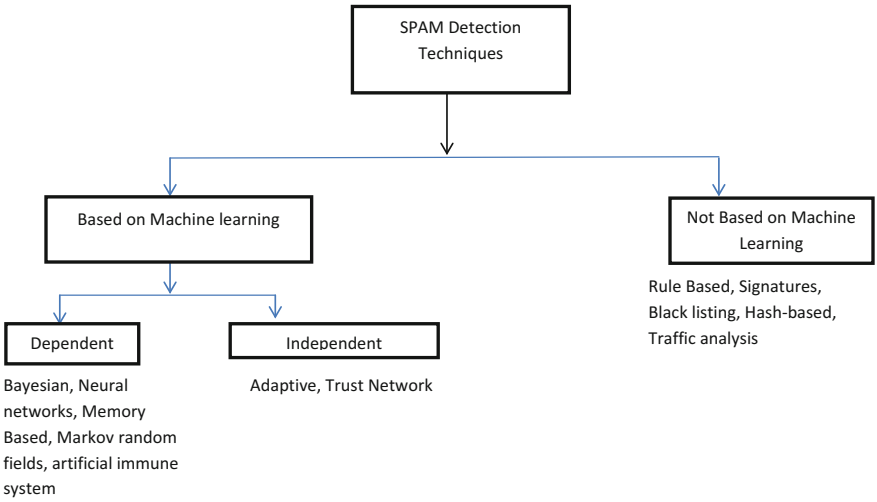


Fig. 6 Types of spam detection techniques

Dependent solutions mainly constitute a part of a bigger spam detection solution (which can be either based on machine learning or not). They act as a secondary system. Independent solutions mainly construct their own database according to which they differentiate the mails and messages.

Some of the commonly used spam detection techniques are as follows:

(i) **Rule-Based Analysis**—It is a quick and simple technique that uses certain predefined rules to find expressions that are similar across spams. But relative to new detection techniques, this method has certain drawbacks. The rule set is fixed. So if a new threat arrives, then the system must be updated to recognize that mail as a spam. If the spam arrives before this updating, then the system fails to achieve its objective.

(ii) **Signatures**—For each identified spam, they generate a distinctive symbol or a value called signature. When a mail arrives, the system compares its signature with the values stored in its database. If an equivalent value is found, the mail is categorized as spam. It generates quite a low level of false positives. But the major limitation is that if a spam is received before its signature has been disseminated, then this method fails to detect it. Moreover, for efficient maintenance of the database, the older signatures are removed, thereby providing the attackers an opportunity to attack.

(A) An Efficient Approach

Bayesian filtering is an effective and a widely used technology for spam detection. It is a popular statistical technique of e-mail filtering. It overcomes most of the limitations of previously known techniques.

Depending upon the types of mails received and user's choice, a rule set is constructed. The sender is unfamiliar to this rule set. The rule set is modifiable and is adaptive to the user's choices.

Two tables are maintained in Bayesian filters—the first one is of spurious or illegitimate tokens, and the second one is of legitimate tokens. A probability value is bound to every spam with the help of which the system categorizes a mail as a spam. Similarly, probabilities are maintained for each spam. The initial values for the classifier are provided, and with each mail that is correctly identified, the values are modified accordingly. On receiving a new mail, it is converted into a set of tokens, and then the probability value corresponding to each token is fetched from the user's records.

All these probability values are then combined, using Bayes' rule to produce a final probability. The involvement of user's feedback improves the accuracy of this filter.

The performance of this filter is more effective at the user level as compared to the mail server level. As each user will differently consider some mails as spam, therefore, a database constructed from user's data will provide more accurate results.

The probability that the received mail is a spam is given by (P):

$$P = \frac{x1 \cdot x2 \cdots xn}{x1 \cdot x2 \cdots xn + (1 - x1) \cdot (1 - x2) \cdots (1 - xn)} \tag{1}$$

where x_i is the probability of a word that was included in previous mails that were classified as spam.

6 Personalized Content Filtering

Censor-ware is used by corporations as part of Internet firewall computers to restrict or control the content which a user is authorized to view on the Internet via the Web, e-mail, or other means. Censor-ware blocks the unwanted content of the Web page or e-mail. As the diverse information on the Internet is available to all the users, the need for content filtering is impeccable. Content filtering ensures security, prevents legal trouble, and improves user productivity.

The simple and easy method is to block Web page based on URL filtering and IP addresses. However, it is not efficient for unknown Websites, and it is difficult to obtain the complete block list. Given that the Internet consist of tens of billions of Web pages with millions added per day, this approach is ineffective at providing protection from objectionable content [8]. Also, the traditional content filtering tools block the entire Web page found objectionable. Instead of completely blocking a page, it is efficient to block only those segments which contain objectionable content since different portions of the Web page holds different contents.

This method provides fine-grained blocking and automatic identification of the segments of the Web page to be blocked.

The objective of the content filtering is to propose a model for Web page segmentation and incorporating personalization to enhance the capabilities of the content filtering process. The model incorporates two methods:

(i) **The Web Page Content Filtering**—There exist many approaches for Web page content filtering such as rating systems [9], text classification-based approach [10, 11]. The approach used in our model is keyword-based blocking method.
(ii) **The Web Page Segmentation**—Web page segmentation is the process of dividing the Web page into segments based on certain criteria. DOM-based Web page segmentation approach is used, in which HTML tag tree's Document Object Model will be used for segmenting.

The model has three main components:

(i) **Segmentor**—This component is responsible for segmenting the Web pages into logically smaller segments.
(ii) **Personalizer**—This component is used for incorporating personalization while filtering content. It consults a list of permitted and denied keywords.
(iii) **Filter**—This component filters the segments which contain objectionable content (Fig. 7).

In this approach, each page which the user requests is segmented into smaller units for the filtration. This is achieved by the segmentor component. The source page is mapped as a DOM tree. After performing the segmentation, each segment is processed individually by the filter component. Each segment contains three components:

Fig. 7 Model of personalized censor-ware

(i) Text
(ii) Link
(iii) Image

Each segment is individually scrutinized for the three components whether they contain objectionable content which needs to be blocked. The model incorporates the personalization aspect. The user can configure according to his requirements. For personalization, the model consults a bag comprising allowed and denied list of keywords. The keywords in the allowed list give a positive value while keywords in denied list give negative value. If the cumulative value of the individual segment exceeds a threshold value, that segment is displayed, else blocked. If the segment is blocked, message "segment blocked" will be displayed.

This model has 88% accuracy in filtering out the segments containing objectionable content [12].

7 SPARTA

The new research in the field of network security and Internet has not only lead to the development of some path breaking technologies, but also has created some difficult to handle and predict attacks and viruses. These new threats lead to sensitive information being coerced or its loss. In such a case, mechanisms to both protect and prevent any such attacks are essential. In order to achieve prevention, we use Network access control.

Network access control (NAC) can be defined as the scheme of enhancing and upholding the network security by limiting the access to resources of the network and enforcing some protocols. A traditional network access control device puts constraints to the amount of data any user can access, due to the implementation of anti-threat applications. The available network access control devices are not equipped enough to handle the avant-garde attacks and are not flexible enough of incorporate the changes brought about by the perpetual research, making them a transient.

The proposed system "SPRATA" [13] is a step toward integrating the various security products that were earlier deemed as incompatible and provide an end to end protection to the host. Its assessment is not limited to the users but extends to the nodal hosts, while ensuring the veracity of those nodes. SPARTA has an open architecture giving it that much needed edge over the present technologies. SPARTA's architecture is composed of two entities: Entrée Retriever (ER) and Access Protocol Governor (APG). However, three entities—protocol point (PP), perilogos reclamation point (PRP), and Synaptic Managers and Controllers are supplements that can be augmented according to network needs [14–17]. It needs to be noted that this technology is only being suggested to aggrandize the access control mechanisms in the threat management technology already present in the host and acts a veneer to the capabilities of the used technology (Fig. 8).

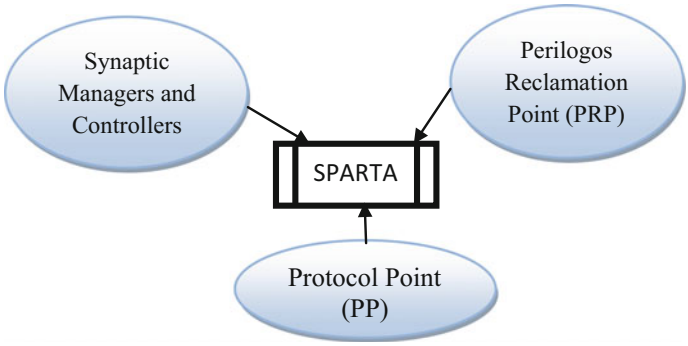


Fig. 8 Components of SPARTA (access control mechanism)

(A) **Major Components**

To give a better idea about the components of SPARTA, their functions have been summarized below

(i) *ER* is responsible for sagacity of the network node, where it tabulates information such as firewall used, OS, and other vital information.
(ii) The ER reports to *APG* about the health and user identity.
(iii) Major job of APG is to authenticate user's identity and evaluate the health status of ER using proprietary protocols also makes decision whether to enable access to network ER.
(iv) Further, APG informs about the decision to *PP* which is responsible for execution of the decision taken.
(v) Controlled access to the network and enforcement of policies is looked after by the PP.

SPARTA user stores all the pre-requisite information gathered by the ER in tabular form. Its main design has three tables each storing some information. The description of the information is given below

(i) **Node-Attestation Table**—The Node-Attestation table has four columns in total: IP address of the source, position, testament number, and timeout value. It is accountable for the packets that source sends. The testament number is given by the base threat management technology being used in the host. APG is the only portion given the authority to add entries to the Node-Attestation table. The entries in the table are removed when either timeout occurs or APG forcefully removes them. Removal by APG takes place when either the entry does not qualify to be a part of the table or the device no longer exists in the network.

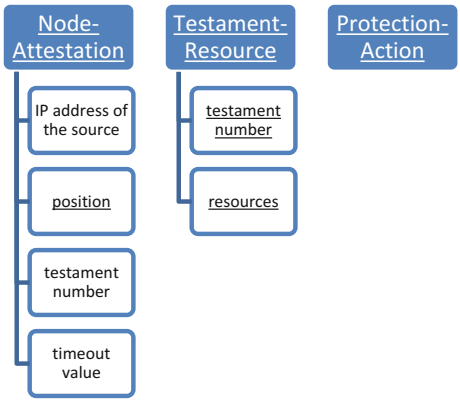


Fig. 9 Hierarchy of ER table

(ii) **Testament-Resource Table**—There are two fields in Testament-Resource table: testament number and resources. This table is used for elaborating the collaboration between testaments and authorized resources.
Both Testament-Resource table and Node-Attestation table contain a common field testament. Using the applications of both the tables, UTM recognizes the IP address of the source and generates dynamic firewall policies to prevent further access. Testament-Resource table is the first thing to be generated and is then stored in the APG network. During the initial setting up of connection between any network protection device and APG, the generated table is pushed into the network.

(iii) **Protection-Action Table**—Mapping up of testament number and salvation protocol is handled by the Protection-Action table. This table along with Testament-Resource table is pushed by the APG when the initial connection is established in the network (Fig. 9).

Access Protocol Governor (*APG*)

APG can easily be described as "intelligence" of the network. This is where network administrator deploys its policies. According to the specifications of our model, out of all the technologies available, XACML can be used for its implementation. Major tasks of APG are as follows:

(i) Resolution of the network policies and their dissection to determine the available resources and their roles which grant the permission to access.
(ii) Authenticating user identity and assigning position to the host.
(iii) Assess the health status of the hosts and assigns host testament number by retrieving host protection abilities.
(iv) It is also responsible for mapping IP address, user, MAC address, position, salvation protocols, and switch information to each other.
(v) In addition to the above, it sends the decisions made to the switches and host threat management technology. Also, APG records testament-resource and user position in the tables in the questions.

(A) **SPARTA Attack Prevention Technique**

Spoofing is one of the major attacks that have been a cause of concern for currently used techniques. In this attack, using various IP addressing masking techniques, the attacker may adopt an IP address which can gain access to the host easily. Due to the masked IP, many of the presently used network security mechanisms are not able to forestall them. However, the technology being developed can detect such attacks by appraising the change in IP address. Here, APG is the main player.

Attacks can be made by the intruders even when there is a slightest window. Sometimes, despite of the presence of the highly protected network, the wrong operations by the user can lead the attacker right inside the network. SPARTA would be required to filter the flow randomly and periodically to ensure that no such attacks make the network vulnerable to the attacks. These further equip the device to periodically check the health status of the network.

8 MONICAN

The proposed system is an integration of many different technologies hence for proper control and management is essential. The sacrosanct requirement of a monitoring system can be felt.

For this purpose, a technology "MONICAN", a new age control and management technology, will be ideal.

The main features of this monitoring device include

- General Management
- Network Routing and Services
- Network Device Management
- Threat protection
- Authentication

Other than the aforementioned capabilities, MONICAN juxtaposes the user-driven protocols with the network monitoring protocols. It gives user the opportunity to define access and the role of the host requesting access. MONICAN acts as the ideal system for not only the proposed integrated system for any other network security-related device in question. The main features of the MONICAN have been elaborated below.

8.1 General Management

Other than providing a user-friendly interface, MONICAN is capable of role-based administration. It has the capability of providing centralized management for

multiple security devices which are virtually incompatible. This system is a self-service portal with a capability to provide one click VPN setup. This system is the archetype of a flexible and mutable model that can be perceived by handler. Other than its general features, a very useful GUI enhances the sniffing capabilities of the user many folds. Overall, MONICAN is the epitome of any control system.

8.2 Network Routing and Services

Multiple routing capabilities such as static, multicast, dynamic, snooping is effectively available in the proposed system. This has the capability of providing auto health check and availability of clustering. This device can balance up to ten appliances with high availability for active/passive clustering. Its interface link aggregation capability is one of the most desirable features in any monitoring device. The contingency attacks that our integrated system is capable of handling are shown with the network information in MONICAN.

8.3 Network Device Management

One of the major gateways for attacks on system can be monitoring devices as they are not well-equipped with capability of intrusion protection. The proposed system can be used for intrusion detection as it performs deep packet inspection. It has the capability of recognizing more than 18,000 patterns which are more than any other monitoring device of its range. It uses pattern matching algorithm and aging for more optimizing results. We are shown the operations being performed by each device separately in the form of screens providing the user opportunity to analyze the functions of each device separately. The networks in the system are shown with a country-wise demarcation, giving us data to analyze the type of data being sent and received by the majority. With separate inbound/outbound settings and exception, a complete protection package is provided to us. To take its protection capabilities to the next level, an identity-based authentication rules and configuration are provided.

8.4 Threat Protection

MONICAN's threat protection capabilities are the better than any device in its range. It can detect and clock network traffic attempting to control the servers using any application layer facility and firewall. This is accomplished by identifying the infected hosts on the network and containing their network activity. Another technique that helps it in thwarting the attacks is by selective sandboxing of

suspicious code to determine malicious intent. MONICAN is equipped with the capability of managing every device in the network and showing their status at the same time to the user.

8.5 Authentication

Taking the network protection to the next level, the proposed system adds another layer to the protection capabilities of the integrated system by adding the feature of server settings check; this is done by combining authentication cache flush for user groups and graphical browsers. Scheduled backend synchronization helps the system working fine at all times. The most striking feature of MONICAN is its policy testing capability tool for URLs that is operating at all times.

With all the features, MONICAN is not only an ideal device for control and management of integrated system but also for any other devices that are involved.

9 Integrated Approach

The proposed approach combines the multiple technologies into one system. Instead of deploying multiple disparate technologies which are difficult to control and monitor, this system provides an easy way to manage and update all the necessary technologies required for the network security through one interface. It has a single platform which analyzes the traffic for suspicious or unexpected behavior, discovers unauthorized access, and prevents the viruses, worms, and infected file from entering the personal network. It analyzes the traffic once by applying defined rules, characterizes, and determines whether it is safe and can be sent further. It blocks the files and applications that do not qualify the defined rules. It performs the necessary logging of information extracted by analyzing for report generation and takes the necessary defense action in an effective and timely manner. MONICAN allows us to centrally control and monitor the system in the most convenient manner. The traffic which is sent to the outside world is also analyzed for access control and to log the activities of each user/groups connected to the system. This system integrates all the necessary technologies and performs the required actions to protect ones network from the known as well as future unknown attacks.

10 Conclusion and Future Work

In conclusion, the proposed integrated system works effectively to provide a secure network. The various components complement each other's job and provide a solution to almost every possible attack. The next-generation IPS prevents

malicious attacks using additional features like user awareness, application awareness. Network breach exposure system (NBES) provides next-level intrusion detection techniques using various methods like cavernous packet examination (CPE), NETGE, PHGE. It produces very few numbers of false positives. Antivirus software is a necessity in today's society where new malwares are continuously developed. Cloud-based antivirus technique is an optimal technique that incorporates both static and dynamic analysis. Omnipresence of the antivirus at both physical and software level is guaranteed by the device. Bayesian filtering is widely used technique that greatly improves filter accuracy. Personalized content filtering blocks only particular portion of Web sites instead of blocking the complete URL. SPARTA provides an ideal solution for access control. MONICAN is a monitoring solution that senses the network and notifies any degradation in performance.

The future work includes studying the upcoming technologies in the network security area and how these can be integrated with our proposed system to make the best out of it. As the technologies in the security area are evolved in future, they should be added to enhance the functioning or replace the old ones in a robust and efficient manner without degrading the system performance.

References

1. Wikipedia. http://en.wikipedia.org/wiki/Honeypot
2. Przemyslaw, K., Dorosz, P.: Intrusion Detection Systems (IDS) Part I—(Network Intrusions; Attack Symptoms; IDS Tasks; and IDS Architecture). www.windowsecurity.com (Articles & Tutorials)
3. Sarkar, S., Brindha, M.: High performance network security using NIDS approach. I.J. Inf. Technol. Comput. Sci. **07** (2014)
4. Ask Karin.: Automatic Malware Signature Detection, 10. http://www.gecode.org/~schulte/teaching/theses/ICT-ECS-2006-122.pdf (2006)
5. What is cloud antivirus and how does it work? https://zeltser.com/what-is-cloud-anti-virus/
6. Oberheide, J., Cooke, E., Jahanian, F.: Cloud N-version antivirus in the network cloud. In: Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI 48109 (2007)
7. Hatem, S.S., Wafy, M.H., El-Khouly M.M.: Malware detection in cloud computing (IJACSA). Int. J. Adv. Comput. Sci. Appl. **5**(4) (2014)
8. Meeting the challenges of web content filtering. http://dansguardian.org/downloads/content_filtering_challenges.pdf
9. Resnick, Paul, Miller, Jim: PICS: internet access controls without censorship. Commun. AGM **39**(10), 87–93 (1996)
10. Du, R., Safavi-Naini, R., Susilo, W.: Web filtering using text classification. In: 11th IEEE International Conference on Networks, ICON, pp. 325–330 (2003)
11. Hu, W., Wu, O., Chen, Z., Fu, Z., Maybank, S.: Recognition of pornographic web pages by classifying texts and images. In IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, Issue 6, pp. 1019–1034 (June 2007)
12. Kuppusamy, K.S., Aghila G.: A personalized web page content filtering model based on Segmentation. IJIST **2**(1) (January 2012)

13. Deng, F., Luo, A., Zhang, Y., Chen, Z., Peng, X., Jiang, X., Peng, D.: TNC-UTM: a holistic solution to secure enterprise networks. In: The 9th International Conference for Young Computer Scientists
14. Taylor, D.E.: Survey and taxonomy of packet classification techniques. ACM Comput. Surv. **37**(3), 238–275 (2005)
15. http://tnc.inform.fh-hannover.de/wiki/index.php
16. http://www.webopedia.com/TERM/N/network_security.html
17. Sophos security made simple UTM feature list

Reliable Data Delivery Mechanism for Mobile Ad Hoc Network Using Cross-Layer Approach

Sandeep Sharma, Rajesh Mishra and Siddharth Dhama

Abstract In the mobile ad hoc networks, there exist various challenges in packet data delivery mechanism. Few of the challenges due to which packet delivery fails are route failure and congestion. Because of these effects, it is very stiff to provide data delivery in an efficient way. So we propose a cross-layer approach in which a buffer is initialized in transport layer to buffer packet during failure of route or congestion or both. Because of this cross-layer approach, packet dropping rate of receiver will decrease. Simulation result shows the efficacy of our approach that our proposed scheme proves to be better than the existing schemes which do not use the cross-layer approach.

Keywords NS2 · Transport layer · Network layer · Cross-layer · Ad hoc network

1 Introduction

Mobile ad hoc network (MANET) [1] is an autonomous system in which the nodes are connected with each other through a wireless link. Ad hoc network are those network that does not have a fix central command node it just use the node present in the network for communication, the nodes act as receiver and transmitter so data transmission from one node to another is achieved by multiple nodes in between. MANET's topology is special kind of topology in a way that it is always in a variable state. There are no fixed nodes present in MANET (also known as dynamic topology) and hence causes instability in the network. The nodes are battery

S. Sharma (✉) · R. Mishra · S. Dhama
School of Information & Communication Technology, Gautam Buddha University, Greater Noida, India
e-mail: sandeepsvce@gmail.com

R. Mishra
e-mail: rmishra@gbu.ac.in

S. Dhama
e-mail: dhamasiddharth@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_47

powered and hence have a small range but they use the multi-hop transmission to overcome the long-distance transmission. To communicate in this network, we need to define protocols so that packet delivery is possible. In a mobile ad hoc network, there exist various challenges in packet data delivery mechanism. Few of the challenges due to which packet delivery fails are as follows: route failure, congestion [2].

Although there are lots of methods to overcome some of these problems [2–10], they do not solve all problems at same time. Some of the protocols are proposed in recent years to support the failure of route and establish an energy efficient route. Some do it with the backup routes [4, 5, 11], but these backup routes have high maintenance. They are costly, time consuming, and difficult. Others do it with more than one route to balance the traffic when the route failure or the congestion occurs. But there are some problems with them, like the overhead increases to maintain so many routes and network performance gets affected. Some protocol gives main attention to the recovery of link at local level. In this, the problem is that if the route discovery takes long time then the packet may have to be dropped. Apart from these problems, there are security issues which can be overcome by techniques like authentication with cross-layer approach [12]. We are going to discuss a way to overcome two of these drawbacks at the same time. So we are going to use a method in which our design is aware of failure of route and congestion, our proposed design [13, 14] uses both network and transport layer. We propose a queue at the transport layer that will be activated in case of congestion, and by using cross-layer the packet of network layer will be buffered in the queue. This will result in the decrease of the packet dropping rate and energy consumption. We are going to learn how this protocol is going to overcome the challenges and compare with the other protocol like AODV. In our proposed design, the received packets are being sent to cross-layer queue at the transport layer and after the congestion or when the node finds a new path they are sent back to network layer and restart the transfer of data. We have divided our paper into eight sections. We start with Sect. 2, in which the related works and the motivation behind this work are discussed followed by our network model and assumptions in Sect. 3. In Sect. 4, we have discussed the proposed cross-layer technique and congestion detection in Sect. 5. Congestion detection and performance evaluation are discussed in Sects. 6 and 7. In Sect. 8, we have concluded the paper with comments on the future scope.

2 Related Work and Motivation

On the basis of past research, the following route failure and congestion can be categorized into flowing types based on their working principle.

One of the types uses a backup route for all active routes. When primary route fails, backup route is used. The example of this type of protocol is AODV-BR [4], but this category suffers from problems like the maintenance of multipath is difficult, costly and energy efficiency is less as a result the performance gets effected.

Other type uses secondary route to send the packets [3]. For example in DSR protocol when congestion occurs, it splits traffic and mitigates congestion; this will increase QoS for the network and as a result the overall maintenance of network increases decreasing the throughput.

The third type focuses on using local recovery process. For example, in case of AODV [8], node checks the signal coming from other nodes and if signals are low, it starts a local recovery and finds a new route instead of sending error message to the transmitting node. Here neighbor node stores information as a backup node, due to this the adjacent node keeps the packet without any reason, and at the end, more than one adjacent node can transmit packets after finding the new route. This results in decrease of network efficiency.

The last type is most recent that focuses on the cross-layer approach. For example, a cross-layer design for resource allocation in [15] and RCECD proposed in [16]. We are proposing a design using this cross-layer approach which will have a queue at the transport layer as proposed in [17].

3 Network Model and Assumptions

In the simulation, we have taken ad hoc network with multiple receiver and sender; every node is acting as sender and receiver and their movements are random. We have taken Institute of Electrical and Electronic Engineers (IEEE) 802.11 as MAC layer protocol. Every node broadcasts a random message to neighbor node. Now because the motion of our nodes is random, link failure may occur. The random message will be sent at equal interval of time by every node so that link connectivity can be checked. We consider RANDOM_INTERVAL is the time between two random message signal, and RANDOM-LOSS allowed is the maximum random message that are lost and can be tolerated. So the time after which link will consider that the link is broken is equal to RANDOM _INTERVAL * RANDOM-LOSS allowed.

4 The Cross-Layer Technique

[16] proposed cross-layer approach for transfer of packets in MANET's. Here, we combine the network layer and transport layer with each other, hence named cross-layer. At the transport layer, we are going to buffer our packet during route failure and congestion. So in case of heavy load, nodes will generate a message that will indicate the congestion and all the respective node will start buffering the packet in their respective transport layer.

4.1 *Buffering of Packets at the Transport Layer*

In MANET, a node acts as a receiver as well as the transmitter, so when it receives the data, in our cross-layer, the nodes will have an transport layer queue (TLQ) to store the packets. Now this TLQ will only be used in case of congestion, and when there is no congestion, the normal operation will take place, and this can be seen clearly in Fig. 1. But when a node detects congestion or node detects that the intermediate link between two nodes is broken, nodes will start using their TLQ to buffer the packet until a new route is formed or there is no more congestion.

In Fig. 1, we can see two different color lines. When there is no congestion, we will follow the blue line but in case of congestion or route failure, we will follow the red line in which the packet will start buffering at transport layer.

In Fig. 2, we can see the mechanism of cross-layer. Our interface will have two components, receiver interface NT (network to transport layer) and TN (transport layer to network layer). Our first interface NT receives packet from the network layer queue and transfers the incoming data to TLQ; NT only works in case of route failure and congestion. In second case, the packet from transport layer is transferred from transport layer queue through TN interface that will on getting the information that congestion is over or in case of route failure that a new route is found, TN transfer will send the data to network layer queue.

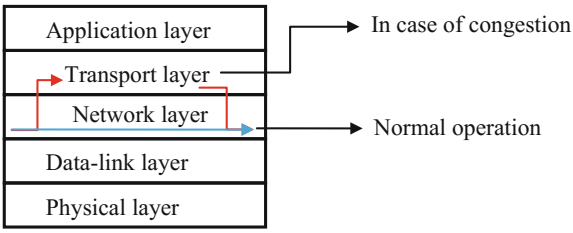


Fig. 1 Flow of packet in cross-layer

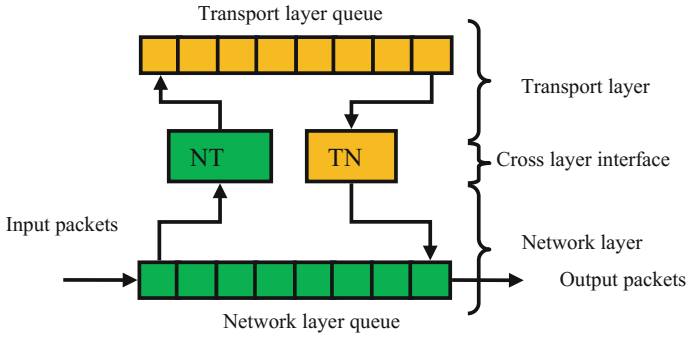


Fig. 2 Interface between transport queue and network queue

Let us take an example that there is a route which has two intermediate nodes C and D. Now take a condition that the link between both the nodes is broken. Now C will detect that the link between both the nodes is broken, so it will start buffering the packets from the network layer to transport layer queue, and C will send a message to other nodes that the route is failed and a RF (route failure) message will be sent. Now as soon as other nodes get the RF message, they will also start buffering the packet to their transport layer queue. Now all the source will stop there transition and wait for the new route notification message. Now if node C finds a new local path, it will send a message new route (NR) to all the nodes. After getting this message, all the nodes will send data through TN interface to the network layer queue from their respective transport layer queue and after that normal operation will begin. This mechanism will decrease packet dropping rate. If no new route is found node, C will send a no new route message (NNR). The source node on receiving this will start a new route discovery.

The procedure to start a new route will be same as finding the route first time, the source node floods the RREQ (route request) packet all over the network in case of not finding the destination node. After that from the single RREQ, it may receive many (RREP) route reply. A route reply carries the source identifier, the destination identifier, the source sequence number, the destination sequence number, the broadcast identifier, and the time to live field. Based on the number of hop count and time to live, the source node will reply with ACK (acknowledgment) packet and then data packets will be sent. After all packets being sent, the destination node will send an ACK packet.

5 Congestion Detection in Proposed Cross-Layer Design

Our cross-layer design detects the congestion so that at time of congestion the packet can be buffered in the transport layer queue. At each intermediate node, we measure the amount of data that is in queue of the network layer, on the basis of this information we measure the level of congestion and according to this the action are taken. A two-bit flag is used in both the packets; the packets are data packets and the acknowledgment of data packet. This is known as congestion level CL flag. The value of our flag is measured on the basis of Table 1.

Table 1 Congestion notification (CL)

Value of CL	Congestion level
00	No congestion
01	Light congested
10	Heavy congested
11	congested

6 Detection of Congestion Level

To determine the congestion, we set minimum and maximum threshold, $Q_{\min}$ and $Q_{\max}$, respectively, for the data present in queue by

$$Q_{\min} = 0.4 \times Q_{\text{size}}, \tag{1}$$

$$Q_{\max} = 0.9 \times Q_{\text{size}}. \tag{2}$$

If the current size of queue is less than $Q_{\min}$, then we can say that there is no congestion, if the queue size is greater than $Q_{\min}$ but less than $Q_{\max}$, then it is light congestion, and if packet length exceeds $Q_{\max}$, then there is congestion. We introduce another parameter Q_{warn}, for warning stated below:

$$Q_{\text{warn}} = w \times Q_{\text{size}}, \tag{3}$$

where w is a weight factor, we choose $w = 0.8$. We then calculate average queue occupancy of a node after every certain interval using exponentially weighted moving average formula as follows:

$$Q_{\text{avg}} = (1 - \alpha) \times Q_{\text{avg}} + Q_{\text{curr}} \times \alpha, \tag{4}$$

where α is a weight factor and Q_{curr} is the current queue size. Now, on the basis of the value of Q_{avg}, the value of CN flags is as follows:

- if $Q_{\text{avg}} < Q_{\min}$ then CN = 00
- if $Q_{\text{avg}} \geq Q_{\min}$ and $Q_{\text{avg}} < Q_{\text{warn}}$ then CN = 01
- if $Q_{\text{avg}} \geq Q_{\text{warn}}$ and $Q_{\text{avg}} \leq Q_{\max}$ then CN = 10
- if $Q_{\text{avg}} > Q_{\max}$ then CN = 11

There can be one more case where the queue size of transport layer and network layer queue is full and in the meantime if no new route is found, node will send a no new route message (NNR). The source node on receiving this will start a new route discovery. So we can say that the threshold to determine failure of the route will be the queue size of transport layer and when $\text{TLQ}_{\text{queue size}}$ is equal to packet queued during congestion then route is fail.

On the basis of above calculation, we can make a congestion control mechanism as given in Table 2.

Table 2 Action taken by node in case of congestion

Congestion level	Action by node
No congestion	Normal operation
Light congested	Do not send RREQ
Heavy congested	Warning message to sources
Congested	Enable TLQ

7 Performance Evaluation

After getting the results, we can see the difference between the throughput of our cross-layer approach and traditional approach, the one that does not include the cross-layer approach. In the simulation scenario, we have considered square area of size 500 * 500 m^2, with 16 random moving nodes. The time for our simulation is 80 s for nodes with transmission range of 250 m. Our source node will send random message at constant interval of time. By this, we can check the connectivity of link. The size of each data packet is 1500 bytes, bandwidth is varied for better result (0.1, 1 and 2 Mbps), and the transport layer protocol is UDP and MAC layer protocol is IEEE 802.11 DCF. Table 3 gives the simulation parameters.

From the analysis, discussion and the simulation results show that our proposed approach perform better than the one without cross-layer. Therefore, our proposed approach provides better throughput than the other protocol that does not have cross-layer design, as shown in Figs. 3, 4, and 5. In these figures, we have taken three different cases of bandwidth 0.1, 1, and 2 Mbps and compared the results with the traditional without the cross-layer technique.

As we can see, our cross-layer design has given better result even in less bandwidth, and in Fig. 6, we can see comparison between throughputs at different bandwidth.

Table 3 Simulation parameters

Parameter	Value
Network area	500 m * 500 m
Number of nodes	16
Number of sources	8
Transmission range	250 m
Transport layer protocol	UDP
MAC layer protocol	IEEE 802.11 DCF
Control packet size	100 bits
Bandwidth	0.1, 1, 2 Mbps
Data burst size	2 Mb/flow
Packet size	512 bytes
Propagation model	Free space
Weight factor	0.2
Simulation time	80 s

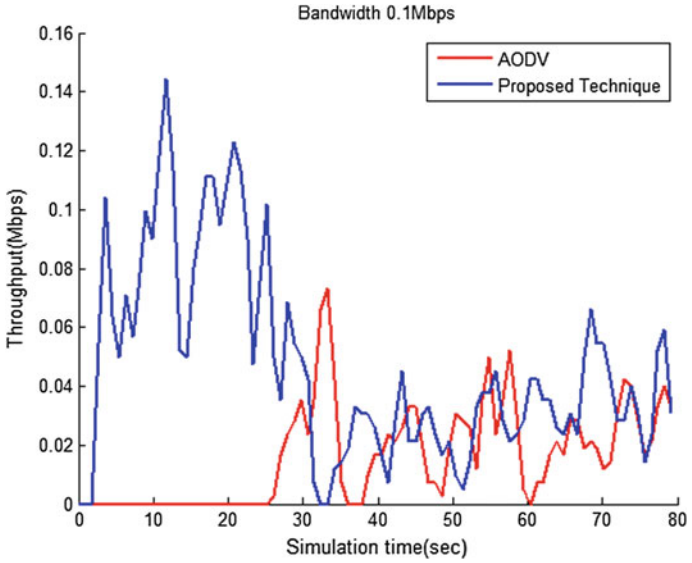


Fig. 3 Compression between AODV and proposed technique at 0.1 Mbps

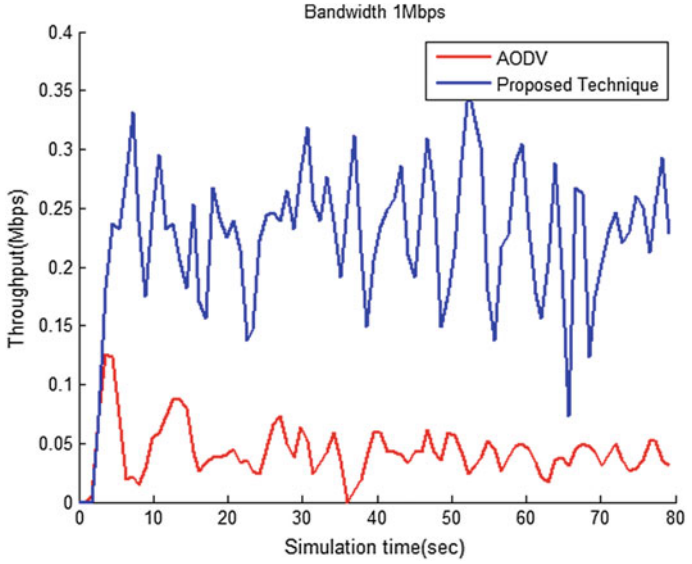


Fig. 4 Compression between AODV and proposed technique at 1 Mbps

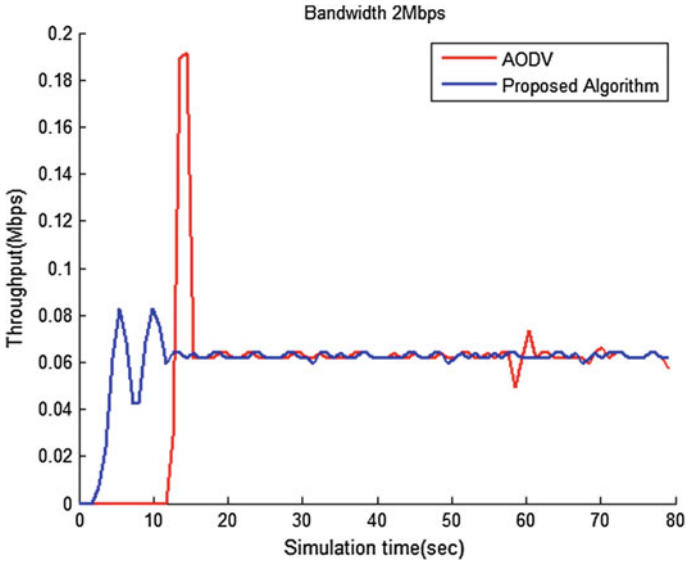


Fig. 5 Compression between AODV and proposed technique at 2 Mbps

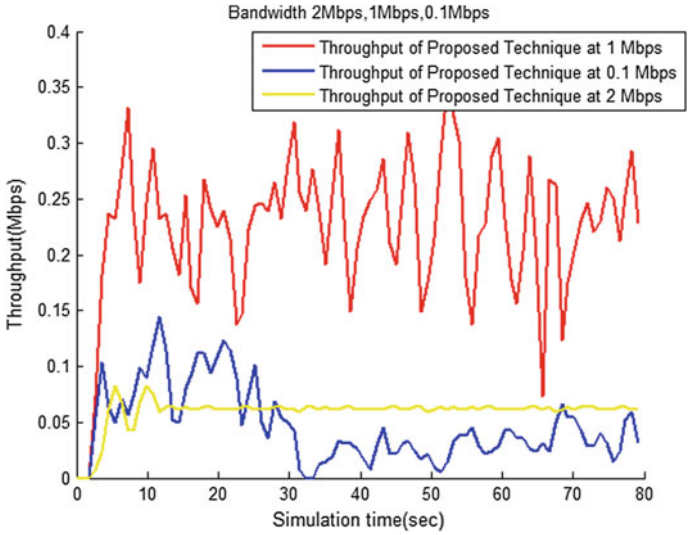


Fig. 6 Compression of throughput at different bandwidth using cross-layer

8 Conclusion

This paper focuses on the network layer where we have proposed a queue that stores the packets from network layer at the time of congestion or failure of route. So a cross-layer design is introduced between these layers. Our design get activated only at the time of congestion or failure of route, upon the discovery of any of these two factors the packet that are being received by node are transferred to the TLQ and after resolving the problem, the data in queue is transferred to network layer queue and normal operation begin. This has increased over throughput as shown by result at different bandwidth. For future work, we can work on different protocol and observe their performance, and we can introduce a new protocol that uses the cross-layer design in normal operation so that we can decrease the load of network layer, so that the overall performance of network can be increased. We can also combine the data link layer with the transport layer thereby making a super layer, violating the traditional boundaries of the protocol stack and redefining new boundaries.

References

1. Jayakumar, G., Gopinath, G.: Ad Hoc mobile wireless networks routing protocols—a review. J. Comput. Sci. **3**(8), 574–582 (2007)
2. Ramanathan, R., Redi, J.: A brief overview of Ad Hoc networks: challenges and direction. In IEEE Communications Magazine 50th Anniversary Commemorative (May 2002)
3. Akintola, A.A., Aderounmu, G.A., Akanbi, L.A., Adigun, M.O.: Modeling and Performance Analysis of Dynamic Random Early Detection (DRED) Gateway for Congestion Avoidance. Issues in Informing Science and Information Technology
4. Wahi, C., Sonbhadra, S.K.: Mobile Ad Hoc network routing protocols: a comparative study. doi:10.5121/ijasuc.2012.3203
5. Abolhasan, M., Wysocki, T., Dutkiewicz, E.: A review of routing protocols for mobile ad hoc networks. Elsevier B.V (2003)
6. Zafar, H., Harle, D., Andonovic, I., Hasan, L., Khattak, A.: QoS-aware multipath routing scheme for mobile Ad Hoc networks. Int. J. Commun. Netw. Inform. Sec. (IJCNIS) **4**(1) (April 2012)
7. Lee, S.J., Gerla, M.: Split multipath routing with maximally disjoint paths in ad hoc networks. In: IEEE International Conference on Communications (ICC), Helsinki, Finland, vol. 10, pp. 3201–3205 (2001)
8. Pingale, H., Kokate, S.R.: A study of congestion aware adaptive routing protocols in MANET. Int. J. Adv. Technol. Eng. Res. (IJATER) **2**(2) (May 2012)
9. Devi, M., Mittal, D.P.: Local route repair in MANET for on demand routing protocol: a review. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **4**(5) (May 2014)
10. Kapoor, S., Pal, P.: Stable AODV protocol in mobile Ad-Hoc network. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **4**(6) (June 2014)
11. Khan, K.U.R., Zaman, R.U.: The performance of the extended DSDV (eDSDV) MANET routing protocol and its suitability in integrated internet-MANET. IJSSST **10**(2)
12. Sharma, S., Mishra R.: Authentication in Wireless Network. IEEE Conference Publications (2015)

13. Singh, S., Hemrajani, N.: Performance evaluation of AODV routing protocol in wireless sensor networks with the constraints of varying terrain areas by varying pause time. Int. J. Emerg. Trends Technol. Comput. Sci. (IJETTCS) **2**(1) (January–February 2013)
14. Hai, J., Zhuang, W., Shen, X.(S.): University of Waterloo. Cross-Layer Design for Resource Allocation in 3G Wireless Networks and Beyond. IEEE Communications Magazine (December 2005)
15. Beebi, P.A., Singha, S., Mane, R.: A study on cross layer MAC design for performance optimization of routing protocols in MANETs. Int. J. Adv. Comput. Sci. Appl. (IJACSA) **2**(2) (February 2011)
16. Hassan, M.M., Kamruzzaman, S.M.: Design of an energy-efficient and reliable data delivery mechanism for mobile ad hoc networks: a cross-layer approach. Published online in Wiley Online Library (wileyonlinelibrary.com). doi:10.1002/cpe.3309
17. Reddy, T.S., Reddy, D.P.: EOCC: energy-efficient ordered congestion control using cross layer support in mobile Ad Hoc network routing. Int. J. Sci. Eng. Res. **3**(10) (October-2012)

Stable Period Extension for Heterogeneous Model in Wireless Sensor Network

Pawan Singh Mehra, M.N. Doja and Bashir Alam

Abstract In past few decades, energy efficiency issue in wireless sensor network (WSN) has attracted researchers due to its constrained power source. Focus on the parameters which affects the energy level of the sensor nodes of the WSN is the key to attain energy optimization. Introduction of heterogeneity increases the capability and lifetime. In this paper, we propose a heterogeneous-model-based energy efficient scheme for clustering. Any clustering algorithm which groups the sensors can contribute in increasing efficiency of the network. This paper proposes an energy conscious clustering method which takes into account the energy of the nodes residing within the proximity of its transmission range. Indecent designed self-organizing clustering algorithm can drop down the lifetime of the nodes. The simulation work of the proposed algorithm is done for heterogeneous energy model with varying parameters. Simulation results ratify the stability period extension of proposed protocol. The proposed algorithm is capable to prolong the stable period of network and balances the overall energy dissipation of the network over its comparatives..

Keywords Clustering · WSN · Heterogeneous · Energy efficiency · Cluster head (CH) · Base station (BS)

P.S. Mehra (✉) · M.N. Doja · B. Alam
Department of Computer Engineering, Faculty of Engineering & Technology, Jamia Millia Islamia, Jamia Nagar, New Delhi, India
e-mail: pawansinghmehra@gmail.com

M.N. Doja
e-mail: ndoja@yahoo.com

B. Alam
e-mail: babashiralam@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_48

1 Introduction

Due to the recent technological innovations and the maturity of communication and microelectronics day by day, development of small size, low cost, minimal powered sensors has become possible. Wireless sensor network has aroused interest of researchers in the pertinent domain. It is a group of huge numbers of sensor nodes which are deployed manually or dropped on the fly over the area of interest to collect the useful data. WSN with clustering acts as a teamwork where each sensor node plays its role and contributes to the goal of the network. The ultimate aim of WSN is delivery of data to base station where it can further be processed as per the requirement. Generally, the WSN is deployed in a field where human intervention is impossible or difficult. Thus, the base station location is at a place far away from the target area. Applications of WSN include tracking and monitoring, e.g. human tracking, animal tracking, enemy tracking, measurement of temperature, humidity or environmental parameters [1]. Deployment of WSN can be done in two ways; deterministically or non-deterministically [2]. Deterministic deployment can be seen where the target area is human approachable, e.g. monitoring of huge structures, animal monitoring in habitat, whereas non-deterministic deployment of sensor nodes is done on the fly where the location of sensor nodes is not known aprior, e.g. volcanic eruption detection, flood, forest fire detection. In such applications, the position of the base station cannot be put in the centre, so the base station in the proposed scheme is located at distant place.

This literature proposes a two-level heterogeneity-based energy conscious protocol. In this model, two base stations are deployed on either side of the target area at a distant place. The target area can be forest fire, landslide, earthquake, etc., where the deployment of base station at the centre is not that easy as presumed in most of the research work. In clustering algorithms, the cluster head has a vital role to play. The election of cluster head in this algorithm depends on the parameters which can affect the energy of the sensor nodes deployed in the network.

Rest of the sections are as follows. Discussion of pertinent research is done in Sect. 2. Section 3 discusses the heterogeneous network model. Section 4 explains the proposed protocol. Simulation work with evaluation of the proposed protocol is examined in Sect. 5. Section 6 finally discusses the concluding remarks.

2 Literature Review

In the past decade, several mechanisms were proposed in different aspect so as to elongate the lifetime of WSN network. Grouping of sensor nodes in order to form a cluster is one of the techniques which helps to conserve energy [3]. Every cluster in the network has one leader called the cluster head whose job is to collect data from the member of the cluster and forward the aggregated data to next level. Clustering has become the first preference for organizing the network. LEACH [4] protocol

proposed by Heinzelman et al. forms cluster in the field so that minimization of energy dissipation can be attained. In this work, a sensor node is selected on the basis of probability-based threshold criteria for the selection. Every node will generate a random number and nodes with value less than the threshold gets elected. Rest nodes in the network join the cluster closest to them but the number of CH for a round is not deterministic. This protocol incorporates single hop communication.

In order to avoid longer distance transmission from CH to BS, HEED [5] take over the multihop transmission and perform far better than LEACH. But problem of hot spot may arise in the region near the base station. LEACH and its relevant protocols along with some of enhancements are discussed in [6], and BEES [7], an algorithm inspired by bee's colony, is proposed by AbdelSalam et al. This proposed work consists of four phases: backbone, tiling, clustering and selection. Challenges like clustering, data aggregation and localization have been overcome, but the clustering is comparatively complex.

SEP [8] protocol was introduced by Smaragdakis et al. This protocol introduced heterogeneity in the network. In his proposed work, he discussed the effects of heterogeneity and instability of proposed work. The stable period is put into consideration for comparison. In this protocol scheme, a sensor node selection depends upon the weight calculated by them for the round. The author makes sure that the CHs are chosen on the basis of their initial energy and ensures load balancing. In SEP, two energy levels are considered. The advance nodes have some additional energy as compared to normal nodes. The weighted probabilities for sensor nodes are given below:

$$\mathrm{P}_{\mathrm{nrm}} = \frac{p_{\mathrm{opt}}}{1 + \alpha m} \tag{1}$$

$$\mathrm{P}_{\mathrm{adv}} = \frac{p_{\mathrm{opt}}(1 + \alpha)}{1 + \alpha m} \tag{2}$$

Here α (alpha) is the extraneous energy, and the percentage of advance nodes is given by m. This protocol extends the lifetime but remnant energy is not considered.

Qing et al. proposed a DEEC [9] for multilevel heterogeneous energy model for WSN. In this protocol, the candidature of cluster head depends upon the ratio between the average energy of the network field and remnant energy of the sensor nodes. DEEC is based on LEACH as the role of the cluster head is rotational among all the sensor nodes deployed in the network so that the energy expenditure of the nodes is uniform. The weight-based probability of each node is calculated as follows

$$P_i = \begin{cases} \frac{p_{\mathrm{opt}} E_i(r)}{(1 + \alpha m)\overline{E}(r)} & \text{for normal node} \\ \frac{p_{\mathrm{opt}}(1 + \alpha) E_i(r)}{(1 + \alpha m)\overline{E}(r)} & \text{for advance node} \end{cases} \tag{3}$$

where r depicts the round, the remnant energy of the sensor is denoted by $E_i(r)$, and $\overline{E}(r)$ is the average energy of field for present round. This protocol requires the energy level index of all the nodes that are deployed in field.

Alam et al. proposed load balancing clustering scheme [10] which considers cluster head index for choosing the cluster head in field. Sensor nodes which are redundant in terms of sensing range are put to sleep mode in order to conserve energy of the field. This protocol is capable enough to extend the lifetime of the field. Mehra et al. proposed LEASE [11] for homogeneous network. In this scheme, remnant energy and dissipation rate of the sensor nodes are taken into account. This scheme outperforms LEACH and heterogeneity-based SEP.

Doja et al. proposed heterogeneous model for multilevel and two-level energy of the sensor nodes [12]. In his scheme, the BS is considered to be at distant place from the target area. The locations of the nodes are estimated through RSSI. Parameters like node density and energy exhaustion by sensor nodes are considered for setup phase. Better lifetime is achieved in the proposed work.

3 Heterogeneity-Based Network Model

This part discusses the heterogeneity-based model of the network. There are N numbers of nodes that are deployed in a $M \times M$ network field randomly. The optimum percentage of the cluster heads for a round, p_{opt} is taken as 10% of nodes which are not dead in the network. As stated above, the locations of the deployed sensor nodes are not known aprior and can be calculated with the help of RSSI or LQI. The network of the target area is presumed to have fixed topology, i.e. the sensor nodes are immovable.

In wireless sensor network, the classification of heterogeneity is energy, link and computational [11]. Link heterogeneity deals with link and reliable data transmission with greater bandwidth. Computational heterogeneity is meant for more processing power and larger storage. Energy heterogeneity deals with more power source. Energy consumption in heterogeneity-based model in comparison with homogeneous model is less, and the network links are comparatively reliable [13].

In this proposed scheme, the two-level energy model is considered. Some nodes (m%) are equipped with extraneous energy called advanced nodes. Leftover nodes are normal nodes. The energy of the sensor nodes in the beginning is E_{o}, and advance nodes are bundled with α times additional energy in comparison with normal nodes. The overall energy of the network can be determined by:

$$E_{\text{total}} = N(1-m)E_{\text{o}} + NmE_{\text{o}}(1+\alpha) = NE_{\text{o}}(1+\alpha m) \tag{4}$$

For energy exhaustion analysis, energy model used in [9] is considered. In order to forward l-bit information to another node at a distance d, energy spend by transceiver of the sensor node is calculated by:

$$E_{\mathrm{Tx}}(l,d) = \begin{cases} lE_{\mathrm{elec}} + l\varepsilon_{fs}d^2, & d < d_{\mathrm{o}} \\ lE_{\mathrm{elec}} + l\varepsilon_{mp}d^4, & d \geq d_{\mathrm{o}} \end{cases} \tag{5}$$

E_{elec} is the energy dissipated per bit by the transceiver circuit and $\varepsilon_{fs}d^2$, and $\varepsilon_{mp}d^4$ depends upon the separation distance. The cluster head energy expenditure for a round is determined by

$$E_{\mathrm{CH}} = n(lE_{\mathrm{elec}} + l\varepsilon_{fs}d^2 + E_{\mathrm{DA}}) \tag{6}$$

where E_{DA} is energy consumed for data aggregation operation and n is the count of cluster members. Two base stations are located on each side of the target area with an assumption that they are resourceful. The deployed sensor nodes are presumed to generate reports for the same event on regular basis. Every node in the network has the capability to adjust communication range and is capable to communicating every other node in the network. The sensor nodes are capable of directional propagation as in [14].

4 Protocol Description

The proposed scheme is divided into two phases: topology setup phase and data collection phase. MSG which includes the position of the base stations is broadcasted by both the base stations one after the other at a specified interval to the target area so that the deployed nodes can have the location of the base stations. The sensor nodes select the base station which is nearer to them. The communication range for sensor nodes is set as in [12] and can be calculated by:

$$R_{\mathrm{c}} = \sqrt{\frac{M^2}{p_{\mathrm{opt}} \times \prod}} \tag{7}$$

In the topology setup phase, to set up the clusters, every alive node in the network calculates its probability to prove its candidature for cluster head by the given formula:

$$\mathrm{CPW}_i = \frac{E_i(r) \times \mathrm{Ch_o} \times \ell_i}{\mathrm{Ch} \times \omega_i(r) \times \delta_i \times \Psi_i} \tag{8}$$

where ℓ_i is distance from sensor nodes to its neighbour nodes, Ψ_i is the mean distance to all neighbour nodes within R_{c}, $Ei(r)$ is the residual energy level, $\omega_i(r)$ is the energy dissipated till round r, Ch and $\mathrm{Ch_o}$ are the count of sensor node being chosen and not chosen as cluster head, respectively, and distance from deployed sensor node to base station is denoted by δ_i. Each node broadcasts its cluster head

probability weightage (CPW_i) within its vicinity, and the sensor node with highest CPW_i is selected to be the cluster head. After being chosen as cluster head, the sensor node broadcasts a join message to all the nodes within the communication range of the sensor node.

The sensor nodes with lower CPW_i sends acknowledgement to the CH to join the cluster. Likewise clusters are formed by other nodes with higher CPW_i. Once all the nodes of the network are assigned a CH, the topology setup phase comes to an end. After the accomplishment of topology setup phase, the second phase, i.e. data collection phase, comes into act. Sensor nodes deployed in the field sense the physical phenomena and forward it to their respective cluster heads. After collecting data from the entire sensor nodes within it cluster, the cluster head fuses the data in order to minimize the transmission overhead. The fused data is then transmitted to base station according to the TDMA schedule provided by the base station so that collision-free communication takes place. In this way, a round is completed by the proposed scheme.

5 Performance Evaluation

The proposed work is simulated with SEP and DEEC for different parameters. The normalized values of results are obtained by several hundred of iterations. Evaluation of the performance is done on two factors; stability period of the network and total count of successful transmitted packets from sensor node to BS. As soon as the physical phenomenon is sensed by the sensor node, the sensor node wraps this information in the form of packet and transmits it to cluster head which in turn after collecting information from all the members fuse the information and forward it to the BS. This successful journey of information generated from the sensor node through CH towards the BS is termed as successful packet transmission. Better stability period exhibits even distribution of energy. The parameters which are incorporated in simulation work are depicted in Table 1.

In Fig. 1, with an initial energy of 0.5 J for normal nodes, stability period of proposed work is 21 and 44% more than SEP and DEEC with 10% advance nodes, whereas for 30% advance nodes, the proposed protocol achieves 22 and 113% better stability period as depicted in Fig. 2.

Table 1 Radio model parameters used in simulation [8]

Parameters	Symbol	Value
Energy dissipation when $d < d_o$ (d is at a short distance)	ε_{fs}	10 pJ/bit/m^2
Energy dissipation when $d > d_o$ (d is at a long distance)	ε_{mp}	0.0013 pJ/bit/m^4
Energy consumption for transmission/reception	E_{elec}	50 nJ/bit
Energy dissipation for data aggregation	E_{DA}	5 nJ/bit/report

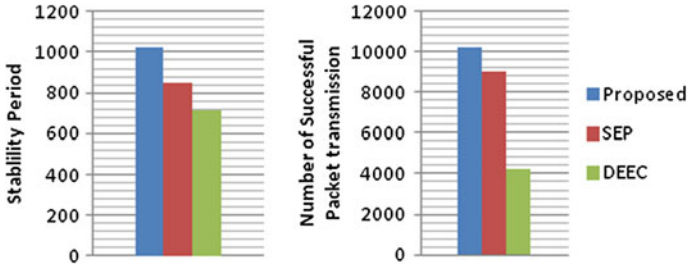


Fig. 1 Evaluation parameters for proposed work, DEEC and SEP when E_o (initial energy) = 0.5 J, α (extraneous energy) = 0.5, m (percentage of advanced nodes) = 0.1, N (number of nodes) = 100, target area size (100, 100) and position of base station 1 (175, 50), base station 2 (−75, 50)

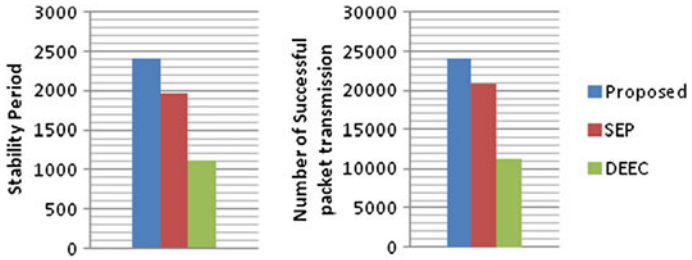


Fig. 2 Evaluation parameters for proposed work, DEEC and SEP when E_o (initial energy) = 1 J, α (extraneous energy) = 1 J, m (percentage of advanced nodes) = 0.3, N (number of nodes) = 100, target area size (100, 100) and position of base station 1 (175, 50), base station 2 (−75, 50)

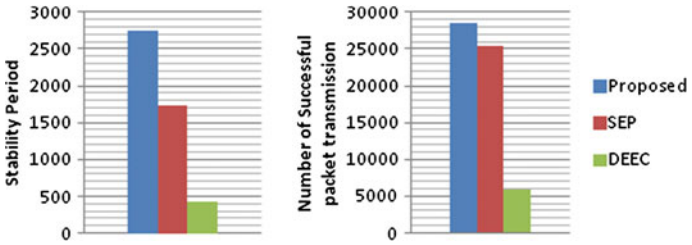


Fig. 3 Evaluation parameters for proposed work, DEEC and SEP when E_o (initial energy) = 1.5 J, α (extraneous energy) = 1.5 J, m (percentage of advanced nodes) = 0.3, N (number of nodes) = 150, target area size (150, 150) and position of base station 1 (262.5, 75), base station 2 (−112.5, 75)

Now, the field size and the number of deployed nodes are increased. Proposed protocol shows remarkable performance. In Fig. 3, the advance nodes are set to 30% with initial energy set to 1.5 J. The proposed protocol has achieved 534 and 60% longer stable period over DEEC and SEP, respectively. If we talk about Fig. 4,

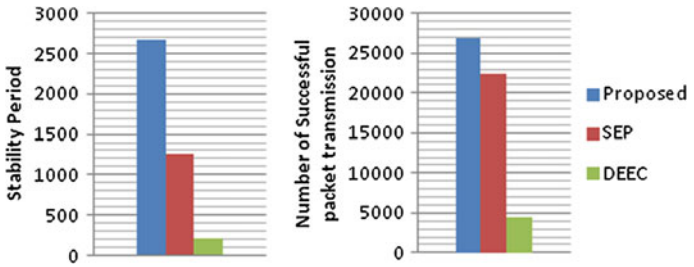


Fig. 4 Evaluation parameters for proposed work, DEEC and SEP when E_o (initial energy) = 2 J, α (extraneous energy) = 2 J, m (percentage of advanced nodes) = 0.5, N (number of nodes) = 200, target area size (200, 200) and position of base station 1 (350, 100), base station 2 (−150, 100)

the stability period is extended 1213 and 112% more than DEEC and SEP for 50% advance nodes with a field size of 200 m^2 with normal nodes having 2 J initial energy.

6 Conclusion

In this paper, heterogeneity-based energy conscious protocol is proposed for two base stations which are located at distant place on either sides of the target area. The proposed work considers the best candidate available for CH as the cluster head's task is energy intensive. Proposed protocol performs well in comparison with SEP and DEEC for two-level heterogeneity energy model.

References

1. Mehdi Afsar, M., Mohammad, H., Tayarani, N.: Clustering in sensor networks: a literature survey. J. Netw. Comput. Appl. **46**, 198–226 (2014)
2. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Comput. Netw. **52**(12), 2292–2330 (2008)
3. Abbasi, A.A., Younis, M.: A survey on clustering algorithms for wireless sensor networks. Comput. Commun. **30**(14–15), 2826–2841 (2007)
4. Heinzelman, W., Chandrakasan, A., Balakrishnan, H.: Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00) (2000)
5. 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)
6. Jindal, P., Gupta, V.: Study of energy efficient routing protocols of wireless sensor network and their further researches: a survey. J. Comput. Sci. Commun. Eng. (2013)
7. AbdelSalam, H.S., Olariu, S., Bees: bio inspired backbone selection in wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. (2012)

8. Smaragdakis, G., Matta, I., Bestavros, A.: SEP: a stable election protocol for clustered heterogeneous wireless sensor networks. In: Second International Workshop on Sensor and Actor Network Protocols and Applications (2004)
9. Qing, L., Qingxin, Z., Mingwen, W.: Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks. Comput. Commun. **29**(12), 2230–2237 (2006)
10. Mehra, P.S., Doja, M.N., Alam, B.: Energy efficient self organising load balanced clustering scheme for heterogeneous WSN. In: 2015 International Conference on Energy Economics and Environment (ICEEE), pp. 1–6, 27–28 Mar 2015
11. Mehra, P.S., Doja, M.N., Alam, B.: Low energy adaptive stable energy efficient (LEASE) protocol for wireless sensor network. In: 2015 International Conference on Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), pp. 484–488, 25–27 Feb 2015
12. Mehra, P.S., Doja, M.N., Alam, B.: Enhanced stable period for two level and multilevel heterogeneous model for distant base station in wireless sensor network. In: International Conference on Computer and Communication Technologies, vol. 379, pp. 751–759 (2015)
13. Kumar, D., Aseri, T.C., Patel, R.B.: EEHC: energy efficient heterogeneous clustered scheme for wireless sensor networks. Comput. Commun. **32**(4), 662–667 (2009)
14. Chen, Y.-C., Wen, C.-Y.: Distributed clustering with directional antennas for wireless sensor networks. Sens. J. **13**(6), 2166–2180 (2013). IEEE

Congestion Control in Vehicular Ad Hoc Network: A Review

Jaiveer Singh and Karan Singh

Abstract Vehicular ad hoc network is a network of moving vehicles in which a set of road side units (RSUs) are used over vehicular networks to assist and communicate with moving vehicles. Numbers of vehicles are increasing day by day, and the numbers of motor vehicle accidents are also increasing. Therefore, quality of service (QoS) has become very crucial and challenging aspect for safe and convenient driving. Congestion control is one of them that provide quality of service (QoS) in vehicular network. Lots of research has been done in congestion control, and lots of research is to be done to ensure safe and reliable communication. Over the last decades, several algorithms have been proposed to address congestion problem in vehicular ad hoc networks (VANETs). In this paper, various congestion control techniques have been reviewed. These algorithms are compared on different parameters.

Keywords VANET · Congestion control · Quality of service

1 Introduction

Vehicular ad hoc networks (VANETs) [1] are special kind of mobile ad hoc network (MANET) [2] in which the mobile nodes are configured as traveling vehicles. Vehicular ad hoc networks (VANETs) [3–5] consist of vehicle-to-vehicle (V2V) [6, 7] and vehicle-to-infrastructure (V2I) communications. It is network of moving and smart vehicles. Besides traveling vehicles, a set of road side units (RSUs) are also

J. Singh (✉)
Department of CSE, Krishna Institute of Engineering & Technology, Ghaziabad, Uttar Pradesh, India
e-mail: jaiveer.siddhu@gmail.com

K. Singh
School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India
e-mail: karan@mail.jnu.ac.in

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_49

used over road networks to assist and communicate with traveling vehicles in VANETs. These RSUs are used as a fixed infrastructure in the VANETs. Transceiver equipments enable the wireless communications between traveling vehicles (V2V-Vehicle-to-Vehicle) and the communication between traveling vehicles and located RSUs (V2I-Vehicle-to-infrastructure).

1.1 Characteristics of VANETs [6, 8, 9]

In VANETs, vehicles move at high speed, travel over long distances, and traffic information may be useful to vehicles hundreds of miles away. Power consumption is not a major concern. Vehicles are mobile power plants. Vehicles have a high cost and therefore can be equipped with additional sensors without significantly impacting the total cost. The topology of VANET is extremely dynamic as vehicles go in and out transmission range quite rapidly. Vehicles travel long distances in a small amount of time when compared to other mobile networks. The transmission power is limited in the WAVE architecture, which limits the distance that data can reach. This distance is up to 1000 m.

1.2 Challenges in Vehicular Ad Hoc Network [10]

A central challenge of VANETs [11, 12] is that there is no central control. Although some applications likely will involve infrastructure (e.g., traffic signal violation warning, toll collection etc.). Another challenge of VANET is highly dynamic topology. VANET topology is changing rapidly, therefore it is unpredictable. Quality of service in VANET is an important task. Quality of service (QoS) is the measure of a service offered by the network to the user. Error-prone shared radio channel, hidden terminal problem, limited resource availability, and insecure medium are challenges which make VANETs inefficient to support quality of service (QoS).

1.3 Applications of VANETs [10, 13]

There are major categories of applications where VANETs [10, 14] are used such as safety applications, convenience applications, traffic information systems, and infotainment applications. The main examples of these applications are traffic signal violation warning, road congestion notification, video streaming, and vehicle's satellite navigation system.

2 Congestion Control

When offered load crosses the certain limit, then there is sharp fall in throughput and increase in delay. This phenomenon is known as congestion. Congestion may occur due to sudden increase in traffic in the network. When too many packets are transmitted through a network, performance collapses completely and almost no packets are delivered. To provide reliable communications in vehicular ad hoc networks (VANETs) [13, 15], it is important to take into account quality of services (QoS) [16]. Delay and packet loss are two main QoS parameters considered by congestion control strategies. Last several years, various strategies or techniques have been proposed to address the congestion problem in VANETs. Congestion control [17–19] algorithm has two main components, congestion detection component and congestion control component.

2.1 Congestion Detection Component

This component may use the three types of techniques for congestion detection. *The measurement-based congestion detection technique* senses communication channels and measures parameters like number of messages queue, channel usage level, and channel occupancy time. Congestion detection component measures the channel usage level periodically to detect congestion situation. *Event-driven detection* technique [20] monitors the event-driven safety message and decides to start the congestion control algorithm whenever event-driven safety message is detected or generated. *MAC blocking detection* technique is based on the control of beacon message transmissions to reduce the congestion and traffic rate control for congestion avoidance.

2.2 Congestion Control Component

Once congestion detected, congestion control component try to tackle the congestion in the VANETs. This component may use three main methods, controlling the transmission range, controlling the transmission rate, and scheduling messages.

3 Review of Congestion Control Techniques for VANETs

3.1 The Congestion Detection Techniques

Congestion detection techniques [8, 9, 11] are three types, the measurement-based congestion detection, event-driven detection, and MAC blocking detection.

3.1.1 The Measurement-Based Congestion Detection Techniques

This technique senses communication channels and measures parameters like channel usage level. The value of the channel usage level is compared with a predefined threshold. Thus, if channel usage level exceeds the threshold, it is assumed that the communication channels are in congestion. In [21], each device periodically senses the channel usage level. This channel usage level is compared with predefined threshold limit. In [22], researchers used the simulation based on channel occupancy time to detect congestion. In [23], channel usage level is used to detect congestion in the VANETs. In [20], authors used channel usage level to detect congestion. This channel usage level is compared with predefined threshold limit (Table 1).

3.1.2 Event-Driven Detection Technique

This technique monitors the event-driven safety message and decides to start the congestion control algorithm whenever event-driven safety message is detected or

Table 1 Review of various congestion detection techniques

Reference	Congestion detection methods	Remarks	Simulator	Performance metrics
[21]	Event driven	Based on queue freezing	WARP2	Delay
[21]	Measurement-based detection	Channel usage level	WARP2	Delay
[22]	MAC blocking detection	MAC blocking happens at a node	NS-2	Packet received
[23]	Measurement-based detection	Channel usage level is compared with threshold	NS-2	Delay, packet loss, throughput
[20]	Measurement-based detection	Channel usage level is compared with threshold	NS-2	Delay, packet loss, retransmission, packet loss ratio, throughput
[25]	Measurement-based detection Event driven	No. of packets in the channel queue is compared with threshold Queue freezing method	Veins	Delay
[28]	Event driven	Queue freezing method	Veins	Delay, packet loss

generated. In [21], authors used event-driven method to detect the congestion in the VANET. Whenever a device detects a safety message, it will start the congestion control immediately to ensure safety applications. In [24], congestion detection is based on event-driven method.

3.1.3 MAC Blocking Detection Technique

This technique is based on the control of beacon message transmissions to reduce the congestion and traffic rate control for congestion avoidance. In [22], congestion detection is done based on MAC blocking detection.

3.2 Congestion Control Techniques

Many algorithms have been proposed by many researchers to address the congestion problem [16]. It is hard to find an efficient algorithm to improve safety of users and transport efficiency in a congested environment. There are three types of congestion control algorithms, proactive, reactive, and hybrid. In [23], authors proposed the reliable congestion control algorithm using meta-heuristic techniques. Proposed algorithm is based on tabu search algorithm for safety applications. Proposed algorithm performs better to reduce the traffic communication channels while considering reliability requirements of applications in vehicular network. In [20], researchers present the congestion control techniques based on tabu search. The proposed algorithm controlled congestion dynamically by tuning transmission range and rate for all kinds of messages (safety and non-safety), whereas delay and jitter were minimized. In [25], authors proposed the congestion control algorithm for event-driven safety messages. Simulation shows that the proposed algorithm is efficient in term of packets delay (Table 2).

In [26], authors proposed a new and integrated method for reducing the road congestion. This system proposes the congestion detection and avoidance by disseminating and exploiting road information. In [24], authors proposed a congestion control approach based on the concept of dynamic priorities-based scheduling to ensure a reliable and safe communications architecture within VANET. In [27], authors proposed the congestion control techniques for fairness and stability analysis. These algorithms adapt transmission rate and power based on network measures such as channel busy ratio. Stability is verified for all typical road density cases. Fairness is shown to be naturally achieved for some algorithms.

Table 2 Review of congestion control techniques

Reference	Strategy used	Quality of service (QoS) parameters	Simulator used	Class
[23]	Transmission range and rate	Delay, packet loss, throughput	NS-2	Reactive
[20]	Transmission range and rate	Delay, packet loss, No. of retransmission, packet loss ratio, throughput	NS-2	Reactive
[25]	Scheduling messages	Delay, packet loss, throughput	NS-2	Reactive
[26]	Sharing congestion information	Average travel time	Java-based simulator	Proactive
[29]	Scheduling messages	Delay	TransModeler	Reactive
[22]	Transmission rate	Packet received	NS-2	Proactive
[24]	Scheduling messages	Bandwidth	UPPAAL verification tool	Reactive
[27]	Transmission range and rate	Stability (in time) and fairness (in space)	MATLAB	Reactive
[28]	Scheduling messages	Delay, packet loss	Veins	Proactive
[30]	Transmission rate	Channel busy time (CBT) and number of packets received per second	NS-2	Proactive

4 Conclusion

In this paper, we have analyzed and classified various congestion detection and congestion control techniques used in VANETs. After reviewing these techniques, we can say that vehicular ad hoc network would play an important role in intelligent transportation system. Existing transportation systems require huge improvement in vehicle safety and transport efficiency. A smart transportation system can reduce road traffic congestion, improve response time to incidents, and ensure a convenience and safe driving. There are huge challenges in VANETs. In a future work, according to our findings, we will propose a congestion control mechanism for congestion detection and avoidance.

References

1. Hartenstein, H., Laberteaux, K.P.: A tutorial survey on vehicular ad hoc networks. IEEE Commun. Mag. **46**(6), 164–171 (2008)
2. Lochert, C., Scheuermann, B., Mauve, M.: A survey on congestion control for mobile ad-hoc networks. Wirel. Commun. Mob. Comput. **7**(5), 655–676 (2007). (Wiley)

3. Mohandas, B.K, Liscano, R., Yang, O.W.: Vehicle traffic congestion management in vehicular ad-hoc networks. In: IEEE 34th Conference on Local Computer Networks, 2009. LCN 2009, pp. 655–660. IEEE (2009)
4. Chen, C., Li, Y., Pei, Q.: Avoiding information congestion in VANETs: a congestion game approach. In: 2014 IEEE International Conference on Computer and Information Technology (CIT), pp. 105–110. IEEE (2014)
5. Zhang, W., et al.: Congestion Control for Safety Messages in VANETs: Concepts and Framework, pp. 199–203 (2008)
6. Sichitiu, M.L., Kihl, M.: Inter-vehicle communication systems: a survey. IEEE Commun. Mag. **10**(2), 88–105 (2008)
7. Yang, X., et al.: A vehicle-to-vehicle communication protocol for cooperative collision warning. In: Proceedings of First Annual International Conference on Mobile and Ubiquitous System, Network Services (MobiQuitous), Boston, USA, pp. 1–10, Aug 2004
8. Sattari, M.R.J., Noor, R.M., Keshavarz, H.: A taxonomy for congestion control algorithms in vehicular ad hoc networks. In: 2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat). IEEE (2012)
9. Darus, M.Y., Bakar, K.A.: A review of congestion control algorithm for event-driven safety messages in vehicular networks. Int. J. Comput. Sci. Issues **8**(5), 49–53 (2011)
10. Seredynski, M., Arnould, G., Khadraoui, D.: The emerging applications of intelligent vehicular networks for traffic efficiency. In: Proceedings of the Third ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, pp. 101–108. ACM (2013)
11. El-Sersy, H., El-Sayed, A.: Survey of Traffic Congestion Detection Using VANET. Foundation of Computer Science FCS, New York, USA, vol. 1, no. 4, Mar 2015
12. Watfa, M. (ed.): Advances in Vehicular Ad-Hoc Networks: Developments and Challenges. IGI Global (2010)
13. Darwish, T., Bakar, K.A.: Traffic density estimation in vehicular ad hoc networks: a review. Ad Hoc Netw. **24**, 337–351 (2015)
14. Yang, Y., et al.: An eMBMS based congestion control scheme in cellular-VANET heterogeneous networks. In: 2014 IEEE 17th International Conference on Intelligent Transportation Systems (ITSC). IEEE (2014)
15. Sepulcre, M., et al.: Congestion and awareness control in cooperative vehicular systems. Proc. IEEE **99**, 1260–1279 (2011)
16. Silva, A.P., Burleigh, S., Hirata, C.M., Obraczka, K.: A survey on congestion control for delay and disruption tolerant networks. Ad Hoc Netw. **25**, 480–494 (2015)
17. Wischhof, L., Rohling, H.: Congestion control in vehicular ad hoc networks. In: IEEE International Conference on Vehicular Electronics and Safety, pp. 58–63. IEEE (2005)
18. Kolte, S.R., Madnkar, M.S.: A design approach of congestion control for safety critical message transmission in VANET. In: 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), pp. 298–301. IEEE (2014)
19. Koti, R.B., Mahabaleshwar, S.K.: Multi agent based congestion control in VANETs. Int. J. Future Comput. Commun. 3(2) (2014)
20. Taherkhani, N., Pierre, S.: Improving dynamic and distributed congestion control in vehicular ad hoc networks. Ad Hoc Netw. (2015)
21. Zang, Y., et al.: Congestion control in wireless networks for vehicular safety applications. In: Proceedings of the 8th European Wireless Conference, vol. 7 (2007)
22. He, J., Chen, H.C., et al.: Adaptive congestion control for DSRC vehicle networks. IEEE Commun. Lett. **14**(2) (2010)
23. Taherkhani, N., Pierre, S.: Congestion control in vehicular ad hoc networks using meta-heuristic techniques. In: Proceedings of the Second ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, pp. 47–54. ACM (2012)
24. Bouassida, M.S., Shawky, M.: On the congestion control within VANET. In: Wireless Days, WD'08. 1st IFIP, pp. 1–5. IEEE (2008)

25. Darus, M.Y., Bakar, K.A.: Congestion control algorithm in VANETs. World Appl. Sci. J. **21** (7), 1057–1061 (2013)
26. Lakas, A., Chaqfeh, M.: A novel method for reducing road traffic congestion using vehicular communication. In: Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, pp. 16–20. ACM (2010)
27. Nasiriani, N., Fallah, Y.P., Krishnan, H.: Fairness and Stability Analysis of Congestion Control Schemes in Vehicular Ad-hoc Networks (2012). arXiv preprint arXiv:1206.0323
28. Qureshi, K.N., Abdullah, A.H., Anwar, R.W.: Congestion control scheduling scheme for vehicular networks. In: 2014 International Conference on Information Technology and Multimedia (ICIMU), pp. 55–59. IEEE (2014)
29. Yuan, Q., et al. A traffic congestion detection and information dissemination scheme for urban expressways using vehicular networks. Transp. Res. Part C Emerg. Technol. **47**, 114–127 (2014)
30. Sepulcre, M., et al.: Application-based congestion control policy for the communication channel in VANETs. IEEE Commun. Lett. 14 (10), 951–953 (2010)

Mathematical Model for Wireless Sensor Network with Two Latent Periods

Rudra Pratap Ojha, Pramod Kumar Srivastava and Goutam Sanyal

Abstract In modern digital era, data is one of the important aspects and sensor node is one of the excellent devices to help in collecting data from any type of terrain but security is one of the issues in collection of data. To consider an epidemic SE_1E_2IR model, where (S)—Susceptible, (E_1)—Exposed category of 1, E_2—Exposed category of 2, (I)—Infective, (R)—Recovered for the transmission of worm in wireless sensor network with two latent categories is formulated. In the present model, we think the trait which creates the difference in worms spreading does not evident itself as a difference in susceptibility; hence, it has only one susceptible state. As per our assumption, the susceptible class enters in E_1 and E_2 with rate p and q where $(p + q = 1)$, respectively. In the digital world, infection less wireless nodes exist without any inactivity. A more infected node will be cured by the higher probability as it normally suffered from a remarkable performance degradation/breakdown. The dynamic study of behavior is evaluated by threshold valued R_0 in the condition when virus and worm are in worm-free equilibrium, if the basic reproduction number R_0 value is ≤ 1, then infection in the nodes vanish; hence, worms dies out. Also, we show that individuals spent different average amount of time in different states. Simulation results are used for validation.

Keywords Wireless sensor network · Basic reproduction number · Equilibrium · Epidemic model · Latent period

R.P. Ojha (✉) · P.K. Srivastava
Galgotias College of Engineering & Technology, Greater Noida, India
e-mail: rpojha@gmail.com

G. Sanyal
National Institute of Technology, Durgapur, India

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_50

1 Introduction

In current time, wireless sensor network is one of the most important areas of attention due to its structure, this is a collaborative and self-organized [1] network and it can be used in any type of terrain [2]. There is numerous application of wireless sensor network like disaster management, intrusion detection, healthcare [3, 4], etc. Sensor node is a type of device which has limited resources like memory, energy, CPU, and coverage range which is used to collect data from environment and sends to base station (sink). The distance between source node and sink is large so the question is that how source send the data to sink node? This can be achieved by multi-hop [5] with the help of neighbor nodes. The sensor field consists of sensor nodes which are shown in Fig. 1 where sink is denoted by black and sensor nodes are denoted by circle, all sensor nodes having the ability to collect and transmit the data to base station thru neighbor nodes ceased due to worms attack in wireless sensor network [6–9]. Some researchers proposed several mathematical models to study the dynamical behavior of worms or virus attack in computer network, attacking behavior of worms or virus shows similarity with the classical epidemic model [10–17]. However, some more researchers discuss about the reproduction number, stability of network, and worm-free equilibrium in different conditions [18–21] by the consideration of dynamical mathematical model in wireless sensor network. In wireless sensor network, yet one of the stinging subject that security which is require to be discuss in the research sphere.

The present paper describes the two different exposed categories of worms transmit in wireless sensor network. Different types of worms are available in the digital environment, and they do not require any human intervention or infrastructure network for transmission. They have capability to transmit directly from device to device through wireless technology, for example, as Bluetooth or Wi-Fi. Wireless devices are targeted by malicious signals, for example, Cabir worm and Mabir worm and spreading behavior of these worms are epidemic in nature [22]. Here, assume that nodes collapse or crash due to the problem of hardware or software when worm attack at the nodes. Initially, it assumes that all nodes are

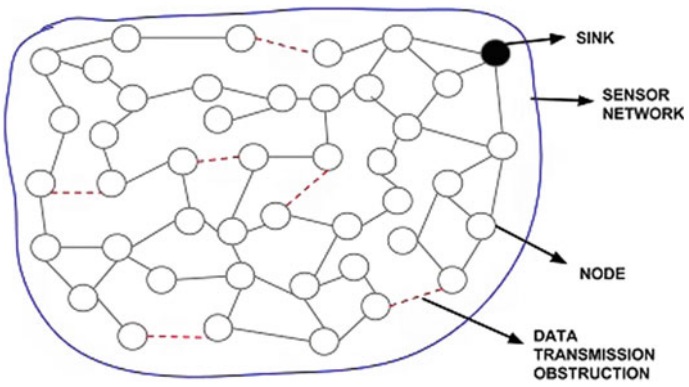


Fig. 1 Wireless sensor network field

susceptible toward worms or virus attack. When nodes get infectious performance of sensor nodes degraded. In this model, there are two latent periods, and it is found that which worms take how much time to become infectious. It is found that average amount of time spend in E_i subclass defined by $1/(\lambda_i + \sigma)$ [23]. Among two exposed subclass to find which categories latent period is less that nodes are send to sleep mode immediately because it becomes infectious quickly and run antivirus to recover from infection or may be removed from network and those nodes are of large latent periods take more time to become infectious so it may be in active state. To minimize worm attack overhead and increase the lifetime of sensor network nodes, it is required to take decision which nodes will work in which mode like active or sleep mode.

This paper is organized as follows: Sect. 2 discusses model formulation; Sect. 3, verification of local stability and existence of positive equilibrium; Sect. 4, stability of worm-free equilibrium stage; Sect. 5, simulation and result ; and Sect. 6, conclusion of paper and its future work.

2 Model Formulation

Different subclass of sensor nodes at any time t are susceptible $S(t)$, infected class of short latent period: $E_1(t)$, infected class of long latent period: $E_2(t)$, infective $I(t)$ and recovered $R(t)$ of total size $N(t)$, i.e., $N = S + E_1 + E_2 + I + R$ for any time $t \geq 0$.

Figure 2 describes the dynamical transfer of subclass. The SE_1E_2IR model is given by:

$$\left.\begin{aligned} \dot{S} &= b - \beta SI - \sigma S, \\ \dot{E}_1 &= p\beta SI - (\lambda_1 + \sigma)E_1, \\ \dot{E}_2 &= q\beta SI - (\lambda_2 + \sigma)E_2 \\ \dot{I} &= \lambda_1 E_1 + \lambda_2 E_2 \gamma - (\gamma + \sigma)I, \\ \dot{R} &= \gamma I - \sigma R \end{aligned}\right\} \tag{2.1}$$

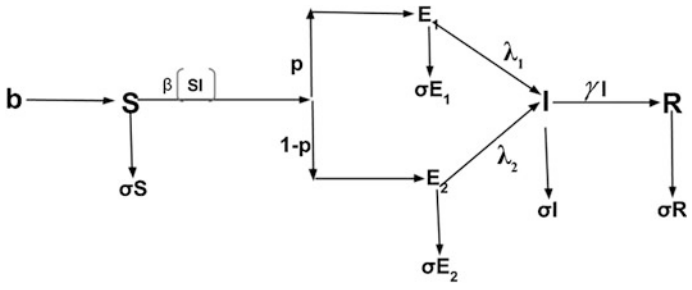


Fig. 2 Schematic diagram for the flow of worms in wireless sensor network

where b is the constant recruitment to susceptible, β is rate at which susceptible class becomes infected, p is the amount from S to E_1 and q is the amount from S to E_2, λ_1, λ_2 ($\lambda_1 > \lambda_2$) is the rate of leaving the infectious state, respectively, and σ is per capita death rate. Clearly, the above first four equations of (2.1) are independent of R, so we will discuss the reduced system in the domain $\Gamma = \{(S, E_1, E_2, I) \in \Re^4_+\}$. It can be verified that Γ is positively invariant for all t greater than or equal to zero.

3 Local Stability and Existence of Positive Equilibrium

For equilibrium points, we have
$\dot{S} = 0;\ \dot{E}_1 = 0;\ \dot{E}_2 = 0;\ \dot{I} = 0;$ and on a simple calculation, the equilibrium points are given as: $P_0 = (S, E_1, E_2, I) = (\frac{b}{\sigma}, 0, 0, 0)$ for worm-free state and $P^* = (S^*, E_1^*, E_2^*, I^*)$ for endemic state, with,

$$S^* = \frac{b}{\sigma R_0}, \quad E_1^* = \frac{pb}{(\lambda_1 + \sigma)}\left(\frac{R_0 - 1}{R_0}\right),$$
$$E_2^* = \frac{(1-p)b}{(\lambda_2 + \sigma)}\left(\frac{R_0 - 1}{R_0}\right), \quad I^* = \frac{\sigma}{\beta}(R_0 - 1),$$

where R_0 [24, 25] is the basic reproduction number given by

$$R_0 = \frac{\beta b}{\sigma(\gamma + \sigma)}\left[\frac{p\lambda_1}{(\lambda_1 + \sigma)} + \frac{q\lambda_2}{(\lambda_2 + \sigma)}\right], \quad p + q = 1$$

It is clear that P^* exist and unique if and only if R_0 greater than one.

4 Stability of the Worm-Free Equilibrium Stage

Theorem 1 *The system* (2.1) *is locally asymptotically stable if its all eigenvalues are less than zero at worm-free equilibrium* P_0.

Proof The Jacobian matrix at worm-free equilibrium point P_0 is

$$J = \begin{pmatrix} -\sigma & 0 & 0 & -\frac{\beta b}{\sigma} \\ 0 & -(\lambda_1 + \sigma) & 0 & \frac{p\beta b}{\sigma} \\ 0 & 0 & -(\lambda_2 + \sigma) & \frac{(1-p)\beta b}{\sigma} \\ 0 & \lambda_1 & \lambda_2 & -(\gamma + \sigma) \end{pmatrix} \tag{4.1}$$

Eigenvalues of (4.1) are: $\omega_1 = -\sigma, \omega_2 = -(\lambda_1 + \sigma), \omega_3 = -(\lambda_2 + \sigma), \omega_4 = -(\gamma + \sigma)$. It is clear that $\omega_1 < 0, \omega_2 < 0, \omega_3 < 0, \omega_4 < 0$; therefore, the system is locally asymptotically stable at worm-free equilibrium point P_0.

Theorem 2 *If R_0 is less than or equal to one, the worm-free equilibrium is the only equilibrium of the system (2.1) is globally asymptotically stable.*

Proof A suitable Lyapunov function L to establish the global stability of the worm-free equilibrium is defined as:

$$L = \lambda_1(\lambda_2 + \sigma)E_1 + \lambda_2(\lambda_1 + \sigma)E_2 + (\lambda_2 + \sigma)(\lambda_1 + \sigma)I$$

The derivative of Lyapunov function L with respect to time t, we get

$$\begin{aligned}\dot{L} =& \lambda_1(\lambda_2 + \sigma)\dot{E}_1 + \lambda_2(\lambda_1 + \sigma)\dot{E}_2 + (\lambda_2 + \sigma)(\lambda_1 + \sigma)\dot{I} \\ =& \lambda_1(\lambda_2 + \sigma)(p\beta SI - (\lambda_1 + \sigma)E_1) + \lambda_2(\lambda_1 + \sigma)((1-p)\beta SI - (\lambda_2 + \sigma)E_2) \\ &+ (\lambda_2 + \sigma)(\lambda_1 + \sigma)(\lambda_1 E_1 + \lambda_2 E_2\gamma - (\gamma + \sigma)I) \\ =& (\lambda_2 + \sigma)(\lambda_1 + \sigma)(\gamma + \sigma)(R_0 - 1)I\end{aligned}$$

If $R_0 \leq 1$, then $\dot{L} \leq 0$ holds. Furthermore, $\dot{L} \leq 0$ if $I = 0$. Therefore, the largest invariant set in $\left\{(S, E_1, E_2, I) \in \Gamma : \dot{L} \leq 0\right\}$ is the singleton set P_0. Hence, the global stability of P_0 when $R_0 \leq 1$ follows from LaSalle's invariance principle [26].

5 Simulation and Result

See Figs. 3, 4, and 5.

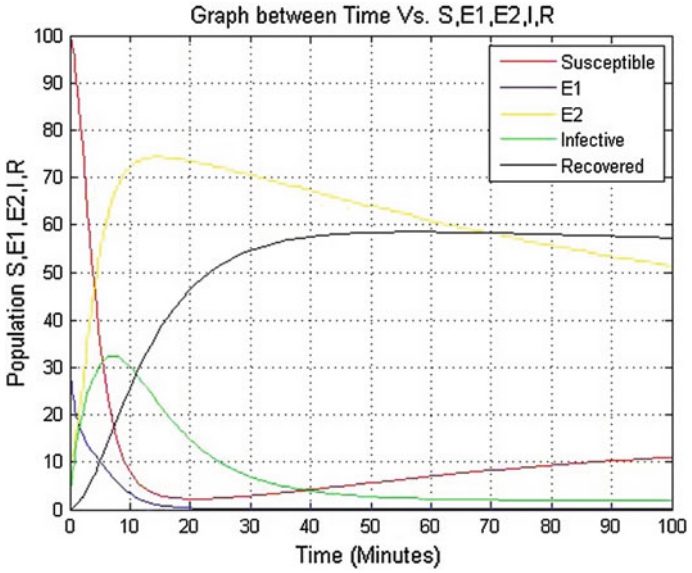


Fig. 3 Dynamical demeanor of the system for different classes when $b = 0.32$; $\sigma = 0.004$; $\beta = 0.01$; $p = 0.3$; $q = 0.7$; $\lambda_1 = 0.476$; $\lambda_2 = 0.0026$; $\gamma = 0.1$

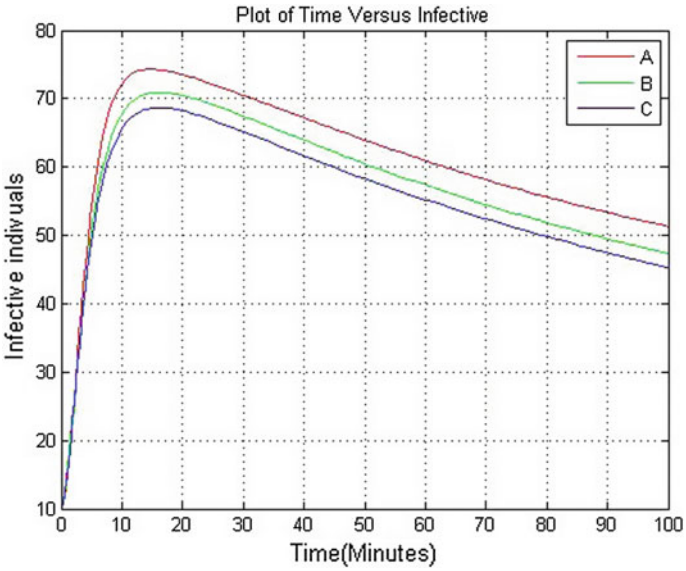


Fig. 4 Dynamical demeanor of infected class with respect to time for **a** $b = 0.32$; $\sigma = 0.004$; $\beta = 0.01$; $p = 0.3$; $q = 0.7$; $\lambda_1 = 0.476$; $\lambda_2 = 0.0026$; $\gamma = 0.1$; **b** $b = 0.32$; $\sigma = 0.004$; $\beta = 0.01$; $p = 0.3$; $q = 0.7$; $\lambda_1 = 0.479$; $\lambda_2 = 0.0028$; $\gamma = 0.18$; **c** $b = 0.32$; $\sigma = 0.004$; $\beta = 0.01$; $p = 0.3$; $q = 0.7$; $\lambda_1 = 0.51$; $\lambda_2 = 0.003$; $\gamma = 0.22$

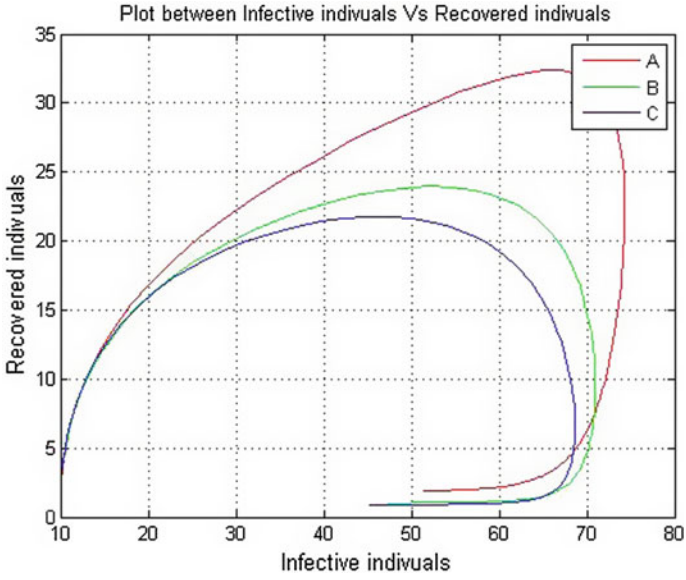


Fig. 5 Dynamical demeanor of recovered class versus infectious class with respect to time for **a** $b = 0.32$; $\sigma = 0.004$; $\beta = 0.01$; $p = 0.3$; $q = 0.7$; $\lambda_1 = 0.476$; $\lambda_2 = 0.0026$; $\gamma = 0.1$; **b** $b = 0.32$; $\sigma = 0.004$; $\beta = 0.01$; $p = 0.3$; $q = 0.7$; $\lambda_1 = 0.476$; $\lambda_2 = 0.0026$; $\gamma = 0.18$; **c** $b = 0.32$; $\sigma = 0.004$; $\beta = 0.01$; $p = 0.3$; $q = 0.7$; $\lambda_1 = 0.476$; $\lambda_2 = 0.0026$; $\gamma = 0.22$

6 Conclusion

Mathematical model has become an important tool for analyzing the spread and control of worms in wireless sensor network. A distinguished feature of SE_1E_2IR model considered the different categories of latent periods. We derive an expression for basic reproduction number R_0. From R_0, it is clear that an infected category of short latent period E_1 spent an average amount of time $\frac{\lambda_1}{(\lambda_1+\sigma)(\gamma+\sigma)}$ and infected category of long period E_2 spend an average amount of time $\frac{\lambda_2}{(\lambda_2+\sigma)(\gamma+\sigma)}$, respectively, in infectious state. Analytical result shows that if $R_0 \leq 1$ the worm-free equilibrium P_0 is locally and globally asymptotically stable in Γ and worms can be eliminated from the wireless sensor network, and also we observe that when recovery rate γ is high then individual spent less time in infectious state, so recovery becomes very fast and system will be stable for long time, and this is shown by simulation also. However, the asymptotic stability for endemic equilibrium point requires more research.

References

1. Li, Y., Thai, M., Wu, W. (eds.): Wireless Sensor Networks and Applications Signals and Communication Technology. Springer (2008)
2. Siva Ram Murthy, C., Manoj, B.: Ad Hoc Wireless Networks: Architectures and Protocols Prentice Hall Communications Engineering and Emerging Technologies Series. Prentice Hall PTR (2004)
3. Britton, C., Warmack, R., Smith, S., Oden, P., Brown, G., Bryan, W., Clonts, L., Duncan, M., Emery, M., Ericson, M., Hu, Z., Jones, R., Moore, M., Moore, J., Rochelle, J., Threatt, T., Thundat, T., Turner, G., Wintenberg, A.: Mems sensors and wireless telemetry for distributed systems. In: Varadan, V., McWhorter, P., Singer, R., Vellekoop, M. (eds.) Proceedings of SPIE: Smart Structures and Materials 1998: Smart Electronics and MEMs, pp. 112–123 (1998)
4. Lenin, R.B., Ramaswamy, S.: Performance Analysis of Wireless Sensor Network Using Queuing Network, Department of Mathematics, Technical Report, University of Central Arkansas Conway (2013)
5. Lai, W.K., Fan, C.S., Lin, L.Y.: Arranging cluster sizes and transmission ranges for wireless sensor networks. Inf. Sci. **183**, 117–131 (2012) (Elsevier)
6. De, P., Das, S.K.: Epidemic Models, algorithms and protocols in wireless sensor and ad-hoc networks. Handbook on Wireless Sensor Networks. Wiley, Hoboken (2007)
7. Tang, S., Mark, B.L.: Analysis of virus spread in wireless sensor networks: An epidemic model, In: 7th International workshop on design of reliable communication networks, pp. 86–91 (2009)
8. Di Pietro, R., Martinelli, F., Verde, N.V.: Introducing epidemic models for data survivability in unattended wireless sensor networks. In: The 2nd IEEE International Workshop on Data Security and Privacy in wireless Networks (D-SPAN'11)
9. Tang, S.: A modified SI epidemic model for combating virus spread in wireless sensor networks. Int. J. Wirel. Inf. Netw. **18**, 319–326 (2011)

10. Kephart, J.O., White, S.R.: Measuring and modeling computer virus prevalence. In: IEEE Computer Security Symposium on Research in Security and Privacy, pp. 2–15. IEEE Press, New York (1993)
11. Kephart, J.O., White, S.R.: Directed-graph epidemiological models of computer viruses. In: IEEE Symposium on Security and Privacy, pp. 343–361 (1991)
12. Yang, L.X., Yang, X.F., Wen, L.S., Liu, J.M.: A novel computer virus propagation model and its dynamics. Int. J. Comput. Math. **89**, 2307–2314 (2012)
13. Mishra, B.K., Pandey, S.K.: Dynamic model of worms with vertical transmission in computer network. Appl. Math. Comput. **217**, 8438–8446 (2011)
14. Yang, L.X., Yang, X.F.: Propagation behavior of virus codes in the situation that infected computers are connected to the Internet with positive probability. Discrete Dyn. Nat. Soc. **2012** (2012) (Article ID 693695)
15. Mishra, B.K., Keshri, N.: Mathematical model on the transmission of worms in wireless sensor network. Appl. Math. Model. **37**(6), 4103–4111 (2013)
16. Mishra, B.K., Pandey, S.K.: Dynamic model of worm propagation in computer network. Appl. Math. Model. **38**, 2173–2179 (2014)
17. Gan, C.Q., Yang, X.F., Liu, W.P., Zhu, Q.Y.: A propagation model of computer virus with nonlinear vaccination probability. Commun. Nonlinear Sci. Numer. Simul. **19**, 92–100 (2014)
18. Wang, F., Zhang, Y., Wang, C., Ma, J., Moon, S.: Stability analysis of a SEIQV epidemic model for rapid spreading worms. Comput. Secur. **29**, 410–418 (2010) (Elsevier)
19. Zhang, Z., Si, F.: Dynamics of a delayed SEIRS-V model on the transmission of worms in a wireless sensor network. Adv. Differ. Equ. **2014**, 295 (2014). doi:10.1186/1687-1847-2014-295
20. Keshri, N., Mishra, B.K.: Two time delay dynamic model on the transmission of alicious signals in wireless sensor Network. Chaos Solitons Fractals **68**, 151–158 (2014). doi:10.1016/j.chaos.2014.08.006
21. Mishra, B.K., Srivastava, S.K., Mishra, B.K.: A quarantine model on the spreading behavior of worms in wireless sensor network. Trans. IoT Cloud Comput. **2**(1), 1–12 (2014)
22. Szor, P.: The Art of Computer Virus Research and Defense. Symantec Press (2006)
23. Diekmann, O., Heesterbeek, J.A.P.: 2000 Mathematical Epidemiology of Infectious Diseases: Model Building, Analysis and Interpretation. Wiley, Chichester, U.K
24. Diekmann, O., Heesterbeek, J.A.P., Metz, J.A.J.: On the definition and the computation of the basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations. J. Math. Biol. **28**(4), 365–382 (1990). doi:10.1007/BF00178324
25. Van Den Driessche, P., Watmough, J.: Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission. Math. Biosci. **180** (1–2), 29–48 (2002). doi:10.1016/S0025-5564(02)00108-6
26. LaSalle, J.P.: The Stability of Dynamical System. SIAM, Philadelphia (1976)

A Review of Underwater Wireless Sensor Network Routing Protocols and Challenges

Subrata Sahana, Karan Singh, Rajesh Kumar and Sanjoy Das

Abstract The underwater wireless sensor networks is a rapidly growing area of research as it monitors and collects data for environmental studies of seismic monitoring, flocks of underwater robots, equipment monitoring and control, pollution monitoring applications. The main purpose is to create a new set of routing protocols optimized various factors from the major differences in the underwater wireless sensor network and terrestrial network. Energy efficiency plays an important role in underwater wireless communication as underwater sensor nodes are powered by batteries which are difficult to replace or charge once the node is deployed. This paper surveys various routing techniques. Modern research trends focus to improve the performance on various issues like propagation delay, mobility, limited link capacity and limited battery power on the sea ground and sea surface.

Keywords UWSN · Routing protocols · Energy efficiency · Underwater communication

S. Sahana (✉) · R. Kumar · S. Das
School of Computing Science and Engineering, Galgotias University, Greater Noida, India
e-mail: subrata.sahana@galgotiasuniversity.edu.in

R. Kumar
e-mail: rajesh.kumar@galgotiasuniversity.edu.in

S. Das
e-mail: sanjoy.das@galgotiasuniversity.edu.in

K. Singh
School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India
e-mail: karancs12@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_51

1 Introduction

Underwater wireless sensor networks (UWSNs) consist of a variable number of sensor node and autonomous vehicles that are deployed to perform collaborative task for various applications. To achieve this objective, sensors and autonomous vehicles are placed in an autonomous network which can acquire to the characteristics of the ocean environment [1].

Wireless communication in underwater is one of the enabling technologies for the development of future ocean-observation systems and monitoring. Applications of underwater sensing range from military purposes to pollution monitoring and include environment monitoring, pollution control, climate status and prediction of natural disasters. It improves the search and survey missions, and study of marine life.

Routing in underwater wireless sensor networks plays important role due to the difference between the characteristics of the acoustic communication to that of the radio-magnetic waves. Various protocols have been designed to satisfy the different requirements of the acoustic communications such as delay efficiency, bandwidth efficiency, reliability, cost efficiency, delivery ratio. But the major requirement that has been highlighted is energy efficiency. Energy efficiency depends on many metrics which should be considered while designing the protocol. We focus basically at helping the protocol designers in providing an overview of the existing protocols and propose an optimized routing scheme to improve performance.

Nowadays, people have proposed and developed some routing protocols. Underwater wireless sensor networks can be divided into deep water and shallow water. Underwater wireless sensor networks routing protocols further can be classified based on communication as acoustic communication, radio wave communication and optical communication. In underwater acoustic sensor networks, there are number of corresponding protocols, for example, VBF [2], MURAO [3], DDD algorithm [4], Void-Aware Pressure Routing [5], GPS-free Routing Protocol [6] and DBMR [7].

2 Related Work

Several researchers worked on routing of underwater wireless sensor networks. Studies have continued significantly to find protocols to support the development in underwater. However, most of the protocols are not implemented so far. The major constraints are speed, propagation delay, limited bandwidth and energy. The purpose to provide a suitable routing protocol can improve a wide communication such as terrestrial network. Routing protocols are classified based on location, path, energy efficient, multi-level and GPS-free. Major work in energy as battery life is a major challenge [1, 8] in underwater networks.

3 Characteristics of Channels

Acoustic channels [9] are well in deep waters and can propagate a long distance. The communication speed is slow and it works in very low frequency. The speed of the sound in water varies on temperature and pressure of water.

Electromagnetic medium [9] requires higher frequencies. It works on large bandwidths (∼MHz). EM works in very short range. The speed of EM is faster than acoustic channels. It reduces propagation delay significantly. EM is quite free from tidal noise and noise from surface area.

Light medium [9] works properly in clear and still water. Optical waves signal is absorbed when depth of water increases as pressure increases. Highly cost-effective and it can send large data bits as well. It works for short range and performance significant in shallow water (Table 1).

4 Differences in Underwater Sensor Network and Terrestrial Networks

Underwater sensor network is very challenging issue over terrestrial networks. We have identified some crucial parameters mentioned in Table 2. These parameters are very essential while designing routing protocols for both the network scenarios.

Table 1 Comparative study of various acoustic mediums

Parameters	Acoustic	Electromagnetic	Light
Speed	Low	High	High
Depth	Deep water	Deep and shallow water	Shallow water
Bandwidth	Less	>Acoustic	>Electromagnetic
Distance	Long distance	Short distance	Very short distance
Frequency	Less	>Acoustic	>Electromagnetic

Table 2 Differences in underwater communication and terrestrial networks

Parameters	Terrestrial sensor networks	Underwater sensor network
Cost	Terrestrial sensor networks will be cheaper and cheaper with the time	UWSNs are expensive
Deployment	Terrestrial SNs are densely deployed	UWSNs are generally more sparse
Power	Not a major issue in terrestrial	UWSNs are higher
Memory	Terrestrial sensors have less capacity	Sensors require large memory capacity
Bandwidth	More bandwidth available	Poor available bandwidth
Path loss	Not frequent, easy path discover	Attenuation provoked by absorption due to conversion of acoustic energy into heat
Noise	Not affected as EM has less impact	Man-made noise, ambient noise
Delay	Less	5 × radio frequency (RF) ground

With respect to terrestrial networks, underwater sensor network required significant attentions in all the parameters while designing a routing protocol. Researchers working in this domain required to consider these parameters for better design and implement of a routing protocol.

5 Routing Protocols

5.1 Vector-Based Forwarding (VBF)

Vector-based forwarding [2] is a routing protocol which needs location information rather than state information. It reduces the energy consumption as interleaved paths are used for routing. It is based on self-adaptive algorithm dropped low benefit packets. It calculates the path based on relative position and the angle of arrival.

5.2 Distributed Minimum-Cost Clustering Protocol (DDD)

In this protocol [4], collector nodes are defined as underwater vehicles. Underwater vehicles admit its presence by sending beacon messages. Underwater vehicles collect the data when it reaches to the sink and reduce the cost of the networks. Number of underwater vehicles can be reduced but it increases collision and overhead.

5.3 Energy Optimized Path Unaware Layered Routing Protocol (E-PULRP)

E-PULRP [4] does not require location information. It is based on formation of sphere around sink. Here, packets are transmitted through multiple hops and energy can be reduced if number of layer is increased up to a significant level. Energy consumption depends on transmission and sphere formation.

5.4 A Mobile Delay-Tolerant Approach (MCCP)

A distributed minimum-cost clustering protocol (MCCP) [10] is proposed cluster head formation based on the assumption. So, energy requirements are comparatively less in cluster head selection. Total energy requirement = residual energy of the cluster head + total energy consumption of the cluster + cluster members and

the distance of the cluster head to the sink. It requires more energy efficiency in comparison with ad hoc networks.

5.5 DBMR Protocol

Depth-based multi-hop routing [7] can work in both multicast and unicast mode. This protocol gives better performance in sparse area. The performance of DBMR is quite impressive in terms of packet delivery and delay. Communication cost is also reduced in this protocol. This protocol is working on neighbour-group and distant node selection. Here, energy is a major issue but compared to DBR, it gives better performance [11]. In this protocol, each and every node is omni-directional. Nodes are deployed randomly and then update the routing table accordingly.

5.6 GPS-Free Routing Protocol

Distributed Underwater Clustering Scheme (DUCS) [6] is based on self-organizing protocol. It follows distributed algorithm. In this protocol, cluster head formation takes place in set up phase. Non-cluster nodes send packet to their heads in a single hop. Cluster head sends packets via multi-hop to the other cluster heads. Cluster head is randomly changed after a certain time to optimize energy consumption. Network operation is performed in steady state. This protocol gives satisfactory results in deep water. It increases very high packet delivery ratio as well as throughput for UWSNs.

5.7 Void-Aware Pressure Routing

Void-aware pressure routing [5] is a simple and robust based on subset of forwarders. It follows two strategies: efficient greedy forwarding and dead-end recovery methods. In these protocols, nodes send packets towards next-hop direction towards the surface. This protocol is very robust to network dynamics such as node mobility and failure. VAPR does not require any recovery path maintenance during recovery. VAPR is composed of two major components, namely enhanced beaconing and opportunistic directional data forwarding.

5.8 Multi-level Routing Protocol

The experiment results show that MURAO [3] achieves much higher delivery rates and delay is very less. It based on multi-level distributed Q-learning scheme. It can

Table 3 Comparative study of various routing protocols [12–14]

Routing protocols	Advantages	Disadvantages
VBF	Energy efficient, data delivery high	Packet delivery low, more delay
E-PULRP	Location based, energy efficient	More delay
DDD	Energy efficient, bandwidth fair	Packet delivery low, cost high Overall performance low
MCCP	Robustness, energy consumption	Packet delivery low, more delay
DBMR	Packet delivery ratio high	Not energy efficient
GPS-free	Packet delivery high, scalable	Deliver ratio less, not reliable
VAPR	Simple and robust, excellent performance, delivery ratio high, delay efficient	Not energy efficient More cost
MURAO	Higher delivery rates Delay is very less	Data delivery rate low, more delay

be deployed in long range in acoustic communication. This protocol consists of cluster formation and update, inter-cluster routing, intra-cluster routing and inter-layer interaction. MURAO adopted dynamic change in networks (Table 3).

6 Conclusions

In this paper, we have explained various routing protocols depicted in underwater wireless sensor networks theoretically. Basic purpose of various routing protocols is to face challenges in UWSN. The protocols are designed to minimize energy as battery life of sensor node is limited. On the other side, keep in mind various application domains for improving delivery speed with minimum packet loss. We have shown two different scenarios: deep and shallow water. Routing protocols depend on various communication medium as bandwidth is a major issue in underwater wireless sensor networks. We have discussed comparative study on various communication mediums. It will be helpful to the researchers for limitations in various application domains. Further, we have given detailed major challenges in underwater wireless sensor networks compared with terrestrial networks.

7 Future Scope

Clustering techniques improve throughput and reliability while minimizing power consumption. Energy harvesting can enhance routing in underwater wireless sensor networks. For long distance, energy harvesting will give a secure and reliable solution towards variety of application such as disaster and pollution control. Optimized path selection towards destination can maximize battery life and speed up communication.

References

1. Akyildiz, I.F., Pompili, D., Melodia, T.: Underwater acoustic sensor networks: research challenges. Ad Hoc Netw. J. **3**(3), 257–279 (2005) (Elsevier)
2. Xie, P., Cui, J.-H., Lao, L.: VBF: vector-based forwarding protocol for underwater sensor networks. In: Networking technologies, services, and protocols; performance of computer and communication networks; mobile and wireless communications systems, pp. 1216–1221. Springer, Berlin/Heidelberg (2006)
3. Hu, T., Fei, Y.: MURAO: A multi-level routing protocol for acoustic-optical hybrid underwater wireless sensor networks. In: 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), pp. 218–226, 18–21 June 2012
4. Pu, W., Cheng, L., Jun, Z.: Distributed minimum-cost clustering protocol for under- water sensor networks (UWSNs). In: Proceedings of the IEEE International Conference on Communications, ICC'07 (2007)
5. Noh, Y., Lee, U., Wang, P., Choi, B.S.C., Gerla, M.: VAPR: void-aware pressure routing for underwater sensor networks. IEEE Trans. Mob. Comput. **12**(5) (2013)
6. Domingo, M.C., Prior, R.: Design and analysis of a gps free routing protocol for underwater wireless sensor networks in deep water. In: SENSORCOMM, Washington, DC, USA, pp. 215–220 (2007)
7. Guangzhong, L., Zhibin, L.: Depth-based multi-hop routing protocol for underwater sensor network. In: 2010 2nd International Conference on Industrial Mechatronics and Automation (ICIMA), vol. 2, pp. 268–270, 30–31 May 2010
8. Heidemann, J., Ye, W., Wills, J., Syed, A., Li, Y.: Research challenges and applications for underwater sensor networking. In: Proceedings of IEEE Wireless Communications and Networking Conference, 2006
9. Gkikopouli, A., Nikolakopoulos, G., Manesis, S.: A survey on underwater wireless sensor networks and applications. In: 2012 20th Mediterranean Conference on Control & Automation (MED) Barcelona, Spain, July 3–6, 2012
10. Gopi, S., Kannan, G., Desai, U.B., Merchant, S.N.: Energy optimized path unaware layered routing protocol for underwater sensor networks. In: IEEE Global Communication Conference, Globecom-2008, pp. 1–6, December 2008
11. Chakraborty, D.: A distant node based multicast routing protocol for sparse area vehicle to vehicle communication. IOSR J. Comput. Eng. (IOSRJCE) **2**(3), 49–55. ISSN 2278-0661 (2012)
12. Jan, K.U., Jan, Z.: Survey on routing protocols for under water sensor networks. IOSR J. Comput. Eng. (IOSR-JCE) **16**(1), 44–46 (2014). Ver. VI, e-ISSN 2278-0661, p-ISSN 2278-8727

13. Sharma, A., Abdul Gaffar, H.: A survey on routing protocols for underwater sensor networks. Int. J. Comput. Sci. Commun. Netw. **2**(1), 74–82
14. Ayaz, M., Baig, I., Abdullah, A., Faye, I.: A survey on routing techniques in underwater wireless sensor networks. J. Netw. Comput. Appl. **34**(6), 1908–1927 (2011)

A Multi-metric-Based Algorithm for Cluster Head Selection in Multi-hop Ad Hoc Network

Jay Prakash, Rakesh Kumar, Sarvesh Kumar and J.P. Saini

Abstract Clustering technique finds wide applicability in wireless networks. Cluster structures enhance resource reuse as well as increases system capacity. Clustering is a desirable task in MANET if the size of multi-hop wireless network becomes too large. In the existing work, number of cluster formation depends on the radius of cluster chosen in a scenario. But here, we propose a new approach in cluster head selection within a cluster. Here, we consider three parameters, i.e. number of node neighbours, node lifetime and stability of nodes which in turn are used for selection of an appropriate cluster head. We simulated our algorithm and measured performance by considering energy consumption, throughput and control overhead as performance metrics. Our approach has been found outperforming to the existing ones.

Keywords MANET · Cluster · Cluster head · Clustering techniques

J. Prakash (✉) · R. Kumar · S. Kumar
Department of Computer Science & Engineering, Madan Mohan Malviya University of Technology, Gorakhpur, Uttar Pradesh, India
e-mail: jpr_1998@yahoo.co.in

R. Kumar
e-mail: rkiitr@gmail.com

S. Kumar
e-mail: sarvu88@gmail.com

J.P. Saini
Department of Electronics & Communication Engineering,
Bundelkhand Institute of Engineering & Technology, Jhansi, India
e-mail: jps_uptu@rediffmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_52

1 Introduction

Mobile ad hoc networks (MANET) have unprecedented worldwide attention in wireless communication technologies. MANETs, without any fixed infrastructure, allow autonomous nodes connected with wireless medium to transmit or receive data with other mobile nodes through base station. The mobile nodes have dual behaviour; they act as a router as well as computing device. In MANET design, stable structure is an important aspect having resource constraints. In some cases, mobile node requires portability because of limited battery life and high mobility. A cluster is a group of similar type of nodes based on some properties. It provides stability and energy efficient routing to the MANETs. There are so many clustering algorithms [1–10] that produce and maintain the clusters. Set of clusters form a network while each cluster has a cluster head and cluster members. A cluster head is used to connect two clusters also either in direct manner or through the gateway nodes. Work assigned to a cluster head is more than the ordinary nodes in a cluster because a cluster head carries the responsibility of transmitting data from source to the destination node. In this process of cluster head selection, cluster head must have sufficient resources for maintaining the information related to cluster member node and able to communicate with member node and also with other clusters. On the other side, to maximize the available resource utilization, we have to choose the minimum number of cluster head which can support the entire node in the network. The different types of cluster selection are based on either of the following: location of node, node mobility, number of node neighbour, battery power, artificial intelligence and weighted clustering.

The following Sect. 2 reviews related work. Section 3 presents our proposal for cluster head selection in multi-hop ad hoc network. Section 4 gives analytical model while simulation model and result analysis have been presented in Sect. 5. Finally, in Sect. 6, we give the conclusions and directions of future work.

2 Related Work

In highest degree algorithm, [11] each node calculates the degree on the basis of distance from other node. All the nodes broadcast its id to a node that present in its communication range. A node with highest degree (maximum number of neighbour) is selected as cluster head. In [12], authors have proposed Lowest ID algorithm in which every node is assign a unique id, and these nodes continuously broadcast their unique id to its neighbours for establish communication. Each node matches its ids with the neighbours, and the node with minimum id to all its neighbours is selected as the cluster head. Distributed Mobility-Adaptive Clustering (DMAC) [13] is based on weight-based clustering algorithm. In this clustering

algorithm, each node assigned a weight (a real number ≥ 0). A node with highest weight is selected as cluster head than any other of its neighbour's weight. In [14], authors proposed weighted clustering algorithm (WCA) that uses the combined weight metrics-based clustering. The algorithm considers four metrics, i.e. node degree, mobility, battery lifetime and transmission power. In this proposed work, the cluster head selection is not periodic and invoked on demand as possible and aimed to minimize the communication and computation cost. In [15], authors have proposed a cluster head selection mechanism by considering battery power and neighbour mobile node connectivity level as selection parameter. Here, author use Battery Power Matrix which contains two columns by storing battery power capacity and residual battery power for each node. Another Circular Distance Matrix (CDM) is used to represent the circular distance of neighbourhood nodes. By considering these two set of values, finally, cluster selection table is computed which in term used to select the cluster head.

3 Proposed Work

In the proposed model, we consider three matrices for cluster head selection, i.e. node neighbour, node lifetime and stability factor.

3.1 Node Neighbour

Node neighbour is an important factor for cluster head selection and can be calculated as the number of nodes surrounded by a node with one hope count distance. Find the neighbour of each node within transmission range and make the adjacency matrix, i.e. Node Neighbour Matrix (NNM) of $[n \times n]$.

Adj (NNM) = (a_{ij})
if $(e(i, j) = =$ true)
$a_{ij} = 1$
else $a_{ij} = 0$

$$\text{Normalized NN}_i = \frac{\text{node neighbour}}{\text{total no. of nodes}} \tag{1}$$

Node neighbour (NN_i) of a node is the summation of row corresponding to that node.

4 Node Lifetime

The lifetime of a node is calculated as the ratio of residual energy and drain rate. The active node that is used for many data transmission consumed more energy and have very shorten lifetime. In every **T** second, node **i** calculates the instantaneous residual energy value and corresponding estimated energy drain rate. Node lifetime is defined as:

$$L_{\mathrm{t}} = \frac{E_r}{E_{\mathrm{dr}i}} \tag{2}$$

$$\text{Avg } E_i = \frac{\sum_1^n E_i}{n} \tag{3}$$

$$\text{Normalized } L_{\mathrm{t}} = \frac{L_{\mathrm{t}}}{\text{Avg } E_i} \tag{4}$$

where $\mathbf{E_r}$ is the residual energy of node **i**, and $\mathbf{E_{dri}}$ is the energy drain rate.

$$E_r = E_{\mathrm{init}} - (R_{\mathrm{s}i}E_{\mathrm{s}i} + R_{\mathrm{d}i}E_{\mathrm{r}i} + R_{\mathrm{f}i}(E_{\mathrm{s}i} + E_{\mathrm{r}i}))$$

where

E_{init} Initial energy
$R_{\mathrm{s}i}$ Packet transmission rate for source node
$E_{\mathrm{s}i}$ Energy for source node
$R_{\mathrm{d}i}$ Packet transmission rate for receiving node
$E_{\mathrm{r}i}$ Energy for receiving node
$R_{\mathrm{f}i}$ Packet transmission rate for forwarding

Drain rate is defined as a metric for energy dissipation rate of a given node. The total energy consumption is calculated in every **T** seconds by nodes, and the drain rate is measured by exponentially averaging the value of previous and newly calculated values.

$$E_{\mathrm{dr}i} = \alpha E_{\mathrm{drold}} + (1 - \alpha)E_{\mathrm{drnew}} \tag{5}$$

$\boldsymbol{\alpha}$ is between 0 and 1 that gives higher priority for updated information. Finally, we make a Node Energy Information (NEI) matrix between n nodes and their initial energy, residual energy, drain rate, node lifetime.

4.1 Node Stability

We define the node stability in terms of relative velocity in which a node must contain higher relative velocity that said to be stable node. A node chosen to be cluster head should be a stable node to minimize the control overhead during exchange of information between nodes.

- When nodes are moving in the same direction as shown in Fig. 1, then the relative velocity is given as under
- When nodes are moving in opposite direction as shown in Fig. 2, then relative velocity is given as under.
- When the nodes coming closer at angle θ as shown in Fig. 3, then the relative velocity is calculated as given in Fig. 3.
- When the nodes moving away at angle θ as shown in Fig. 4, then the relative velocity is calculated as given in Fig. 4.

Fig. 1 Nodes moving in same direction

Rel. Vel. = $v1 + v2$

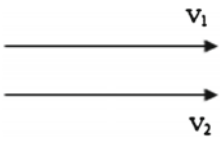


Fig. 2 Nodes moving in opposite direction

Rel. Vel. = $|v1 - v2|$

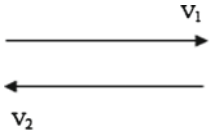


Fig. 3 Nodes coming closer at angle θ

Rel. Vel. = $\sqrt{v1^2 + v2^2}$

$\Theta = \tan^{-1}(v1/v2)$

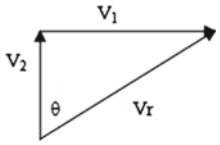
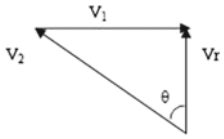


Fig. 4 Nodes moving away at angle θ

Rel. Vel. = $\sqrt{v1^2 - v2^2}$

$\Theta = \tan^{-1}(v1/v_r)$



$$\text{Mobility} = \frac{1}{\text{rel. velocity}} \tag{6}$$

After finding the relative velocity, we make the Node Mobility Matrix (NMM) of $[n \times n]$ and then calculate the Node Stability Matrix (NSM) using the formula node stability factor as

$$\text{NSF}_i = \frac{\sum_{j=0}^{n} \text{NMM}_{ij}}{\text{NN}_i} \tag{7}$$

$$\text{Avg Node vel.} = \frac{\sum_{1}^{n} v_i}{n} \tag{8}$$

$$\text{Normalized NSF}_i = \frac{\text{NSF}}{\text{Avg node vel.}} \tag{9}$$

Finally, we find above three matrixes such as Node Neighbour Matrix (NNM), Node Energy Information (NEI) and Node Stability Matrix (NSM) and get their normalized value then we calculate the combined Node Weight Matrix (NWM) between 'n' nodes and their normalized value of $[n \times 3]$ multiply with weighing factor W_1, W_2, W_3, of $[3 \times 1]$ where $W_1 + W_2 + W_3 = 1$ and node having higher weight among entire node selected as cluster head.

5 Analytical Model

5.1 Node Neighbour Matrix

In this Node Neighbour Matrix (NNM) of $[n \times n]$, $m_1, m_2 \ldots m_n$ represent N nodes, and a_{ij} is 1 if there is $e(i, j) = =$ true (a path exists b/w i and j) otherwise a_{ij} is 0.

$$\text{NNM} = \begin{array}{c|cccccc|c} & m_1 & m_2 & m_3 & m_4 & m_n & NN_i \\ m_1 & a_{11} & a_{12} & \cdot & \cdot & a_{1j} & nn_1 \\ m_2 & a_{21} & a_{22} & \cdot & \cdot & a_{2j} & nn_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ m_n & a_{i1} & a_{i2} & & & a_{ij} & nn_n \end{array}$$

5.2 Node Energy Information

In this Node Energy Information Matrix (NEI) of $[n \times 4]$, e_1, $e_2 \ldots e_n$, e_{r1}, $e_{r2} \ldots e_{rrn}$, $e_{\mathrm{dr}1}$, $e_{\mathrm{dr}2} \ldots e_{\mathrm{dr}n}$ and l_1, $l_2 \ldots l_n$ represent the initial energy, residual energy and lifetime, respectively.

$$\mathrm{NEI} = \begin{array}{c} \\ m_1 \\ m_2 \\ \cdot \\ \cdot \\ m_n \end{array} \begin{array}{c} E_i \\ e_1 \\ e_2 \\ \cdot \\ \cdot \\ e_n \end{array} \begin{array}{c} E_r \\ e_{r1} \\ e_{r2} \\ \cdot \\ \cdot \\ e_{rn} \end{array} \begin{array}{c} E_{\mathrm{dr}i} \\ e_{\mathrm{dr}1} \\ e_{\mathrm{dr}2} \\ \cdot \\ \cdot \\ e_{\mathrm{dr}n} \end{array} \begin{array}{c} L_{\mathrm{t}} \\ l_1 \\ l_2 \\ \cdot \\ \cdot \\ l_n \end{array}$$

5.3 Node Stability Matrix

In this Node Stability Matrix (NSM), v_{ij} represents the relative velocity between node i and node j that can be calculated as

$$\mathrm{NNM} = \begin{array}{c} \\ m_1 \\ m_2 \\ \cdot \\ \cdot \\ m_n \end{array} \left| \begin{array}{cccccc} m_1 & m_2 & \cdot & \cdot & m_n & \mathrm{NSF} \\ v_{11} & v_{12} & \cdot & \cdot & v_{1j} & sf_1 \\ v_{21} & v_{22} & \cdot & \cdot & v_{2j} & sf_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ v_{i1} & v_{i2} & \cdot & \cdot & v_{ij} & sf_n \end{array} \right. \qquad \mathrm{NSM} = \begin{array}{c} \\ m_1 \\ m_2 \\ \cdot \\ \cdot \\ m_n \end{array} \begin{array}{c} \mathrm{NSF} \\ sf_1 \\ sf_2 \\ \cdot \\ \cdot \\ sf_n \end{array}$$

5.4 Node Weight Matrix

Finally, we make the Node Weight Matrix (NWM) between the 'n' nodes and normalized node neighbour, normalized node lifetime and normalized node stability factor of $[n \times 3]$ multiply with weighing factor of $[3 \times 1]$ where $w_1 + w_2 + w_3 = 1$. A node with higher weight is chosen as a cluster head.

$$\mathrm{NWM} = \begin{array}{c} \\ m_1 \\ m_2 \\ \cdot \\ \cdot \\ m_n \end{array} \begin{array}{c} \mathrm{norNN}_i \\ nn_1 \\ nn_2 \\ \cdot \\ \cdot \\ nn_n \end{array} \begin{array}{c} \mathrm{norL_t} \\ nl_1 \\ nl_2 \\ \cdot \\ \cdot \\ nl_n \end{array} \begin{array}{c} \mathrm{norNSF} \\ nsf_1 \\ nsf_2 \\ \cdot \\ \cdot \\ nsf_n \end{array} \times \begin{array}{c} w_i \\ \\ w_1 \\ w_2 \\ w_3 \\ \\ \end{array} \qquad \mathrm{NWM} = \begin{array}{c} \\ m_1 \\ m_2 \\ \cdot \\ \cdot \\ m_n \end{array} \begin{array}{c} w_i \\ w_1 \\ w_2 \\ \cdot \\ \cdot \\ w_n \end{array}$$

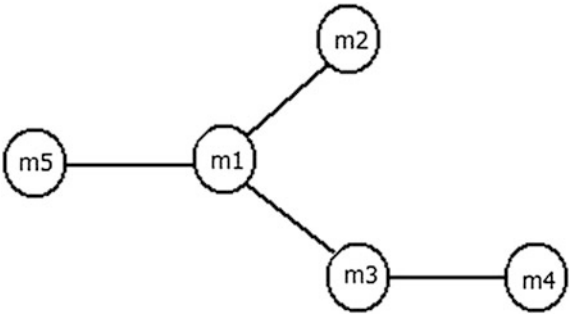


Fig. 5 Five nodes scenarios for proposed scheme

6 Explanatory Example

We take an example of five nodes m_1, m_2, m_3, m_4 and m_5 where m_2, m_3, m_4, m_5 are present in the transmission range of m_1 as shown in Fig. 5.

(i) First, we make the Node Neighbour Matrix (NNM) and calculate the node neighbour of five nodes.

$$\text{NNM} = \begin{array}{c|ccccc|c} & m_1 & m_2 & m_3 & m_4 & m_5 & \text{NN}_i \\ m_1 & 0 & 1 & 1 & 0 & 1 & 3 \\ m_2 & 1 & 0 & 0 & 0 & 0 & 1 \\ m_3 & 1 & 0 & 0 & 1 & 0 & 2 \\ m_4 & 0 & 0 & 1 & 0 & 0 & 1 \\ m_5 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}$$

(ii) Secondly, we make the Node Energy Information Matrix (NEI) between nodes and their energies and calculate lifetime L_t.

$$\text{NEI} = \begin{array}{c|cccc} & E_i & E_r & E_{dri} & L_t \\ m_1 & 1000 & 750 & 2 & 375 \\ m_2 & 1200 & 620 & 2.5 & 248 \\ m_3 & 1300 & 930 & 1.2 & 620 \\ m_4 & 900 & 720 & 0.9 & 800 \\ m_5 & 800 & 540 & 0.6 & 900 \end{array}$$

(iii) And then we make the Node Mobility Matrix (NMM) between the nodes and calculate the node stability factor.

$$\text{NNM} = \begin{array}{c|ccccc|c} & m_1 & m_2 & m_3 & m_4 & m_5 & \text{NSF} \\ m_1 & 0 & 5 & 7 & 0 & 3 & 5 \\ m_2 & 7 & 0 & 0 & 0 & 0 & 7 \\ m_3 & 3 & 0 & 0 & 2 & 0 & 2.5 \\ m_4 & 0 & 0 & 8 & 0 & 0 & 8 \\ m_5 & 6 & 0 & 0 & 0 & 0 & 6 \end{array} \qquad \text{NSM} = \begin{array}{c|c} & \text{NSF} \\ m_1 & 5 \\ m_2 & 7 \\ m_3 & 2.5 \\ m_4 & 8 \\ m_5 & 6 \end{array}$$

(iv) At last, we make the Node Weight Matrix (NWM) of [$n \times 3$] between the nodes and normalized node neighbour, normalized node lifetime and normalized node stability of [$n \times 3$] multiply with weighing factor of [3×1] $w_1 = 0.2$, $w_2 = 0.3$, $w_3 = 0.5$ where $w_1 + w_2 + w_3 = 1$.

$$\text{NWM} = \begin{array}{c} \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{array} \begin{array}{c} \text{norNN}_i \\ 0.6 \\ 0.2 \\ 0.4 \\ 0.2 \\ 0.2 \end{array} \begin{array}{c} \text{nor}L_t \\ 0.36 \\ 0.23 \\ 0.59 \\ 0.76 \\ 0.86 \end{array} \begin{array}{c} \text{norNSF} \\ 1.6 \\ 5 \\ 2.5 \\ 5 \\ 5 \end{array} \times \begin{array}{c} w_i \\ \\ 0.2 \\ 0.3 \\ 0.5 \\ \\ \end{array} \quad \text{NWM} = \begin{array}{c} \\ m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{array} \begin{array}{c} w_i \\ 1.028 \\ 2.609 \\ 1.507 \\ 2.768 \\ 2.798 \end{array}$$

From the above calculation, we find that node m_5 has the highest weight value among the entire nodes, so we make m_5 as cluster head.

7 Simulation Model and Performance Analysis

To evaluate the performance of proposed protocol with existing protocol, we have implemented these protocols in network simulator [16] version 2.34 (NS2). The simulation deployed 40 nodes randomly in the area of 1000 m × 1000 m. The IEEE 802.11 standard [17] was applied as the medium access control (MAC) layer protocol with a channel capacity of 2 mbps. The Constant Bit Rate (CBR) traffic pattern is used with a network traffic load of 4 packets/second, and the length of packet is 512 bytes. The simulation parameters are summarized in Table 1.

For evaluating the performance of proposed protocol, the metrics chosen are energy consumption, throughput and control overhead.

Table 1 Simulation parameter

Parameter	Values
Area of network	1000 m × 1000 m
Number of nodes	40
Simulation time	100 s
Transmission range	200–400 m
Routing protocol	CBRP
MAC	IEEE 802.11
Radio propagation model	Two ray ground reflection
Mobility model	Random way point

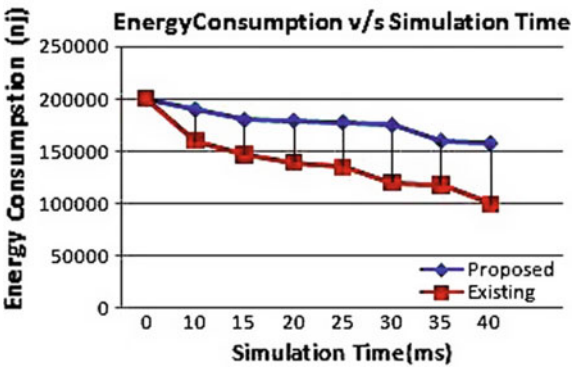


Fig. 6 Comparison for energy consumption versus simulation time

7.1 Energy Consumption

It defines as energy consumed by each node during the packet transmission between the nodes over the network. As the simulation result shown in Fig. 6 which is drawn in between energy consumption (nJ) and simulation time (ms). As shown below, initial energy for each node in multi-hop wireless network is 200,000 nJ, while it is reduced to 160,000 nJ in existing scheme and 190,000 nJ in proposed scheme after 10 ms. So we achieve 18.8% less energy consumption against existing approach.

7.2 Throughput

It is defined as the number of data packet successfully transmitted per unit time. Another performance parameter is throughput, which is considered for evaluation of performance of our scheme with respect to existing scheme and the outcome is drawn in Fig. 7. As per of the traces generated after simulation, we plotted the result by considering throughput (Kbps) on *y* axis and simulation time (ms) on *x* axis. We have found that our proposed technique has achieved 6.7% higher average throughput value.

7.3 Control Overhead

It is defined as the ratio of control packet transmitted to the number of data packet deliver. We considered control overhead as a performance parameter. Figure 8 is being plotted in between control overhead and number of nodes. We have 15.81% more overhead as compared to existing approach.

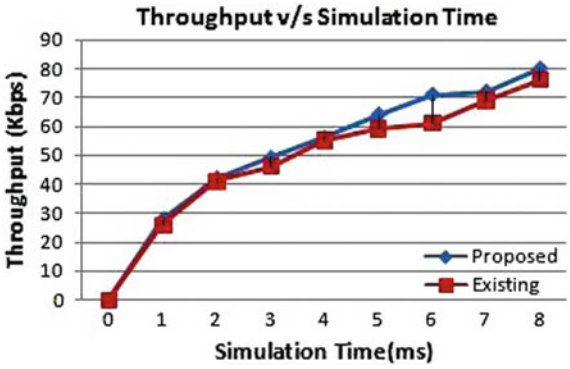


Fig. 7 Comparison for throughput versus simulation time

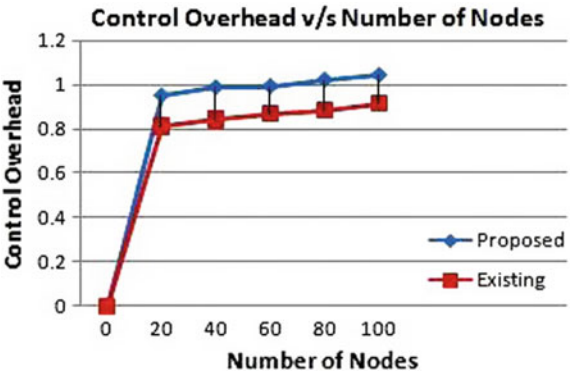


Fig. 8 Comparison for control overhead versus number of nodes

8 Conclusion and Future Work

In this paper, we proposed a cluster head selection scheme based on multi-metric approach. A node with greater lifetime and highly stable is selected as a cluster head. The simulation results show that our proposed scheme selected cluster head that consumes less energy, has lesser control overhead and also has higher throughput compared to the exiting approach. The results are also validated analytically.

Further research work shall focus on incorporating security and providing guaranteed QoS (Quality-of-Service) in multi-hop ad hoc network and also in heterogeneous networks.

References

1. Yu, J.Y., Chong, P.H.J.: A survey of clustering schemes for mobile ad ho networks. IEEE Commun. Surv. Tutor. **7**(1), 32–48 (2005)
2. Krishna, P., Vaidya, N.H., Chatterjee, M., Pradhan, D.K.: A cluster-based approach for routing in dynamic networks. ACM SIGCOMM Comput. Commun. Rev. **27**(2), 49–64 (1997)
3. Tolba, F.D., Magoni, D., Lorenz, P.: Connectivity, energy and mobility driven clustering algorithm for mobile ad hoc networks. In: Proceedings IEEE Global Telecommunications Conference, pp. 2786–2790, Nov 2007
4. Lo, S.C., Lin, Y.J., Gao, J.S.: A multi-head clustering algorithm in vehicular ad hoc networks. Int. J. Comput. Theory Eng. **5**(2) (2013)
5. Ucar, S., Ergen, S.C., Ozkasap, O.: Multi-hop cluster based IEEE 802.11p and LTE hybrid architecture for VANET safety message dissemination. IEEE Tran. Veh. Technol. (2015). ISSN 0018-9545
6. Zhang, Y., Ng, J.M.: A distributed group mobility adaptive clustering algorithm for mobile ad hoc networks. In: IEEE International Conference on Communications. ICC, pp. 3161–3165 (2008)
7. Wang, Z., Liu, L., Zhou, M., Ansari, N.: A position-based clustering technique for ad hoc inter vehicle communication. IEEE Trans. Syst. Man Cybern. Part C: Appl. Rev. (2008)
8. Bali, R.S., Kumar, N., Rodrigues, J.J.: Clustering in vehicular ad hoc networks: taxonomy, challenges and solutions. Veh. Commun. **1**(3), 134–152 (2014)
9. Bentaleb, A., Boubetra, A., Harous, S.: Survey of clustering schemes in mobile ad hoc networks. Commun. Netw. 8–14 (2013)
10. Talapatra, S., Rai, A.: Mobility based cluster head selection algorithm for mobile ad hoc network. Int. J. Comput. Netw. Inf. Secur. 42–49 (2014) (Published Online)
11. Gerla, M., Tsai, J.T.C.: Multi-cluster, mobile, multimedia radio network. Wirel. Netw. **1**(3), 255–265 (1995)
12. Baker, D.J., Ephremides, A.: A distributed algorithm for organizing mobile radio telecommunication networks. In: Proceedings of the 2nd International Conference on Distributed Computer Systems, pp. 476–483 (1981)
13. Basagni, S., Chiamtac, I., Syrotiuk, V.R., Woodward, B.A.: A distance routing effect algorithm for mobility (DREAM). In: Proceedings of the 4th International Conference on Mobile Computing and Networking, pp. 76–84. Dallas, Texas, US (1998)
14. Chatterjee, M., Sas, S.K., Turgut, D.: A weighted clustering algorithm (WCA) for mobile ad hoc networks. J. Clust. Comput. **5**(2), 193–204 (2002)
15. Govil, K., Gupta, S.K., Agrawal, A.: Cluster head selection technique for optimization of energy conservation in MANET. In: International Conference on Parallel, Distributed and Grid Computing, pp. 39–42. Solan, H.P., India, Dec 2014
16. The Network Simulator ns-2, Information Sciences Institute, USA: Viterbi School of Engineering. Available: http://www.isi.edu/nsnam/ns/, Sept 2004
17. Iwata, A., Chiang, C., Pei, G., Gerla, M., Chen, T.: Scalable routing strategies for ad hoc wireless networks. IEEE J. Select. Areas Commun. **17**(8), 1369–1379 (1999)

Maximizing Lifetime of Wireless Sensor Network by Sink Mobility in a Fixed Trajectory

Jay Prakash, Rakesh Kumar, Rakesh Kumar Gautam and J.P. Saini

Abstract Maximization of lifetime of wireless sensor network (WSN) is an emerging area of research in present scenario. Many authors are performing their research work, so that they could achieve lower energy consumption for the sensor network which leads to increase in lifetime of network. Our work focuses on sink mobility in a fixed trajectory within a wireless sensor network while sensed data are required to be collected. We divide the whole sensor network into two different regions as direct communication area (DCA) and multi-hop communication area (MCA). Sensors node that lies in DCA is at one hop count distance from the sink node trajectory while sensors within MCA are at more than one hop count from the trajectory. We considered all the sensors that are within DCA as subsink nodes. During sink mobility, whenever a subsink is closer to the mobile sink node, then it starts transmitting its data to the sink node. But those sensors that are within MCA needs to search an appropriate sink node for sending its sensed data to the subsink so that on further stage, that subsink could provide those data to the sink node whenever it is in nearest proximity of that subsink. Basically, a sink node is the ultimate destination for the data while a subsink node acts as a relay node for the nodes that are within MCA. So our work is to find out the appropriate subsink node from a given set of subsinks. For doing so, we used location-aided routing on global positioning system (GPS)-enabled sensors and sink node. Our work is validated through simulation experiments using NS-2.

J. Prakash · R. Kumar · R.K. Gautam
Department of Computer Science and Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur, Uttar Pradesh, India
e-mail: jpr_1998@yahoo.co.in

R. Kumar
e-mail: rkiitr@gmail.com

R.K. Gautam
e-mail: rakesh808615@gmail.com

J.P. Saini (✉)
Department of Electronics & Communication Engineering, Bundelkhand Institute of Engineering & Technology, Jhansi, Uttar Pradesh, India
e-mail: jps_uptu@rediffmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_53

Keywords Wireless sensor network · Sink mobility · Data collection · Network lifetime

1 Introduction

A WSN [1–10] is a collection of many sensors that have capability to sense, and the sensed data get processed and later on they are transmitted. All the sensed information ultimately gets collected on a place which is sink in WSN. The use of WSN is very wide; generally, it is used to monitor areas, persons, animals or sense humidity, temperature, the presence of seismic and acoustic waves, etc. It can also be used for object-tracing and remote monitoring purposes in various environments. Since sensors are low-complexity and low-cost devices which are characterized by a number of constraints such as limited battery power, low data transmission rates and reliability, short range of transmission, and low computational and processing power. So a WSN should be designed to keep in mind all these things to curb the limitations. Energy saving is a prime concern in this case because recharging and replacing the battery are not a convenient way to make the network function properly. In spite of doing this, we are required to reduce the energy consumption of WSN [10–15].

We worked toward energy saving technique by searching a closest subsink for MCA zone belonging nodes. As we discussed above, we divide the whole network into two different regions as DCA and MCA, and the nodes within DCA required subsink as a gateway/relay node which in turn able to send the received packets to the sink nodes in further stage of processing. Our aim is to find out the appropriate subsink, here we use location-aided routing on GPS-enabled sensor nodes. Since a source node which has some sensed data calculates its distances from all the available subsinks. The subsink placed at smallest distance from the source node is the appropriate subsink node that is acted as a relay node for the source node. Now, what is required is to select the suitable multi-hop path from source to the subsink (destination node). A flooding-based approach is applicable for choosing a path. After it is selected, source sends its sensed data to the subsink through this path.

The rest of the paper is organized as follows: In Sect. 2, related works is given while the detailed proposed approach has been presented under Sect. 3. System simulation and performance analysis are given in Sect. 4. Finally, the paper ends by presenting conclusion and future scope in Sect. 5.

2 Related Work

Nesamony et al. [2] have presented a model for sink mobility inside the sensor network region to gather the sensed data from the sensors in one hope distant nodes fashion. The shortest distance route that passes through the transmission range of

sensors is considered. Traveling salesman problem with neighborhoods and a heuristic is used as the solution in [2]. This work is further extended for multiple sinks in [3].

Gandham et al. [4] described the effect of sink mobility in wireless sensor network lifetime. Times are divided into periods of equal length. Within that time period, they assume that the data paths and sinks are static. Two different MILP models are described to reduce the maximum energy depletion of each sensors and total energy depletion of all sensors, respectively.

Azad et al. [5] extended the framework used in [4] and used two additional heuristics. In first, sinks are placed at points nearer to the sensor node having highest residual energy while in second, once the sink position is decided where difference between the minimum and maximum residual power of sensors is reduced.

In [6, 7], the authors propose a fix trajectory sink supporting multi-hop transmission. They have suggested a protocol and speed control algorithm of sink node to enhance the performance and set of data gathered by sink node. Here, a shortest path tree (SPT) is used to select the cluster heads and route information, which may cause imbalance in traffic and energy dissipation. In this, if a mobile sink is placed on public transportation like bus, the movement speed cannot often be changed freely for the purpose of information collection.

Keskin et al. [8] provide a mathematical model which unites WSNs design decisions on sensor fields, actions schedules, information routes, track of the mobile sink(s), and then presents two heuristic methods for the solution of the model. They demonstrate the efficiency and accuracy of the heuristics on several randomly generated problem instances on the basis of extensive numerical experiments. Both of the heuristics make use of the idea of fixing values of some of the binary variables aiming at facilitating the restricted model. The period iteration heuristic achieves this by limiting the number of whole intervals and enhancing it separately until no progression is achieved between two successive iterations. It uses the solution and the corresponding objective value of the previous iteration to speed up the solution procedure of the current iteration. The sequential assignment heuristic, on the other hand, makes use of the natural hierarchy.

In paper [9], authors have proposed a new information collection scheme, called the maximum amount shortest path (MASP) using improved ant colony optimization. MASP is formulated as an integer linear programing problem and then solved with the help of improved ant colony optimization. MASP scheme is implemented using zone-based partition. In this, the residual energy of every sensor is calculated, and the selection of optimal route is based on residual energy, shortest path, channel noise, and delay. An improved ant colony optimization algorithm is based on the basic ant colony algorithm. In this algorithm, ants are divided into two groups separately for searching the path, and rotary table is maintained for avoiding stagnation. Therefore, searching probability of optimal path is optimized. The search probability of the route in previous one is introduced in each search to speed up the search. The optimal path satisfies multi-constrains like delay, delay jitter, bandwidth, and cost.

3 Proposed Work

In our proposed work, subsink selection is based on a location-aided routing (LAR). We assume that each sensor in the network is consists with GPS facility so that their location can be accessed by sensors in WSN, so that each sensor can calculate its distance from other in the network. Since subsink is acted as a relay node, most of the energy get utilize in transmitting sensed data to the subsinks, and a few part of energy is used in subsink to sink communication. So our focus is to find out an appropriate subsink corresponding to each sensor within MCA. The selection relies on shortest distance parameter. The subsink that is at the nearest position to the source sensor node is selected as a relay node. Further, we have calculated the appropriate multi-hop path from the sensor to the subsink so that the sensed data could be transmitted through the efficient multi-hop path.

Consider the following scenario of WSN given in Fig. 1. Here, nodes colored in black are sensor nodes, red color nodes are subsink nodes, and single sink is green colored. Subsink nodes are always at one hop count distance from the fixed trajectory on which single sink is mobile. Here, sink is the ultimate destination, and the subsinks are responsible for gathering the sensed data from the sensor nodes.

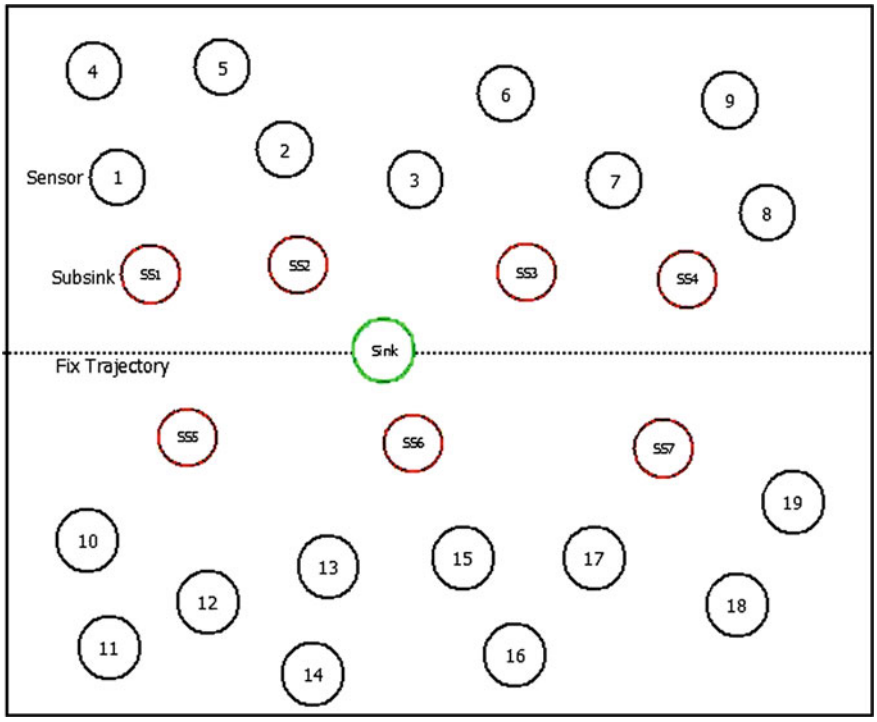


Fig. 1 Wireless sensor network

Now, the main focus is to search for the efficient subsink. This selection is done by using location-aided routing.

In the above diagram, node 5 is a sensor node which required an efficient subsink for sensed data transmission. Here, in the given scenario, three different subsinks are available, i.e., SS1, SS2, SS3. What is required here is to calculate the distance from node 5 to all the subsinks which are d1, d2, d3 as shown above in Fig. 2. By just calculating their values, the smallest one has chosen as the more appropriate subsink node from the originating source node. Here, d2 is the smallest distance from all we have calculated. Hence, SS2 subsink is a correct choice as per rule for further data transmission from node 5.

The next issue which we have also focused is to discover the more suitable and appropriate multi-hop path exists in b/w sensor nodes and selected subsink node.

When we talk about the routing protocols in WSN, then we have basically two classes which are reactive and proactive routing. The reactive routing is on-demand routing because the route discovery begins whenever there are some data to send. While the proactive routing is a table-driven routing protocol where each node shares the information about routes to the others continuously even though we do not have anything to send. Proactive routing is not a desirable approach when we

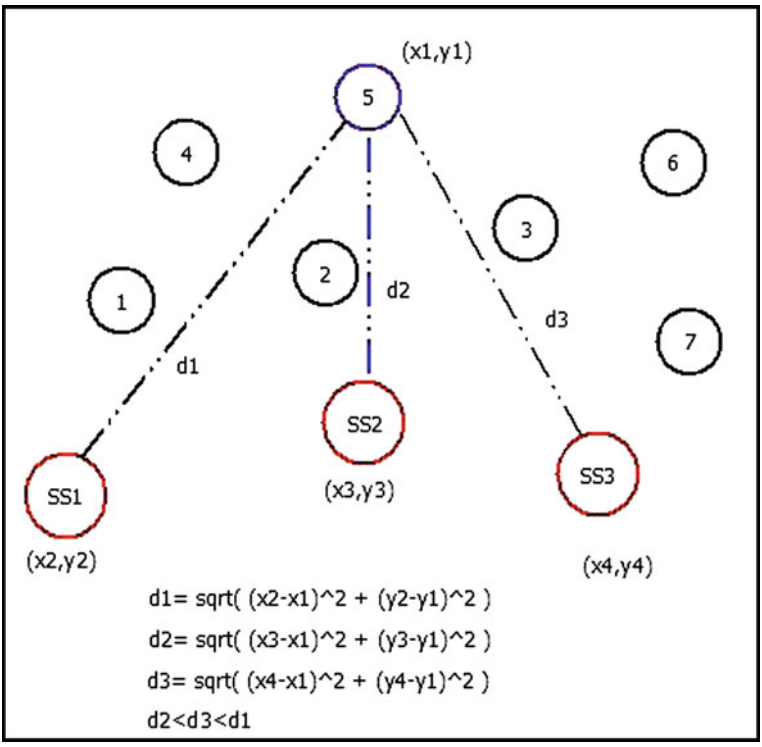


Fig. 2 Subsink selection scenario

have less data to send due to its routing overhead. Proactive routing is suitable in case of when nodes have fewer amounts of data to send. But we can make these routing algorithms more efficient by exploiting the feature of locations of the node. By using location information, the location-aided routing (LAR) protocols limit the search for a new route to a smaller request zone of the ad hoc network.

The proposed methodology is termed location-aided routing (LAR) which reduced routing overhead by using location information. In this, location information may be provided by the global positioning system (GPS) to the LAR protocol. Due to GPS-enabled mobile node, there is possibility for each mobile node to know physical location of other nodes. But some amount of error occurs when position information of a node provided by GPS. So there is difference between coordinates calculated by global positioning system and the real coordinates.

In Fig. 3, there is a node *S* as a source node which needs to find a path from node S to destination node *D*. Consider source node *S* which knows about node *D* that its location was at time t_0 is *L,* and current time of *D* is t_1. According to node *S*, the expected zone of *D* at time t_1 is the area where node *S* expects to the destination node *D*. Expected zone of *D* can be find based on the information of *D* that its location was at time t_0 is *L*. Consider node *D* is traveling with average speed v, then the expected zone of *D* is a circular region with radius $R = v\ (t_1 - t_0)$. If the traveling speed of *D* is greater than average speed, then position of node *D* at time t_1 may be outside the expected zone. Hence, expected zone is only an approximate calculation which is done by node *S* for finding the region of *D* which is covered by the node *D* at time t_1.

Again, consider source node *S* which needs to find a path from node *S* to destination node *D*. The proposed LAR protocol uses flooding technique for route request with one modification. In this, source node *S* creates a request zone for route request then it sends a route request only to that node which are belong to request zone. To increase the probability that the route request will reach node *D*, the request zone should include the expected zone.

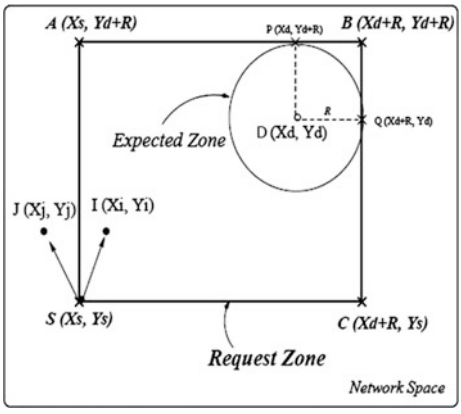


Fig. 3 Division of request and expected zone

In Fig. 3, suppose that source node *S* which knows about node *D* that was at location (x_d, y_d) at time t_0. But node *S* find new route discovery to destination node *D*. We suppose that node *D* is moving with average speed v and node *S* also knows that average speed. Using average speed *v*, the expected zone can be created by node *S* with radius $R = v\,(t_1 - t_0)$ which is a circular region centered at location (x_d, y_d). Thus, four corners of the expected zone can be determined by the source node *S*. In this, node *S* considers their coordinates for sending route request message at the time of route discovery. Node *S* sends a route request to other node and that node receives a route request and forward to other one if it is belong to request zone otherwise discarded. The request zone is defined with four corners *S*, *A*, *B,* and *C* of rectangular. In Fig. 3, node *S* sends a route request to node *I* then I forward that route request to its neighbors because I know that it belongs to request zone. However, when node *S* sends a route request to node *J* and node *J* discard that route request because *J* know that it not belongs to request zone. At last, destination node *D* receives route request message with intermediate nodes of request zone and node *D* sending a route reply message to the source node *S* with same intermediate nodes. In LAR, for route reply message, destination node *D* considers its current location and current time. When route reply message is received by the source node *S,* then node *S* records the location of the destination node *D*.

3.1 Route Discovery Phase

Whenever we have some data for a particular sensor node, then firstly, we discovered a path so that we can send our data to the intended recipient. The route discovery path that we are using in our proposed methodology is quite similar as in AODV protocol. The diagram given below dictates the route discovery phase.

As shown in Fig. 4, sensor node *S* initiates route discovery phase so that it broadcasts the RREQ packets to all its neighbors and further all neighbors to theirs. Similarly, the RREQ packet finally reaches to destination node SS. The neighbors nodes lie outside of the request zone are not taking participation in the route discovery which is explained in LAR technique above. Somewhere, in route discovery phase, duplicate packets are received by the nodes, so to prevent unnecessary flooding within the network the RREQ packet received firstly get entertained and other packets carrying same node id and broadcast id get simply discarded. In the above diagram, the red lines represent the RREQ packets get discarded due to duplicity.

Here, in this Fig. 5, the path through S → 4 → 9 → 14 → SS gets selected. The data carried by source node are then forwarded by this path only.

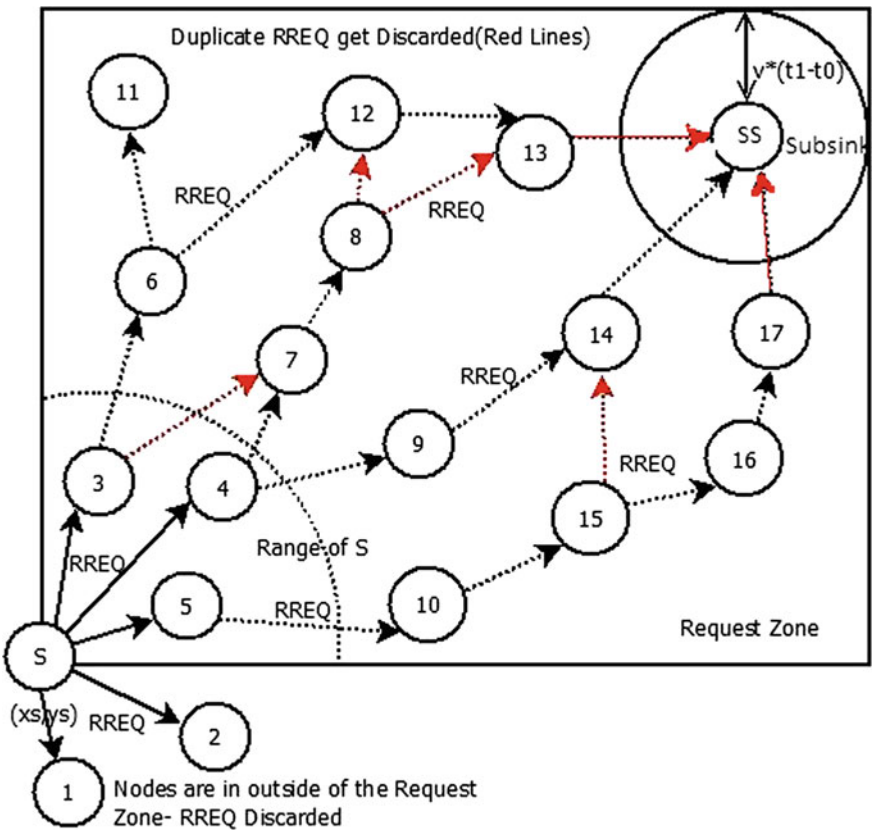


Fig. 4 Route discovery inside request zone (all RREQ packets outside the request zone get discarded)

4 System Simulation and Performance Analysis

The performance of proposed scheme for data collection using sink mobility in fixed trajectory is measured using NS-2 simulation tool. Sensor nodes are placed in 600 m * 800 m canvas. Initial energy for each sensor node, subsink node, and sink node is set, and the speed of mobility of sink node is constant. We also considered that the subsinks and sensor nodes are also mobile, and they have random waypoint mobility model (Table 1).

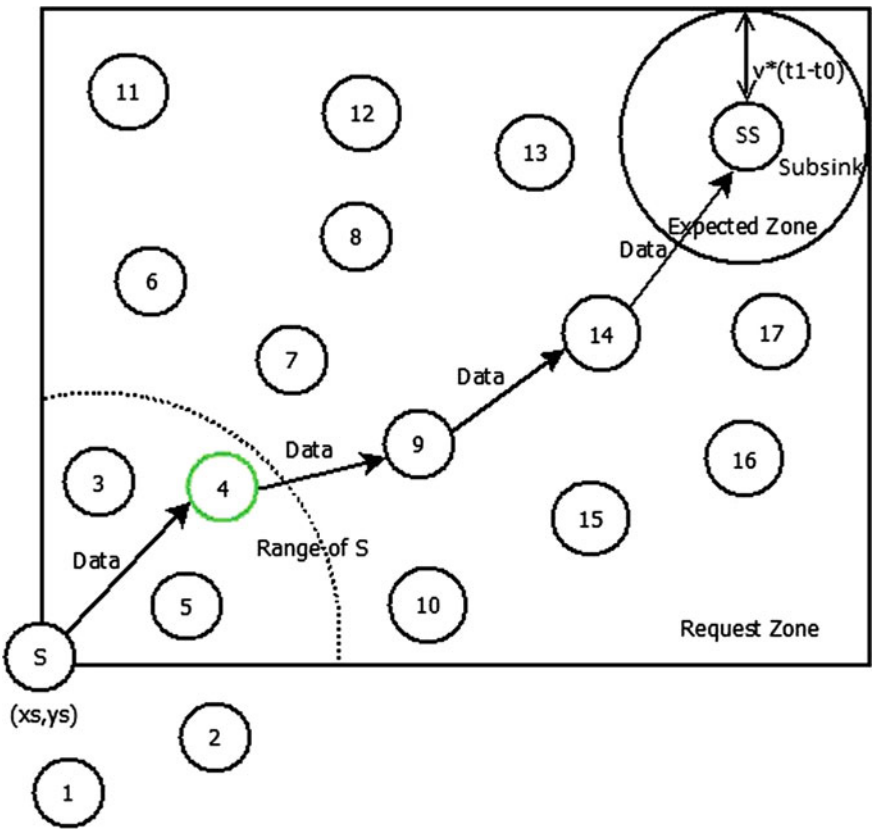


Fig. 5 Final path selected between *S* and *D*

Table 1 Simulation parameters

Parameter name	Value
Network area	600 m × 800 m
Number of nodes	40
Simulation time	10 s
Transmission range	[200–400]m
Routing protocol	LAR, AODV
MAC	IEEE 802.11
Radio propagation model	Two ray ground reflection
Mobility model	Random way point

4.1 The Following Metrics Are Used to Evaluate the Performance

1. Data collected by single mobile sink in one round on fixed trajectory.
2. Total amount of energy get consumed by all sensors while one round of sink is completed.
3. Lifetime of network is proportional to the number of rounds the mobile sink travelled since beginning till first node energy exhaustion.

Graph shown in Fig. 6 is drawn in between data count and time. Data count is the total information retrieved by mobile sink in one round of movement of its trajectory. The outcome dictates that the amount of information retrieved by sink node in proposed scenario is higher than the existing one.

In Fig. 7, a graph is drawn in between network lifetime and number of nodes. Network lifetime is measured as the total number of rounds a mobile sink travelled till the first node of the network has energy exhaustion. Result came out from the simulation work represents that we have achieved higher lifetime than the existing

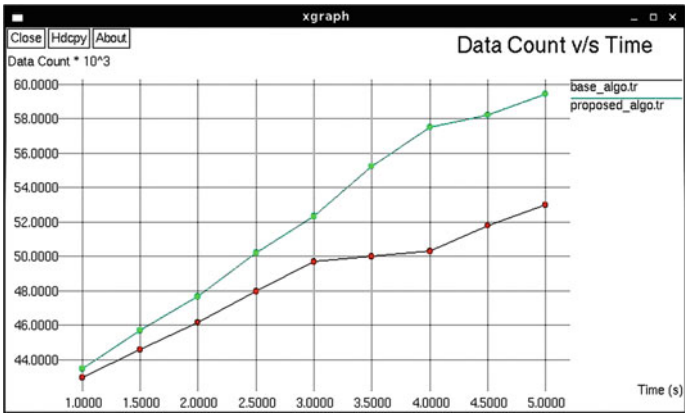


Fig. 6 Data count versus time

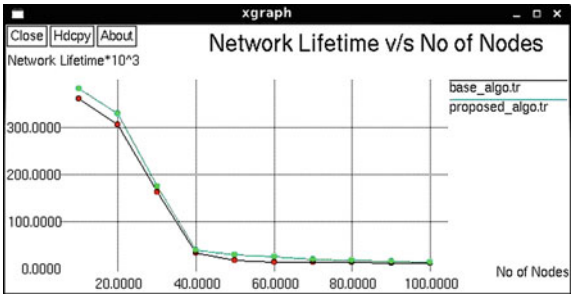


Fig. 7 Network lifetime versus number of nodes

approach, but as we increase the number of nodes in our scenario, the lifetime reduces abruptly,and after 70 nodes, it is about to be the same value as it is in existing protocol.

5 Conclusion and Future Work

This paper proposes an efficient mechanism for maximizing wireless sensor network lifetime using sink mobility in fixed trajectory. The proposed approach efficiently selects subsink node using LAR technique with flooding mechanism for route selection. Subsinks are used as relay nodes for the sensors that transmit data to the mobile sink when the sink is nearer to the subsink nodes. The simulation results show that our method achieved more data count, i.e., amount of data collected per round by sink node and also maximize lifetime for the sensor network.

Future work shall be incorporation of more QoS parameters in the proposed approach to model real life situation more accurately.

References

1. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Elsevier Comput. Netw. **52**, 2292–2330 (2008)
2. Nesamony, S., Vairamuthu, M.K., Orlowska, M., Sadiq, S.: Optimal route computation of mobile sink in a wireless sensor network. In: Technical Report, The University of Queensland (2006)
3. Valle, A., Cunha, A.S., Aioffi, W.M., Mateus, G.R.: Algorithms for improving the quality of service in wireless sensor networks with multiple mobile sinks. In: ACM, 2008, 1454545, pp. 239–243
4. Gandham, S.R., Dawande, M., Prakash, R., Venkatesan, S.: Energy efficient schemes for wireless sensor networks with multiple mobile base stations. In: IEEE, vol. 1, pp. 377–381 (2003)
5. Azad, A., Chockalingam, A.: Mobile base stations placement and energy aware routing in wireless sensor networks. In: IEEE, vol. 1, pp. 264–269 (2006)
6. Kansal, A., Somasundara, A., Jea, D., Srivastava, M., Estrin, D.: Intelligent fluid infrastructure for embedded networks. In: Proceedings of the 7th Annual International Conference on Mobile Systems, Applications and Services (MobiSys), pp. 111–124 (2004)
7. Somasundara, A., Kansal, A., Jea, D., Estrin, D., Srivastava, M.: Controllably mobile infrastructure for low energy embedded networks. IEEE Trans. Mobile Comput. **5**(8), 958–973 (2006)
8. Emre Keskin, M., Kuban Altinel, I., Aras, N., Ersoy, C.: Wireless sensor network lifetime maximization by optimal sensor deployment, activity scheduling, data routing and sink mobility. In: ELSREVIE, Ad Hoc Networks, pp. 1570–8705 (2014)
9. Kumar N.V.A., Thomas, A.: Energy efficiency and network lifetime maximization in wireless sensor networks using improved ant colony optimization. In: ICCCNT'I2, July 2012, Coimbatore, India
10. Yun, Y.S., Xia, Y.: Maximizing the lifetime of wireless sensor networks with mobile sink in delay-tolerant applications. IEEE Trans. Mobile Comput. **9**(9), 1308–1318 (2010)

11. Gatzianas, M., Georgiadis, L.: A distributed algorithm for maximum lifetime routing in sensor networks with mobile sink. IEEE Trans. Wireless Commun. **7**(3), 984–994 (2008)
12. Basagni, S., Carosi, A., Melachrinoudis, E., Petrioli, C., Wang, Z.M.: Controlled sink mobility for prolonging wireless sensor networks lifetime. Wireless Netw. **14**(6), 831–858 (2007)
13. Chang, J., Tassiulas, L.: Maximum lifetime routing in wireless sensor networks. IEEE Trans. Networking **12**(4), 609–619 (2004)
14. Wang, W., Srinivasan, V., Chua, K. C.: Using mobile relays to prolong the lifetime of wireless sensor networks. In: Proceedings of the ACM MobiCom, pp. 270–283 (2005)
15. Guney, E., Aras, N., Kuban Altinel, I.K., Ersoy, C.: Efficient solution techniques for the integrated coverage, sink location and routing problem in wireless sensor networks. Computers OR **39**(7), 1530–1539 (2012)

Secure Communication in Cluster-Based Ad Hoc Networks: A Review

Ajay Kumar Gupta and Shiva Prakash

Abstract Mobile Ad Hoc Network (MANET) is an association of wireless mobile nodes with limited transmission range, resources, quick and easy setup and has no fixed infrastructure. As the nodes in the MANET are mobile so it uses wireless connections for communication with various networks. For the environment of continuous changing topology, routing algorithms with special features are required. The algorithm or protocols have to be chosen based on size, density, and the mobility of the nodes. Currently, there are still ongoing researches on MANETs. These researches may result to even better protocols having better QOS and security measures but it may also possible new protocols will face new challenges. This paper presents an elaborate view of security issues, services, attacks, and security challenges for MANET. Moreover, various cluster-based secure communication methods and their comparison based on a set of measurement schemes are discussed.

Keywords MANET · Mobile IP · Multi-hop · Internet · Routing protocol · On-demand routing protocol · Cluster head

1 Introduction

MANET [1, 2] is an association of various autonomous mobile nodes that move freely and communicate directly over a common wireless channel through multi-hop relay. To communicate with the other nodes in its wireless range nodes in the MANET are equipped with a wireless transreceiver. If nodes are not in wireless range, they exchange information with each other by multi-hop communication obeying a set of rules. The nodes cooperate with each other such that a valid and

A.K. Gupta (✉) · S. Prakash
Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology, Gorakhpur 273010, UP, India
e-mail: ajay25g@gmail.com

S. Prakash
e-mail: shiva.plko@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_54

optimum chain of mutually connected nodes is formed. So, each node plays role of both host as well as a router. In MANET, each node is free to join any network as well as leave current network. This property is also called open network boundary. Dynamic topology and open network boundary make security the major challenge in MANET [3]. The important challenges of the ad hoc network are the basic routing mechanism, medium access scheme, provisioning of QoS, security, energy management, scalability, deployment considerations. The goal of paper is to provide analysis on MANET's cluster-based secure communication methods and their comparison based on a set of measurement schemes.

Rest of this paper is organized as follows: Sect. 1 presents basic of MANET and classifications of routing protocols; Sect. 2 presents security challenges, criteria, possible attacks, and security steps to avoid these attacks in the Mobile Ad hoc Networks; Sect. 3 presents security enhancement through cluster heads; Sect. 4 presents comparative study of existing well-known protocols; finally, Sect. 5 concludes the paper and elaborates some future works.

2 Security Aspects in Mobile Ad Hoc Networks

Dynamic topology and open network boundary make security the major challenge in MANET. In this section, we focus on various security challenges in implementation, attacks, and the measure that should follow to overcome these unwilling attacks.

2.1 Security Challenges and Requirement

Absence of centralized management, power supply limitation, internal threats, insecure boundaries are the major security challenges in MANETs. Potential security protocol should assure that it meets the following requirements to establish secure communication between mobile nodes:

1. **Authentication**: Authentication is the assurance that sender and receiver or modifier in communication is right person and if there is any possibility of impersonators then find it out.
2. **Authorization**: In this process, an entity gets a credential from the certificate authority, which specifies privileges and permissions the entity has.
3. **Availability**: Availability states that the node should able to provide all the incorporated services irrespective of the security state.
4. **Integrity**: Integrity confirms the id of the message when they are sent on the channel.
5. **Data freshness**: Data freshness states that the fresh data is present and any outdated data has not been replayed.

2.2 Security Attacks on Protocol Stacks

Absence of centralized administration makes MANETs prone to various types of security attacks and dealing with these is one of the main challenges for the developers. Some of the possible security attacks in MANETs are Denial of Service, Man in the middle on Multilayer Attack, Repudiation, Mobile virus and worm attacks on Application Layer, SYN flooding attacks and Spoofing victim node IP address on Transport Layer, Wormhole, Black whole, Flooding, Rushing attack, Location disclosure attack, Resource consumption, Routing table overflow attack on Network Layer, Traffic monitoring and analysis, Disruption on MAC DCF and back-off mechanism on Data link Layer, and Jamming or radio interference, interception, Eavesdropping on Physical layer.

2.3 Security Measures to Avoid Attacks in Mobile Ad Hoc Network

1. **Secure Routing**: Providing trustworthiness of users in the network is one of the major challenges of secure routing. Distributed communication environment is more vulnerable to attacks. In this type, authentication is open so any unauthentic node may compromise routing traffic for the objective of disrupting the communication. Author in [4] presents a secure routing protocol using IPSEC in mobile ad hoc network. Authors in [5] present a trust-based protocol for routing. In MANET, there exist multiple paths between pair of nodes. Choosing better path for sending packet considering both factor of routing method and security constraints will good for improving security.
2. **Key Management Methods**: Certified Authority (CA) is a method for key management and various approaches of this used for key management to solve high mobility issue. Additionally, it provides a better method to reduce control overhead.
3. **Intrusion Detection System**: Intrusion detection is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise system and network resources. IDS is used to detect and report about malicious activities.

3 Security Enhancement Through Cluster Heads

The problems such as key distribution can be easily solved by clustering. For security objectives, clustering is important. Authors in [6, 7] present mechanism for key distribution via clusters. Clustering solves some of security challenges but creating cluster and its maintenance is tough part to solve because of MANET's

continuous changing topology. A cluster head in each cluster works as a coordinator. It does the work of channel assignment, battery energy control, time division frame and its synchronization. Introducing clustering architecture, each cluster contains its single cluster head. Each host may be a cluster head (CH) or it may adjacent to one or more CHs. The nodes participating into more than one cluster is called *gateways*. A common gateway is used for the communication between any two adjacent clusters. Any two cluster heads cannot adjacent to each other. They must be maximum two hops away distance from each other in the clustering architecture. It can be categorized into two types: overlapping and non-overlapping. In overlapping clustering architectures, the hops which are not a CH, may participate common to more than one cluster, these nodes are called *gateway*. Nodes belonging to single cluster are called *ordinary nodes*. In non-overlapping clustering architectures, non-cluster-head nodes which belonging to only one cluster are called *an ordinary node*. In Fig. 1, for example, the pair of nodes 9 and 10 forms a *DG*.

Clustering Algorithm:

Basically, two cluster creation algorithms [8] have been proposed for MANET's.

1. **Lowest ID Clustering**: Each node is given a unique ID. The nodes broadcast its neighboring and own information at some regular intervals [9]. A node which only listen the nodes with ID higher than himself is a cluster head (CH). A node which participates in two or more CHs is termed as gateway. Other nodes are ordinary node.
2. **K-means**: These algorithms use concept of the Euclidean k-medians and geometric k-center problem [10]. The first problem mainly focuses on to reduce the sum total of distances to closest center, and second problem aims to reduce the maximum distance from every node to its nearest center.

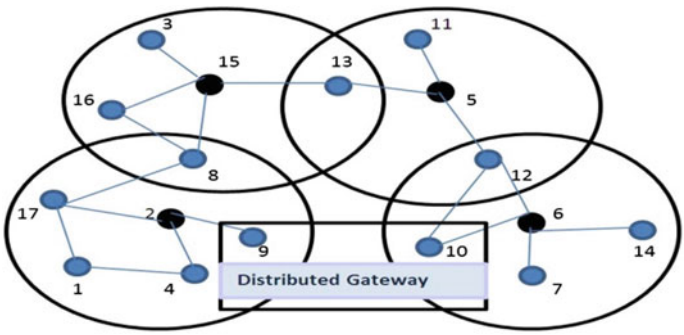


Fig. 1 Clustering architecture

Cluster Creation: The network is partitioned into several two-hop clusters, where in each cluster, a node can act as cluster head, ordinary node, secondary cluster head or gateway.

Cluster Management: The objective of clustering is to efficient use of resources, manage routing, location problem-solving with consideration of reducing communication and computational overheads. Cluster maintenance involves two parts which are given below.

1. Intra-cluster maintenance: It involves routing within a cluster.
2. Inter-cluster maintenance: It involves routing among cluster.

Cluster-Head Election: Cluster heads responsible for route maintenance, intra- and inter-cluster data exchange; it is desirable that clusters will work for large time when chosen. Cluster head can be elected by calculating mobility of each node in which the lowest mobility node is CH.

It is the responsibility of cluster heads to monitor all the routing activities within the cluster. Cluster-head-based protocol uses a hierarchical network topology, unlike other table-driven approaches [11] that employ flat topology. Clustering is advantageous as it evolves managing a set of ad hoc hops; code separation between clusters, link access, and routing issues. There are some works related to secure leader election but they are incapable to give solution to the problem like if maliciously, nodes list itself as coordinator then what actions would be follow. So, issues for cluster formation such as secure coordinator election and inter-cluster routing need to be considered. The clustering schemes can be one of many type firstly it can be trust based, or it can be based on cryptography or it may be hybrid schemes as shown in Fig. 2.

Pure cryptographic-based clustering techniques are not able to find insider malicious nodes. The trust and reputation management mechanism are required to defend from insider attackers. For defending from both internal and external malicious nodes and attackers, we need some complex security solutions that integrate both cryptography-based mechanisms and reputation management systems with clustering algorithms, hybrid trust-based clustering algorithms serve for this objective.

Lack of trust between communicating nodes in traditional MANET's routing protocols makes the network more vulnerable to malicious attacks. Many time behaving as a selfish nodes it do not forward packets of sender nodes, moreover malicious nodes may perform activity such as modification and impersonation attacks to the network traffic.

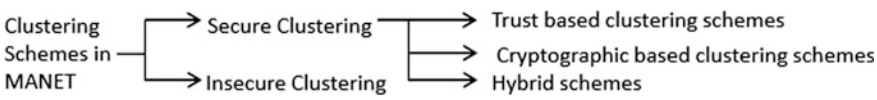


Fig. 2 Classifying clustering schemes from security perspective

4 Comparative Analysis

Based on survey of Yu and Chong [12] and Bechler et al. [13], clustering techniques of MANETs are typically categorized into following types: dominating set based, mobility based, energy based, weight based, load balancing, topology based, and combine metrics based. Table 1 shows comparison of the clustering objectives of various schemes.

In DS-(abbreviated as Dominating Set) based clustering schemes, a group of node works as CH to pass routing packets, these set of nodes are called dominating set. The key concept in mobility aware clustering is to grouping similar speed mobile nodes in one cluster.

There are many clustering techniques for MANETs based on various schemes. We have to consider the metrics for the evaluation purpose. Table 2 shown in this section compares a list of important schemes given by authors. Chong et al. [12] present a survey on various clustering methods. These methods mainly focuses on minimizing number of clusters, maximizing lifespan of mobile hops in the network, low overhead, minimum CHs changes, minimized bandwidth consumption. But security is ignored in these schemes. Safa et al. presented a cluster-based trust aware routing protocol (CBTRP) [20] for the objective of secure routing path via use of the weighted clustering protocols to choose cluster head. In weighted clustering algorithm (WCA), weighted degrees such as battery power, number of neighbors, and mobility of the nodes are taken into consideration. The trust value is measured in terms of behavior of node such as whether node is selfish and may prone to a black hole, modification attack, and latency delays. When a malicious hop is found, it is removed from the network so that no packet will pass from it. Chatterjee et al. [21] present a secure trusted auction-based cluster-oriented routing protocol (STACRP) to facilitate trusted framework for MANETs. Selfish nodes are detected by this method and it enforces to cooperate between nodes to achieve good throughput and lesser routing overhead.

Table 1 Comparison of schemes

Clusters methods	Goal
DS based	Lesser number of participating hops in route search
Mobility based	Use mobility characteristics for cluster creation
Energy based	Reduce unnecessary battery energy consumption
Load balancing	Equalize the workload of each cluster
Combine metrics based	Using various metrics to determining the weighing factor

Table 2 Comparative study of various proposed secure cluster-based schemes

Authors	Scheme	Technique used	Key concepts used	Benefits	Limitation
Becheler et al. [13]	Id based	AODV	Threshold cryptography mechanism used to give certification authority	Instead of a registration authority, arbitrary nodes with respective warranty certificates may warrant for a new node's identity	Scheme is not practical, as warrantor unaware of the new node to be guaranteed
Chatterjee et al. [14]	Weight based	AODV	Calculate the combined weight for each node	Reduces information exchange, computation/communication costs, performs load balancing	Trust level of nodes while choosing the cluster head not cared
Sudarshan et al. [15]	Common evaluation algorithm (CEA). Value based	AODV	Secure coordinator election model using Dijkstra-Scholten termination detection protocol	Avoids activities of selfish nodes and manage the energy consumption between nodes for increasing the lifetime of MANETs	Malicious property of the hops is not cared
Vaidya et al. [16]	Combine metrics based—height of node (5-tuple)	TORA	The trust values are calculated using direct observation which is transitive	Establish a trustworthiness end-to-end route	Malicious property of the nodes is not cared
Pirzada and McDonald [17]	Trust based	AODV	Confidence level is entertained as a weight for computing the trust value	Enhances the trust measures by considering the confidence level of trust of each node	The routes selected may not be cryptographically secure
Ghosh et al. [18]	Trust based	AODV	To distinguish between selfish and cooperative nodes, a set of statistical tests are entertained	In the case of wrong accusation, it gives solution for securing the network against colluding malicious node	If there is no accusation at all from a malicious node, the algorithm does not able to obtain a secure end-to-end path
Milan et al. [19]	Reputation-based mechanism	GAME THEORETIC MODEL	Analyze the effect of collisions on a node-by-node reputation-based mechanism	The cooperation in malicious selfish nodes without central authority is possible	Not suited for non-uniform topologies and routing, these results in interaction asymmetries and impair cooperation

5 Conclusion and Future Scope

This paper presents common issues related to MANET security, various cluster-based secure communication schemes and their comparison based on a set of measurement schemes. MANET has vast potential; still, it has many challenges left to be solved. In our paper, we have overviewed 'What are the security threats vulnerable to attacks in MANET?' In our survey, we describe a variety of attacks that may present on different layers. We tried to answer 'How the services like confidentiality, integrity, and authentication can be obtained in MANET?' MANET needs very specialized security; a single approach does not fit for all the security schemes, as nodes can be any type of devices. Security in the nodes depends on its type, and we cannot make assumptions on security.

Acknowledgements This survey paper work is partially funded by the Technical Quality Improvement Programme Phase II (TEQIP-II).

References

1. Padma, P., Suresh, R.: Literature survey on latest research issues in MANET. IJARCET **2** (2013)
2. Singh, G., Singh, J.: MANET: issues and behavior analysis of routing protocols. IJARCET **2** (4) (2012)
3. Sheikh, R., Chande, M.S., Mishra, D.K.: Security issues in MANET: a review. In: Presented at the Seventh International Conference on Wireless and Optical Communications Networks (WOCN) (2010)
4. Panaousis, E.A., Ramrekha, T.A., Politis, C.: Secure routing for supporting ad-hoc extreme emergency infrastructures. In: Future Network and Mobile Summit (2010)
5. Salmanian, M., Li, M.: Enabling secure and reliable policy-based routing in MANETs. In: Presented at the Military Communications Conference, MILCOM (2012)
6. El-Sayed, A.: Clustering based group key management for MANET. In: Advances in Security of Information and Communication, Networks Communications in Computer and Information Science, vol. 381, pp. 11–26 (2013)
7. Zefreh, M.S., Fanian, A., Sajadieh, S.M., Khadivi, P., Berenjkoub, M.: A cluster-based key establishment protocol for wireless mobile ad hoc networks. Advances in Computer Science and Engineering Communications in Computer and Information Science (2009)
8. Ramachandran, L., Kapoor, M., Sarkar, A., Aggarwal, A.: Clustering algorithms for wireless ad-hoc networks. In Proceeding, Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Boston (2000)
9. Basu, P., Khan, N., Little, T.D.C.: A mobility based metric for clustering in mobile ad hoc networks. In: Proceedings of IEEE ICDCS 2001 Workshop on Wireless Networks and Mobile Computing, Phoenix, AZ, April 2001
10. Kanungo, T., Netanyahu, N.S., Wu, A.Y.: An efficient k-means clustering algorithm: analysis and implementation. In: IEEE Transactions on Pattern Analysis and Machine Intelligence (2002)
11. Siva Ram Murthy, C., Manoj, B.S.: Ad-hoc Wireless Networks: Architectures and Protocols. Pearson Education, May 2004
12. Yu, J.Y., Chong, P.H.J.: A survey of clustering schemes for mobile Ad Hoc networks. IEEE Communications Surveys and Tutorials (2005)

13. Bechler, M., Hof, H., Kraft, D., Pählke, F., Wolf, L.: A cluster-based security architecture for Ad Hoc networks. In: Proceedings of INFOCOM-04, March 2004
14. Chatterjee, M., Das, S.K., Turgut, D.: An on-demand weighted clustering algorithm (WCA) for ad-hoc networks. In: Proceedings of IEEE GLOBECOM 2000, November 2000
15. Vasudevan, S., Decleene, B., Immerman, N., Kurose, J., Towsley, D.: Leader election algorithms for wireless ad hoc networks. In: Proceedings of DARPA Information Survivability Conference and Exposition (2003)
16. Vaidya, N., Welch, J., Malpani, N.: Leader election algorithms for mobile ad hoc networks. In: Fourth International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Boston, MA, August 2000
17. Pirzada, A.A., McDonald, C.: Establishing trust in pure ad-hoc networks. In: Proceedings of the 27th ACSC '04 (2004)
18. Ghosh, T., Pissinou, N., Makki, K.: Towards designing a trusted routing solution in mobile Ad Hoc networks. Mobile Networks and Applications (2005)
19. Milan, F., Jaramillo, J.J., Srikant, R.: Achieving cooperation in multi hop wireless networks of selfish nodes. In: Proceedings of the Workshop GameNets '06, October 2006
20. Safa, H., Artail, H., Tabet, D.: A cluster-based trust-aware routing protocol for mobile Ad Hoc networks. Wireless Networks (2010)
21. Chatterjee, P., Sengupta, I., Ghosh, S.K.: STACRP: a secure trusted auction oriented clustering based routing protocol for MANET. Cluster Computing (2012)

Cluster Head Selection and Malicious Node Detection in Wireless Ad Hoc Networks

Shrikant V. Sonekar, Manali M. Kshirsagar and Latesh Malik

Abstract Mobile ad hoc networks are self-categorizing and self-configuring multihop networks competent of adaptive reconfiguration network. Node mobility in MANET may cause frequent network topology changes and the impact of noise, fading, and interference degrades the capacity of wireless networks. Due to the lack of infrastructure and the incapability of preventive measures such as encryption, authentication, and cryptography for detecting the newer attacks leads the wireless networks more susceptible to be attacked than wired one. Moreover, the false alarm is one of the major challenges in intrusion detection and prevention measures not assured to work, there is a need to supervise the network and look for abnormal behavior of the node. The mathematical approach for cluster head selection based on the distance and energy gives the realistic result. The proposed algorithm for intrusion detection aggregates all the information before declaring any node as malicious. The proposed algorithm also suggests how the cluster head communicates the malicious node information to all the heads which are in the radio range.

Keywords MANET · Attacks · Abnormal behavior · Dirty packets · Cluster head

1 Introduction

With the rapid increase of wireless devices during the recent years, the potentials, magnitude, and the use of wireless networks have become noticeable. There exist three types of mobile networks: rigid networks, ad hoc networks, and hybrid networks. A mobile ad hoc network is formed by a group of nodes without the help

S.V. Sonekar (✉) · M.M. Kshirsagar · L. Malik
Department of CS, GHRCE, Nagpur, India
e-mail: srikantsonekar@gmail.com

M.M. Kshirsagar
e-mail: manali_kshirsagar@yahoo.com

L. Malik
e-mail: latesh.malik@raisoni.net

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_55

of predetermined infrastructure [1]. Each node is well acquainted with a transmitter and receiver, which helps node to converse with other nodes in its radio range. The cooperation algorithms are needed when the node wants to forward a packet that is not in its communication range [2, 3]. Therefore, nodes in the MANET act as host and a router. Due to the lack of infrastructure and the incapability of preventive measures such as encryption, authentication, and cryptography for detecting the newer attacks leads the wireless networks more susceptible to be attacked than wired one. Moreover, these preventive measures cannot work because of scarce resources such as computational power and bandwidth. As the cost of information processing and accessibility to the Internet falls, more number of organizations are becoming exposed to a wide variety of cyber threats. As per recent survey by CERT/CC [4], attacks have rapidly increased over the past decade. Data mining-based intrusion detection techniques are categorized namely: misuse detection, anomaly detection, and specification-based [5]. The most widely used method for protecting against cyber threats is signature-based detection. The major advantage of this method is that it can detect known attacks that have a signature database, but fails under novel attacks. Mobile ad hoc networks are more open to attacks than traditional networks due to the lack of association among the nodes, unreliability of wireless links between nodes, accommodating algorithms, open medium, and topology changing when the nodes move in and out [6].

The MANET is susceptible to submissive and energetic attacks [7]. The submissive attacks typically involve only eavesdropping of data, whereas the energetic attacks involve actions performed by adversaries such as imitation, modification, and deletion of data. Internal intrusion attempts are more damaging in nature since malicious nodes acts as authorized member of the network. Chaki and Chaki [8], these nodes are called compromised nodes. The external intrusion attempts create jamming problem, propagate incorrect routing information to the nodes, and prevent services from working properly. Moreover, most of the routing protocols proposed for mobile ad hoc networks assume that every node is cooperative and not malicious [9]. Therefore, only one compromised node can split the entire network. The radio channel which is used for communication is broadcast and is shared by all the nodes. Therefore, a malicious node can easily obtain the transmitted data. The directional antennas can be used to reduce the problem up to some extent [10].

In Zhang et al. [11], a network model has proposed to detect the abnormal behavior of the node, the loopholes of this model is that if any links fail and the intruder moves away, then it will be very difficult to detect it. In Subhadrabandu et al. [12], proper placement of the intrusion detection active nodes covers the entire network. It works fine for the network with hypothesis that it will be moderately static in behavior. In Stamouli et al. [13], a prototype for IDS has presented where each node runs IDS at local level and cooperates with all IDS running in the network. The performance of the system degrades when there is a high mobility among the nodes, and it also suffers from high bit of exchanged messages.

The rest of the paper is organized as: In the next section, we discuss cluster head formation concepts. Section 3 presents the proposed system for malicious node detection and state-of-the-art scenario. Finally, Sect. 4 draws conclusions.

The aim of the paper is to study the challenges in MANET and the process to detect the malicious node in the network by continuously monitoring the network.

2 Cluster Head Formation

Mostly in ad hoc wireless networks, the nodes are continuously moving and are not stable; this affects the efficiency of the protocol. Bandwidth reservations are of no use if the node mobility is very high. Moreover, MAC protocol does not influence the mobility of the nodes [14]. The cluster head is acknowledged by its own identification number and is responsible for running entire network. For cluster head election, different researchers have used different concepts. It is very difficult to find out whether any abnormal activity is carried out by malicious node or there is a failure in the routing link. Node clustering is essential in MANET, so that nodes communicate with the cluster head and cluster head communicates aggregate information among them, this helps in minimizing the congestion and energy could be saved [15]. The algorithm for cluster head selection is given in Fig. 1.

Consider an example of node 0, the preliminary simulation shows that node 6 is the neighbor node of node 0. The *x*-position of node 0 is 549 and *y*-position is 100 and node 6 *x*-position is 800 and *y*-position is 200. After putting these values in the mathematical formula, we get 270.

```
Input :- Node with initial energy
Output :- Cluster head with maximum residual energy and distance less than
300.

# Calculation of clusterheads
Create node= node_id;
Set Channel=802.11
Set InitialEnergy= $inienergy;
Set Residual Energy= $ resenergy;
Set radiorange= default;
If(( node in radio range) && (next hop!=Null)
{      Capture data_load (node_all);
  Create node_Configure (rreq,rrep, tsend, tsend, trecv, tdrop, inienergy,
resdualenergy);
{  pkt_type;
       Time;
 tsend, trecv, tdrop, rrep, rreq; }
}                for (i=0; i<nn; i++)
     consumeenergy[i] = finalenergy[i] - initialenergy[i]
     totalenergy[i] = consumeenergy[i]
     if(maxenergy[i] < consumeenergy[i]){
            maxenergy = consumeenergy[i]
            node_id = i; }
            if (dist<300 && maxenergy[node_id]>
energyneighbour[node_id])
{  maxenergy node is clusterhead ; }
```

Fig. 1 Pseudo code for cluster head selection

Table 1 Brief summary of node energy and probable cluster head

Node number	Initial energy (J)	Total energy (J)	Residual energy (J)	Probable cluster head
0	17.0433	72.9567	55.9134	0
5	38.0174	51.9825	13.9651	0
6	38.0433	51.9567	13.9134	0
11	42.9690	47.0309	04.0619	0
12	42.9716	47.0295	04.0579	0
16	22.0423	67.9577	45.9154	0
17	22.0433	67.9567	45.9134	0
18	22.0439	67.9555	45.9116	0
19	22.0440	67.9578	45.9138	0

$$\begin{aligned}\text{distance} &= (\text{sqrt}(\text{pow}((\$\text{node } x2 - \$\text{node } x1), 2) + \text{pow}((\$\text{node } y2 - \$\text{node } y1), 2))) \\ &= (\text{sqrt}(\text{pow}((800 - 549), 2) + \text{pow}((200 - 100), 2))) \\ &= (\text{sqrt}(\text{pow}((251), 2) + \text{pow}((100), 2))) \\ &= (\text{sqrt}(63001 + 10000)) \\ &= (\text{sqrt}(73001)) \\ &= 270\end{aligned}$$

Table 1 shows the initial level energy and residual energy, the condition if (dist < 300 && maxenergy [node_id] > energy neighbour [node_id]) is satisfied here. Therefore, Node 0 is selected as Cluster head.

3 State-of-the-Art Scenario and Proposed Algorithm

Each node maintains data_table for storing elected cluster head id and the key value generated by the cluster head. Elected cluster head sends <*CH id*> to all members of the cluster. There is less probability of malicious node occurrence if this process is done before the transmission of packets.

Requesting all members of the cluster:

Send REQUEST to all cluster members for maintaining (<*CH id*>) in data_table. On receiving the REQUEST, cluster member [CM] sends REPLY message to the elected CH. CM[j] places (<*CH id*>) in data_table [j].

Executing the network:

Cluster head sends and receives the packet only if it gets reply message from all the members of the cluster.

Releasing the position of cluster head:

When an energy level or signal strength drops below the threshold or cluster head wants to release voluntarily. Exiting cluster head sends a time stamp RELEASE message to all cluster members. On receiving RELEASE message, CM[j] removes (<*CH id*>) from its data_table and keeps only the exit time stamp of cluster head in data_table.

The time stamp field gives the exact time when cluster head exits. This helps in finding the malicious node. The overhead here is it takes $3(N - 1)$ messages. Synchronization delay is 2T [16].

The proposed algorithm for intrusion detection is shown in figure. After gathering the network information, we set up an array for initial threshold value and initial time frame for attacks to be detected. Initially the tag bit associated with the node is set to 0 and if any node is behaving abnormally or dropping the packets above the threshold, then the tag bit is change to 1, such packets is called as dirty packets. The mistrustful table consists of doubtful node address, the total number of dirty packets sent by the node, total packets received by the node, and the total which is numeric value gives the information about total number of packets sent and received by the node including dirty packets. The map table correlates with threshold, time interval between the malicious node detected and the misbehavior of the node [17]. After capturing the network profile, audit the data analysis and check the abnormal behavior of the node, if it is observed checks for such misbehavior incident occurred earlier from the same node or not. Then insert the suspicious node address in the database and increment the value of count1 and total by 1 [18]. Then different operations takes place on the mistrustful table, at each dirty packet sent by the node, the values of the count1 and total is increment by 1, respectively. The proposed algorithm declared the node as intruder or malicious when it crosses the threshold value and within the time frame with the matching of abnormal behavior from the database [19]. The cluster head communicates the malicious node information to all the heads which are in the radio range using the transfer (dna, targetcluster_head). The proposed algorithm for intrusion detection is given in Fig. 2.

Table 2 shows the two categories, normal case and attack case. Table gives the overall summary of the network. It has been observed that the proposed algorithm could identify 533 attack cases out of 828 numbers of packets sent from the doubtful node. The total numbers of packets received are 804; there are 482 cases of the attack identified by the proposed algorithm.

```
// Gather network information to generate a normal profile of the network.
  Define_Normal_Profile();
//Initialize variables after resolve period
// Network Profile capture by sniffer
// Mistrustful_Table ←——— {information} // information
(doubtful_node_address, Count1, Count2, Total)
 doubtful_Node_Address ←———  alphanumeric
Count1 ←———  numeric // Total number of dirty packets sent by the node
Count2←——— numeric // Total number of packets received by the node
Total ←——— numeric// Total packets sent and received by the node
Map_table(); // correlates attacks with threshold, time_ intervals,
mis_behavior counters
 Initial_thresholdvalue []; //depends on the type of Attack and type of
Network
Initial_TimeFrame []; // specific to attack model
//Set three Dimensional Arrays for each of the nodes in the network
 mis_behavior count [node][attack][misincident];
//do a mapping and perform correlation of mis_behavior with corresponding
attacks
        Capture_NetworkProfile () {
Audit_data_analysis()
      {If (mis_behavior takes place and sensed) {
    mis_behavior _analysis (); //analyze mis_behavior
Store mis_behavior _information ();
 // store mis_behavior _information means type of network, source node,
destination node, number of messages send and receive}
  If (sender node has generated such mis_behavior earlier)
       insert_row_info(dna){
 Count1 = 1; // node sent dirty packet for the first time
                Total = 1;
                Doubtful_Node_Adddress= dna;
add (Doubtful_Node_Address, Count, Total); // adds new record to the
Mistrustful table }
      {If (current mis_behavior = earlier ones)
   {  Then ask for ( cIuster head id or exit time stamp of previous cluster
head) increment counter for the sender node}
increment_count1 (dna){
                    Count1 = Count1+1;
                    Total = Total+1;}          {  get_info(dna, cnt1,
cnt2, total) // Getting complete information about the doubtful node}
{ ask for doubtful_Node_Address = dna;
                  cnt1 = Count1;
                  cnt2= Count2;
                  total = Total; } else
add this to a variant of mis_behavior  database for this attack type
           } //determine if attack is taking place
If (threshold is crossed && within time frame && this variant of
mis_behavior for this type of attack)
            {Sender node has launched an attack
              transfer (dna, targetcluster_head)
{          ask for doubtful_Node_Address =dna;
                cnt1 = count1;
                total = Total;
                triple= <dna, cnt1, total>;
      send (targetcluster_head, triple);}}}}
```

Fig. 2 Proposed algorithm for intrusion detection

Table 2 Brief summary of network

Parameter	Normal case	Attack case
Send	828	533
Receive	804	482
Routing packets	99	219,882
Packet delivery fraction	97.1	90.43
Normalized routing load	0.12	456.19
Average end-to-end delay (ms)	852.04	751.64
Number of dropped data (packets)	23	51
Number of dropped data (bytes)	23,852	44,556

4 Conclusion

MANET is more exposed to be attacked than wired network. Preventive measures such as encryption and authentication may be used as the first line of resistance for reducing the attack possibilities. These techniques are unable to protect a network from newer attack. The research on security is still in its early stage. The existing systems are typically attack oriented; they first identify the threats and then augment the existing protocols to prevent it. They may work well for predefined attacks, but fail under unanticipated attacks. Therefore, there is a requirement of more motivated security system that results in depth protection for anticipated and novel attacks. It is difficult to find a generic solution which works efficiently against all types of attacks, since attack has its own distinctiveness. Sometimes, it is very difficult to comprehend whether any abnormal activity is carried out by the node or there is a link collapse. The mathematical approach for cluster head selection based on the distance and energy gives the realistic result. The proposed algorithm for intrusion detection aggregates all the information before declaring any node as malicious. The proposed algorithm also suggests how the cluster head communicates the malicious node information to all the heads which are in the radio range.

References

1. Zhang, Y., Lee, W.: Intrusion detection in wireless ad hoc networks. In: Proceedings of the 6th International Conference on Mobile Computing and Networking (Mobi-Com 2000)
2. Perkins, C.E.: Ad Hoc Networking, pp. 198–264. Addison-Wesley, New York (2001)
3. Perkins, C.E., Royer, E.M.: Ad hoc on-demand distance vector routing. In: Proceedings of the 2nd IEEE Workshop on Mobile Computing and Applications, vol. 3, pp. 99–100. New Orleans, LA, USA (1999)
4. Successful Real-time Security Monitoring. Riptech Inc. White paper (September 2001)
5. Lazarevic, A., Ozgur, A., Ertoz, L., et al.: A comparative study of anomaly detection schemes in network intrusion detection. In: Proceedings of the 2003 SIAM International Conference on Data Mining, pp. 25–36. Society for Industrial and Applied Mathematics (1 May 2003)

6. Zhang, Y., Lee, W., Huang, Y.: Intrusion detection techniques for mobile wireless networks. ACM/Kluwer Wireless Netw. J. (ACM WINET) **9**(5) (September 2003)
7. Mandala, S., Ngadi, M.A., Abdullah, A.H.: A survey on MANET intrusion detection. Int. J. Comput. Sci. Secur. **2**(1)
8. Chaki, R., Chaki, N.: IDSX: A Cluster Based Collaborative Intrusion Detection Algorithm for Mobile Ad Hoc Networks, 6th (CISIM '07), University of Calcutta. IEEE
9. Endorf, C., Schultz, E., Mellander, J.: Intrusion Detection & Prevention. McGraw-Hill. ISBN: 0072229543 (2004)
10. Smith, J., Clark, A., Gill, R.: Specification-based intrusion detection in WLANs. In: Proceeding of the 22nd Annual Computer Security Applications Conference (ACSAC'06) (2006)
11. Zhang, W., Rao, R., Cao, G., Kesidis, G.: Secure routing in Ad hoc networks and a related intrusion detection problem. In: Proceedings of IEEE Military Communications Conference (October 2003)
12. Subhadrabandu, D., Sarkar, S., Anjum, F.: Robust intrusion detection in Ad hoc networks. In: Proceedings of the Fourth International IFIP-TC6 Networking Conferences
13. Stamouli, I., Argyroudis, P.G., Tewari, H.: Real-time intrusion detection for Ad hoc networks. In: Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, pp. 374–380 (2005)
14. Rani, V.G.: Maximum Trusted Cluster Head Selection Algorithm for MANET, vol. 10, no. 9. Asian Research Publishing Network, May 2015. ISSN 1819-6608
15. Chen, H., Megerian, S.: Cluster Sizing and Head Selection for Efficient Data Aggregation and Routing in Sensor Networks. University of Wisconsin Madison, USA
16. Chandy, K.M., Lamport, L.: Distributed snapshots-determining global states of distributed systems. ACM Trans. Comput. Syst. **3**(1), 63–75 (1985)
17. Nadkarni, K., Mishra, A.: Wireless internet networking laboratory. Virginia Tech, a Novel Intrusion Detection Approach for Wireless Ad Hoc Networks. IEEE Communications Society
18. Nadkarni, K.: An intrusion detection scheme for wireless mobile Ad hoc networks based on DSDV protocol. Master's thesis, Department of Computer Science, Virginia Tech
19. Malladi, R., Agrawal, D.P.: Current and future applications of mobile and wireless network (University of Cincinnatti, OH). Commun. ACM **45**(10), 144–146 (2002)

Attack in Smartphone Wi-Fi Access Channel: State of the Art, Current Issues, and Challenges

Kavita Sharma and B.B. Gupta

Abstract Today, Smartphone device uses are increasing day-by-day such as email, gaming, Internet banking, which requires it to always remain connected with Wi-Fi. This makes it vulnerable to numerous attacks. In this paper, we explore different Smartphone vulnerabilities, malwares, and security challenges. In addition, we also present a classification of various security solutions proposed in the literature. It provides better understanding about current security issues and challenges in Smartphone Wi-Fi access channel, current solution space, and future research direction to protect it from variety of DDoS attacks.

Keywords Smartphone · Smartphone Wi-Fi · DDoS attack · SSL protocol · Access channel

1 Introduction

The mobile phones are categorized into two different categories based on its feature, i.e., dump phone and Smartphone. Whenever mobile phone has features such as voice, Short Message Service (SMS), and Multimedia Message Service (MMS), then it is called as a dump phone, and if a dump phone has some extra features such as Wi-Fi [Wireless Fidelity although it give the impression stimulated by "hi-fi" (high fidelity)], Bluetooth, then it is called as a Smartphone. It means Smartphone is equipped with Wi-Fi facility, high-speed multi-core process and enough gigabytes, and user-friendly operating environment [1].

K. Sharma (✉) · B.B. Gupta
Department of Computer Engineering, National Institute of Technology, Kurukshetra, India
e-mail: kavitasharma_06@yahoo.co.in

B.B. Gupta
e-mail: gupta.brij@gmail.com

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_56

Smartphone is an essential device for our personal and professional work. Smartphones have novel features and access to novel applications are provided with the help of Wi-Fi access point. This leads to security issues in Smartphone, and it is the biggest challenge for defense and detection of Smartphone Wi-Fi access point malware.

The Wi-Fi is an important feature of Smartphone. Smartphone provides the facility of anywhere and anytime to connect with public or private network through its Wi-Fi feature. Wi-Fi technology is facilitated to device for wireless communication, and the most common usage is Internet access [2].

Smartphone is a programmable device that is designed for user-friendly environment. Since Smartphone has more confidential information, higher level of security is required. Today, every place has open access Wi-Fi hot spot such as airport, coffee shops. Attacker can steal the Smartphone's confidential information when they access the public place.

Therefore, Smartphone is faced with many security challenges. When attackers set up the fake Wi-Fi access point and disconnect all existing connection, it is called denial-of-conveniences attack. It disables the Wi-Fi feature to prevent the Smartphone from this attack [3]. In this paper, we explore different Smartphone vulnerabilities, malwares, and security challenges. In addition, we also present a classification of various security solution proposed in the literature. It provides better understanding about current security issues and challenges in Smartphone Wi-Fi access channel, current solution space, and future research direction to protect it from a variety of DDoS attacks. Rest of the paper contains the following sections: Sect. 2 describes the attack on Smartphone Wi-Fi and different types of attacks. Section 3 explains the role of DDoS attack in Smartphone Wi-Fi. Section 4 describes the defense mechanisms against DDoS attack on Smartphone Wi-Fi access channel. Finally, Sect. 5 has conclusion and future work.

2 Attack on Smartphone Wi-Fi

With the usage of Smartphone, the use of Wi-Fi access has increased which is freely available in all places inside and outside the home. All Smartphone users are fully dependent on the Internet for access of emails, chat, video conferencing, new interesting applications, and games through the Wi-Fi access points, and thus, they face the security issues. It is a big challenge to find the attack and its defense. In public network, Wi-Fi attacker provides the fake access point, easily accessed by the users, and steals the user confidential data with encrypted nature of public network, and fake off physical barriers to receiving all packets on the network. There is little vulnerability faced when such an access is done through Wi-Fi access points [4].

(i) **Man-in-the-Middle Attack**

Attacker eavesdrops himself in middle of an online session between Smartphone and hot spot from the attacking place. The attacker configures his laptop which behaves in public place as a Wi-Fi hot spot and gives its name in public area such as airport or coffee shop [5]. Then, the attacker waits for Smartphone to connect with the fake Wi-Fi hot spot to steal all confidential information, user id, credit card number, net banking id and password, etc. Smartphone connects with access point and accesses the server service, but man-in-the-middle attack configures the fake server set-up between access point and server.

(ii) **Rogue Access and Hot Spot**

The rogue access point identifies the authenticate user AP which is controlled by attacker. Attacker uses own hardware access point and software which is used to connect with legitimate through rogue access point.

(iii) **Denial of Service**

The DoS attack takes place on the user bandwidth when Smartphone users access the network. The attacker could flood the network with fake packets, basically consuming up all of the allowable bandwidth and making the network slow. It may be possible that the attacker easily identifies; however, the attacker can spoof sender address on the bad packets [6].

(iv) **Evil Twin Access Point**

The attacker uses unsuspected people to connect with the fake access point through evil twin access point. If user connects with the access point, then attacker steals all confidential data and captures the email and file transfer protocol connection. The attacker also spoofs DNS cache to display a fake website, and if user accesses the fake website, then the attacker captures the user's login credentials [7].

3 Role of DDoS Attack in Smartphone Wi-Fi

Smartphone is a programmable device that is designed for user-friendly environment. Since it has more confidential information, it requires higher level of security. Researchers are active in the field of Smartphone security, but there is no sufficient analysis of Smartphone security threats. The Smartphone vulnerability is categorized in two groups: internal and external. In internal, Smartphone vulnerability includes implementation error, incompatibility, and user unawareness. In external, it includes wireless networks and external objects [8].

These vulnerabilities lead to potential threats, which need to be resurfaced. Smartphone threats are divided in two groups: threats caused by attackers and threats caused by user unawareness or intention.

While jamming the Wi-Fi signals, attacker can create fake Wi-Fi AP, connect with the legitimate user, and access the useful information. Wi-Fi is a very common environment for personal and business purpose. It is mobile, convenient, and friendly for Smartphone users. Most wireless devices face the problem of eavesdropping and jamming. The attack on Apple, Google, Skyhook, and Microsoft location services is described, as these are four of the major location service providers and work on dual-band hardware. An implementation of the Wi-Fi-based location services attack is done on dual-band hardware [9].

When attackers set up the fake Wi-Fi access points and disconnect all the existing connections, then it is called denial-of-conveniences attack. This attack uses the Internet access validation protocols, in which the cellular network sends a secret key phrase to an Internet validation server. This attack is for attempt to retrieve this secret key phrase by the recently established Wi-Fi channel to authenticate the Wi-Fi AP. This paper [10] explored the three approaches to establish this attack as well as its defense techniques and proposed a novel approach to implement them on Android platform.

Wi-Fi direct technology increases local services that enable social interaction of the grid to provide the interconnection in between Smartphones. The device-to-device (D2D) network supports more resourceful proximity-based applications and decreases reliance on middle unit. The D2D modifies the information process and exchanges the information and resource sharing. This paper explored the role of DDoS attack over D2D underlying network [11]. Wi-Fi direct underlying network has lots of security issues, but denial-of-service attack is the major one. Wi-Fi Pineapple is used for security for such attacks. Wi-Fi Pineapple is a tool to protect the connection with the fake Wi-Fi AP in the network. The Wi-Fi routers are very vulnerable as the user does not change the router password and IP address [12].

4 Defense Mechanisms Against DDoS Attack on Smartphone Wi-Fi Access Channel

Here, we demonstrate the different approaches which provide the secure channel and maintain the confidentiality, integrity, and authentication of the phone data and network access channel.

(i) **Static Identifier Validation Technique**

The Microsoft Windows currently used network awareness protocol which has NCSI feature. This works as Wi-Fi authenticator. Wi-Fi authenticator automatically connects and verifies Wi-Fi AP; its functioning connects with the Internet without user interaction.

(ii) **Dual Channel Validation Technique**

To remove the static identifier validation problem, use dual channel validation. In this approach, validation key changes every time a validation test performed five steps process to validate [13].

(iii) **SSL Network Protocol**

The SSL protocol provides the communication between client and server. It maintains the confidentiality, integrity, and availability in communication data channel. This provides the end-to-end security against the MITM attack. SSL don't implement themselves using SSL library such as open SSL, GUI TLS, JSSE, crypto APT. [14].

(iv) **Fine-Grained Permission System**

This is the permission access Wi-Fi approach. To take permission access the access point then we scan the nearest Wi-Fi Access point and collect sensitive information. According to researcher survey, 51 out of 100 top applications on Google play store use the permission access Wi-Fi approach. Many types of applications are bandwidth-sensitive application such as audio, video, and play virtual reality online game. To use Permission system for detecting stable Wi-Fi connection to used data transfer. If the exact information about all access points is obtained, then, we use in our system fine-grained permission information system [15].

(v) **Trained Mean Matching Algorithm**

When rogue AP gets infected, then interpacket arrival time (IAT) server is observed. The IAT server matches the higher trained mean of two wireless hops. To use analysis the user applies two hop networks to communicate with remote server. Quadric mean technique is used.

(vi) **HOP Differentiating Technique**

HDT algorithm is more accurate to detect evil twin attack and calculates the accurate value of IAT. The ratio of server IAT to access point IAT shows the metric that is represented by the Server-to-AP-IAT (SAIR) (Table 1).

Table 1 Defense mechanism against attack on smartphone Wi-Fi access point

Year	Defense	Description	Weakness
2014	Use defense approach to multiple location service technologies, multiple bands, and fingerprinting	The attackers connect with legitimate user through the fake Wi-Fi access point and steal useful information	The complexity and cost of jamming plus impersonation attack decreasing because it is typical to do the cellular based location service. Which uses triangular to get an exact location
2013	To defense by fine-grained permission system	To trace the location and attack on the confidential information. Break the security model CIA	The application with some sensitive permission sets is actually benign from the result of static analysis; those permission sets might not be used by real-world attackers very often. In such cases, there is a good reason to remove it from the sensitive permission database
2012	To defense by using the improved and secure SSL validation protocol	To beak the SSL validation certificate protocol	The SSL certificate validation protocol in libraries and many security critical applications is completely broken
2011	To use trained mean matching (TMM) and hop differentiating technique (HDT)	To distinguish network traffic between wired and wireless nodes, use round trip time (RTT)	The demerits of this technique are distance and packets hops
2010	To use attack detection technique, TMM, and HDT algorithm	The evil twin attack compromised the security	TMM is time-consuming, trained knowledge is difficult, direct apply to another network

5 Conclusion

Smartphone devices play a very important role in everybody's life. With the increasing number of Smartphone usages, security threats are also increasing every day. This paper explored the Smartphone Wi-Fi access point features and issues against the malware threat to access the access point. It also describes the detection and defense techniques against the Smartphone security. In future, there is a need to develop an efficient model which can provide more secure Wi-Fi channel when Smartphone user accesses the Internet facility anywhere.

References

1. Dondyk, E., Rivera, L., Zou, C.C.: Wi–Fi access denial of service attack to smartphone. Int. J. Secur. Netw. **8**(3), 117–129 (2013)
2. Wang, Y., Streff, K., Raman, S.: Smartphone security challenges, pp. 52–58 (2012)
3. Leavitt, N.: Mobile security: finally a serious problem? Computer 11–14 (2011)
4. Gupta, B.B., Joshi, R.C., Misra, M., Meena, D.L., Shrivastava, G., Sharma, K.: Detecting a wide range of flooding DDoS attacks using linear prediction model. In: IEEE 2nd International Conference on Information and Multimedia Technology (ICIMT 2010), vol. 2, pp. 535–539 (2010)
5. Li, B., Im, E.G.: Smartphone, promising battlefield for hackers. J. Secur. Eng. **8**(1), 89–110 (2011)
6. Shrivastava, G., Sharma, K., Rai, S.: The detection & defense of DoS & DDos attack: a technical overview. In: International Conference on Computer Engineering and Technology, pp. 274–282, 2010
7. Wei, T.-E., Mao, C.-H., Jeng, A.B., Lee, H.-M., Wang, H.-T., Wu, D.-J.: Android malware detection via latent network behavior analysis. In: The 2012 International Symposium on Advances in Trusted and Secure Information Systems (TSIS 2012), Liverpool, UK, pp. 1251–1258 (2012)
8. Husted, N., Saïdi, H., Gehani, A.: Smartphone security limitations: conflicting traditions. In: Proceedings of 2011 Workshop on Governance of Technology, Information, and Policies, ACM, pp. 5–12 (2011)
9. La Polla, M., Martinelli, F., Sgandurra, D.: A survey on security for mobile devices. IEEE Commun. Surv. Tutorials **15**(1), 446–471 (2013, First Quarter)
10. Hadiks, A., et al.: A study of stealthy denial-of-service attacks in Wi-Fi direct device-to-device networks. In: 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), pp. 507–508. IEEE (2014)
11. Ramu, S.: Mobile malware evolution, detection and defence. Term Survey Paper, April 2012. http://blogs.ubc.ca/computersecurity/files/2012/04/SRamu_EECE572_SurveyPaper-Srikanth Ramu.pdf
12. Mancinelli, D.: Public Wi-fi: Friend or Foe?, pp. 1–9 (2014)
13. Feng, J.L.R., Gong, G.: Vulnerability Analysis and Countermeasures for Wi-Fi-based Location Services and Applications, pp. 1–12 (2014)
14. Patil, S., Vanjale, S.: A survey on malicious access point detection methods for wireless local area network. Int. J. Comput. Sci. Eng. **2**, 22–25 (2014)
15. Zheng, X., et al. Accurate rogue access point localization leveraging fine-grained channel information. In: 2014 IEEE Conference on Communications and Network Security (CNS). IEEE (2014)

Evaluating Pattern Classification Techniques of Neural Network Using *k*-Means Clustering Algorithm

Swati Sah, Ashutosh Gaur and Manu Pratap Singh

Abstract In the era of digitization, there is huge amount of digital data being processed and collected in the repositories. Lots of useful information and data patterns are hidden in this bulk data usually known as Big Data these days. So, it is now becoming important to store and manage this huge data for extracting important patterns and information for future decision-making. Classification is one of the important techniques while dealing with this huge amount of data. It is important to understand the diversity in the given set of data. Classification is the prediction of certain outcome on the basis of given input. In real life also, classification is the most common activity of human life. It is quite common phenomena of the day-to-day life, especially when we are involved in analytical task. It supports the decision-making task in business, research, etc. The classification problem is applicable on assigning label to an object among predefined group of elements on the basis of its properties and behaviour. Classification is the process of classifying the data in the different labels as per similarity measures of the defined groups. These days almost every field of research, medicine, business and industry, etc., are dealing with classification problems. Fraud detection, diagnosis of diseases, pattern recognition, loan approval and others are some of the examples of the classification problem. Data classification and clustering are the important techniques used in data mining. With the emergence of large volume of digital data, it becomes major challenge to manage this data in effective and efficient manner. Data mining is one of the techniques used for extracting required information from the large set of data. Various methods have been adopted in data mining in which data classification and clustering are used for labelling/grouping of data. Data classification may be defined as grouping of objects as per their similar characteristics on the basis of

S. Sah (✉) · A. Gaur
Bharati Vidyapeeth Deemed University Institute of Management & Research, New Delhi, India
e-mail: swati.sah@bharatividyapeeth.edu

A. Gaur
e-mail: gaur.ashutosh@bharatividyapeeth.edu

M. P. Singh
B.R. Ambedkar University, Agra, India

D.K. Lobiyal et al. (eds.), *Next-Generation Networks*, Advances in Intelligent Systems and Computing 638, https://doi.org/10.1007/978-981-10-6005-2_57

prior knowledge available to the system, i.e. classification groups the entities as per their similar features with available prior knowledge (supervised). Clustering is the method of grouping of objects as per their similar features without having prior knowledge (unsupervised). Neural network or artificial neural network is the mimic of human brain. It is the network of interconnected artificial nodes to process the information and provide its final output. Neural network is one of the tools of classification used in soft computing techniques. Various research studies have been done on neural network for classification task due to its best performance. Neural networks are treated as black box due to its hidden data processing. It can adjust its weight by itself. Usually, neural networks have the ability to learn the pattern itself by means of training process in the network. The error updation feature in the neural network adjusts the error after each iteration to make it more accurate (learning process of the ANN). Neural networks can approximate given function with arbitrary accuracy. Neural networks are nonlinear models, which help them flexible in modelling real world complex relationships. The objective of this paper is to evaluate pattern classification techniques of neural network using clustering technique. The focus of this paper is on the application of data mining in large database system and analysis of pattern classification techniques of neural networks in the database using *k*-means algorithm.

Keywords Data mining · Pattern classification · Cluster analysis
K-means algorithm · Neural network · Back-propagation algorithm

1 Introduction

In the era of digital processing, it is difficult to manage the large volume of digital data, results in data storage and management problem globally. These days' data is processed and stored in digital form everywhere. Even availability of cheap storage devices may also lead to increase in the usage of digital data storage. Lots of data is available, and people are thinking to manage this data. Apart from the data management problem, some of the scientists/practitioners are focusing on the extracting/mining the important patterns from this data. So the management of Big Data is now become the commercial phenomena. Data mining is one of the techniques to extract information from the data so that it can help in business decisions. The numbers of databases are increasing exponentially which leads to data management requirement issues. Extracting information in these databases has become slow and complicated process due to large volume of data. So, it is the requirement of the time to have a feasible resolution for data storage and management problem. The process of significant modelling and their evaluation in knowledge discovery in the database are also called as data mining, and it may be defined as way of extracting information from the large database to support business decisions and requirements. Data mining discovers hidden information which is not visible, but potentially helpful in an efficient and effective way.

The term data mining has been extended further than its limits for using it in data analysis. There are different definitions of data mining which are as follows:

1. Data mining can be defined as extraction of unknown information, which can be useful for business decisions. It contributes number of different technique, like clustering, data cleaning, learning, classification, and analysing changes [1].
2. Data mining is the search of global patterns that exist in large data sets but are usually "*invisible*" among the huge amount of data. Relationship among the data can be explored by mining the data. These relationships can be proved as valuable information about the data and the objects in the database [2].
3. Data mining refers to "*application of variety of tools and techniques to explore useful information to support day-to-day decision-making process within the organization. It supports classification as well as prediction task on various domains. It is the hidden information in the data that is useful for different class*" [3].

Neural network is an essential software used for categorization. Current research trend shows that neural networks are good substitute for different classification methods. The benefit these neural networks have is that neural networks are data-driven self-adaptive and self-learning methods that can change their self to the expected data without any clear requirement of practical or distributional form for the original model. The neural networks can estimate any task with random precision. They are basically neural estimators; they are the nonlinear models, which model actual world compound associations. They are also helpful in estimating later probability, which is the base for creating categorization and carrying out data analysis.

Clustering is the grouping technique to group the similar objects in the clusters. It is widely used in classification task. However, it comes under unsupervised learning technique. Clustering can be classified as hierarchical and partitional. In cluster analysis, *k*-means algorithm is a partitioning algorithm. The *K*-mean algorithm is developed by MacQueen in 1976 [2]. *K*-means clustering is a partitional clustering technique which has the objective of creating *k* clusters and then partition that partitions the data into analogous *K* classes. Data items which are nearby are considered to be similar and can be grouped together under one label. Partitional clustering algorithms are done in order to assemble data that is near to each other. In partitional algorithms, count of cluster to be created should be mentioned in advance. One of the goals of partitional algorithm is to divide the data items into similar groups and then each of these groups is divided into further groups, and so on. Another clustering technique, hierarchical clustering results in dendrogram, is a top-to-bottom approach of clustering.

In the *K*-means algorithm, apart from data, input to the algorithm must have *k,* i.e. the total number of cluster, to be developed on the given data set. Following are the basic steps of algorithm (Fig. 1) as:

Algorithm :-

- ***Select k, number of clusters to be find out***
- ***Select k objects arbitrarily as the original cluster center***
- ***continue***
  - *Allocate each object to their neighboring cluster center*
  - *Using Euclidean distance*
  - *Calculate new cluster centers*
  - *Compute mean points*

Till*No alteration in cluster centers or*

- *No object change its cluster*

Fig. 1 Step of *K*-means algorithm

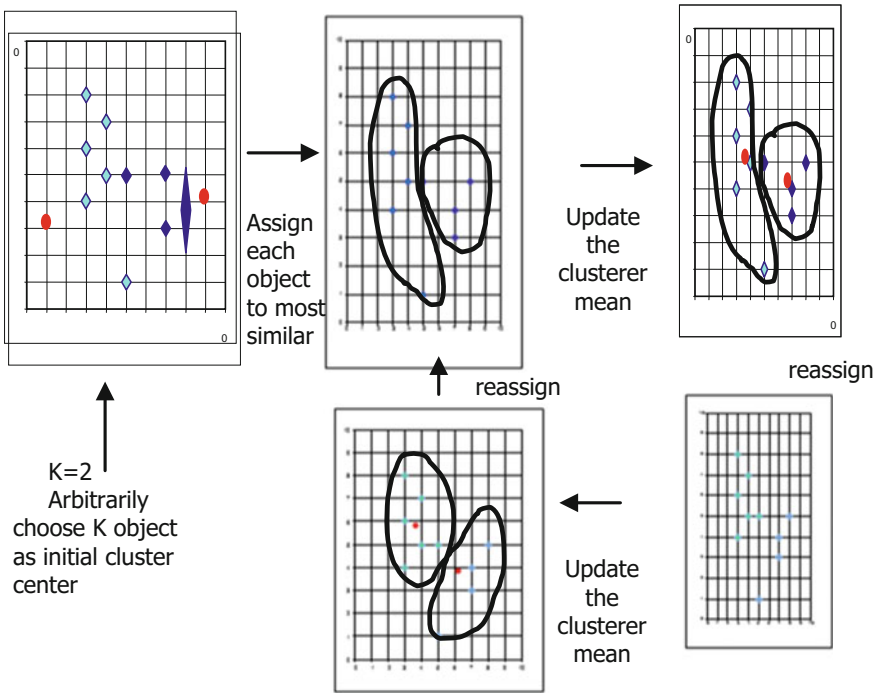


Fig. 2 Object grouping on the basis of minimum distance considering Euclidean distance

1. Find out the centroid coordinate of given data set.
2. Find out the distance of each object to the centroids in the data set.
3. Object grouping on the basis of minimum distance considering Euclidean distance (show the Fig. 2).

The algorithm discussed in Fig. 1 can be viewed as the following diagram.

Cluster analysis is a grouping technique applied usually on multivariate data analysis with like features which are identified and classified (grouped) accordingly. Although in cluster analysis, thick and thin region among the data set can be identified easily, and diverse distribution patterns must be accomplished consequently. The notions of likenesses and dissimilarities are calculated in cluster analysis either by using Euclidean distance or by Manhattan distance method. Unlike methods might be used in finding out the resemblances and differences in the given data set. This learning uses the Euclidean distance measure in cluster analysis. The Euclidean distance measure is generally used as a distance calculating tool, also it is simple to use in 2D planes. Number of dimension is directly proportional to computation time. That is by increasing number of dimensions, computation time also increases [4].

The Euclidean distance can be represented as,

$$d(i,j) = \sqrt{(x_{i1} - x_{j1})^2 + (x_{i2} - x_{j2})^2 + \cdots + (x_{ip} - x_{jp})^2}$$

Now, assuming the similarity metrics:

$$i = (x_{i1}, x_{i2}, \ldots, x_{ip}) \text{ and}$$
$$j = (x_{j1}, x_{j2}, \ldots, x_{jp})$$

are two data objects whose dimension is p. The above formula states the distance between two data objects $d(i, j)$, and X_{ip} is the amount of object i in dimension p. Step of Euclidean distance with k-means algorithm is represented in Diagram 1.

Classification is the most popular tool used in data mining techniques to dig useful information from the dump data [3]. Classification aims at forecasting the

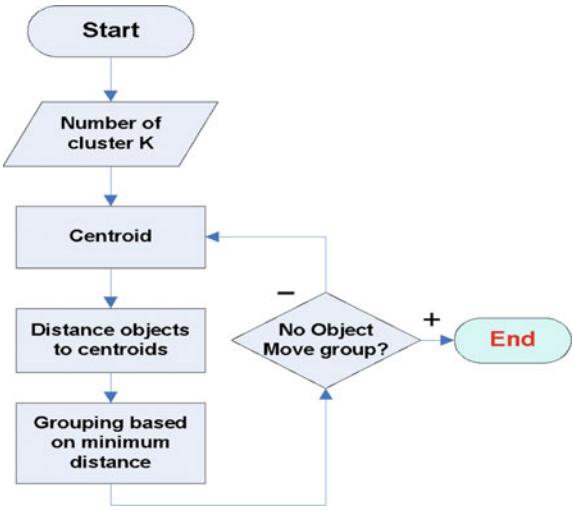


Diagram 1 Euclidean Distance using K-means algorithm

values of a user-defined output labels. Also, we can say that classification method discovers common features in a group of given items in a data set and then categorizing them differently. On the other side, data mining explore the similar properties among the given data set to classify them in similar groups or labels. Although the elements are similar in the assigned group but are very much dissimilar from the other group's elements (Fig. 3).

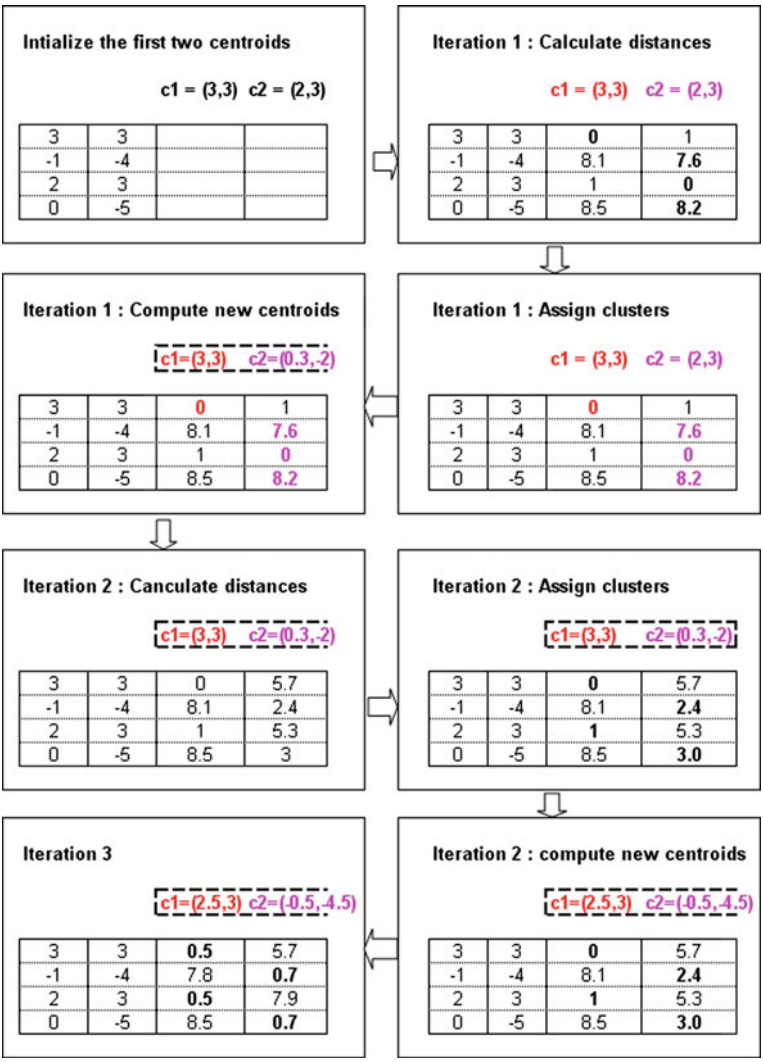


Fig. 3 Step-wise element grouping

In data classification method, there are many possibilities to check the specified model.

The most looked feature of discovered rule is to forecast the new class of elements.

For example, if we want to evaluate the new loan applicant while keeping in mind its features. There are numerous options to check this forecasting ability.

(1) Data set is split into learning and test data set.
(2) When data set is unique and some different techniques are used for estimating the classification procedure, for example *N*-field cross-validation.

N-field cross-validation is the other exceptional method that can be used when we have a single data set for calculating the classification algorithm. This validation method slices up the data set to *N* likewise selected subset of the similar dimension for every stage of entire *N* stages of procedure, one sub data set is applied for testing and the remaining subset is for training the algorithm.

For better understanding, the classification rule can be represented as:
if <certain states are fulfilled > then
<Forecasted _output _of_main_value>

Example of classification rule is
if (Work="Yes") and (UnpaidLoan="No") then
(Credit ="Good")

Above illustration states that forecasting values are Work and Unpaid Loan, and main value is Credit score, forecasting values are {"yes", "No"} and main a value is "Good" or "Bad".

This endeavour can be considered as simplification of classification assignment. The only point where it distinct is that we can choose the goal attribute in advance and THEN part can have as many attributes. One constraint is that the goal attributes cannot be the part of IF rule. Learning and evaluation are same as classification [5, 6].

In this paper, we have purposed data accessing process using data mining techniques. We used *k*-means clustering algorithm for data clustering and neural network techniques for data classification. In this paper, we are analysing multilayer feed-forward (acyclic) networks qualified with gradient descent with back-propagation algorithm approach.

Classification process has two parts: for building a model supervised learning training data set *c* and after that categorizing the facts depending upon the pattern. Some of the classification methods may be decision tree, neural network, KNN, Bayesian classification, SVM, etc. The activation functions are usually sigmoidal. When we classify a tuple, some of the attributes from the row are inputted to the

directed graph at the input vertex. The results derived show the probability of the respective input rows belonging to that class. Tuple is then passed to membership the class with the maximum possibility of association [7].

There are various advantages of using neural networks technique for classification task:

1. The performance of neural network can be increased by training. It can continue even after applying training set.
2. For enhancing output, application of neural network can be increased.
3. When a suitable training is applied, we can see reduced error rate and greater accuracy.

Although the *K*-means algorithm frequently shows superior outcomes, it takes lot of time and does not gel well with global clusters. By saving distance information from one iteration to the next, the actual number of distance calculations can be reduced [8]. Time complexity of *K*-means is O (tkn) (where t = number of iterations, k = number of clusters and n = total number of objects). *K*-means algorithm discovers a local optimal and can overlook the mean defined on the attribute type.

Only convex-shaped clusters are found in *K*-means algorithm. It sometimes does not handle outliers as well. One variation of *K*-means, *K*-modes, can handle categorical data. Instead of using means, it uses modes in categorical data [9]. *K*-means algorithm is an unsupervised learning technique of clustering (no information is assumed to be known for the different samples).

Patterns Classification Approach with Neural Network

Artificial neural networks (ANN) are the networks of "neurons" based on the neural structure of the brain. It process the data and train itself which ultimately helps in learning of the network. The bugs generated from the first iteration in classification are passed in response to the network and used to adjust the weights of the networks, and so on for many iterations [10] (Fig. 4).

The inputs are stored in input layer of the network. It is called as an input vector

$$(X = \{x_1, x_2, x_3, \ldots, x_n\})$$

where n = number of attributes to be used for further processing as input.

Input Layer: elements or nodes to be classified.

Hidden Layer: The number of nodes in the hidden layer and the number of hidden layers depends on the nature of the network as well as the application (***O_j, j = 1, 2, 3, 4*** …, ***#hidden nodes***). The hidden layers are constructed for the process of learning by computation on their nodes and arc weight. The network can have one or more hidden layers, and number of nodes in the hidden layer(s) is determined via experimentation.

Output Layers: The result of the classification is the output of a node in output layer (***O_k, k = 1, 2, 3, 4***,…, ***#classes***).

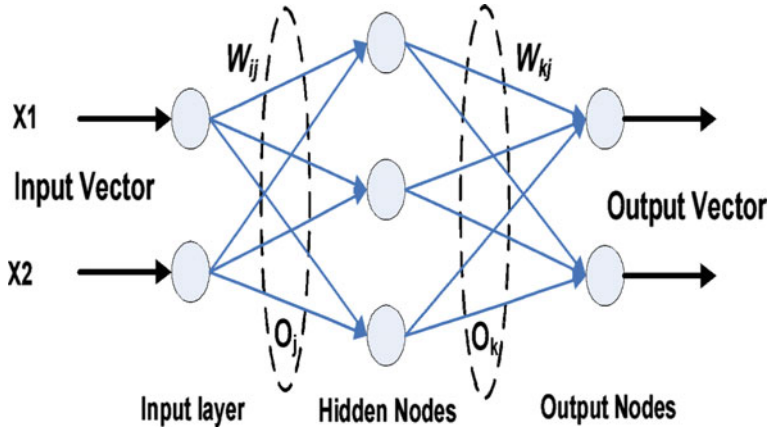


Fig. 4 Artificial neural network representation

User can define following things:

1. Number of elements in the input layer,
2. Number of hidden layers,
3. Number of elements in each hidden layer and
4. Number of elements in the output layer.

Entered values are standardized from range 0.0 and 1.0 owing of momentum in learning part. While training a network if the results are inaccurate and hence unacceptable, the network is trained again with other network configuration or other input weight. This is back-propagation of neural network to update/adjust the weights. The back-propagation trains by repetitively processing various learning patterns.

It relates the network's outcome for each output with the input class [11].

From Fig. 5, the outputs of input vector X are the inputs to weight vector W which are outputs from the previous layer which are multiplied by their respective weights to produce weighted sum, which is added to the bias associated with unit $\boldsymbol{j}$. A nonlinear activation function f is used for data mining the net output [12].

The weights are modified to minimize the mean squared error between the network's output and the actual input. Manipulations are back traced from output layer to every hidden layer passing down to first hidden layer [13, 14].

The steps for the algorithm are:

1. Set initial weights of input layer
   The weights and the biases are initialized between the range −1.0 to 1.0.
2. Disseminate the inputs ahead.

The input and output of every element in the given hidden and output layers are processed accordingly. The training data sample is passed to the input layer of the network. To compute the net input to the element, each input connected to the

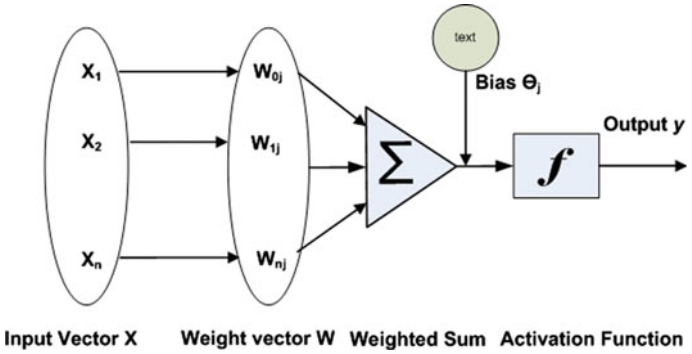


Fig. 5 Back-propagation of neural network

element is multiplied by its corresponding weight and summed to get the final output:

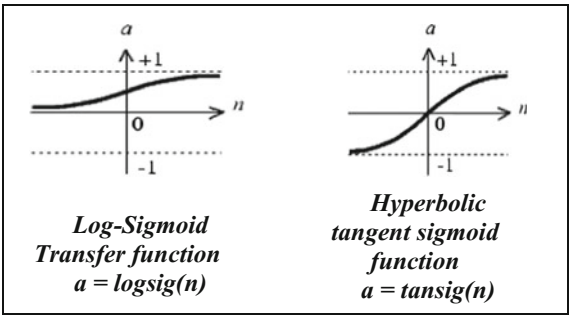
$$I_j = \left(\sum w_{ij}.O_i\right) + \theta_j$$

where W_{ij} = connection weight from the preceding layer to unit *j*. O_i is the output of unit *I* from the previous layer. θ_j is the bias of the unit.

For every element in the hidden and output layers acquire the net input and then the activation function is applied to it. The function signifies the stimulation of the neuron corresponding to that element. Here, any type of the nonlinear differentiable output signal function can use to compute the output, i.e.

Log-Sigmoid Transfer Function

$$O_j = \frac{1}{1 = e^{-I_j}}$$



Hyperbolic Tangent Sigmoid Function

This $O_j = \frac{e^{I_j} - e^{-I_j}}{e^{I_j} + e^{-I_j}}$ transfer function picks the input (whose value ranges from $+\infty$ to $-\infty$ and crushes the throughput in between 0 and 1 for log-sigmoid transfer function and -1 to 1 for hyperbolic tangent sigmoid function [15–17] (Fig. 6).

1. **Back-propagation error**

By adjusting the weights, the bugs/errors are propagated backwards and bias to consider the inaccuracy in networks prediction. For unit j in the output layer:

$$\text{Err} = O_j(1 - O_j)(T - O_j)$$

Somewhere, O_j is the real output of unit j, T_j remains the output and $O_j(1 - O_j)$ is derived from the logistic function [18, 19]. The error of a hidden layer unit j is given as:

$$\text{Err}_j = O_j(1 - O_j)\left(\sum_k \text{Err}_k . W_{jk}\right)$$

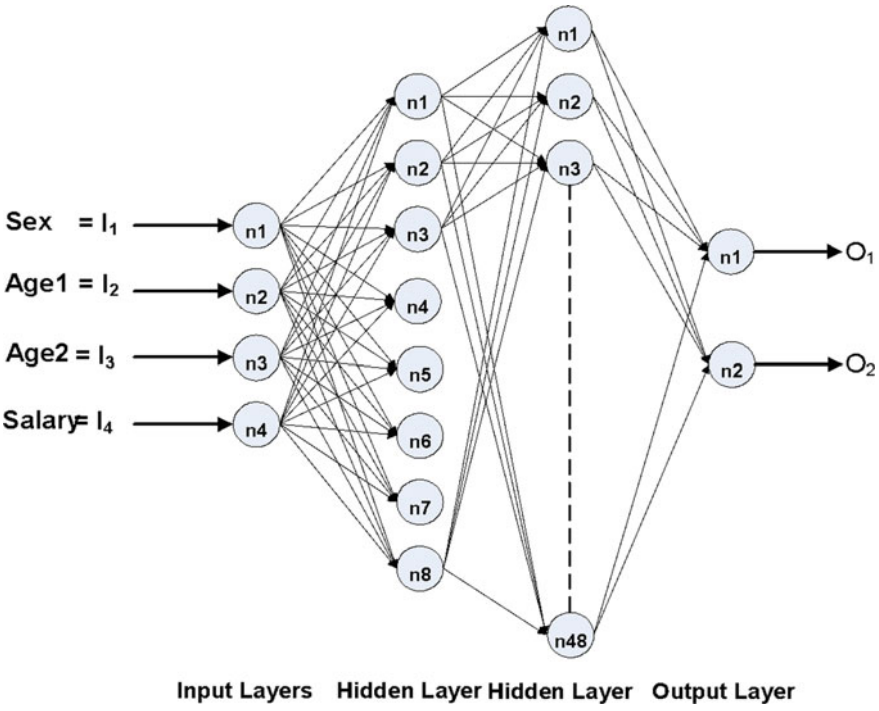


Fig. 6 Architecture of a multilayer feed-forward neural network

Table 1 Example of raw data (shown in 10 records from 3,127 records)

Attributes	Subinterval	Convert data
Sex	['F'], ['M']	0, 1
Age	[<=20], [21, 30], [31, 40], [41, 50], [51, 60] [>=61]	1, 2, 3, 4, 5, 6
Salary	[<=10000], [10001, 20000], [20001, 30000], [30001, 40000], [40001, 50000], [50001, 60000], [60001, 70000], [70001, 80000], [80001, 90000], [>=90001]	1, 2, 3, 4, 5, 6, 7, 8, 9, 10

where w_{jk} is the weight of the connection from unit $\boldsymbol{j}$ to a unit $\boldsymbol{k}$ in the next higher layer Err_k can be considered as error of unit $\boldsymbol{k}$. The weight and biases are revised to reflect the propagated errors [20]:

$$\Delta w_{ij} = (l)\mathrm{Err}_j O_i$$

$$w_{ij} = w_{ij} + \Delta w_{ij}$$

where $\Delta w_{ij} i$ is the changed weight w_{ij} and l is the learning rate. A constant l whose value lies between 0.0 and 1.0. The procedure is to fix the learning rate to $1/t$, where t is the number of repetitions. Bias of the network can be updated by following equations [21, 22]:

$$\Delta\theta_j = (l)\mathrm{Err}_j \tag{9}$$

$$\theta_j = \theta_j + \Delta\theta_j \tag{10}$$

where $\Delta\theta_j$ is the change in bias θ_j.

1. **Terminating condition**

Learning stops as: all Δw_{ij} in the earlier epoch are so little as under particular threshold or the percentage of sample misclassification in the earlier epoch is under some threshold pre-specified number of epochs have terminated. In the weights and biases, even though the weight and bases are far from their optimal values.

The data investigation and representation process comprises of different stages. They are data preparation, data selection and transformation, data mining and presentation. After that, in the prepared data, the data selection and transformation process will be carried out (5) (Table 1).

PERS ID	Sex	Age	Salary
060819019	0	2	2
061202052	0	5	2
061202065	0	5	2
080603038	1	3	3
080916013	0	2	5

(continued)

(continued)

PERS ID	Sex	Age	Salary
081001011	1	2	5
081001037	1	3	5
081001095	1	5	6

In this example, Table 2 is the pattern of data input for clustering with *k*-means algorithm. These attributes value consist ***pers_id, sex, age and salary***.

In this clustering process, defined $k = 720$.

The patterns of output are shown in the Table 3. In this work, four inputs are defined to training data with neural networks (back-propagation algorithm). Set consists of sex (2 groups), age 1 (6 groups), age 2 (6 groups), salary (10 groups). Such as, we generate pattern of network inputs and network targets (default = zeros) for training neural networks. This is represented in Tables 4 and 5.

Input I_1, I_2, I_3, I_4 are attributes to order *sex, age1, age2, salary,* and T_1 and T_2 are not mandatory and specifically used for networks that require targets.

The inputs are added to the neural network to incorporate the bias in each hidden unit, and the training data set consist of 3,217 records. Therefore, the initial networks follow Table 6. The neural network results for pattern classification are presented in Table 6 and Fig. 8.

The network has 4 input nodes and 8, 48 hidden nodes and 2 output nodes. Since, architecture of a multilayer feed-forward neural network for the purpose is shown in Fig. 6.

Step of data classification algorithm with MLFF follow:

Input:

(1) Patterns chosen to be classified I_1, I_2, I_3, I_4; $\{I_1 = sex, I_2 = age1, I_3 = age2, I_4 = salary\}$.
(2) Neural network weights matrix W.
(3) Vector of aim classes C.

Table 2 Pattern of data input for clustering with *k*-means algorithm

PERS_ID	Sex	Age	Salary
060819019	M	29	13,560
061202052	M	52	19,740
061202065	M	60	19,740
080603038	F	38	22,880
080916013	M	23	44,930
081001011	F	21	44,930
081001037	F	37	44,930
081001095	F	60	54,000
081021017	F	27	44,930
090601011	F	21	44,930

Table 3 Patterns of output for clustering with *k*-means algorithm

11	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
12	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
13	−1	−1	−1	−1	−1	−1	−1	−1	−1	−1
14	−1	−0.777778	−0.555556	−0.333333	−0.111111	0.111111	0.333333	0.555556	0.777778	1

Table 4 Parameters for network inputs and network targets (default = zeros) for training neural networks

Sex	Age	Salary	Group of data (720 groups, k = 720)
0	2	2	1
0	5	2	2
0	5	2	2
1	3	3	4
0	2	5	5
1	2	5	6
1	3	S	7
1	5	6	3
1	2	5	6
1	2	5	6
0	2	5	5
1	3	5	7
1	3	5	7
1	2	4	14
−1	5	4	15
1	2	4	14
1	4	5	17
−1	2	5	6
1	2	5	6
−I	2	2	20

Table 5 Pattern of network inputs and network targets (default = zeros) for training neural networks

T1	−0.960784	−0.921569	−0.082353	−0.843137	−0.803922	−1	−1	−1	−1	−1
T2	−0.960704	−0.921569	−0.082353	−0.843137	−0.803922	−1	−1	−1	−1	−1

Table 6 Parameters used for training of back-propagation feed-forward neural *networks*

Parameter of NNs	Value
Input layers	4
Hidden layers 1	8
Hidden layers 2	48
Output layers	2
Weight/bias	Random values between 0 and 1
Momentum constant	0.9
Learning rate	0.01
Performance gradient	$1e^{-10}$
Iteration train (epochs)	3000
Train goal	0

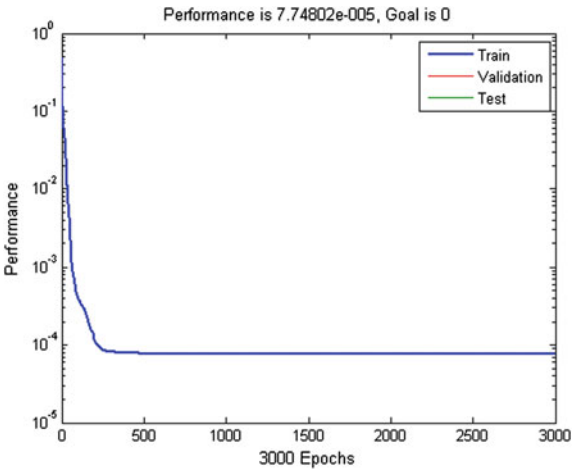


Fig. 7 Plotting of training with multilayer feed-forward (MLFF) neural network

Output:
Class of X
Algorithm:

(1) Enter I_1, I_2, $I_3, \ldots, I_n$ ($n = 4$).

(2) Calculate output in hidden layer $y_j^{(1)} = \varphi\left(\sum_{i=0}^{h} w_{ji}^{(1)} y_i^{(0)}\right)$; $y_j^l(n)$ is output of neural j, w_{ji} is weight that joins the node j and the previous layer to the node n and $\varphi(x)$ is activation function.

(3) Calculate output in output layer $y_j^{(2)} = \varphi\left(\sum_{i=0}^{h} w_{ji}^{(2)} y_i^{(1)}\right)$.

4) Allocates output to satisfying $O_j = y_j^{(2)}$.

The results of patterns of data classified by neural networks are shown in Fig. 7. The performance of train data is 1 to −1. Performance of this work equals to 7.774802e−005 and Goal is 0; the provided data output to correct 100% outcome can be seen from data points and best linear consolidation to direct line and line of Targets (T) = Output A. These are all patterns in section. We perform to elucidate implementation and simulation design section.

2 Implementation and Simulation Design

In this segment, we are considering the experiments to test the performances of the methods for accessing the data in artificial and fast manner to use data clustering with k-means algorithm and data classification with neural networks (back-propagation algorithm). The experiment will simulate the analysis of performance between the k-means clustering algorithm and pattern classification with

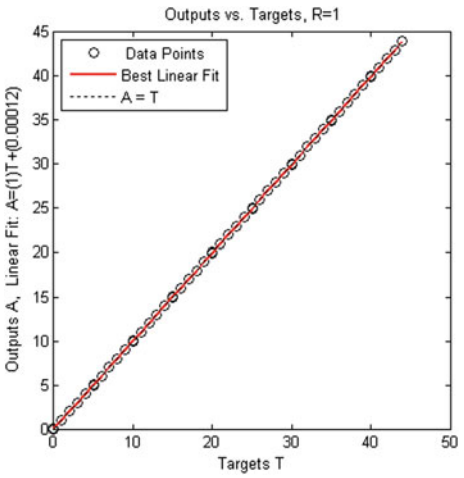


Fig. 8 Plotting and result of training with back-propagation model (hyperbolic tangent sigmoid function) for $K = 750$ and 3,000 epochs—Net type: $4 \times 8 \times 48 \times 2$

neural network for the conditioned database, for these experiments, design pattern of data input ***(pers_id, sex, age, salary)***.

We use personal

Return class label $\boldsymbol{C_i}$ satisfying $\boldsymbol{O_i = Max\ (O_j)}$.

For the output of training data with neural network, we represent with graph shown in Fig. 8. The total data set which is used at the present is about 3,217 records. The database management system used in the experiment is the Microsoft SQL Server 2005. This system is selected to use for following reasons;

(a) The software used for analysis is well-suited and proficient to use with the database management systems and
(b) Secondly, analysed data has been approved and developed continually by the public.

2.1 Experiments

In this experiment, we create model using data mining concept. It is presented here with block diagram (show in Fig. 9).

Figure 9 shows all methods and steps of experiment. In each step, they have so many methods such as, prepare and create data, select data and process data input. We are explaining the simulation as follows:

1. Select attributes (pers_id, sex, age, salary) for input pattern from database. After that, import and clean data into next process.
2. Convert and integrate data. Clustering of the data with *k*-means algorithm for different value of *k* as: 120, 240, 360, 480, 600 and 720.

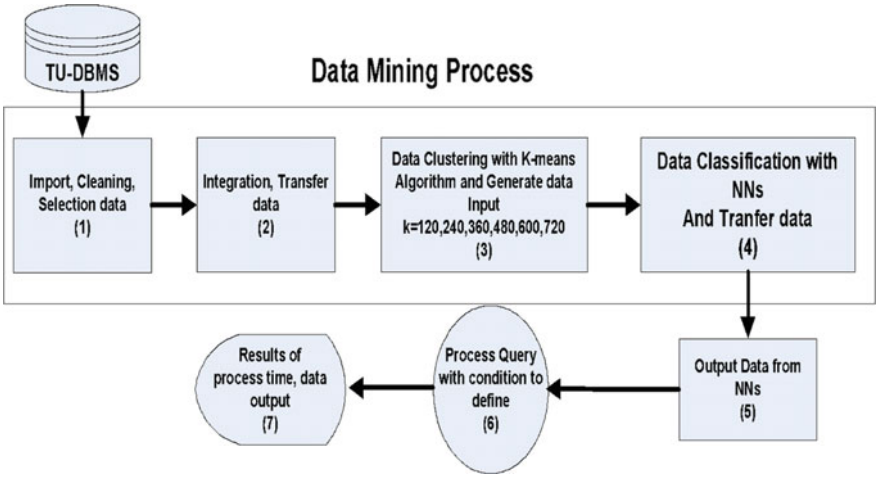
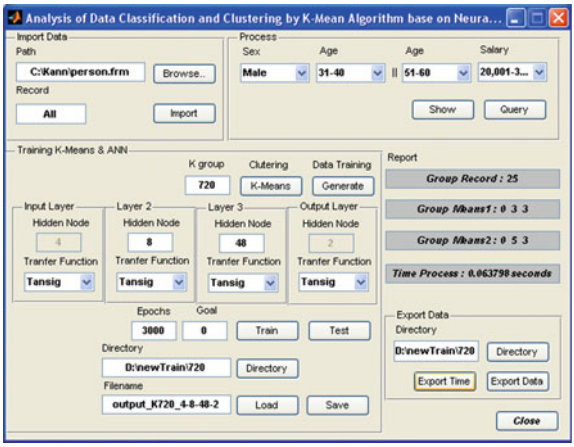


Fig. 9 Block diagram of experimental model

3. Pattern classification with multilayer feed-forward neural network (MLFF) using back-propagation algorithm.
4. Prepare data output of MLFF for query process.
5. Query data from MLFF output with condition for data output and process time.
6. Show output with graph and data in table (show all tables and figures in Sect. 4).

We have implemented program for experiment into the above steps (1)–(7). It is shown in Fig. 10 with user interface.

Fig. 10 User-interface for experimental analysis



The software used for implementation is MATLAB version 2006, because it can simulate data for experiment and is compatible with the database management system.

We separate the above program into two main processes for all steps, (1)–(7) as:

Steps (1)–(6) are data mining process steps.

In first step, we import the data, convert the data, clustering for data, and generate the data of input pattern for neural network and data classification in order. In these steps, we use 3,000 epochs and input 4 layers node, hidden 8 layers node and 48 layers node, output 2 layers node and use transfer data with hyperbolic tangent sigmoid function. This function calculates layer's output from its net input and is a good trade-off for neural networks. The pattern of data output of data classification is shown with data table and data graph in Tables 4, 5 and Fig. 8, respectively, and save data output to MATLAB file format.

Steps (6)–(7) evaluate access data time. We begin the evaluation from the sent request, classify data process from data output of neural network and fixed conditions of selected data as follows ***{Sex = 'M' and (Age = 31-40 or Age = 51-60) and Salary = 20001–30000}***.

Another processes, the K values are assigned to different six values (120, 240, 360, 480, 600 and 720), for K values are the result from calculating by this method, Sex = 2, Age = 6 * 2 = 12, Salary = 10. The minimum value of K is 120 and the maximum value of K is 720.

The main objective of the experiment is the comparison of data clustering with k-means algorithm and data classification with neural networks for the evaluation of access time for the conditioned data. The summary of the experiment and simulation explores with graphs and data table.

3 Results and Discussion

The results presented in this section demonstrate the simulation of data mining process. The derived outcome from data clustering with k-means algorithm and data classification with neural network is formed by 4 layers (input layer = 4 nodes, hidden layer 1 = 8 nodes, hidden layer 2 = 48 nodes, output layer = 2 nodes). We use fixed input data 3,217 records, set K values of 120, 240, 360, 480, 600, 720 and maximum limit of 3,000 iterations. The algorithm uses back-propagation feed-forward neural network and trains data with hyperbolic tangent sigmoid function (***tansig function in MATLAB Software***). Hence after process, we will show pattern data output with graph and data tables in Tables 7 and 8 and Figs. 11, 12, 15, 14 and 16.

The proposed output should have 2 values, i.e. table format and data access time. For example, the process time of defined K value clustering which is assigned to 720, equals 0.063798. We define K values for

Table 7 Output of data classification with neural network consisting of 5 columns (pers_id, sex, age, salary and group data), the number of data group depends on clustering with *k*-means algorithm values

Output			
K = 120, 240, 360, 180, 600, 720			
PERS_ID	Sex	Age	Salary
140607033	M	33	29,810
150802055	M	55	29,000
211002031	M	31	25,160
220509031	M	31	23,520
220514068	M	60	26,180
230416037	M	37	21,120
240401087	M	60	21,170
240921033	M	33	25,160
241202038	M	38	21,130
300102039	M	39	23,010
310504058	M	58	25,160
310504061	M	60	22,980
320201079	M	60	27,510
330301055	M	55	22,080
330501037	M	37	21,170
351201062	M	60	20,610
360401066	M	60	21,550
370601054	M	51	21,120
370901093	M	60	23,260
380201064	M	60	20,510
380601073	M	60	23,010
380601099	M	60	21,120
390401094	M	60	20,610
420501033	M	33	20,160
420601032	M	32	22,560

Table 8 The results of general structured query language (SQL), consist of 4 attributes (pers_id, sex, age, salary)

Output				
K = 120, 240, 360, 480, 600, 720				
PERS_ID	Sex	Age	Salary	Group data classify
140607033	0	3	3	13
150802055	0	5	3	22
211002031	0	3	3	13
220509031	0	3	3	13
220514068	0	5	3	22
230416037	0	3	3	13
240401087	0	5	3	22
240921033	0	3	3	13
241202038	0	3	3	13

(continued)

Table 8 (continued)

Output				
K = 120, 240, 360, 480, 600, 720				
PERS_ID	Sex	Age	Salary	Group data classify
300102039	0	3	3	13
310504058	0	5	3	22
310504061	0	5	3	22
320201079	0	5	3	22
330301055	0	5	3	22
330501037	0	3	3	13
351201062	0	5	3	22
360401066	0	5	3	22
370601054	0	5	3	22
370901093	0	5	3	22
380201064	0	5	3	22
380601073	0	5	3	22
380601099	0	5	3	22
390401094	0	5	3	22
420501033	0	3	3	13
420601032	0	3	3	13

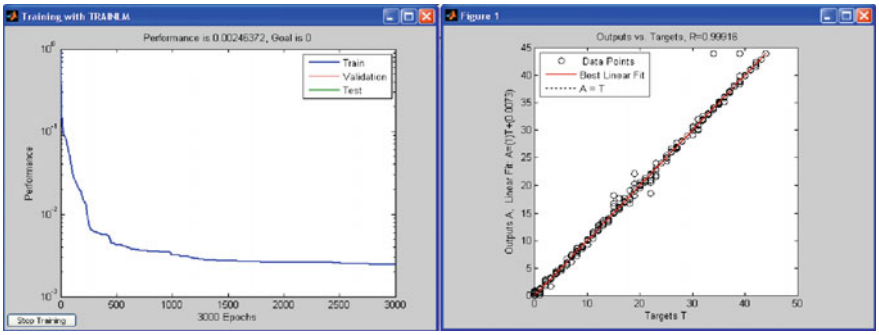


Fig. 11 Comparison graphs of data classification with back-propagation feed-forward neural network and train data with hyperbolic tangent sigmoid function

Table 7 shows output of data classification with neural network consisting 5 columns (*pers_id, sex, age, salary and group data*), the number of data group depends on clustering with *k*-means algorithm values. Table 8 shows the results of general structured query language (SQL), the results consist of 4 attributes (*pers_id, sex, age, salary*).

"SELECT PERS_ID, SEX, AGE, SALARY
FROM PERSON
WHERE SEX = 'M' AND

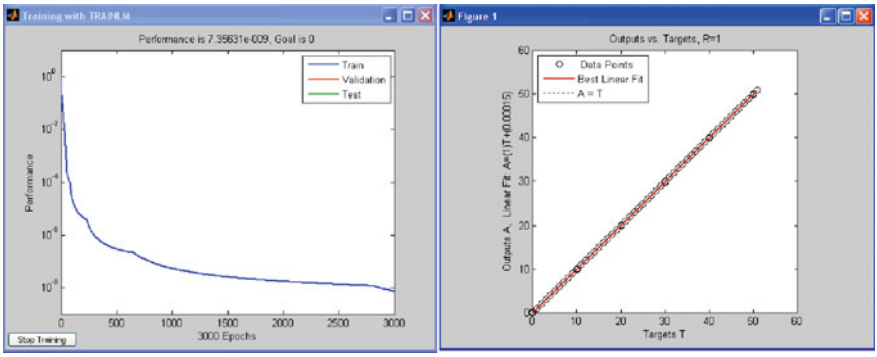


Fig. 12 Comparison graphs of data classification with back-propagation feed-forward neural network and train data with hyperbolic tangent sigmoid function

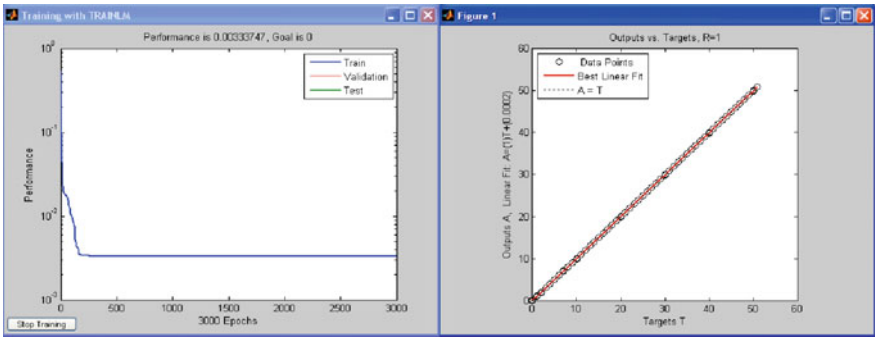


Fig. 13 Comparison graphs of data classification with back-propagation feed-forward neural network and train data with hyperbolic tangent sigmoid function

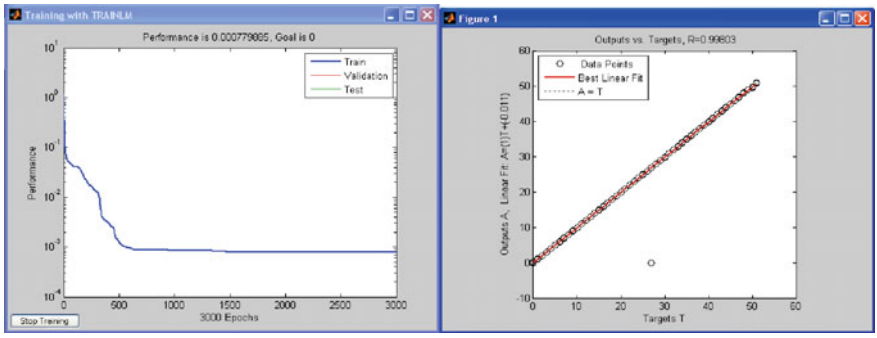


Fig. 14 Comparison graphs of data classification with back-propagation feed-forward neural network and train data with hyperbolic tangent sigmoid function

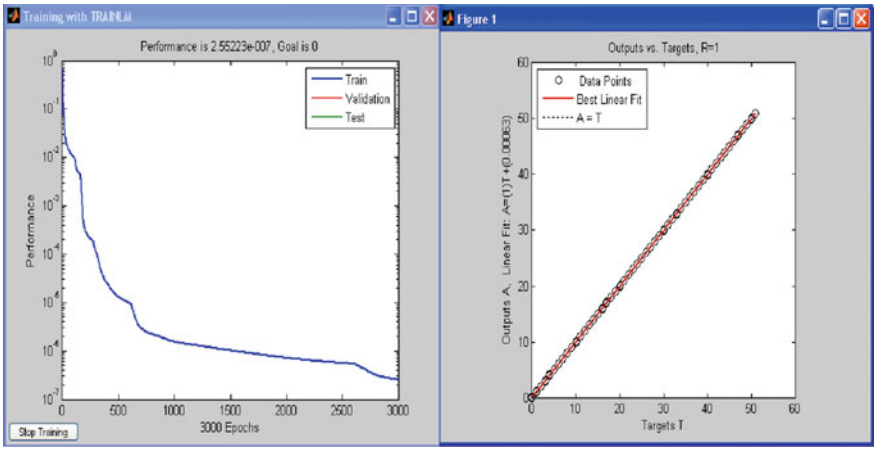


Fig. 15 Comparison graphs of data classification with back-propagation feed-forward neural network and train data with hyperbolic tangent sigmoid function

((AGE > 30 AND AGE <= 40) OR
(AGE > 50 AND AGE <= 60)) AND
(SALARY > 20000 AND SALARY <= 30000)"

As such, Table 7 shows same data output of data mining process at all processes but different K values, and Table 8 shows data output from structured query language (SQL). We compare data output from these two methods. The results are same. However, has different time of access data? The methods of access data with data mining process take lesser time than methods of access data with SQL.

The following graphs represent the data training process with hyperbolic tangent sigmoid function and the efficiency of the data classification. The graphs show the number of epochs and performances in the program to demonstrate the training data. After training data for iterations of 3000 epochs, the graph in which the performance runs close to −1 shows the best performance. After training data process, we show efficiency of data classification with graph. The best efficiency of the data classification is represented by the graph in which the data point and the best linear fit are on the same straight line.

The graph of the training data which runs close to the −1 shows the consolidation of best linear fit and the data point.

Figures 11, 12, 13, 14, 15 and 16 are representing the comparisons graph of data classification with back-propagation feed-forward neural network and train data with hyperbolic tangent sigmoid function. The data access time depends on defined K values of clustering and number of iterations. Example, in Fig. 11, data points and best linear fit do not fix data group into direct line. Its effective access data time equals to 0.395740, when $k = 120$.

In Table 9, the performances of train data have values into −1 because we use train data with hyperbolic tangent sigmoid function (initial values 1 to −1). The closer the performance values are to −1, the more effective data access time is.

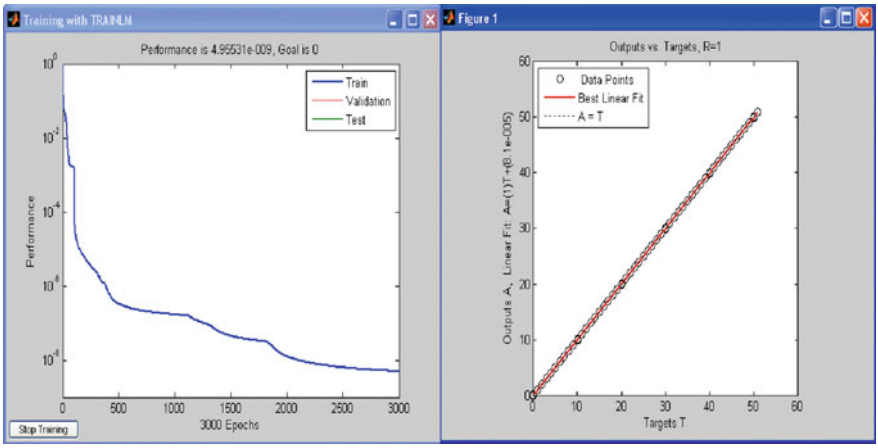


Fig. 16 Comparison graphs of data classification with back-propagation feed-forward neural network and train data with hyperbolic tangent sigmoid function

Table 9 Performances of training data

K cluster	Access time	Performance
120	0.394740	2.463720E−03
240	0.043960	7.356310E−09
360	0.063740	7.798850E−04
480	0.164756	3.337470E−03
600	0.067528	2.552230E−07
720	0.063798	4.955310E−09

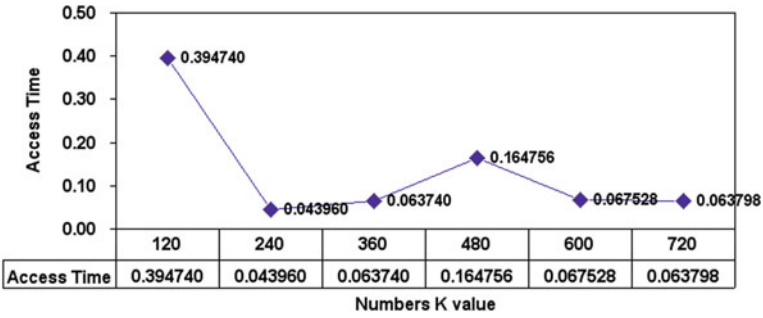


Fig. 17 Plotting graph to show the relation between *K* values clustering and data access time

Example, we set $K = 240$, after train data with neural network, have performance of 7.3563 E−09 and result of access time equal to 0.043960. It is less than all of *K* values in the experiments.

We use *K* values and data access time in order to conduct plotting graph to show the relation between *k* values clustering and data access time (shown in Fig. 17).

4 Conclusion

The results described in this paper indicated the performance of *K*-means clustering method with classification method of neural network. This comparison has been done for different values of *K* in *K*-means algorithm. The appropriate *k* values have effective data accuracy because the patterns of data output from *k*-mean algorithm clustering are the input for data classification. The results from experiment have commendable accuracy and best access time depend on number of *k* values for clustering and number of iteration training.

In this experiment, we used the approach of data clustering and data classification with neural network. The consolidation of all methods can be called as data mining. The clustering methods are separated into data groups; such as, (k = 120, i.e. 120 groups), data classification is respect to either same or near data into the group data class. Here, we use pattern of group data class in order to get access data optimization.

From this study, we found that, in each and every case, the clustering of data with different *K* values on same data set affects data access time. The most effective access time depends on defined numbers of clustering and defined iteration of appropriate training data.

It is found that though we put big amounts of data, the access data will use the same time for the equal *k* values. So, it is reasonable fact to conclude that the amount of data does not have any effect on data access. We can also use this concept for any database and any data attribute and also help to develop new methods about access data for best performance optimization in the future.

References

1. Han, J., Kamber, W.: Data mining concepts and techniques. Morgan Kaufmann Publishers, USA, pp. 5–10 (2005)
2. Dunham, M.H.: Data Mining *Introductory* and Advanced Topics. Southern Methodist University. ISBN 81-7758-785-4 Third Impression (2008)
3. Marakas, G.M.: Modern Data Warehouse Mining and Visualization Core Concepts. Kelley School of Business Indiana University. ISBN: 81-297-0210-X
4. Yuqing, P., Xiangdan, H., Shang, L.: The K-means Clustering Algorithm Based on density and ant colony. In: IEEE International Conference on Neural Networks and Signal Processing Nanjing, China, pp. 457–460, 14–17 Dec 2006
5. Tchaban, T., Griffin, J.P., Taylor, M.J.: A comparison between single and combined Backpropagation Neural Networks in the Prediction of Turnover. url: http://www.citeseer.nj.nec.com/188602.html
6. Thearling, K.: An Introduction to Data Mining. http://thearling.com/text/dmwhite/dmwrite.htm. 01 December 2003
7. Luke, B. T., K-Means Clustering. http://fconyx.ncifcrf.gov/~lukeb/kmeans.html. 20 October 2004

8. Neural Network Design Martin T. Hagan Oklahoma State University, Howard B. Demuth University of Idaho Mark Beale MHB, Inc Capture 11 Backpropagation Algorithm, ISBN : 0534-94332-2
9. Kanungo, T., Mount, D., S. Netanyahu, N., Piako D.C., Silverman, R., Wu, A.Y.: An efficient K-means clustering algorithm: analysis and implementation. IEEE Trans. Pattern Anal. Mach. Intell. **24**(7) (2002)
10. Tchaban, T., Griffin, J.P., Taylor, M.J.: A comparison between single and combined Backpropagation Neural Networks in the Prediction of Turnover. url: http://www.citeseer.nj.nec.com/188602.html
11. Jacek, Z.M.: Introduction to Artificial Neural Systems. PWS Publishing, Boston (1995)
12. Lu, J., Zhao, Y., Xue, Y., Hu, J.: Palmprint recognition via locality preserving projections and extreme learning machine neural network. In: Proceedings ICSP, 2008, pp 2096–2099
13. Kevin Takasaki, Critical Capacity of Hopfield Networks, MIT Department of Physics, 2007. url http://web.mit.edu.physics/
14. Davey, N., Hunt, S.P., Adams, R., High capacity recurrent associative memories. Neuro—Computing—IJON **62**, 459–491. doi: 10.1016/j.neucom.2004.02.007 (2004)
15. Storkey, A.: Increasing the capacity of a hopfield network without sacrificing functionality. Artificial Neural Networks—ICANN'97, pp 451–456 (1997)
16. Tarkowski, W., Lewenstein, M., Nowak, A.: Optimal architectures for storage of spatially correlated data in neural network memories. ACTA Physica Polonica B **28**(7), 1695–1705 (1997)
17. Reiss, C., Wilkes, J., Hellerstein, J.L.: Google–cluster traces: format+schema. Google Inc., White Paper, November 2011
18. Chen, Y., Ganapathi, A., Griffith, R., Katz, R. : Analysis and Lessons from a Publicly Available Google Cluster Trace. University of California, Berkeley, CA, Technical Report (2010)
19. Liu, Z., Cho, S.: Characterizing machines and workloads on a Google cluster. In: 41st International Conference on Parallel Processing Workshops (ICPPW) IEEE (2012)
20. Reiss, C., Tumanov, A., Ganger, G.R., Katz, R.H., Kozuch, M.A.: Heterogeneity and dynamicity of clouds at scale: google trace analysis. In: Proceedings of the Third ACM Symposium on Cloud Computing, ACM (2012)
21. Alam, M., Shakil, K.A.: A decision matrix and monitoring based framework for infrastructure performance enhancement in a cloud based environment. In: International Conference on Recent Trends in Communication and Computer Networks, Elsevier, pp. 174–180, November 2013
22. Di, S., Kondo, D., Cirne, W.: Host load prediction in a Google compute cloud with a Bayesian Model. In: Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis (SC), Salt Lake City, UT, November 2012