ON SECURITY AND PERFORMANCE ENHANCEMENT IN WIRELESS MESH NETWORKS

A Thesis

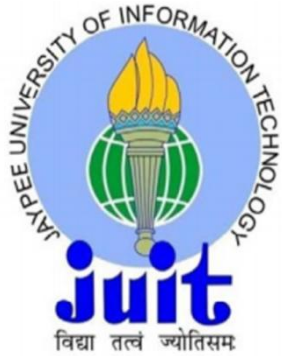
Submitted in fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

By

GEETANJALI
Enrollment no. 146201

COMPUTER SCIENCE AND ENGINEERING



Under the Supervision of

Dr. Hemraj Saini

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING AND INFORMATION TECHNOLOGY

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT, SOLAN-173234, HIMACHAL PRADESH, INDIA

April 2017

TABLE OF CONTENTS

DECLARATION BY THE SCHOLAR

I hereby declare that the work reported in the Ph.D. thesis entitled **"On Security and Performance Enhancement in Wireless Mesh Networks"** submitted to the Department of Computer Science Engineering and Information Technology, **Jaypee University of Information Technology (JUIT), Waknaghat, India,** is an authentic record of my work carried out under the supervision of **Dr. Hemraj Saini,** Associate Professor, JUIT. The work in this thesis is my original investigation and has not been submitted elsewhere for the award of any other degree or diploma. I am fully responsible for the contents of my Ph.D. Thesis.

Geetanjali
Department of Computer Science and Engineering
Jaypee University of Information Technology,
Waknaghat, India
Date:

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the Ph.D. thesis entitled "**On Security and Performance Enhancement in Wireless Mesh Networks**" submitted by **Geetanjali** at **Jaypee University of Information Technology, Waknaghat**, **India,** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree or diploma.

Dr. Hemraj Saini
Department of Computer Science and Engineering
Jaypee University of Information Technology,
Waknaghat, India
Dated:

ACKNOWLEDGEMENTS

I am extremely indebted to my supervisor, Dr. Hemraj Saini for unswerving supervision in this research work. I have learnt several things from him while pursuing my research work. He gave me every possible solution which can help me in exploring new dimension in my research. I am very fortunate to become closer to my supervisor and friendly getting the knowledge and encouragement from him. I am heartily thankful to the GOD for blessing me with the opportunity to accomplish my work under such a knowledgeable personality.

I would like to devote my very special thanks particularly to Prof. Dr. Ghanshyam Singh in JUIT who guided and supported me during copious important phases and decisions. I am grateful to Prof. Dr. Samir Dev Gupta, Director & Academic Head and Prof. Dr. Vinod Kumar, Vice Chancellor**,** Jaypee University of Information Technology, Waknaghat, for providing admirable research atmosphere and amenities for my research. I am also thankful to Prof. Dr. Satya Prakash Ghrera, Head of Computer Science & Engineering and Information & Communication Technology, Waknaghat, for his support, valuable suggestions and comments throughout the presentations. I am ceaselessly appreciative to my affectionate younger brother Mr. Akshay Kumar and sister Ms. Amisha. Furthermore, I am gratified beyond words for my most devoted fiancé Dr. Naveen Jaglan for his endless support. Without their continual moral support, my work would have been impossible.

I strongly commit and devote this accomplishment to my father Dr. R.B.S. Rathee and my mother Mrs. Meena Kumari who are providing their holiness and strength for my encouragement and have blessed me with their presence**.**

Geetanjali
Department of Computer Science and Engineering
Jaypee University of Information Technology,
Waknaghat, India
Date:

I would like to dedicate this dissertation

To

The most lovable and valuable persons in my life my father Dr. R.B.S. Rathee and my mother Mrs. Meena Kumari

And

Motivating strength of my younger brother and my sister and beyond the words my most devoted fiancé Dr. Naveen Jaglan.

ABSTRACT

Wireless Mesh Network (WMN) is considered as a next generation key promising technology which is attractive in the areas where infrastructure is either existing or absurdly expensive because of multi-hop, self-healing, self-organizing and dynamic features. Advancement in networking technologies has allowed for organizations to use the network not only to share the resources but also to store large pool of data for analysis. Therefore, securing such data and resources of organization on a network is a big concern. Client, infrastructure and hybrid are the different types of WMN architectures consisting of two sorts of nodes; mesh routers (MR's) and mesh clients (MC's). MR's acts as backbone which provides the network services to the clients and responsible for forwarding the data packets to their intended destination nodes and MC's are the end point those accesses the network services via mesh routers. Whenever, a MC moves outside the boundary range of its current serving mesh router then the corresponding signal-to-noise ratio (SNR) of that serving MR will falls due to signal attenuation. A significant drop in SNR ratio makes the MC to search for a new mesh router having good signal strength for continuing its network services by triggering the handoff procedure. Since, the nodes are dynamic, unstable and limited by security disputes with new performance issues, a significant delay in handoff procedure may cause copious performance concerns such as network attacks and delay in the network. Therefore, during the handoff procedure, it is prerequisite that roaming clients ample access authentication process not only with a short delay but also with the fortification for the roaming clients with handoff networks. Further, if a node either inter-domain (communicate between two domains) or intra-domain (communicate within a domain) wants to send some messages to its intended destination node, the information is being passed among multiple MR's. However, to prevent the data exposure at each intermediate node, the messages must be encrypted by some security techniques or an ornate encryption technique which is required to guarantee that even if the message is forged by an intruder then it may not be able to decrypt it anyway. Due to the dynamic nature of WMN, where information is being passed over multiple hops or MR's, data encryption time is taken to be an important parameter. Furthermore, the most significant factor that impacts the WMN performance is the nature of fundamental routing protocols used for promoting the data packets. Presence of any malicious or misbehaving node within a

routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network.

Although, numbers of scientists/researchers have proposed various handoff authentication procedures with message encryption and secure routing techniques, However, the issues arises by the intruders that encounters number of malicious nodes or threats to disrupt the network performance. In addition, by increasing one parameter such as to ensure the security, others parameters (such as end-to-end delay, network throughput, packet delivery ratio) get affected drastically. Therefore, there is a need to propose an efficient security technique having reduced authentication delay, less encryption/decryption time and secure routing mechanism against routing layer attacks with the aim of optimizing the other network parameters. Therefore, in order to provide an efficient and secure communication process, the security is ensured at three different aspects i.e. authentication of handoff clients, encrypted message transmission between source and destination and secure route discovery to route the transmitted data packets. In future each MC joining the network must be provided with a unique key by the AS in order to identify the MC for authentication. Further studies, the proposed algorithm will be tested under high packet flow and large number of attackers (by considering black hole and wormhole attacks) and then their results will be compared on various performances. However, the energy consumption in the large number of network sizes during the packet transmission/reception is a potential issue which will be reported in future communication.

LIST OF ABBREVIATIONS

AAA	Authorization, Authentication and Accounting
ACK	Acknowledgement
AEHO	Advanced Encryption through Homomorphic operation
AODV	Ad hoc On-Demand Distance Vector
ARAN	Authenticated Routing for Ad-hoc networks
AS	Authentication Server
$Auth_{rqt}$	Authentication Request
BS	Base Stations
BSSID	Base Service Set Identifier
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access/collision avoidance
CTAR	Context Transfer Activation Request
DCU	Data Collection Unit
DDL	Data Link Layer
Di	Destination
DNS	Domain Name Server
DOS	Denial of Service
DS	Domain Server
DSR	Dynamic Source Routing
DYMO	Dynamic Manet On-demand
E-Routers	Edge Routers
FMR	foreign mesh router's
FTP	File Transfer Protocol
GMK	group based master key
GPCR	greedy parameter circuit routing
HMR	Home Mesh Router
HOVER	Hybrid On-demand Distance Vector Routing
HWMP	Hybrid Wireless Mesh Protocol
ID	Identity

IGW	Internet Gateway Routers
IoT	internet-of-things
ITS	Intelligent Transportation System
LAN	Local Area Network
LLC	Logical Link Control
LSU	link state updates
MAC	media access control
MANETS	Mobile Ad hoc Networks
MAP	Mobile Access Point
MC	Mesh Client
MCC	Mobile Cloud Computing
MDR	message delivery ratio
MEA	Mesh Enabled Architecture
MGK	Multi-BS group key
MIMO	Multiple Input Multiple Output
MK	Master Key
MR	Mesh Router
NS	Network Simulator
OFDM	Orthogonal frequency-division multiplexing
OLSR	Optimized Link State Routing Protocol
OSI	Open System Interconnection
PCT	private communication transport
PHY	Physical
PKD	public key distribution
PL	Packet Loss
PMK	pair-wise master keys
Pr	Private Keys
P-Routers	Probe Routers
PTK	Pair wise Transparent Key
Pu	Public keys
QID	Query identifier
QSEQ	Query sequence number

RAOLSR	Radio Aware Optimized Link State Routing
RE	Residual Energy
REP	route reply packet
RTCP	Real Time Transport Protocol
RTP	Real time protocol
SA	security association
SAK	secret authentication key
SAODV	Secure Ad hoc On-Demand Distance Vector
SAR	Security-aware ad-hoc routing protocol
SDES	Synchronous Dynamic Encryption System
SEAODV	Security Enhanced Ad hoc On-Demand Distance Vector
SHA	Secure Hash Algorithm
SIG	Signature
SITO	Social Impact Theory Optimizer
SLSP	Secure Link State Routing Protocol
SNR	Signal-to-Noise ratio
SRM	Secure Routing Mechanism
SSK	secret session key
SSL	Secure Socket Layer
SSRP	*Secure Routing Protocol*
SYN	Synchronization
TAK	Ticket Authentication Key
TCP	Transport Control Protocol
TDMA	time division multiple access
TLS	Transport Layer Security
TMC	Traffic Management Centre
TPA	Trusted Party Authority
TTL	Time to live
TV	Trust Value
UDP	User Datagram Protocol
UWB	Ultra Wide Band
VANETS	Vehicular Area Networks

WMN	Wireless Mesh Network
WSN	Wireless Sensor Networks
WTR	Weight Trusted Routing

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 PROBLEM STATEMENT

Wireless Mesh Network (WMN) is considered as a next generation key promising technology which is attractive in the areas where infrastructure is either non-existing or absurdly expensive because of its multi-hop, self-healing, self-organizing and dynamic features [1-3]. Advancement in networking technologies has allowed for organizations to use the network not only to share the resources but also to store large pool of data for analysis. Therefore, securing such data and resources of organization on a network is a big concern. Client, infrastructure and hybrid are the different types of WMN architectures consisting of two sorts of nodes; mesh routers (MR's) and mesh clients (MC's). MRs acts as backbone which provides the network services to the clients and responsible for forwarding the data packets to their intended destination nodes and MC's are the end point that access the network services via mesh routers [4-6]. Whenever a MC moves outside the boundary range of its current serving mesh router then the corresponding signal-to-noise ratio (SNR) of that serving MR will falls due to signal attenuation. A significant drop in SNR ratio makes the MC to search for a new mesh router having good signal strength for continuing its network services by triggering the handoff procedure. Since, the nodes are dynamic, unstable and limited by security disputes with new performance issues, a significant delay in handoff procedure may cause copious performance concerns such as network attacks and delay in the network. Therefore, during the handoff procedure, it is prerequisite that roaming clients ample access authentication process not only with a short delay but also with the fortification for the roaming clients with handoff networks. Further, if a node either inter-domain (communicating between two domains) or intra-domain (communicate within a domain) wants to send some messages to its intended destination node, the information is being passed over multiple MR's. However, to prevent the data exposure at each intermediate node, the messages must be encrypted by some security techniques or an ornate encryption technique is required to guarantee that even if the message is forged by an intruder then it may not be able to decrypt it anyway. Due to the dynamic nature of WMN, where information is being passed over multiple hops or MR's, data encryption time is taken to be an important parameter. Furthermore, the most significant factor that impacts the WMN performance is the nature of

fundamental routing protocols used for promoting the data packets [7, 8]. Presence of any malicious or misbehaving node within a routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network [9, 10].

Although, numbers of scientists/researchers have proposed various handoff authentication procedures with message encryption and secure routing techniques, however, the issues are raised by the intruder that encounters number of malicious nodes or threats to disrupt the network performance. In addition, by increasing one parameter such as to ensure the security, others parameters (such as end-to-end delay, network throughput, packet delivery ratio) get affected drastically. Therefore, there is a need to propose an efficient security technique having reduced authentication delay, less encryption/decryption time and secure routing mechanism against routing layer attacks with the aim of optimizing the other network parameters. Therefore, in order to provide an efficient and secure communication process, the security is ensured at three different aspects i.e. authentication of handoff clients, encrypted message transmission between source and destination and secure route discovery to route the transmitted data packets.

1.2 RESEARCH SCOPE

This work addresses the security techniques at three different aspects of communication procedure that are 1) Clients' handoff; where the nodes are mobile from one domain to another domain. The mobility of the clients diminishes the boundary range of their current serving mesh routers, so, in order to continue its network services, the mobile clients need to connect to another domain's mesh routers by proving its authenticity. However, during the authentication process, there is a possibility that a malicious user may encounter and try to authenticate itself with the foreign mesh router or the domain by forging the identity of a legitimate mesh client. 2) The second security process is data encryption technique where the source node secures its transmitted messages (from the malicious activities done by intruders) by applying any of the encryption processes and finally 3) Secure routing technique; where the data is securely routed from the intermediate malicious nodes involved during the message transmission process in mesh environments. The recently developed methods for enhancing the security at these aspects also undergo from faults at certain levels such as to optimize one of the parameter i.e. security, other parameters are affected adversely such as end-to-end delay, packet delivery ratio, packet loss ratio and network throughput etc. This research

improves more than one parameter at each level and is verified through analytical simulations and experimental investigations. To prove the legitimacy of the work, an application is considered consisting of all the proposed problems with rigorous comparative analysis against previously proposed approaches.

1.3 RESEARCH OBJECTIVE

The objective of this research is to provide a secure transmission mechanism at three aspects of the communication procedure that is 1) client's handoff 2) message encryption process and 3) secure routing algorithms. This study will look at whether the anticipated purposed work is achieved at each level and effectiveness of proposed algorithms is improved in significant manner. In order to achieve the research objectives, valid network environment needs to be established and many basic properties of WMN need to be understood.

1.4 CONTRIBUTIONS

The contribution of the thesis is divided into three major parts.

1.4.1 Secure Handoff Procedure Against Wireless Threats

Although multi-hop, ticket based and proactive key distributions are some recent authentication techniques to ensure security during mobility in mesh environments. However, a significant delay to compute and verify the security process and authenticity of legitimate user may enforce number of internal vulnerabilities. This chapter propose a secure and an efficient handoff procedure with reduced authentication delay in different scenarios where instead of doing the computation and verification at mesh client (as mesh clients are limited in resources) Authentication Server (AS) is responsible for generating the keys and the tickets for authenticating the clients. Further, the generation and distribution of tickets/keys by AS protects the network from several security threats. The proposed technique is analyzed over NS2 simulator under different probabilistic scenarios of authentication delay, request delay and is legitimated by discussing an empirical study over certain security threats against reported literature.

1.4.2 Secure Message Transmission With Reduced Encryption/Decryption Time

WMN is deliberated as a key technology due to its self-healing and self-configuring characteristics with the provisions of large scale exposure in industrial and academic fields.

Security is considered as a vital constraint in WMN owing to its broadcasting and dynamic nature. Due to this nature of WMN where information is being passed over multiple hops, data encryption is taken to be an important parameter. Researchers have proposed various encryption techniques to provide the message security, but the foremost shortcoming in most of the approaches is their processing time. An encryption technique having large encryption/decryption timing increases overhead which may cause copious perilous attacks (i.e. passive eavesdropping etc.). Further an encryption technique with large file size may increase the load on the server during file transmission. In order to overcome these hitches, the chapter proposes an end to end encryption based on algebraic operations i.e. Advanced Encryption through Homomorphic operation (AEHO) with reduced processing time where a cipher text is generated using OR/XOR operations. Further, a Trusted Party Authority (TPA) server is anticipated to provide the authenticity. To establish the legitimacy of the proposed solution, the experimental results are explained in terms of reduced encryption/decryption timing and increased throughput.

1.4.3 Secure Routing Technique Against Wireless Routing Attacks

In order to ensure a secure routing technique to detect and eliminate the malicious/misbehaving nodes involved during routing path formation in hierarchical mesh environments, the Dijkstra's shortest path routing algorithm is used whose weights are deliberated using certain parameters (i.e. node distance, node's previous interactions, packet loss percentage and trust values of each node). The malicious nodes involved during route discovery process are eliminated by calculating the trust value of each node using Social Impact Theory Optimizer (SITO). Here, we have discussed the network performance trade-off caused by secure path formation in conventional methods and proposed a Weight Trusted Routing (WTR) mechanism for eliminating these issues (packet-loss ratio, end-to-end delay and route discovery delay). We have numerically simulated and compared the network metrics for both conventional and proposed approaches. Moreover, the proposed technique is validated by discussing an empirical study over routing attacks.

1.4.4 Application Based Scenario

Here we have exploited the secure routing mechanism that is WTR mechanism and secure handoff routing mechanism to detect and eliminate the malevolent/malicious nodes involved during the routing path formation and handoff for smart-home environments where the routing between the communicating entities is performed through the mesh architecture. In

order to provide a secure communication against malicious behavior of nodes, the proposed mechanism uses Dijkstra's shortest path routing algorithm in which the weights are deliberated using certain parameters such as node distance, packet-loss percentage and trust value of each node which is computed using SITO. Further, we have discussed the network performance trade-off caused by secure path formation with conventional method and have proposed the WTR mechanism for eliminating the potential issues such as packet-loss ratio, end-to-end delay and network throughput. The NS2 simulator is used to simulate and compare the network metrics for both conventional and the proposed approach and is validated through experimental results over end-to-end delay and message delivery ratio against reported literature.

1.5 OUTLINE OF THESIS

The organization of thesis is divided into seven chapters. The introduction section, research background and problem statement, research scope and research objectives are reported in CHAPTER 1. In this chapter the need of security in current wireless technology i.e. WMN is discussed. The research subarea with its problem statements is covered in this chapter.

CHAPTER 2 evidences the background and preliminaries for the research in this thesis. This chapter states the introduction of network history and need of security in a network. Further the architecture of WMN with its benefits, applications and authentication protocols is introduced. The security issues that arise at each level of WMN are elaborated in this chapter only. Finally the lesson is closed by defining the current open research challenges in WMN security.

CHAPTER 3 deals with the need of security during handoffs in WMN. The proposed secure handoff procedure is validated and verified by showing the simulation results. CHAPTER 4 presents the data encryption approach during transmission between source and destination.

CHAPTER 5 presents the generic approach for secure routing in WMN. This chapter briefs the results for the proposed approach with proper simulation.

CHAPTER 6 validates the above mentioned three problems of chapter 4 and 5 through an application where the results are verified by showing a rigorous comparative study between the proposed approaches and existing (basic) approaches in terms of time complexity. CHAPTER 7 concludes the thesis. The chapter includes the thesis summary, concluding remarks, contribution of the work done, suggestions for the future scope in this field.

CHAPTER 2

BACKGROUND AND PRELIMANARIES

Present networks are the basis of recent communication. The existence of networks is inspiring our society in innumerable different ways. Now days, wireless mesh network is measured as a promising technology for posturing the self-organizing, healing and configurable characteristics however one of the primary challenges in the venture of these networks is their vulnerability to security attacks. In order to conquer these threats, several security techniques are proposed, however, authentication is considered as a vital parameter to offer a secure communication. In this chapter, a review is conferred from beginning to the recent networking technology i.e. WMN. In addition, WMN security is explored with modern applications such as intelligent transportation system, smart grids and multimedia systems etc. Further an obvious outline of security with respect to each layer is explicated and finally the chapter is bankrupt by exactness of the future work which is the next step of this research.

2.1 INTRODUCTION

The revolt of devices in 1990, now enduring in the 21st century comprises “computer networks” that is a combination of devices/computers which allows a computer to converse the data or distribution of hardware and information [11]. Today, networks are the backbone aid for current correspondence whose presence is enriching our social order in endless separate approaches. Concerning illustration, the associations or organizations depend intensely on the capacity to allotment data in an effective and profitable manner. As the societies heavily depend on the ability to stake their information in a productive and efficient manner [12], Computer networks are now becoming the part of each and every organization firm in which computers can pursue a pathway anyhow. When it comes to locate up the classification of the network, an organization has two selections; wired network and wireless network (as depicted in Figure 2.1).

2.1.1 Types of Network

Wired networking is the widespread type of Local Area Network (LAN) technology [13] where the acquaintances among the technologies are made using a cable or physical wire. It is

simply a gathering of two or more devices connected through an Ethernet cables. To fix a computer or to the network, an Ethernet adapter is required, which attach the devices either externally or internally. The wired networks are further isolated under two parts; point to point and Multipoint.

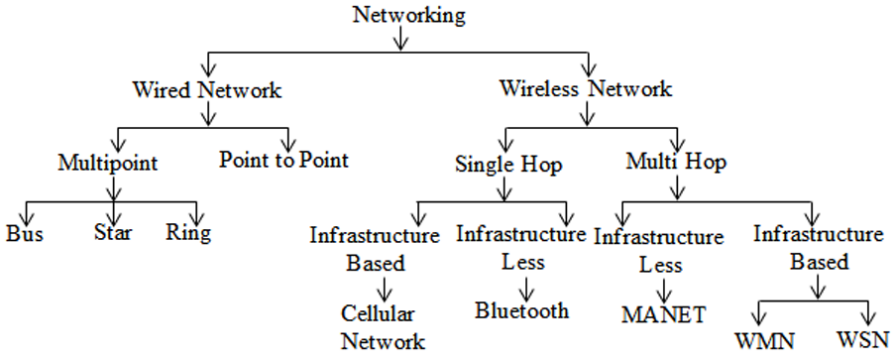


Figure 2.1 Network Classification

Point-to-point networks utilizes a real length of link to interface two closures of devices and gives a devoted connection between these devices [14] where the whole limit of the connection is held just between the two devices as depicted in Figure 2.2 (a). Multipoint system is one in which more than two devices share a solitary connection as appeared in Figure 2.2 (b). There are essentially three system topologies in multipoint organizing. Star Network is the naive part of system which has at least two PCs associated with one focal center point [15] and this sort of system is to be utilized for private venture and home systems. Figure 2.2 (c) demonstrates the chart of star systems administration [16]. The benefits of a star system is that it is easy to handle but difficult to wire, introduce and keep up notwithstanding, from another side, it requires more link length and is more costly than transport topology. The star systems administration is valuable when some handling must be brought together. Bus networks (as appeared in Figure 2.2 (d)) are utilized for impermanent systems, simple expansion and execution. The disadvantages of these networks are that it is constrained to a link length and a simple blame in the link can bring about the decimation of the entire system. This kind of systems is basically utilized for modern applications. Ring Network is to some degree like bus network since it has no focal host PC. Every PC on this system has two neighboring hubs having their own particular applications freely. It is as a shut circle where every hub can transmit the information by devouring the token as presented in Figure 2.2 (e).

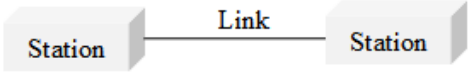


Figure 2(a) Point to Point Network

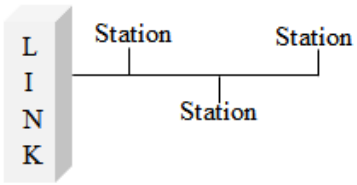


Figure 2(b) Multi Point Network

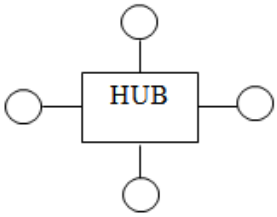


Figure 2(c) Star Network

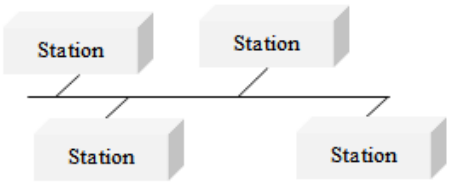


Figure 2(d) Bus Network

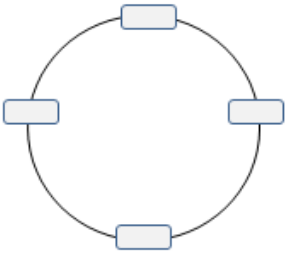


Figure 2(e) Ring Network

Figure 2.2 Point-to-point and Multipoint Network

Broadcasting of information is speedy in ring system, yet as the information parcels must go through each PC between each source and goal, information turns out to be moderate and disappointment of any hub can bring about the unsuccessful information transmission. As all these wired systems are settled and experience with specific downsides, for example, they are non-compact, static in nature, penetrate the openings into the dividers, handoff is least and requires the cost of fiber+ copper +co-hub link [17], the wireless systems administration innovation appeared. Further, the moving of wired systems causes the entire rewiring which consolidates the significant disadvantage in wired innovation. Peter Gold around 20 years back presented the idea of wired city i.e. the interconnection of phones in the workplaces and between the workplaces, faxes, and so forth. A wireless system is the one which utilizes high recurrence radio flags rather than wires to impart between hubs [18]. The single hop and multi-hop are the two noteworthy sorts of remote systems.

Single hop is a solitary association between the devices. Infrastructure less and framework based are further expansions of single hop systems administration. Infrastructure less has no settled structure between the hubs as in Bluetooth while Framework or infrastructure based has settled structure like in cell systems. Multi-hop is another sort where at least two jumps

exist between each source and goal. Multi-hop is additionally classified into framework based and less infrastructure. Cases of foundation based are remote sensor systems and remote work systems and at any rate the case of framework less is Vehicular Area Networks (VANETS). The cost of systems administration is proceeding to decrease and has turned into a fundamental part in finishing day by day business undertakings [19]. Progression in system innovation has considered associations to utilize the system to share assets, as well as to store extensive pool of information for investigation. In this manner, securing such information and assets of association on system is an incredible concern. As no PC system is totally secure.

2.2 SECURITY

Security is generally characterized as the condition of being free from risk or danger [20]. The biggest PC related crime in US history was conferred by Kevin Mitrick which cost of 80 million dollars in US licensed innovation [21]. The fundamental comprehension about the security methods is vital for the exploration being done today. A web is subjected to assault/attack from pernicious sources and these assaults can be separated into two classifications: passive assault and active assault [22].

Active assaults are additionally arranged into specific levels, for example, 1) masquerade where one element puts on a show to be an alternate substance. 2) A replay assault happens if the last catches the message from the sender and gets the inactive/replay message. 3) Modification of messages, the adjusting and reordering is finished by making an unapproved impact and 4) DOS assault where an aggressor may stifle all messages sent to the beneficiary [23]. Today, network services (i.e. Email, www and so on.) have turned into a fundamental need in everyday correspondence [24]. For giving the benefits to these systems more adequately, WMN has soured into a famous topology which assembles elite framework. To supply a last mile broadband access, WMN is a promising innovation. It is a most conspicuous development of system engendering. Let’s have a short portrayal on WMN, architecture, favorable position and its applications.

2.3 HISTORY OF WIRELESS MESH NETWORKS

2.3.1 Wireless Mesh Network

WMN is an augmentation of multi-hop Ad-hoc system and it is a mix of Ad-hoc and Mesh organizing. Ad-hoc system is one where every device can specifically speak with whatever

other device inside its radio reaches while in mesh networks; every hub goes about as a switch and has the ability to retransmit the parcel to goal hub [25, 26].

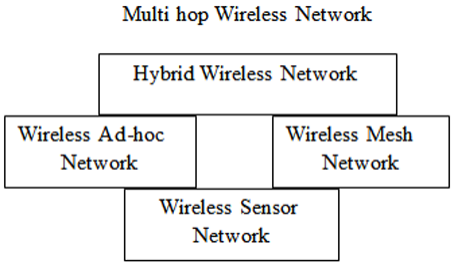


Figure 2.3 WMN Technology

Figure 2.3 demonstrates the extent of Wireless Mesh Network Technology. Like system classification, on the premise of availability, WMN is characterized into three gatherings i) Point to Point, ii) Point to Multipoint and iii) Multipoint-to-Multipoint. Point to Point systems are reliable; however their versatility and adaptability level is down. Multipoint-to-Multipoint networks have direct versatility; however have the low unwavering quality and flexibility. So as to surmount the above confinements, Multipoint-to-Multipoint systems are spearheaded which supply with high unwavering quality, versatility and flexibility [27]. The transmitting energy of every hub is downsized as the quantity of clients in the work increments.

Table 2.1: WMN types

WMN	Reliability	Adaptability	Scalability
Point to Point	High	Low	Low
Point to Multipoint	Low	Low	Moderate
Multipoint to Multipoint	High	High	High

To expand the scope without need of transmitting force, Multipoint-to-Multipoint network utilizes the multi-hop characteristic. The IEEE 802.11 family principles are utilized by Multipoint-to-Multipoint systems [28]. The systems which use these guidelines are called mesh networks and WMN are a specific class of Multipoint-to-Multipoint organizes. Table 2.1 demonstrates the parametric contrast between Point to Point, Point to Multi-indicate and Multipoint systems.

2.3.2 WMN Architecture

The architecture of WMN is ordered into three fundamental gatherings i) Infrastructure/spine WMN ii) Client WMN and iii) Hybrid WMN.

Infrastructure/backbone WMN produced by mesh routers for clients to narrate them. Various cases of radio technologies are engaged to make the backbone WMN. IEEE 802.11 is the most extensively used technology, however in case of different radio technologies; clients must converse with base station.

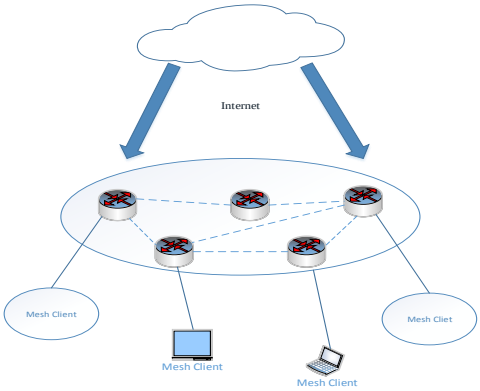


Figure 2.4 Infrastructure WMN

Backbone WMN is the most frequently used wireless network as all the networks of neighborhood can be built using infrastructure meshing. In this, mesh networks are put on the upper side to serve as the access points for clients. The routers generally utilized two sorts of radios i.e. for backbone correspondence and for client correspondence. Figure 2.4 demonstrates the infrastructure WMN. Client WMN blesses with peer to peer systems among the devices. In this, client nodes encompass routing as well as giving an end user application to client's from a individual type of getting set on devices [29]. Client WMN architecture is appeared in Figure 2.5. Hybrid WMN is a combination of two i.e., infrastructure and client WMN. The network can be retrieved by mesh client either through a router or direct meshing with mesh client only. In this, the infrastructure WMN provides association to other network and clients routing competence delivers improved connectivity and reporting [30]. Figure 2.6 indicates hybrid WMN. The discussed architecture of WMN comprises of different types of nodes, for example, WMN router, WMN client and WMN gateway. WMN client is the end client user that gets the system for utilizing the email, VoIP, gaming and area discovery applications. The end client devices can be tablets, PDA's, advanced cells, and so forth.

The WMN clients have confined power and steering capacity [31, 32]. It might possibly be associated with the system as its versatile nature.WMN Router is utilized to course the activity of systems. The WMN routers are dependable and have a negligible utilization of transmission power. To empower the versatility in multi-hop mesh condition, various channels and numerous interfaces are used at the MAC in the chain of mesh routers.

WMN Gateways have the direct access to the internet. These are expensive in nature as they have multiple interfaces to connect to wired/wireless networks.

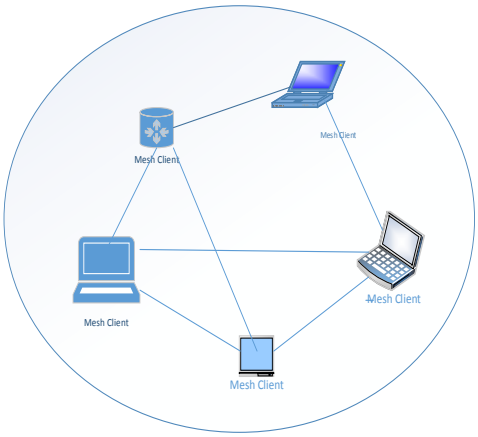


Figure 2.5 Client WMN

2.3.3 Benefits of WMN

WMN are more affordable than customary systems and eradicates the establishment cost of cables and fibers. For a larger scope region, WMN is predominantly utilized [33]. WMN is expendable, adaptable and can be included or taken away based less or more coverage region. WMN is utilized where network setups are blocked and has the low line of sight [34]. WMN supports high requesting indoor and open air availability and perfect to convey high throughput and solid networks. A self-organized and configured characteristic of WMN reduces the maintenance cost and setup time by enhancing the network performance. [35].

2.3.4 Applications of WMN

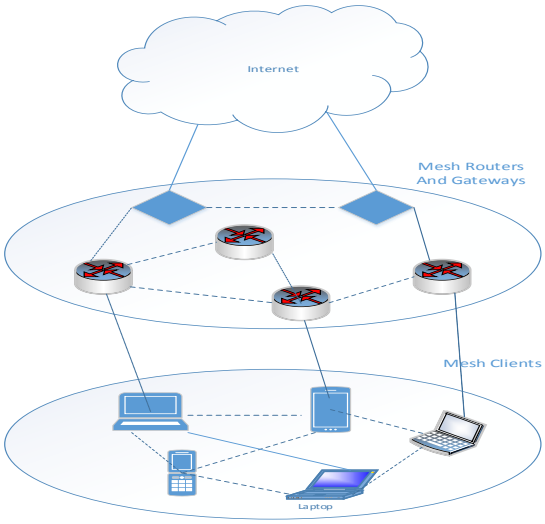


Figure 2.6 Hybrid WMN

Peer to Peer mesh topology helps to overwhelm the various placement challenges such as installation of Ethernet cable, deployment models, etc. In case of network failure, the mesh topology results top quick reconfiguration. Mesh routers can be located anyplace as they are attached with freedom of mobility. These characteristics of WMN draw the community to practice it in a diversity of applications. Some of them are given as below.

a) WMN in Smart Grids

To improve the electrical infrastructure or to augment the power savings, smart power system is becoming a naive global commercial initiative. A smart power system is essentially a streamlined electric grid, which proposals effective and authentic distribution of energy by using communication techniques and digital information. The system was brought out to diminish the costly environmental influences and to confirm energy efficiency. Figure 2.7 depicts the key ideas of smart grids.

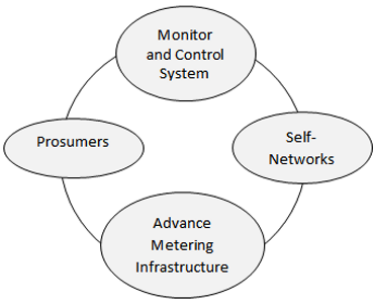


Figure 2.7 Smart Grid Concepts

b) WMN in real time traffic information systems

A probe method is a technique which gathers continuous movement information. To transmit the data information to the TMC (Traffic Management Center), a possible and cost effective remote correspondence is required.WMN is an architecture which is independent from some other wired/remote system and needs low correspondence cost. A WMN based activity framework comprises of two parts i) Probe vehicle during roving on roads consequently assembles the continuous traffic data and transmit to TMC over WMN. Probe vehicle is furnished with Data Collection Unit (DCU) and vehicular remote terminals. ii) WMN comprises of mesh routers and mesh clients. In this, mesh clients are our probe vehicles. WMN is framed powerfully by probe vehicle through remote associations. Data gathered on the vehicles compasses to the closest mesh routers that afterwards communicate with TMC.

c) WMN in Motorola

Mesh networking offers a consistent portability in changing remote information correspondence for subjects and gives financial and wellbeing benefits. Motorola has built up

a MEA (Mesh Enabled Architecture) that empowers practical and versatile network. The resonant out of mesh networking is basically performed in two modes i) framework based-it is honed to make wide or metro region systems and ii) Client networks that empowers the remote networks. The solitary element of work design in Motorola is that connections and courses are naturally framed between clients. Motorola has propelled different cross sections empowered arrangements that are Moto mesh (consolidates authorized and unlicensed radio in a solitary get to point) and mesh track that enables a faster and accurate user location.

d) WMN in Streaming Multimedia

Multipath existence between any pair of source and goal is one of the unparalleled characteristics of WMN. A video record may have different imitations, if reserving is incorporated at hubs in WMN, subsequently, if another customer ask for a video document, it might get that document from numerous sources. At whatever point different customers are keen in different video documents, then enlightening a numerous multicast tree may not be the best decision. Rather than organizing a different multicast tree, existing multipath normal for WMN is more productive. To build up a shared spilling framework and to discover the best video source area, let us assume that each WMN hub has pretty much memory space to spare nearby duplicates and disseminate these duplicates to peering WMN hubs. The association status is occasionally ordered by the media server. The server gathers the document area data and jellies them in a DMT.

e) WMN in Cloud Computing

Distributed computing is measured as an on-request fifth utility application. The design of portable distributed computing (MCC) is commonly erect upon intrigue driven mists, which enables the use of cloud administrations to versatile clients. Customarily MCC access experiences high cost and WAN execution issues. To rule over these issues, a scaled down cloud idea has developed, known as cloudlets. A cloudlet is a neighborhood server farm having the upside of self-overseeing; speedier access control, diminished cost in utilization and arrangement. By mixing a cloudlet with a remote availability i.e. WMN, nearby business can offer superior cloud administrations to bunch MCC clients. A WMN is a mix of two hubs, i.e. mesh client and mesh router which has the capacity to build up work availability among them. In light of self-mending, versatility and sorting out components, WMN can embrace to topology amid portability and blunder recuperation. Because of portability administration strategies, a mesh cloud design is being utilized which adequately underpins transmission between system switches and doors and possibly bolsters high data transfer capacity cloud

administrations, low reaction time, unwavering quality so along. The reconciliation of WMN and the mesh cloud system offers self - sorting out, self-administration and adaptable access to cloud administrations.

As WMN is a crisp worldview of remote systems administration, it offers a quick, modest and simple arrangement of systems. Today, every association is utilizing this innovation, in this way; it is the obligation of WMN to give administrations to clients in a secured and powerful way. One of the essential difficulties of conveying these systems is a security matter.

2.4 SECURITY ISSUES IN WIRELESS MESH NETWORK

2.4.1 Security Issues in Smart Grid

The most obligatory enabling mechanisms of the smart grid is the communication; merely in this there exist abundant scalability and defense matters. Security is one of the most acute concerns in smart grids that generally arise during the pre-serration of integrity and confidentiality of smart metering data in AMI.

2.4.2 Security issue in Intelligent Transportation System (ITS)

The primary objective of ITS is to provide a public safety by eliminating the accidents due to human mistakes. ITS innovation has been relentlessly presented in autos, yet security is one of the real worries in ITS. There exist two noteworthy security dangers i) ITS security risk, that is a string where hammers make rises around the vehicles to disturb the getting and transmission execution and ii) Wireless correspondence danger such as DOS, where system can be made inaccessible by flooding the false messages that take up all the usable data transmission. Therefore, digital security ought to be done on accessibility, confirmation and secrecy.

2.4.3 Security Issues in Multimedia

A similar security issues come up in mixed media i.e. integrity, confidentiality, non-repudiation, authentication, accountability, availability and encryption process are one of the real security dangers.

2.4.4 Security Issues in Cloud Computing

As cloud computing offers a cutting edge business for frameworks in light of strong, adaptable, effective and versatility exercises, overseeing bodies are still moderate in letting it

be known. A few issues and difficulties are aligned with it. Security is one of the significant difficulties which harpers the development of cloud. Security issues in cloud computing are i) information misfortune where programmer may see your significant information or might erase the objective information.

Table 2.2: Security concerns in various applications

Applications	Security issues
Smart Grids	Confidentiality, Authentication, Integrity.
ITS	Authentication, Availability, Confidentiality
Multi Media	Integrity, Confidentiality, Authentication, Encryption process, Availability, Non-repudiation,
Cloud Computing	DOS, Data loss, Confidentiality, Integrity, Accountability, Availability

An information misfortune may happen when proprietor of information misfortunes the key. ii) Account captured where if your record is seized by an assailant, then it might utilize the energy of your notoriety. An assailant having the control over record can listen in the exchange, control data, false harm reaction and soalong.iii) DOS-this assault is gotten in surge hour movement, where clients will be placarded by the aggressor's cloud benefit and there is no space to go to the goal with the exception of sit and anticipate. Thus, the integrity, confidentiality, accountability and accessibility are significant security assaults in distributed computing. Table 2.2 demonstrates the security issues in various utilizations of WMN. Open System Interconnection model (OSI Model) established by ISO describes a networking framework to device the protocols in seven layers. The OSI model assistances to breakdown the networking purpose into seven layers [36]. The OSI seven layer model trails in order when computer grasses data while it imitates to its reverse order when info enters into the data processor. The diagram of OSI model is shown in Figure 2.8. The detailed description of all seven layers is discussed below.

2.5 SECURITY ISSUES AND TRENDS IN OSI MODEL

2.5.1 Physical Layer

(a) Responsibility

It is accountable for carrier frequency generation, frequency selection, modulation, data encoding and signal detection. Existing wireless radios are capable to provision multiple

broadcast rates by combination of divers encoding and modulation rates. In society to surge the ability of wireless nets, numerous high speed physical skills have been designed i.e. Orthogonal frequency-division multiplexing (OFDM), Ultra Wide Band (UWB) [37]. To further surge the capacity, multiple antenna system has been castoff for wireless communication like smart antenna technology and antenna diversity, however due to high cost and complexity, fully adaptive smart antenna systems are castoff only in the base stations of cellular networks. In multiple antennas Multiple Input Multiple Output (MIMO) system are practical.

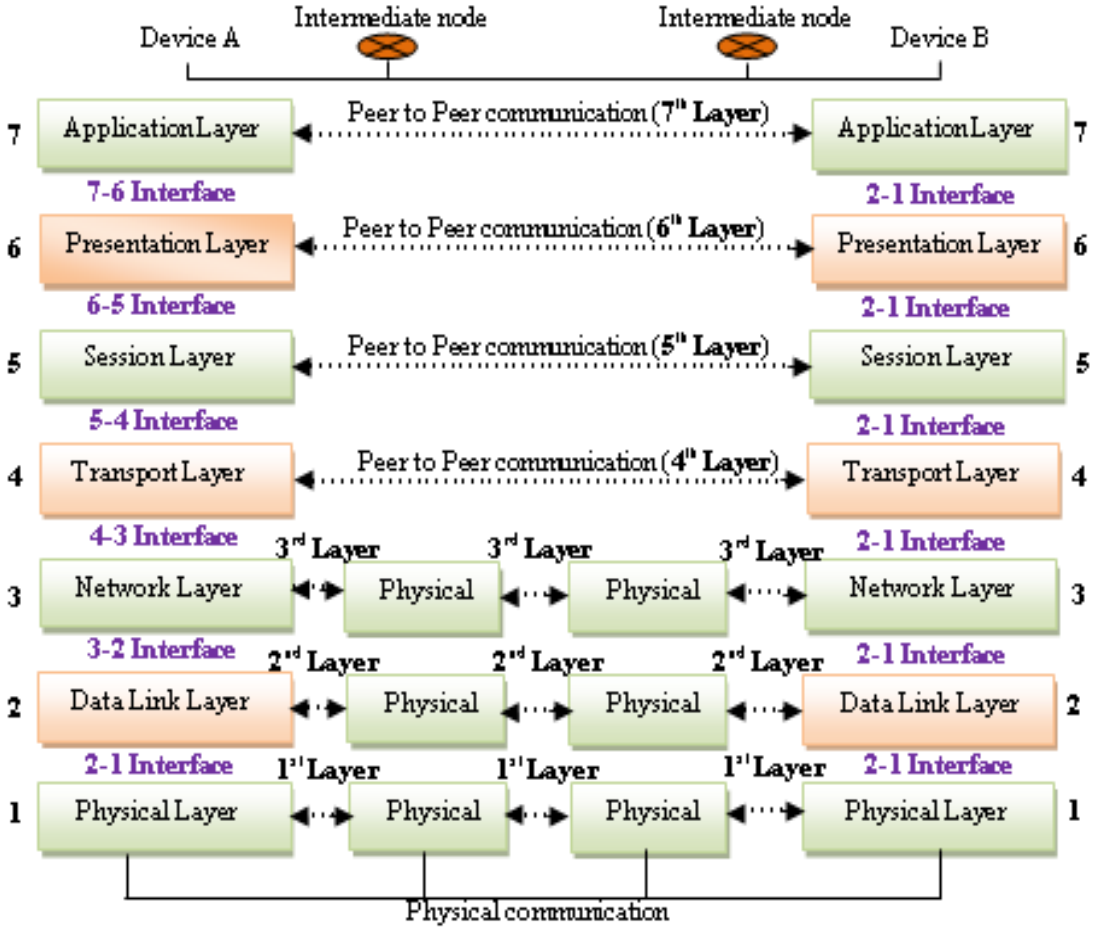


Figure 2.8 OSI Model Layer

(b) Attacks possible at Physical Layer

The physical layer is in charge of flag identification, tweak and encryption of data. As WMN conveys through radio based medium, the most effective assault at this layer is jamming assault. Jamming assault blocks the radio frequencies that disjoin the whole system correspondence [38]. On the off chance that assaulting gadgets don't obey MAC layer convention and become difficult to recognize them. The point of jamming assault is to

interfere in radio frequencies which are utilized amid the correspondence in WMN. It might happen in three diverse ways i) jamming source: which disturbs the whole web. ii) Less capable jamming source: in this enemy conceivably upsets the system by going around the jamming source. iii) Intermittent jamming source: it demonstrates horrible as some correspondence in WMN might be time delicate.

(c) Mechanisms Against various Attacks on Physical Layer in WMN

The jamming attack can be encouraged by engaging different spread spectrum technologies:

In Frequency hopping spread spectrum, a virtual random sequence is exploited which is known to both recipient and transmitter. By rapidly substituting a carrier signal, signals are troupe among many frequency networks. Thus, it is uncontrollable for an intruder to predict the, sequence and frequency selection and to jam it [39].

Direct sequence spread range exploiting a spreading code, each piece of sole flag is labeled by numerous bits. Spread code spread the flag finished a wide recurrence band, to slow the odds of intrusive from some other tuner.

(d) *Physical layer open research issue*

The research issue comprises improving the broadcast rate and public performance of physical layer technology over enhancement of the role of multiple antennas. MAC layer protocols essential to be deliberate carefully to top use the advance feature delivered by the physical layer.

2.5.2 Data link layer

(a) Responsibility

It secures the underlying association setup by isolating the data into information outlines. Data Link Layer (DLL) handles the acknowledgment from a beneficiary that the information made it effectively. DLL isolates the information parcels into casings. Data bundles are encoded and decoded into bits. It gives error handling, stream control and edge synchronization. The DLL is separated into two layers; i) MAC layer ii) Logical Link Control (LLC) layer. The MAC layer controls how a PC accesses the information while the undertaking of the LLC is to control the synchronization of edges.

(b) Attacks Possible at DLL

Jamming, MAC addressing, eavesdropping, spoofing and replays, are some probable attacks on link layer of WMN.

Jamming attack on link layer is additional hard to detect in contrast with the physical layer. In this, an intruder regularly conveys a MAC header on the channel so that, trusted nodes after the channel are demanding may lead to denial of service attack.

In ***Eavesdropping***, due to the distribution nature, wireless systems may dispose to to passive eavesdropping attack within the range of message nodes. Passive eavesdropping does not instantly bear upon the functionality of the network; however conciliate confidentiality and data integrity.

Replay attack, is also known as man-in-middle attack. Replay attack can be hurled by external clients or internal clients. If an attack is ended by external nodes, then to influence the access over network resources, an intruder will convey the messages later, whereas an attack completed by internal nodes, the attacker may retain copies of all data to gain sanctioned contact of resources [40].

(c) Security Mechanisms at Link Layer

To protect against frame collision attacks, numerous error-congestion codes were castoff and to deliver the protection in contradiction of passive eavesdropping, message confidentiality service is used [41].

Depending on permutation vector generation, Omari et al. have proposed a Synchronous Dynamic Encryption System (SDES). The SDES is vigorous against key cooperation ii) biased bytes analysis and integrity violation. In this, the security is confirmed using two types i) secret session key (SSK) and ii) secret authentication key (SAK). Deng et al. have proposed a threshold identity based authentication scheme where key generation phase is answerable for allocating the Pu/PR or master key for each client and authentication is appreciated by identity based mechanism. Another author projected a wireless intrusion detection mechanism in which a system entails of a number of devices which are situated near an access spot.

(d) *MAC layer research issues*

As scalability of WMN can be talked by the MAC layer in 2 ways i) upgrading the current MAC conventions or proposes an another MAC convention to expand near end throughput and ii) allow transmission of numerous depressions in each client for instance Carrier Sense Multiple Access/impact shirking (CSMA/CA).

Hence, current open issues in the MAC are employed on most of the existing MAC protocols founded on CSMA/CA solve partial problems of general issue, however raise different problems, i.e. how to basically improve the scalability in multi-hop ad-hoc network.

2.5.3 Network Layer:

(a) Responsibility

Switching and routing information is delivered by the network layer. This layer varieties a virtual circuit to convey the data from one node to another node. The persistence this layer is internetworking, addressing, congestion control and error handling.

(b) Attacks at network layer

Information and control packets are two cases of threats on the network layer. These efforts are either passive or dynamic [42] in nature. Control packet attack goals the router functionality where the intruder's objective is to access to the route available. Data packet attack goals the data forwarding functionality where attacker's aim is to source the DOS by injecting malevolent data into the mesh. We initially deliberate the control packet attacks, and then spot data packet attacks.

Control packet attack, targets on claim routing is rushing attack. In rushing attack, a route is demanded from the root node to destination node by flooding the RREQ (Route REQuest) data with sequence numbers. A delay is ended between the receiving of the RREQ messages by a precise node and advancing the nodes to next node. Attacker promotes a malevolent node among source and destination [43]. The determined of malevolent node is to onward the RREQ message to target node earlier any intermediate node. Thus, route among source and destination comprises the malicious client that leaves out the packet flow subsequent DOS attack [44].

In Wormhole attack, the impartial is same as rushing attack, however, it can be proficient by applying diverse schemes. If more than one malevolent node launches a tunnel among source and destination, the RREQ messages are promoted between malevolent nodes [45]. As between each origin and destination malevolent nodes are comprised, it's up to the malevolent node either to terminate the entire parcel or some discerning packets that are poignant among source and goal.

In Black hole attack, as malevolent node always retorts for positive RREQ, then approximately all the nodes dealings within a province of malevolent node is intended towards the malevolent node. The result origins a DOS attack. *The Gray hole attack* is a deviation of black hole approach. The sinking of whole packets may chief to easy revealing of malevolent nodes. So, attacker presented another attack, i.e. gray hole attack that may live hidden for longer duration of time by falling selected packets [46]. *Data Packet attacks* are chiefly launched by self-centered node. The most susceptible attack in this is inert

eavesdropping where the nodes are reliant on each other to onward the data. The selfish nodes may not achieve data promoting functionality. Selfish nodes either drop the discerning packets or entire packets. The malevolent node may familiarize trash packets to surge the packet or the bandwidth process time of the network.

In Multicast Routing Attacks, the intruder's aim is to intrude network communication by scrutinizing the traffic or leading to packet dropping.

(c) Security mechanisms at Network Layer

Authenticated Routing for Ad-hoc networks (ARAN) is an on demand routing protocol that is engaged to offer an authenticated setup, route discovery and path maintenance. It provisions the security by cryptographic certificates [47].

Handle: The public key of the reliable certificate server is exploited where the key is recognized to all. Each node accepts a certificate supplied by the server whenever a node seams the network, the certificate conveys the IP address of node, creation timestamp of certificate, public key node and expire time of the certificate. During the route discovery process, signed route discovery packet (RDP) is directed by a node which grips the IP address of the destination node, time stamp, source node certificate and a nonce. The node in the route discovery authenticates signature of preceding node and eliminates the certificate of previous node after recognizing the IP address of it. The client ciphers the context of the data, adds its own certificate signed by its individual key and conveys it to the promoting node. A route reply packet (REP) is produced by destination node and unicast the packet beside the same route. The REP comprises the source IP address, nouns, certificate, identifier of packet character and timestamp. As REP spreads to the source node, it confirms the nuance and signature of the destination node. Whenever an attacker familiarizes a malicious, an error is created because certificate of that node miscarries to found the genuineness.

Drawbacks: If the intruder injects a large bit of spurious control packets, then a node may not be capable to confirm the force and signature a node to discard some control packets.

Security-aware ad-hoc routing protocol (SAR) is dissimilar the traditional routing protocol that feats location metrics and hop count for setting the routing path, SAR routines trust values and relationships metrics amongst the nodes. A client is talented to forward the RREQ to next node only if it accepts the obligatory authorization or trust level. A shared secret apparatus or a key distribution mechanism is realistic to regulate the trust levels amongst the guests. Trust levels will not work at different security levels [48].

Drawbacks: To offer the security at dissimilar floors, a protocol wants different keys. As the number of keys surges at each level, its conservation and stored computational overhead also rises.

Secure Routing Protocol (SRP) involves a security association (SA) survival between source and destination pair. SA launches a shared secret key amongst two nodes. Query sequence number (QSEQ) (castoff by destination to check legitimacy of RREQ) and a random key identifier (QID) (to recognize specific request) are conveyed by the basis node. The source node's RREQ message is endangered by MAC which is calculated using shared key amongst source and destination. Each node onwards the received RREQ message, by accumulating the identifier. The ranking of a query is preserved by all nodes. The rate produced queries have the highest precedence. At the destination node, after checking the cogency of a query, destination node proves the authenticity and integrity of data and produces the RREP route responses using diverse paths. The authenticity and integrity of RREP are patterned by the same process as RREQ [49].

Drawback: The modification of unlicensed routes by malevolent clients cannot be prohibited by SRP.

Secure Link State Routing Protocol (SLSP) process is split into three parts; i) public key distribution and management (PKD) ii) Neighbor discovery and iii) link state updates. PKD is castoff to convey the public key certificates with zone while the NLP (Neighbor Lookup Protocol) is exploited to allocate the link state information [50]. The signed HELLO message (containing the sender MAC address and IP address) is castoff by NLP. The task of NLP is to generate a communication notification to SLP about wary observations. Wry explanations are those where a node privileges the MAC address of the existing node or the same MAC address is castoff by two diverse IP addresses. The introducing nodes' IP addresses are illustrious by link state apprises (LSU).Whenever a client accepts an LSU, it validates its signature by a public key. The ranking priority of each neighborhood node is preserved by all node; nodes with lower rates of LSU have the uppermost precedence. Whenever a malevolent node deluges spurious control message in the mesh, due to cohort of high rate traffic, the node will be accredited to lower precedence and will never be comprised in the itinerary.

Drawback: it has higher computational overhead as there is a usage of asymmetric key cryptography.

(d) ***Network Layer Open Issues***

Routing protocols for WMN are diverse from those in wired network and the cellular net. Despite the convenience of numerous routing protocols for ad-hoc networks, enterprise of routing protocols for WMN is still an active research area for numerous reasons: network performance metrics essential to be recognized and castoff to better the operation of routing protocols. Scalability is the most critical question in WMN.

2.5.4 Transport Layer

(a) Responsibility

As data packets portable in the form of segments, the transport layer is accountable for end to end connectivity amongst source and goal. Transport Control Protocol (TCP) and User Datagram Protocol (UDP) are the two chief protocols for transport layer. Reliable data transport and real time delivery are two suitcases of protocols. Reliable data transport is an ad-hoc transport protocols can be detached into two types: i) TCP variants ii) new transport protocols. An improved version of TCP supported networks is TCP variants. TCP acknowledge and TCP data revenue diverse paths in WMN which involvements latency, diverse packet loss and bandwidth while in ATP broadcast are rate founded which attains better recital. Real time delivery is usually to offer end to end delivery TCP are castoff instead of UDP. Additional protocols, i.e. Real Time Transport Protocol (RTCP) and Real time protocol (RTP) are castoff for congestion control.

(b) Possible attacks in transport layer

Synchronization (SYN) flooding attack, session hijacking attacks and de-synchronization attack are some probable attacks at the transfer layer. SYN flooding attacks are informal to launch at TCP, until resources essential by each connection are fatigued, an attacker may recurrently make new joining request. SYN Flooding Attack is a three way handshaking apparatus is practical to quality the session amongst two pairs of nodes as indicated in Figure 2.9.

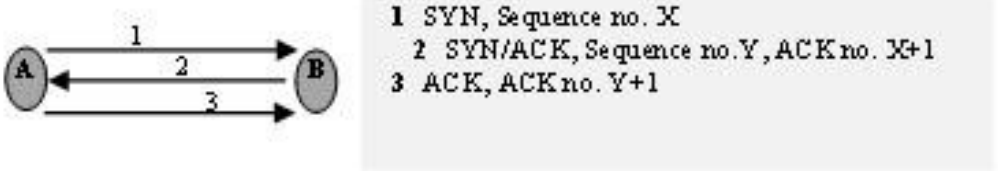


Figure 2.9 SYN Attack

Let's accept if node A desires to create a communiqué with node B then node A directs SYN packet beside with a sequence number another node B. Node B refers SYN sequence, ACK sequence number lastly node A finalizes the handshake procedure by distribution ACK with ACK bit. Straight off, the intruder by distribution too many SYN envelopes to node B may achievement and takeoff the return SYN protocol. *In Security Hijacking*, the security devices are accessible only at established time, however not at the on-going session. Thus, the intruder may accomplish the IP destination of a prey node and a form created sequence number and expected of victim node and then performs a DOS attack on victim node. Sequence number of victim node. In *de-synchronization attack*, the disturbance of an existing linking refers to a de-synchronization attack. De-synchronization attack indications to a TCP Acknowledgement (ACK) storm tricky. In this, the intruder inserts false messages by initiation a session hijacking in an enduring session amongst two clients. ACK of the interactive pair obtains this false message and refers an ACK to different client. Another end node is not proficient to discriminate the sequence number of this ACK so; it efforts to re-synchronize the session within its interactive peer. Thus, in this ACK containers go back and forth source an ACK storm.

(c) Security Mechanism at Transport Layer

The protocols hired for fortifying transport layers are Secure Socket Layer (SSL), private communication transport (PCT) and Transport Layer Security (TLS). To secure the session, SSL/TLS custom asymmetric key cryptography technique. EAP-TLS, an upper layer authentication protocol was planned by Ababa and Simon. EAP-TLS proposals mutual authentication amongst MR and MC. In this each terminal turns as an authenticator for its previous node.

(d) Transport layer Research Issues

It comprise several protocols occur for consistent real time delivery and data transport. Reliable data transport distresses with ACK, TCP data, ATP. In WMN, TCP acknowledgement and data surveys different path outcomes bandwidth, packet loss and reaction time. Even if same path usages face transmission in ATP and network asymmetry problems is rate based and for real time delivery, the protocols castoff are RTP, UDP and RCTP.

The current open research concerns are occupied on is to escape asymmetry amongst acknowledgement and data paths, it is expected for a routing protocol to choice an optimum route for both ACK and data packets but without increasing the budget items.

2.5.5 Application Layer

Application layer provisions the end user processes. It delivers electronic mail; network software's and files transfer facilities. File Transfer Protocol (FTP) and Telnets are the claims that endure in this layer only.

(a) Responsibility

It confirms the user to contact the network and offers the user provision for services, i.e. email, file transfer and network virtual terminal.

(b) Attacks at Application Layer

Flooding and Snooping are the two major attacks in WMN. Flooding attack disturbs the accessibility of victim and huge serving of the network while snooping attack disturbs the unity of the message being connected.

(c) Mechanisms

IDS and firewalls are most normal conducts of securing application layer. Firewalls proposal the protection alongside spywares and malware etc.

2.6 CONCLUSION AND OPEN RESEARCH CHALLENGES

In the event that any association's system is hacked, programmers may get to all the individual databases of customers as effectively as its representatives. Thus, the main thing to keep your system secure is to give the get to just to approve clients. WMN designs comprising of two sorts of hubs, work switches (MRs) and work customers (MCs). Work switches go about as spine which give the system administrations to the customers and are in charge of sending the information parcels to their expected goal hubs though MCs are the end focuses that get to the system administrations through work switches.

Whenever a MC moves outside the boundary range of its current serving mesh router then the corresponding SNR of that serving MR will fall due to signal attenuation. A significant drop in SNR ratio makes the MC to search for a new mesh router having good signal strength for continuing its network services by triggering the handoff procedure. The SNR value is used to measure the signal strength between source and destination. It is important because by measuring this it is easy to predict at what distance a router can be placed between source and destination so that the signal will reach to its destination without any distortion. This concept of SNR is used in handoff authentication process where during the handoff procedure mesh client needs to search a new mesh router for resuming its

communication by measuring its SNR value. Since the nodes are dynamic, unstable and limited by security disputes with new performance issues, a significant delay in handoff procedure may cause copious performance concerns such as network attacks and delay in the network. Therefore, during the handoff procedure, it is prerequisite that roaming clients ample access authentication process not only with a short delay but also with the fortification of the roaming clients as well as the handoff networks. Further, if a node either inter-domain (communicating between two domains) or intra-domain (communicating within a domain) wants to send some messages to its intended destination node, the information is being passed among multiple MRs. However, to prevent the data exposure at each intermediate node, the messages must be encrypted by some security technique or an ornate encryption technique is required to guarantee that even if the message is forged by an intruder then it may not be able to decrypt it anyway. Due to the dynamic nature of WMN where information is being passed over multiple hops or MRs, data encryption process is taken to be an important parameter. Furthermore, the most significant factor that impacts the WMN performance is the nature of the fundamental routing protocols used for promoting the data packets. Presence of any malicious or misbehaving node within a routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network.

Although, a number of scientists/researchers have proposed various handoff authentication procedures and message encryption and secure routing techniques, however, the issues arise due to the intruders that encounter a number of malicious nodes or threats to disrupt the network performance. In addition to this, by increasing one parameter such as to ensure the security others parameters (such as end-to-end delay, network throughput, packet delivery ratio) get affected drastically, therefore, there is a need to propose an efficient security technique having reduced authentication delay, less encryption/decryption time and secure routing mechanism against routing layer attacks with the aim of increasing the other network parameters. Therefore, in order to provide an efficient and secure communication process, the security is ensured at three different aspects i.e. authentication of handoff clients, encrypted message transmission between source and destination and secure route discovery to route the transmitted data packets.

CHAPTER 3
SECURE HANDOFF TECHNIQUE WITH REDUCED AUTHENTICATION DELAY IN WIRELESS MESH NETWORK

The aim of this chapter is to propose a safe handoff method by creating the tickets for the mobile client's which are partitioned into various zones of mesh router as per their communication range. An authentication server investigates the whole system after a particular interim of time and is in charge for creating and refreshing the comparing tickets of customers as indicated by their mobile client's. At any point a client goes into the scope of another space; to get to the administrations from mesh router, mobile client's needs to demonstrate its authenticity to the comparing zonal router. Each mesh router stores the ticket of its zonal router client issued from the authentication server and approves the roaming client by coordinating the ticket. The proposed approach lessens the issue of capacity overhead and security dangers at mobile client as each ticket is put away in validation server database and is issued upon the demand. The proposed system is approved over confirmation delay and distinctive probabilistic situations of authentication and is demonstrated true by examining an observational review against announced writing.

3.1 INTRODUCTION

WMN, an auspicious communication prototype, is an unusual kind of multi-hop wireless technology which has emerged to address the precincts of traditional wireless networks. There exist three kinds of WMN architecture (client, infrastructure/backbone and hybrid) consisting of two sorts of nodes i) MR and ii) MC. MRs, which are generally static or have minimal mobility in the network provide the internet connectivity to mesh clients by forming a wireless backbone while MCs are mobile and access the network services via mesh routers. Handoff in mesh environments is an important parameter to support the mobility in the network and is defined as connecting with the new mesh router by leaving the current serving router's range due to fall in signal attenuation during mobility [51]. Whenever MC moves outside the range of its current serving mesh router, the SNR falls due to signal attenuation,

therefore, the significant drop of SNR ratio makes the MC to search a new mesh router having good signal for improved services by triggering the handoff procedure in the network.

Since, the nodes are dynamic, unstable and limited by security disputes with new performance issues, a significant delay in handoff procedure may cause copious performance concerns such as attacks and delay. During handoff, it is prerequisite that roaming clients ample access authentication not only with a short delay, but also with the fortification for the roaming clients as well as the handoff networks. Several handoff protocols have been proposed in the literature to reduce handoff latency. A study of Xu et al. [52] concludes that the delay can be reduced without the involvement of AS. The MRs can directly authenticate MCs using the tickets generated by routers. Although one of the parameters i.e. authentication delay [53-55] is reduced but as the number of MRs and MCs are resource limited (having limited storage and energy constraint), there may be a chance to increase the possibility of active attacks and other security threats [56-58]. Research community has designed several handoff routing protocols for WMN, however there is a need to improve performance metrics based on security, fast and resilient nature.

The aim of this chapter is to propose a secure handoff procedure with reduced authentication delay under different probabilistic scenarios. The potential contribution of the chapter is described as follows.

- Ticket generating-assigning phase is used to generate the keys and the tickets between communicating nodes.
- Handoff authentication phase explains the actual handoff procedure in the network.
- Authentication delay is analyzed under different probabilistic scenarios through NS2 simulator and an empirical study is done over certain security threats to prove the legitimacy of the work.

The proposed scheme is analyzed against ticket based handoff technique [53]. The objective of the proposed handoff protocol is to support an efficient handoff process in a secure manner. The major difference between proposed protocol and ticket based handoff is that in our scheme, keys and tickets are generated and stored by AS, while in ticket based handoff, tickets and keys are generated by AS but stored at MRs and MCs which may lead to resource constraint problems i.e. storage overhead and makes the network vulnerable to several security threats. Further, our scheme is resistant against user privacy, black hole, forgery and denial of service attacks as there is no direct link of AS with the MCs or an attacker. Proposed approach is both centralized in case of handoff and distributed during

normal communication which reduces the extra overhead of key management at server's side. The remaining structure of the chapter is organized as follows. Section 2 discusses the related work. The network model of the entire chapter with proposed handoff technique is deliberated in section 3. Further, section 4 debates the performance evaluation of proposed technique by showing the probabilistic scenarios and request delay of both the techniques. Moreover, an empirical analysis of additional networking parameters i.e. key management overhead, storage overhead, ticket generation overhead and user privacy concerns proves the legitimacy of the proposed work in this section only. Finally section 5 concludes the chapter.

3.2 RELATED WORK

Proactive [59, 60], ticket-based [61] and multi-hop [62] are three different handoff techniques to authenticate the clients in WMN. In multi-hop technique, roaming client needs to re-authenticate itself to AS which is at multi-hop distance from it. Proactive authentication reduces multi-hop distance by pre-distributing pair-wise master keys (PMK) and certificate of log-in authentication before moving of a roaming client to another access point while ticket based protocol reduces handoff latency by using the tickets as successful log-in authentication.

PANA [63] and EAP-TLS [64] are the two multi-hop authentication protocols in which the client authenticates itself to AS by passing the messages through multiple hops. Let us consider a scenario in which there is a fall in the SNR ratio due to which the mobile client needs to leave its current serving MR and search for a new MR. To access the services, roaming client needs to re-authenticate itself with the new MR, for that, the roaming client sends a request containing its media access control (MAC) address and the Base Service Set Identifier (BSSID) of the old MR. Upon receiving the request message, the new MR sends this request message to AS in order to verify old MR. If BSSID is valid then AS will send an accept message to the new MR containing the security information for handoff communication between the old and new MR. Park et al. [65] proposed a proactive protocol in which after successful authentication of a roaming client, AS will send a PMK to its associated MR with its client, after which the client will perform the same calculation as the AS to obtain the same PMK. Further, MR and MC use PMK to obtain Pair wise Transparent Key (PTK) for packet encryption.

The major limitation of this mechanism is that the pre-distribution of keys incur extra traffic overhead. In ticket based authentication, authenticity is measured by generating and

verifying the tickets by the AS, however, AS has to generate a large number of tickets in the network which may cause storage overhead. In order to reduce handoff latency, a number of schemes have been proposed by the researchers.

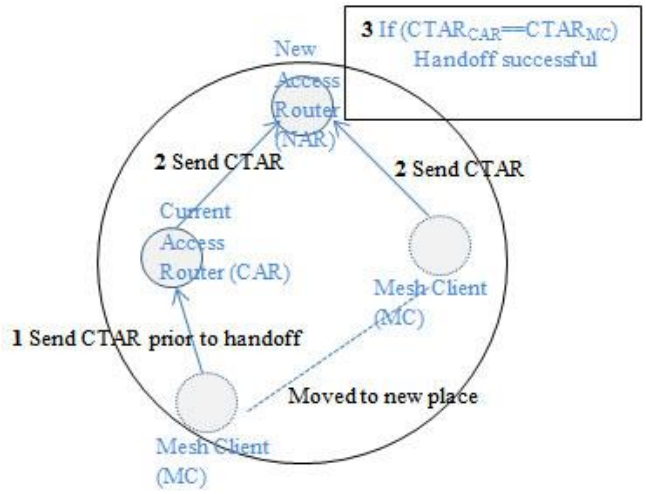


Figure 3.1 Context transfer activation request technique

The below text explains some more efficient handoff techniques related to our work. In Huang et al. [66], a profligate handoff is done by sending a context transfer activation request to the new servicing MR. As depicted in Figure 3.1, before the handoff procedure, roaming client will send a Context Transfer Activation Request (CTAR) as a token to its current accessing MR and move to a new router's range. After getting the request from MC, previous servicing MR sends the activation token to the new router. Upon reaching in the range of new MR, for completing the handoff authentication, MC sends its activation request to it.

The new servicing router computes the activation token using the parameters supplied by previous MR and if the token sent by the previous MR matches with the client's token then the handoff verification procedure completes successfully. The advantage of this technique is that handoff procedure completes with less communication steps between router and client but the technique may be prone to other performance issues i.e. Every time the roaming MC first needs to send the activation request to its previous MR after which the previous MR will forward the request to the new MR which may cause significant handoff latency. Further, the storage overhead surges at MC as it has to store the context transfer request in its routing table. There are some other techniques proposed in [67-69], in which after completing the initial full authentication, handoffs will be provided by deriving a PMK between individual MCs and AS, as presented in Figure 3.2. A separate PMK is derived between each MC and AS. Before the handoff procedure, neighboring routers need to interact with AS in order to get n^{th} PMK.

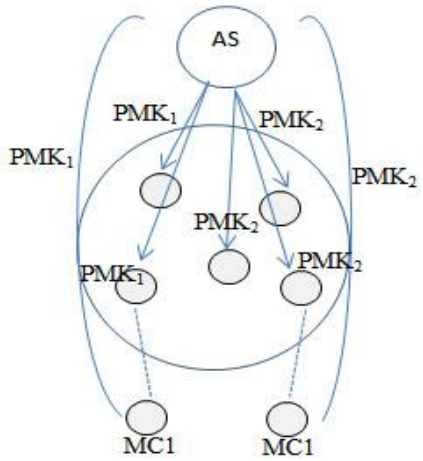


Figure 3.2 Proactive key distribution technique

Although, the approach may lead to reduced significant handoff latency but an independent PMK is used between AS-MC which is difficult to maintain, moreover, servicing MRs need to interact with AS for PMK which may increase communication time in the network. Further, a Group-based Handoff [70, 71] technique was proposed where in order to support fast handoff, a group key is shared among all the Base Stations (BSs). Authorization, Authentication and Accounting (AAA) server issues a multi-BS group key (MGK) to all the BSs. A single MGK is used by all the BSs in order to reduce key management and fasten the handoff procedure. PMK is shared between user and serving BS. The current serving BS computes a ticket for the handoff client using MGK after identifying the roaming client. The ticket contains PMK based on which the handoff procedure authenticates. During handoff, the roaming client sends the ticket issued by current serving BS to the new accessing BS. New BS decrypts the ticket using MGK and PMK and completes the handoff if PMK is authenticated. The major limitation in this approach is that, as a single group key is shared among all the BSs, if one of the BS is compromised, then the entire network may prone to an attack and with the same PMK, it is easy to forge the ticket used among all the MCs.

Further, the approach discussed by Xu et al. [53] which is taken as the base paper of our chapter is Ticket-based Handoff. The author proposed a ticket based technique for handoff by defining the procedure in two different phases. i) Ticket issuing phase is used to generate the tickets for handoff procedure while ii) re-authentication phase is done in the actual handoff authentication. In this approach, each MR and MC stores the keys and the tickets of their domains into their databases. During handoff procedure, whenever a MC enters into a foreign mesh router's (FMRs) domain to access the services, MRs communicate with each other to know the domain and to get the ticket and the key of the servicing MC to authenticate its

legitimacy. The limitation in this approach is that the communication between MRs may indulge a number of security threats i.e. Denial of Service (DOS) attack, message forging attacks and lead to significant delay and communication overhead issues. Further, the storage of keys and the tickets at MCs involve several resource constraints such as memory, energy consumption and storage problems. Moreover, attackers can easily attack on MCs and communicating MRs to forge or modify the data and affect the network performance by adding the delay process.

In a summary, none of the existing techniques provide guarantee for reduced authentication delay [72] and resiliency against security attacks [73]. So, the main focus of the proposed protocol is to reduce authentication delay, request delay and ensure a secure communication under various security threats. The proposed protocol is analyzed over certain probabilistic scenarios of authentication delay to highlight the output results.

3.3 PROPOSED NETWORK MODEL

This section describes the proposed approach with its architecture, trusted and handoff models before discussing the actual technique. Below subsections deliberate the network architecture, handoff structure and the trust model assumed by the proposed technique.

3.3.1 Network Architecture

The proposed model considers a hierarchical WMN architecture consisting of three layers. For framed model, the AS is present at the topmost layer and generates and distributes the tickets to the next stratum. The second layer consists of MRs which takes the data and forwards the traffic to the AS through multi-hop mode.

The third layer consists of the wireless user devices which access the internet services. Figure 3.3 presents a hierarchical network model in which dashed lines indicate wireless links and solid lines designate wired links. The whole network consists of two backbone routers which form a mesh infrastructure with self-healing, self-organizing and self-configuring characteristics. The backbone network is built using IEEE 802.11 technologies. The clients are divided into multiple domains. Each domain is connected with at least one mobile access point that is connected to the MR. The wireless devices may be connected with each other directly via MRs or may be connected through access points called BS and MR. The below subsection discusses the handoff model

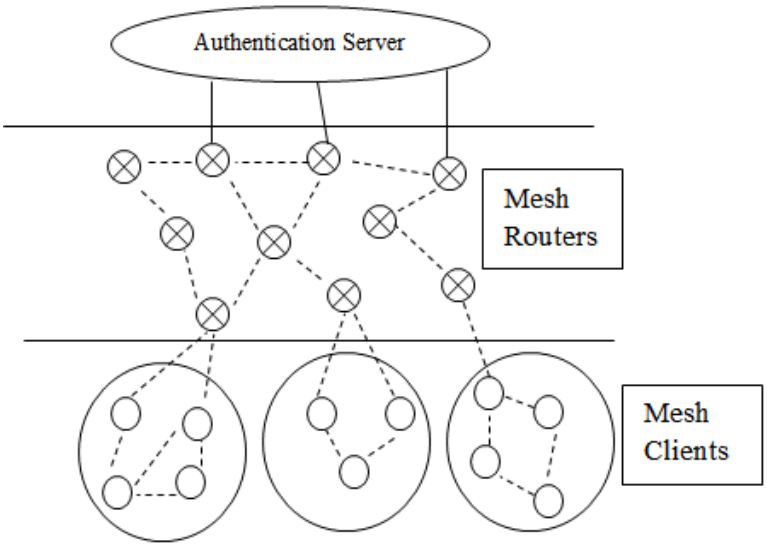


Figure 3.3 The network architecture of proposed technique

3.3.2 Handoff Model

Figure 3.4 depicts the handoff mechanism in which a mobile client is initially connected to its Home Mesh Router (HMR) and then moves to the new location B.

As the distance between HMR and MC increases, the SNR ratio falls down. So, when it moves from location A to location B, it needs to handoff from HMR to FMR. After successful authentication, MC will connect to FMR at point B. According to the network model framework of Figure 3.5, both HMR and FMR are connected to the backbone network and a MC completes the handoff procedure.

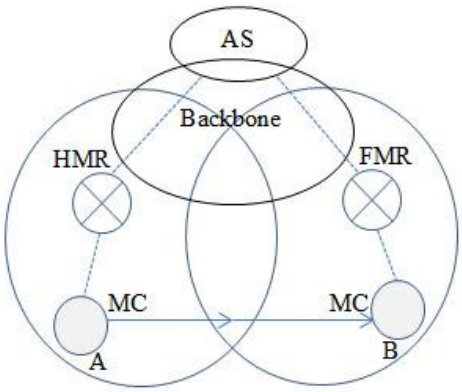


Figure 3.4 Handoff procedures during mobility

3.3.3 Trust Model

The proposed trust model (as shown in Figure 3.5) is built upon the concept of tickets, keys and AS which generates and issues the tickets and can be trusted by various entities in a mesh network.

The tickets are used to establish the trust relationship among entities. The below text discusses the trust relationship among entities as depicted in Figure 3.5.

1. Trust between HMR and AS: The trust between HMR and AS is established via group based master key (GMK) generated by AS.
2. MR: Any two MRs either HMR or FMR trust each other via their GMK in a mesh network.
3. MR and MC: The mutual trust between MR (HMR or FMR) and MC is established via ticket generated by AS.
4. *MC*: The mutual trust is based upon PMK issued by AS and is established by exchanging the messages between the clients.

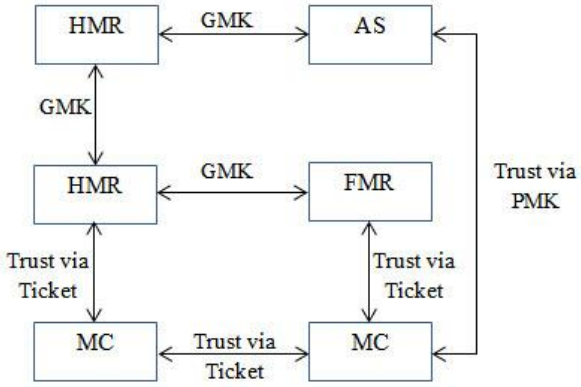


Figure 3.5 Trust Model of Wireless Mesh Network

3.3.4 Proposed Approach

This sub section defines a secure and efficient handoff technique in WMN. The proposed scheme is explained in three different phases, local authentication phase, ticket generating-assigning phase and handoff authentication phase. In local authentication phase, MC will prove the validity to its HMR by exchanging some local messages while in phase two, AS generates the tickets using GMK shared between AS-MRs. AS issues the same tickets to MRs which are at 1-hop or single hop distance from each other.

The advantage of issuing same tickets is that it reduces computational overhead at AS and storage overhead at MRs and MCs. The tickets generated by AS will be used by MC and MR for the future use.

Further, in phase three, handoff authentication process will be successful if the parameters of the tickets sent by previously accessing MR matches with the ones sent by roaming MC. As the new MR may contact with previously accessing router, there is no need for full handoff. In response of full handoff procedure the HMR deletes the history of the roaming

MC from its database on moving into the range of another router i.e. FMR. The deletion of history will increase the computational overheads to re-authenticate the same MC when it will come back again into the range of HMR. However, in our case, the HMR does not remove its history so that in future, when the same MC comes back into the range of HMR, there is no need to re-authenticate it again which leads a reduced amount of computational overhead. Moreover, a localized or half handoff procedure is triggered between roaming MC and new MR which reduces handoff cost and latency. The taxonomy used throughout the chapter is presented in Table 3.1.

Table 3.1: Taxonomy used

Notations	Meaning
ID_{MC}	Identity of mesh client
ID_{HMR}	Identity of home mesh router
Sig_{server}	Signature of authentication server
T_i	Ticket of i^{th} node
H_{GMK_i}	Group master key of HMR
ID_{FMR}	Identity of foreign mesh router
n	Nonce
t	Expiration time
GMK_i	Group master key of i^{th} node where i=1,2,…n

- ***Pre-deployment Phase***

Prior to WMN deployment, there was an assumption that MRs and MCs are loosely synchronized and server does the following operations.

- AS and MRs maintain trusted relationship and establish secure connections.
- Full authentication is performed by running EAP-TLS

Phase 1: Local Authentication Phase

After the complete deployment of network architecture whenever a client wants to access the services with its HMR then it can be done via exchanging some messages. Each MR and MC initially authenticate to the AS using their keys and get the signature of the server for mutual communication. Figure 3.6 depicts the local authentication procedure.

1. During the initial communication, MC sends the $ID_{MC}, ID_{HMR}, Sig_{server}$ as a message to its HMR.
2. After getting the message from the client, MR verifies the legitimacy of that client by verifying it's sig_{server} and sends the message as $ID_{MC}, ID_{HMR}, Sig_{server}$ to the client.

3. Correspondingly, if MC also wants to check the validity of the MR then it may check it by seeing the router's message.

   If ($message_{MC}$==$message_{MR}$)

   Client is legitimate and can access the network services

   Else

4. Not a legitimate user

Phase 2: Ticket Generation-Assigning Phase

The purpose of this phase is to generate the keys between AS-MC, AS-HMR and HMR-MC. The AS generates the tickets based on the keys generated between AS-MC. The current accessing MR is called as HMR and the targeted handoff MR is defined as FMR. The following steps and Figure 3.7 show the details of this phase.

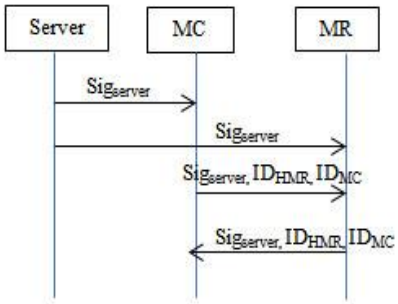


Figure 3.6 Local authentication phase

1. A Master key (MK) is generated between AS-MC to establish a secure channel among each other. Further, PMK between AS-HMR and HMR-MC is generated via MK.

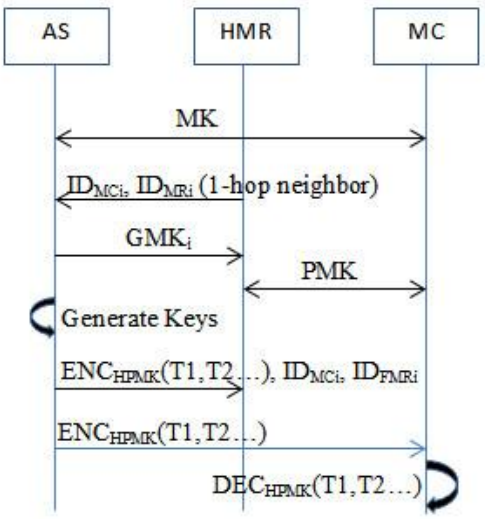


Figure 3.7 Ticket generation-assigning phase

2. Due to routing functionality, each MR is aware of its 1-hop neighbor routers as depicted in Figure 3.8. Each MR will send ID of MC and its 1-hop neighbor routers to AS. Then, AS will generate a GMK based on routers' ID.

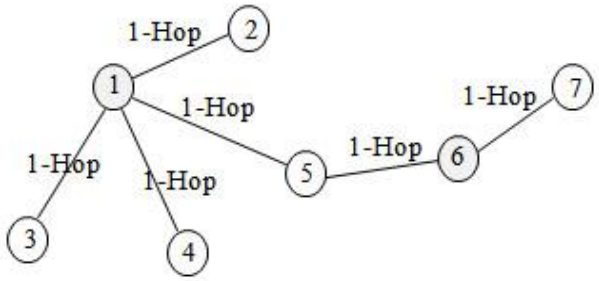


Figure 3.8 Single hop neighbors

Routers which are at 1-Hop away from each other will share the same MK as depicted in Table 3.2. Finally, a secure channel between HMR-MC is established by sharing PMK derived from mesh clients' MK.

3. By choosing an expiration time t, nonce n and using the identities of clients and mesh routers, AS will generate the corresponding handoff ticket T_i for the handoff authentication and then store the ticket T_i along with sending it to the corresponding mesh router $MR_i$for future use as present in equation (1).

$$TAK_i = H_{GMK_i}(ID_{HMR}, ID_{FMR}, ID_{MC}, n, t, sig_{server}) \text{ and}$$

$$T_i = (TAK_i, ID_{HMR}, ID_{FMR}, ID_{MC}, n, t)$$

(1)

During handoff procedure, targeted MR or MC will request for the tickets directly from AS.

Table 3.2: Authentication Server routing table

MRs ID	Keys	Tickets
1	GMK_1	T_1
2	GMK_1	T_1
3	GMK_1	T_1
4	GMK_1	T_1
5	GMK_1	T_1
6	GMK_2	T_2
7	GMK_2	T_2

Phase 3: Handoff Authentication Phase

The handoff authentication procedure takes place by degrading the SNR between HMR-MC due to increase of communication distance. The below steps discuss the communication steps encountered during handoff authentication phase.

Roaming MC searches for an FMR_i based on good SNR ratio. The FMR_i is chosen by taking the distance between MC-MR as the main criteria. A threshold value of SNR is fixed and then calculated as signal strength using equation (2). MRs having good signal strength will be chosen as FMR_i.

$$Signal\ strength = \frac{Distance}{SNR} \tag{2}$$

The SNR is defined as the ratio of signal power to the noise power. The major consideration in calculating the SNR ratio is signal power since, the noise power is considered as negligible to create the simulation environment. The initial energy of the node plays an important role in calculating the signal power. According to the relation that the power is defined as the energy per unit time, as the simulation time progresses the initial energy also decreases as presented in equation (3).

$$Avg.power = \frac{\Delta E}{\Delta t} \tag{3}$$

Each node in the network has a limited amount of energy and is consumed exponentially, so a node requires certain amount of energy to transfer the data from one node to another. This amount is measured exponentially with the distance as power of e. The threshold limit after which a node is considered vulnerable is 10-30% of the initial energy left at the node and below this a node is not allowed to no longer send or receives the packets and will be a dead node.

During the simulation environment, the distance between MRs is known to us as the signal strength which depends on SNR value and distance between the routers. From the known distance we can easily calculate the signal strength. The node which is mobile can initiate the handoff when it gets better signal strength from other routers. After choosing its new MR, MC sends a handoff authentication request to HMR by leaving the HMRs range.

1. Upon receiving the MCs request, HMR will forward the request to AS to get mesh client's ticket T_i and will subsequently send the corresponding ticket T_i to FMR_i (as each MR is connected and able to communicate with each other).

2. Now, to authenticate itself, MC will request for ticket T_i from AS and send its ticket T_i to FMR. As FMR already has the ticket T_i of that MC, so it will verify the tickets by matching them with each other.

If (MC_{ticket}==FMR_{ticket}) **then**

Then client is authentic

Else

Client is not authentic

3. After verifying the ticket, a temporary session key will be generated between FMR-MC by generating some random numbers. Both MC and FMR will generate their random numbers as $g^r MC$and$g^r MR$. Mesh client will send a message as ($g^r MC$ and Ticket T_i) to FMR. Correspondingly, FMR will send its message ($g^r FMR$ and ticket T_i) to MC.

If ($g^r MC^{MR}$ ==$g^r MR^{MC}$) **then**

Temporary session key is generated between MC and FMR

A ticket based key is added to the packet from phase two to compute the overheads of all the three phases and a 32-bit ticket is generated which is matched between each roaming MC and FMR pairs. Therefore, a total of 80 bits are added to the packet envelope containing a maximum of 512 bits of data which can be measured as the overhead generated by all three phases of proposed mechanism. In order to check the accuracy of generated tickets a cyclic redundancy check (CRC) method is used where the received packet verification is done on the basis of the CRC bits. In this method, 8-bit CRC is added to the envelope and can be verified using the CRC sequence (11000101). Modulo 2 additions is then performed between the received message and the CRC polynomial and if the remainder is zero then the received code is considered as error free.

3.4 RESULTS AND DISCUSSION

The simulation of proposed approach is done over NS2 simulator where the low pass filters such as channel type and radio propagation models are described initially to extract the accurate information from the noisy signals. The environmental setup for simulation is presented in Table 3.3. A 500 m ×500m network area is constructed having total number of 70 nodes. The numbers of clients are all mobile in nature (which means they can leave their HMR and connect to other HMRs range at any time). The mobility speed of mesh clients is setup as 0 to 5 m/s with the transmission range of 25 m/s. Further, the transmission ranges of

mobile access point (MAP) routers are 120 m/s and MAC layer protocol used is 802.11. The simulation time for the experiment is setup as 30 seconds. The architecture of WMN proposed in the chapter consists of an AS, responsible for generating the tickets to MRs and MCs, two internet gateway routers (IGW), which provide the connectivity between internet and MRs, 10 MRs which provide the network services to MCs and 60 MCs which actually utilize the internet services. As presented in Figure 3.4, mesh clients are divided into different zones. A MR which provides the services to its zone's or domain's MCs is known as HMR. The domains are constructed according to communication range of MCs with their HMR. The number of clients having good SNR ratio from their HMR is considered as one domain.

Table 3.4(a) and Table 3.4(b) give the detailed analysis of the values obtained during the simulation of existing approach considered as basic approach over proposed mechanism. The experimental results and empirical study in next subsections proves that proposed approach verifies to be better than existing protocol considered as basic approach in the output results.

Table 3.3: The network parameters of the proposed technique

Network Parameter	Value
Network Area	500 m ×500 m
Number of Nodes	70
MAC	802.11
Simulation Time	30 seconds
Mobility Speed	0-5 m/s
Clients	60
Mesh clients Transmission Range	0-25 m/s

Table 3.4(a): Simulation results values of both the approaches

Simulation Parameters with their Approaches		**Different Network Size (by varying number of nodes)**				
Network Parameters	**Approach**	10	20	30	40	50
Average Authentication Delay	Basic Approach	0.33	0.37	0.42	0.46	0.51
	Proposed Approach	0.23	0.27	0.29	0.32	0.36
Maximum Authentication Delay	Basic Approach	0.34	0.39	0.45	0.51	0.58
	Proposed Approach	0.26	0.31	0.35	0.42	0.45
No Authentication	Basic Approach	0.531	0.544	0.612	0.695	0.768
	Proposed Approach	0.428	0.467	0.496	0.512	0.526
False Authentication	Basic Approach	3.214	3.658	3.984	4.346	4.854

	Proposed Approach	2.121	2.467	2.926	3.065	3.264
Correct Authentication	Basic Approach	5.717	5.26	4.866	4.421	3.841
	Proposed Approach	6.913	6.568	6.041	5.885	5.672

3.4.1 Empirical Analysis

The handoff client accesses the network services from FMR after authenticating itself by verifying the ticket generated by the AS in the proposed mechanism. If the ticket stored in FMR database matches with the ticket sent by the handoff client then it will access the services from the FMR. The proposed mechanism has computational significance against authentication delay and different probabilistic scenarios of authentication while empirical significance against routing attacks encountered during handoff mobility. The below subsections discuss and present how proposed mechanism is resistant over mentioned attacks and ensure the security during communication. The threats are assumed manually in the network by indulging several attacks and showing the number of steps to overcome these threats.

Table 3.4(b): Simulation results values by varying the speed of node

Simulation Parameters with their Approaches		**Different Network Size (by varying the speed (m/s) of node, number of nodes taken as 50)**				
Network Parameters	**Approach**	5	10	15	20	25
Average Authentication Delay	Basic Approach	0.47	0.54	0.62	0.69	0.78
	Proposed Approach	0.32	0.39	0.44	0.51	0.58
Maximum Authentication Delay	Basic Approach	0.57	0.64	0.69	0.73	0.77
	Proposed Approach	0.41	0.46	0.53	0.61	0.64
No Authentication	Basic Approach	0.711	0.763	0.798	0.834	0.865
	Proposed Approach	0.512	0.546	0.557	0.589	0.612
False Authentication	Basic Approach	4.645	4.831	5.012	5.334	5.978
	Proposed Approach	3.117	3.243	3.564	3.887	4.213
Correct Authentication	Basic Approach	3.754	3.534	3.231	3.011	2.954
	Proposed Approach	5.742	5.422	5.013	4.887	4.734

- ***User Privacy***

Lemma: Suppose an attacker{W} initiates a privacy attack by forging the ID of legitimate mesh clients {X,Y,Z} in the mobile network.

Proof: The Users also termed as MCs can share the information with complete privacy. In the proposed approach a message authentication is used in which the MC can send the message to router with a specific key generated by the AS for both MR and MC. Consider the scenario where A is the mesh router and X, Y and Z are its clients.

Start

$X_{info} \rightarrow A, where X_{info}\, includes ID_{MC}, ID_{HMR} and Key assigned by Authentication Server$

$Verify(X_{info}), function verifies the information given by X$

$If(ID_{HMR} matches with the X_{info}) then,$

$Authentication Granted$

End

This provides the double security as there are keys issued by the AS to both the MRs and MCs.

- ***Forgery Attack***

Lemma: suppose an attacker {A} wants to forge the information of MCs {x, y, z} or mesh routers i.e. ID_{MC}, ID_{MR}.

Proof: The proposed approach is secure against the forgery attack as it uses a two key authentication process which is provided by the AS. All the Authentication related issues are directly handled by the authentication server while MRs and MCs only forward their information to the AS.

Start

$M_R, M_C, AS\ are\ the\ Mesh\ Router\ , Mesh\ Clients\ and\ Authentication\ Server\ respectively$

$\boldsymbol{Send} M_C(X_{info})$

$\rightarrow M_R, where X_{info}\ includes\ ID_{MC}, ID_{HMR}\ and\ Key\ assigned\ by\ Authentication\ Server$

$\boldsymbol{Pass} M_R\left(M_C(X_{info})\right) \rightarrow AS$

$[xkey, ykey] \leftarrow \boldsymbol{Verify}\left(M_C(X_{info})\right) and\ handle(issues)$

$\boldsymbol{Send} AS[xkey, ykey] \rightarrow M_R$

$\boldsymbol{Pass} M_R \rightarrow M_C$

End

- ***Black Hole Attack***

Lemma: Let a fake node n_i generated by an attacker drop all the information coming from a legitimate node.

Proof: In black hole attack, a fake node is created by the attacker and all the data in the network passing through that is lost. The proposed approach is also secure against the black hole attack. All the MCs have a unique encrypted key and unique id which they share only with the MRs before authentication. The MR further forwards the info received from the

clients along with their own encrypted key and unique id to the AS which then verifies the info and selects any one of them i.e. authentication, no authentication. Any fake node can be easily detected with its fake id.

$\boldsymbol{Start}$

$M_C, F_C, M_R, AS\ are\ the\ Mesh\ Client\ , Fake\ Clients, Mesh\ Router\ and\ Authentication\ Server\ respectively$

$\boldsymbol{Send} M_C(X_{info})$

$\rightarrow M_R, where X_{info}\ includes\ ID_{MC}, ID_{HMR}\ and\ Key\ assigned\ by\ Authentication\ Server$

$\boldsymbol{Pass} M_R\left(M_C(X_{info})\right) \rightarrow AS$

$\boldsymbol{if}(F_C is\ in\ routing\ path);$

$Status \leftarrow AS\_Verify(F_C)$

$\boldsymbol{if} Status\ not\ verified,$

$\boldsymbol{Abort}\ transferring\ data$

$\boldsymbol{End}$

- ***Denial of service attack***

Lemma: Let an attacker hacks the system or a node and makes it unavailable for its users or suspends its tasks.

Proof: An attacker hacks the system or a node and makes it unavailable for its users or suspends its tasks. In the proposed approach the AS keeps track of transferring of data in the network. If any router or client denies any service after authentication then authentication server initiates the process and suspends the node and also informs the other mesh routers about the potential threat.

$\boldsymbol{Start}$

$M_C, F_C, M_R, ASaretheMeshClient\ , FakeClients, MeshRouter\ and\ Authentication\ Server\ respectively$

$\boldsymbol{Send} M_C(X_{info})$

$\rightarrow M_R, where X_{info}\ includes ID_{MC}, ID_{HMR} and\ Key\ assigned\ by\ Authentication\ Server$

$\boldsymbol{Pass} M_R\left(M_C(X_{info})\right) \rightarrow AS$

$\boldsymbol{if}(F_C isdetectedbytheAS);$

$\boldsymbol{Broadcast}\big(F_C(ID)\big), Broadcasts\ information\ to\ all\ M_R's$

$\boldsymbol{End}$

- ***Mutual Authentication***

Lemma: The information is exchanged between MR and MC in a secure manner.

Proof: The proposed methodology adapts the centralized system for authentication and a two key process shared by the central AS. The Authentication process is performed by the central system while MCs forward their info to the MRs and MRs further forward the MCs information along with their own key and ID to central server through internet gateway. So, the authentication process performed by the MRs is discarded in the approach and thus reduces the delay in authentication and increases the security.

- ***Key Management Overhead***

Lemma: The overhead in the system's array of number of Pair-wise master key and master key generated by AS.

Proof: The keys are managed and generated by the central AS. So the overhead in terms of the size of packets in bits is reduced in the network and the MR and MC work in distributed nature for the communication of data.

3.4.2 Performance Evaluation

The purpose of this chapter is to optimize the two parameters i.e. authentication delay and request delay. Further, probabilistic scenarios under different authentication phase i.e. false authentication, no authentication and correct authentication are constructed to prove the legitimacy of the proposed approach.

Authentication Delay is defined as how much time an approach requires for re-authenticating the roaming client.

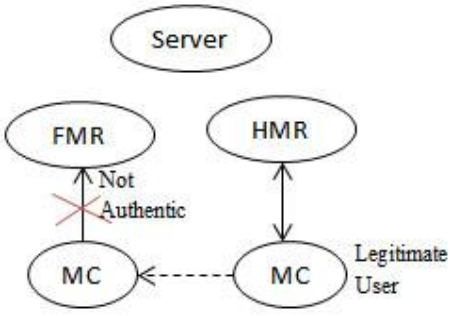


Figure 3.9 False Authentication

Here, a network of 60 mobile clients is constructed having maximum mobility rate of 0-5 m/s. The technique is analyzed over different scenarios. *False authentication* is defined as the situation where roaming client is legitimate but the FMR is not able to authenticate it. Both the approaches are experimented under this scenario i.e. how many times a roaming client is

able to authenticate itself with the FMR. While *No authentication* is demarcated as a situation where an attacker is able to authenticate itself with the FMR and the FMR identifies that it is an attack.

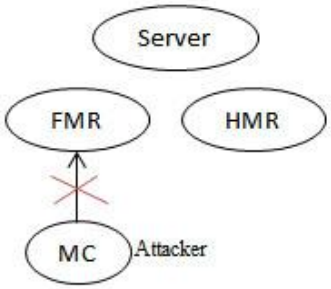


Figure 3.10 No Authentication

Finally *Correct Authentication* is when a legitimate roaming user authenticates itself with the FMR and is able to authenticate itself. Both the approaches are analyzed under these three scenarios (as depicted in Figure 3.9, 3.10 and 3.11) and measured that how many times a roaming client comes under false authentication, no authentication and correct authentication phase. The significance of considering these scenarios is to measure and validate number of times the proposed approach performs better in order to legitimate the nodes in comparison of existing approach.

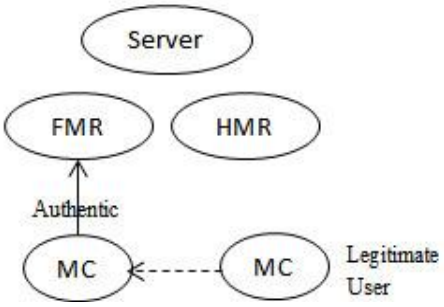


Figure 3.11: Correct Authentication

- ***Authentication Delay***

The reason of outperformance results of proposed approach is that although AS is available at multi-hop distance away from MCs, however, it is faster than the existing technique because MRs need to communicate with each other between the domains to search the keys/tickets from their databases.

The significant search of the keys/ticket of a moving client domain by the FMR may lead to an excessive delay and security threats as compared to direct communication and interaction with the AS in a secure manner. In Figure 3.12, the average authentication delay

for both basic and proposed approach is compared for different mobile clients. It can be clearly seen that the average authentication delay of proposed approach outperforms basic approach which is 0.12 seconds faster than existing approach. As can be seen from the graph, proposed approach gives almost same results for small network sizes but as the number of nodes increase, the communication time for searching and authenticating the roaming client will also increase in case of basic approach while there is no effect of increasing nodes in proposed approach.

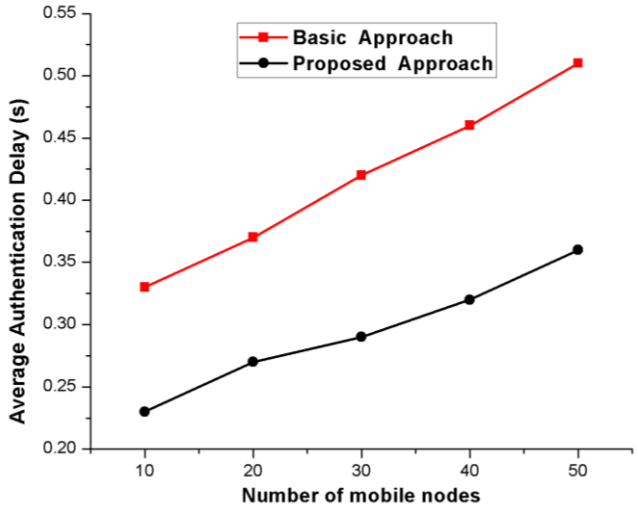


Figure 3.12 Average Authentication Delay

Similarly if the maximum authentication delays in both the cases are considered, then it is concluded that the proposed approach proves to be optimized as compared to existing.

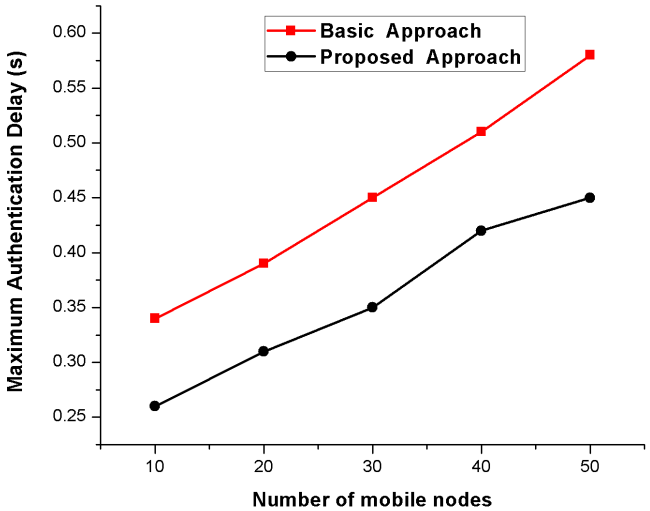


Figure 3.13 Maximum Authentication Delay

From Figure 3.13, it is observed that the maximum delay of a roaming client reaches to 0.42 seconds in the proposed approach as compared to 0.59 seconds in case of basic approach.

- ***Probabilistic Scenarios***

To prove the legitimacy of proposed work in terms of authentication delay, a number of authentication probabilistic scenarios are considered and compared against basic approach.

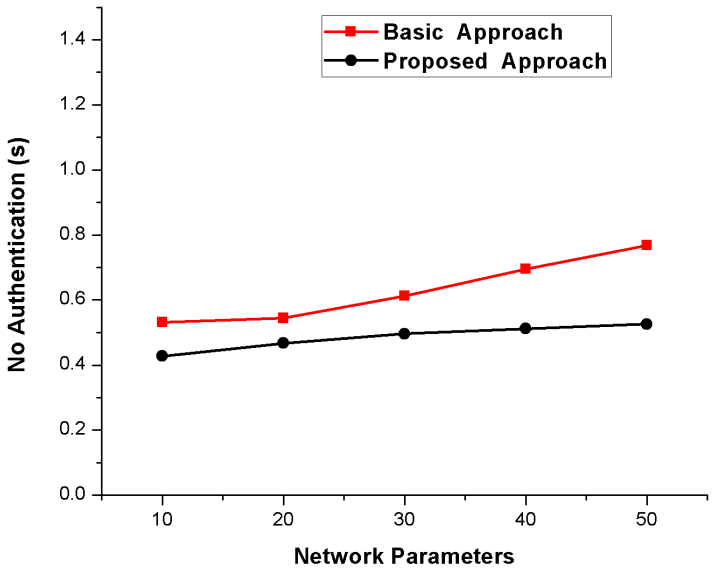


Figure 3.14 No Authentication

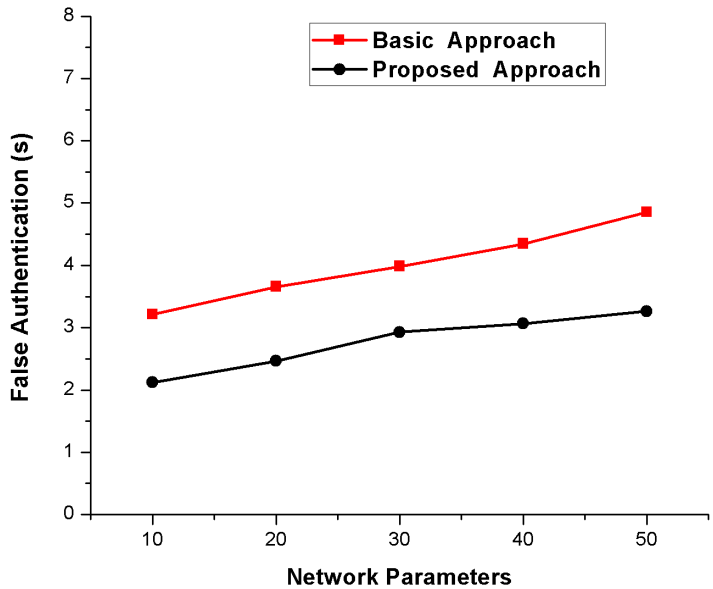


Figure 3.15 False Authentication

During the communication between the MRs, there may be a chance of introduction of various security threats by an intruder to drastically affect or increase the authentication delay. Although, proposed approach uses AS phenomenon which is available at multi-hop distance away from MC, however, it can securely authenticate the roaming clients with less authentication delay in comparison with the basic approach because of their GMK concept as discussed in subsection 3.4.3 of section 3.

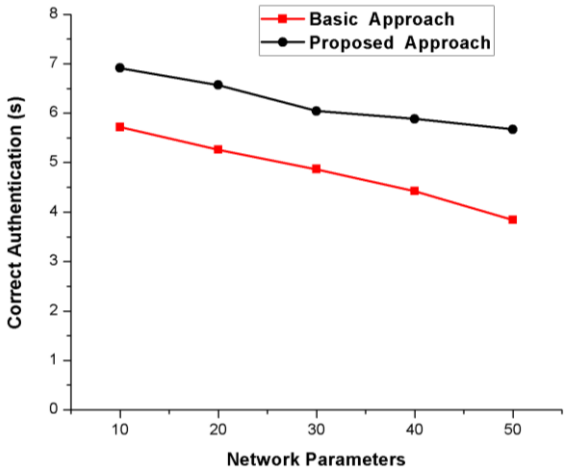


Figure 3.16 Correct Authentication

The probabilistic study of false, no and correct authentication is done over both the approaches having maximum mobility rate of clients. As depicted in Figure 3.14, 3.15 and 3.16 of no, false and correct probability scenarios of both the approaches, it can be seen from the graphs that the number of false and no authentication process increase in case of Xu et al. technique.

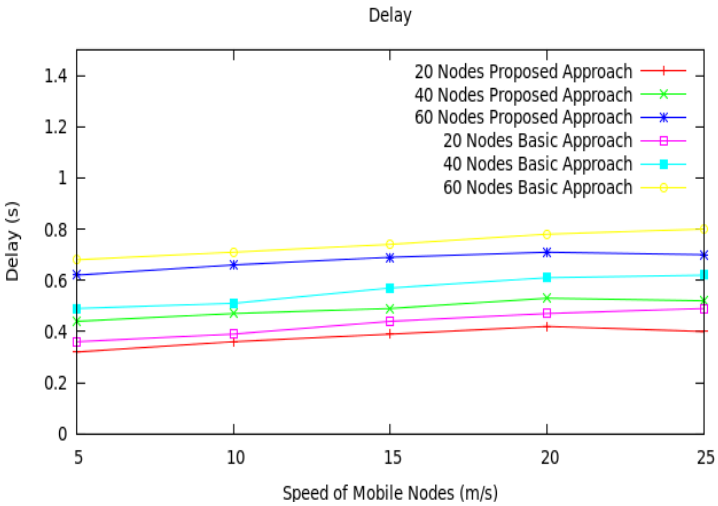


Figure 3.17 Different Network Sizes Delay

The output results are compared with the existing approach considered as basic approach with the proposed mechanism. The reason behind this is that as the tickets and keys are stored in MRs or MCs, attacker may directly attack on any of these and may forge the user privacy while in case of proposed approach, there is no direct contact with AS.

Even if an attacker may launch an attack, only the corresponding zones MC or MR get affected without any privacy loss as earlier there is no information stored on MCs or MRs.

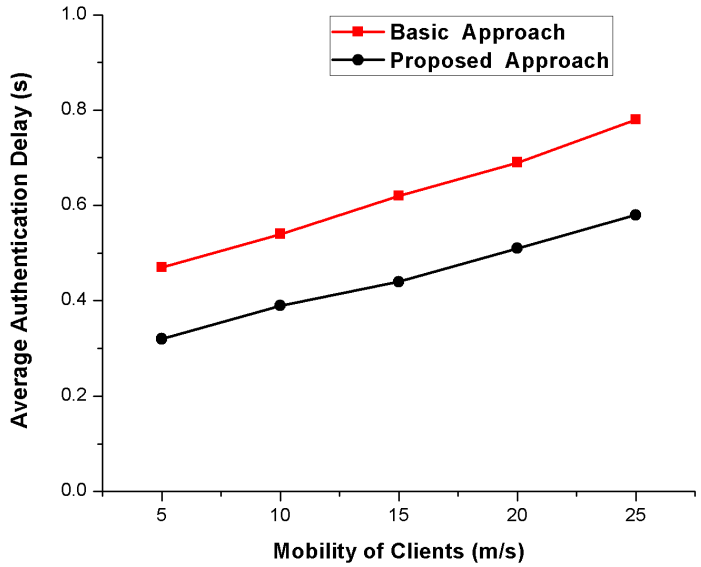


Figure 3.18 Average Delay over clients mobility

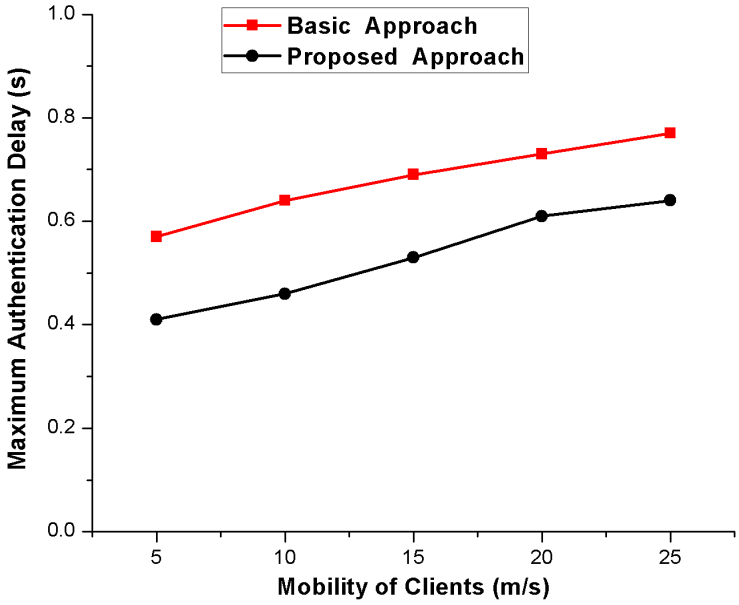


Figure 3.19 Maximum Delay over clients mobility

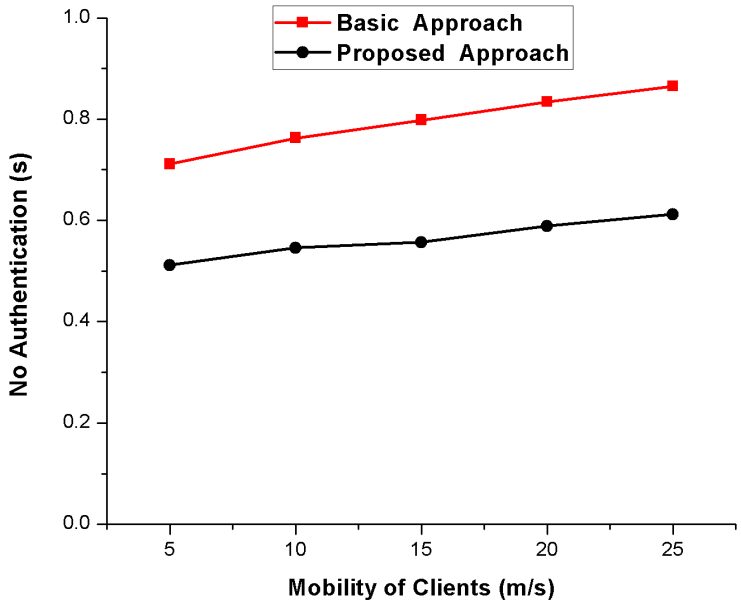


Figure 3.20 No Authentication over clients mobility

- ***Delay***

The request delay or request time is the difference between the time taken by the roaming client to send the request and the time to authenticate it. Figure 3.17 shows the delay of proposed and basic protocol during mobile clients in the network size of 20, 40 and 60 number of nodes.

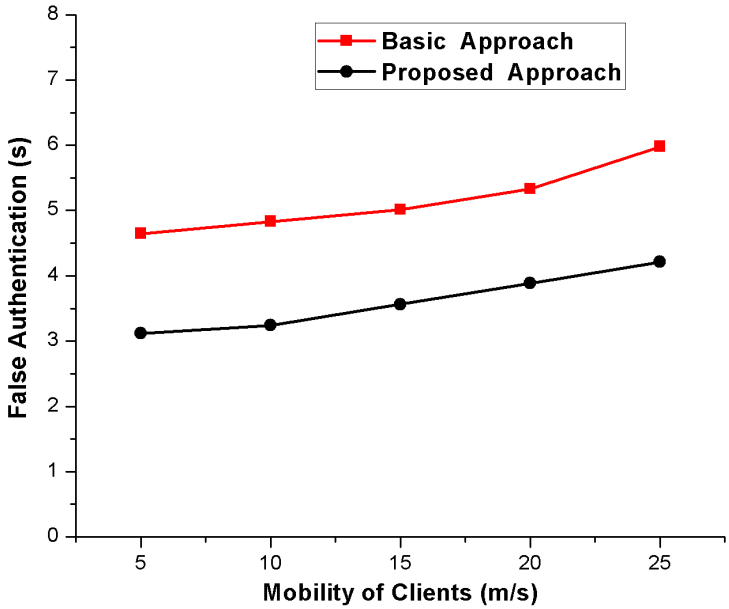


Figure 3.21 False Authentication over clients mobility

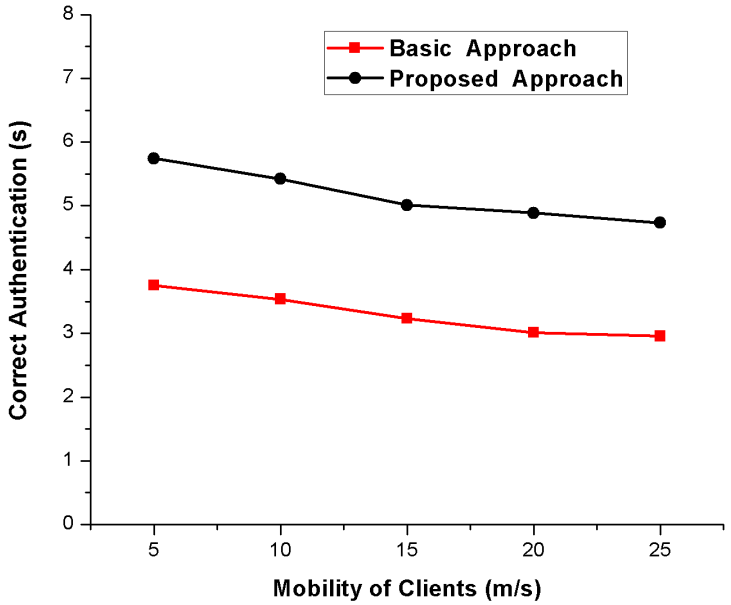


Figure 3.22 Correct Authentication over clients mobility

Moreover, the proposed approach gives better results against basic approach by comparing against probabilistic scenarios of authentication over increasing the mobility speed of mesh clients as depicted in Figure 3.18, 3.19, 3.20, 3.21 and 3.22. The proposed approach will be applicable in smart applications such as internet connectivity of movable devices like mobile phones, personal wearable etc. In general, the mobility of user results in the degradation to the range of HMR which further leads a new connection to another FMR to access the services. The handoff clients will be allowed to access the services only after proving their legitimacy to its FMR.

3.5 HANDOFF SECURITY AGAINST MALICIOUS THREATS ALONG WITH REDUCED AUTHENTICATION DELAY

However, the problem that exists with the previously proposed approach is authentication delay. As the mesh clients need to communicate with the authentication server through various mesh routers to access their tickets this may increase the authentication delay between the server and mesh clients. Therefore, to overcome this issue, the proposed approach is modified where instead of communicating with the authentication server, the mesh clients will directly communicate with the mesh router. The authentication server will distribute the tickets to their intended domains' mesh routers where instead of storing the entire tickets, the routers will store some random tickets distributed by the authentication server.

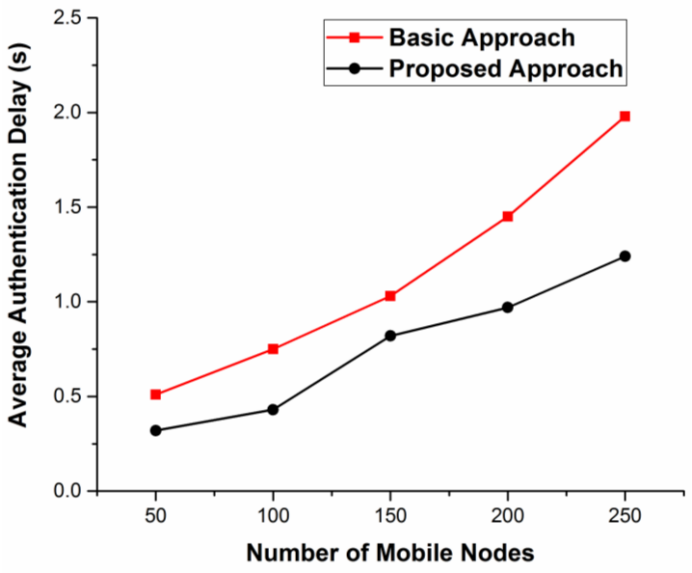


Figure 3.23 Average authentication delay

The depicted Figure 3.25 briefs the extended proposed mechanism of ticket generation and distribution. The proposed approach is distributed during communication which may reduce the extra overhead of key management at server's side.

The technique is analyzed over NS2 simulator under different probabilistic scenarios of authentication delay, request delay as depicted in Figure 3.23, 3.24, 3.26, 3.27 and is legitimated by discussing an empirical study over certain security threats against reported literature.

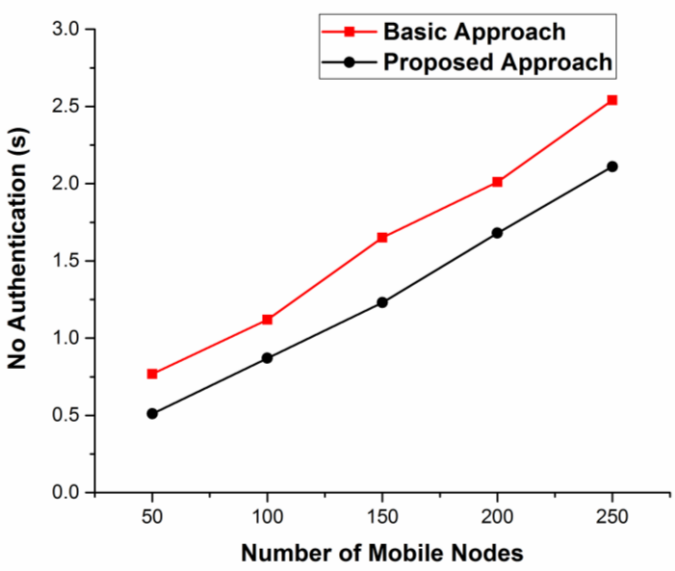


Figure 3.24 No authentication value

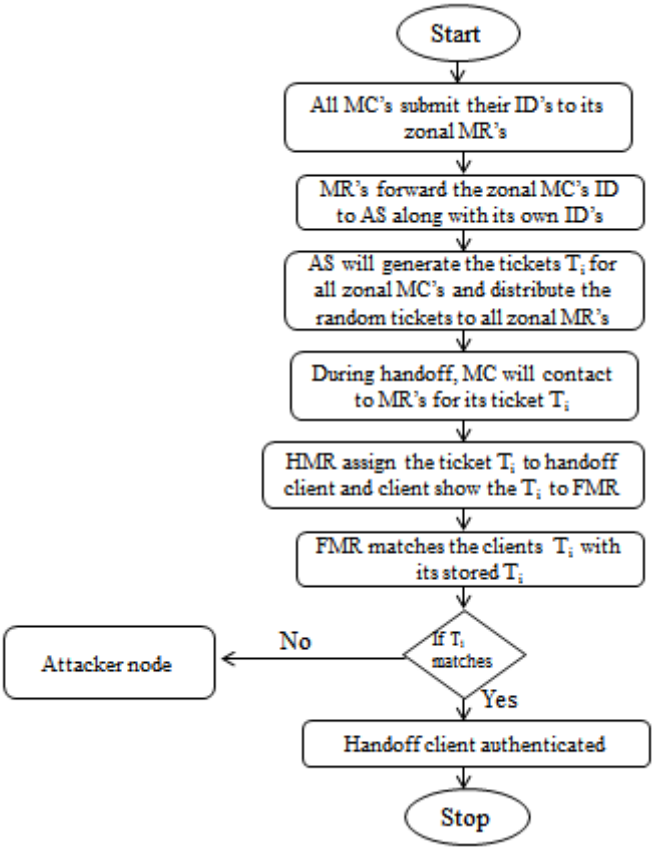


Figure 3.25 Flowchart of the extended secure handoff mechanism

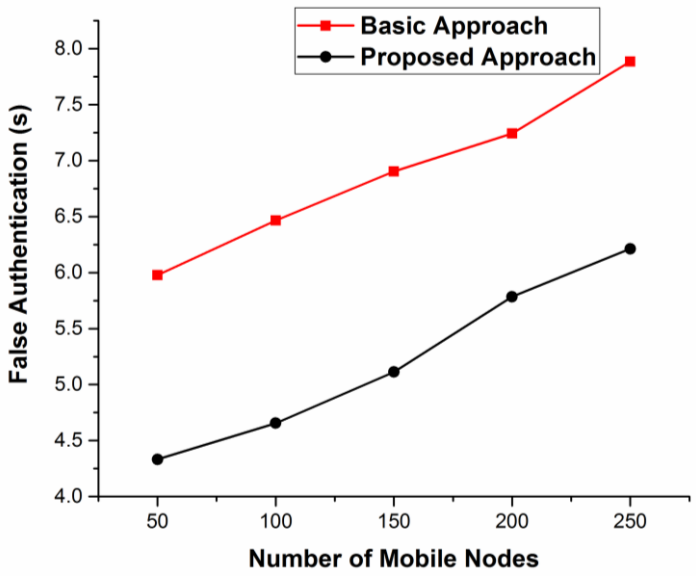


Figure 3.26 False authentication value

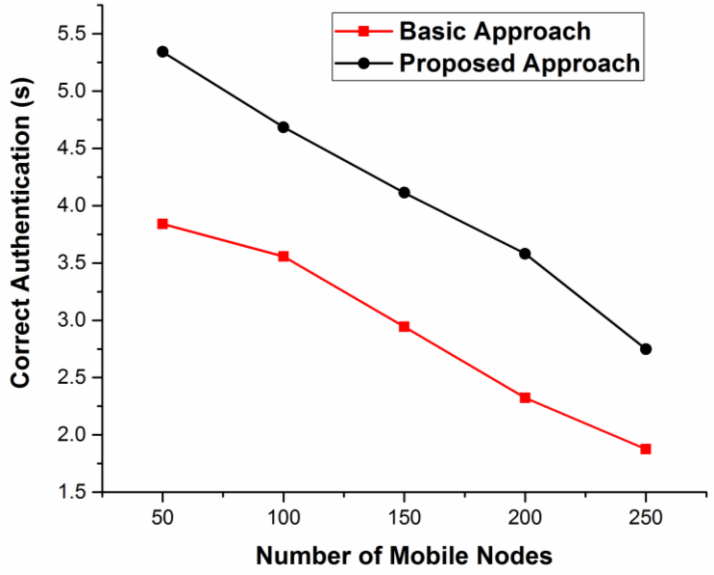


Figure 3.27 Correct authentication value

3.6 CONCLUSION AND FUTURE WORK

In this chapter, a secure handoff mechanism using ticket generation process has been proposed against different probabilistic scenarios of authentication process for wireless mesh environment. An authentication server is responsible for generating and updating the corresponding tickets of mesh clients where they authenticate themselves with the new mesh router by verifying their generated tickets. The proposed technique has significantly resolved the issues of storage overhead and security threats during client's mobility in mesh environments. The simulation over NS2 simulator validates the proposed mechanism and illustrates that the proposed technique's results are better than average authentication delay and maximum authentication parameters. In addition to this, the approach is validated against different probabilistic scenarios of authentication process which has not been yet considered by any other author. In future communication, each mesh client joining the network must be provided with the unique key by the authentication server in order to identify the mesh client for authentication.

CHAPTER 4

END TO END ENCRYPTION BY ALGEBRIC OR/XOR

WMN is deliberated as a key technology due to its self-healing and self-configuring characteristics with the provision of large scale exposure in industrial and academic fields. Security is considered as a vital constraint in WMN owing to its broadcasting and dynamic nature. Due to the nature of WMN where information is being passed over multiple hops, data encryption is taken to be an important parameter. Researchers have proposed various encryption techniques to provide the message security, but the foremost shortcoming in most of the approaches is their processing time. An encryption technique having large encryption/decryption timing increases overhead which may cause copious perilous attacks (i.e. passive eavesdropping etc.). Further an encryption technique with large file size may increase the load on the server during file transmission. In order to overcome these hitches, the chapter proposes an end to end encryption based on algebraic operations i.e. AEHO with reduced processing time where a cipher text is generated using OR/XOR operations. Further, a TPA server is anticipated to provide the authenticity. To establish the legitimacy of the proposed solution, the experimental results are explained in terms of reduced encryption/decryption timing and increased throughput.

4.1 INTRODUCTION

WMN is the most admired proxy technology for a last mile anchor for home, community and proximate networks. It comprises of mesh clients and mesh routers where clients are divided into different zones depending to their signal strength (as depicted in Figure 4.1). In WMN, security [74] can be easily compromised due to its distributed, broadcasting and dynamic nature. If a node either inter-domain or intra-domain wants to send some message to destination node, information is passed among multiple hops. So, to prevent the data exposure at each intermediate node, message must be encrypted by some technique or an ornate encryption technique is requisite to guarantee that even if the message is forged by an attacker then it may not be able to decrypt it anyway. Encryption time is defined as the time required by a client to encrypt a message (to change the plaintext into cipher text).

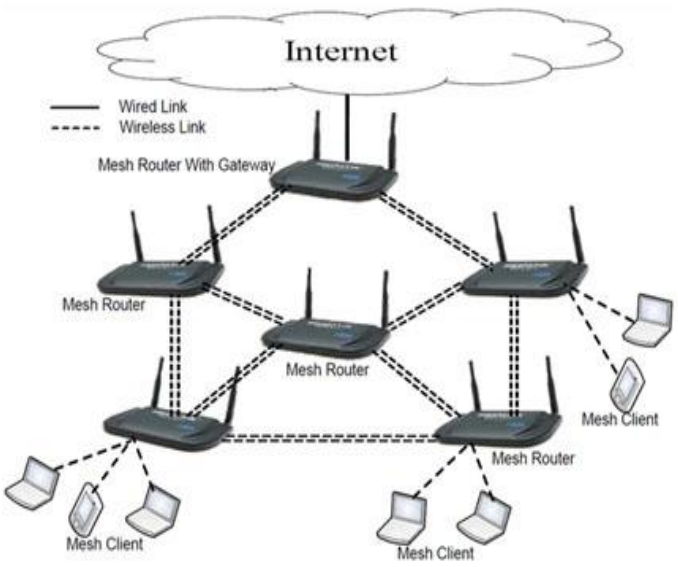


Figure 4.1 Wireless Mesh Network

Researchers have proposed numerous message encryption [75, 76] techniques but the foremost shortcoming in most of the approaches is encryption/decryption timing. With the ease of data privacy, encryption/decryption delay is taken to be an important parameter. A large deferment encryption technique transpires a long delay, resulting passive eavesdrop, security threats [77]. A complex encryption technique may prevent the data from an attacker but may increase the size of file in the network. A technique having large file size may chock the server during transmission. So, there is a need to propose a technique which takes less encryption/decryption time and does not increase the load on server during file transmission from source to destination.

4.2 RELATED WORK

Multilevel [78] and end to end [79] encryptions are the 2 ways to encrypt the data, Soft encryption [80] and hard encryption [81] are the further categories to encrypt the data in WMN. Although numerous folks manipulated that end to end encryption WOULD work in WMN but nobody spoke with a firm that it would work due to the dynamic nature of WMN. Technique discussed by Li Xi [82] and NTRU [83] are multilevel encryptions where data is verified at each node and forwarded to next node after judging its integrity. Li Xi encrypts the client data using soft encryption in which author is encrypting the parameter of client MAC address using PMK which is generated by AS based on MAC address of access point from where the user authenticates itself for first time in WMN. The technique proposed by the author is infeasible because every time when a new client joins WMN then the client simply

connects to the access point based on which message can be easily decomposed by black nodes. Further it is easy to decrypt as there is no encryption algorithm applied other than the MAC address of access point only.

On the other hand NTRU is a strong encryption technique which prevents the user data from an attacker and may not be easily decrypted. In this the message is represented in the form of polynomial ring based cryptosystem. But the major drawback of this approach is that it may increase the server load during transmission. The encrypted file size is very large using NTRU and may slow down the server during file transfer to destination node. Further Yahui Li [84] proposed an ID based broadcast encryption scheme where all the mesh routers which are selected to forward the data packets take part in trust domain and broadcast their transmission key to adopt the cryptographic protection on data packets.

The drawback with this approach is that all the intermediate mesh routers between source and destination will forward the data packet to next node after verifying with sender transmission key which means packet encryption or decryption at each node may increase the risk of different security threats i.e. DoS, passive eavesdrop and increase the encryption/decryption time. Although the researchers are able to resolve some limitations but major drawbacks in these approaches are that the data is exposed unblemished at each node and increases the processing time of encryption/decryption. Now, to remove the above limitations, several researchers felt that end to end encryption SHOULD work well in WMN because of its dynamic nature. Edward L. Witzke [85] gave some experiments to encrypt the data through IP Sec but the approach was not able to satisfy the challenges of RF shadow and shifting paths.

So, if existing techniques are considered then to optimize one parameter other parameters are affected adversely. Even though Li Xi encryption approach does not increase the load on server but it can be easily decrypted by applying some permutation and combination on the other hand NTRU approach resolves the Li Xi limitation but suffers from large size, further Yahui increases the encryption/ decryption time. Therefore, there is a need to propose an end to end technique which is resilient against these parameters. A brief summary of previous approaches is shown in Table 4.1. In addition to that, in order to overcome the listed drawbacks, a new desired encryption technique is to be deliberated by using some of the existing methodologies i.e. homomorphic encryption [86], identity based cryptosystem [87] and quantum cryptosystem [88]. Homomorphic encryption is a direct arithmetic operation performed on a plaintext. It encrypts the plaintext by applying some algebraic operations, for

example addition, subtraction and multiplication and outputs the results by decrypting the operations in reverse order.

4.2.1 Chapter Contribution

This chapter proposes an end to end encryption that has the advantage of not decrypting the data at each node. End to end encryption not only lessens processing overhead but also eradicates exposing the data unblemished at intermediate nodes. The proposed technique takes less encryption/decryption time with reduced file size and increased throughput. The approach is based upon two different techniques, i.e. polynomial ring cryptosystem (NTRU) and homomorphic encryption. NTRU algorithm is used to generate the private keys in order to send the data and to produce the cipher text in order to strengthen the security and lessen the possible attacks. While Homomorphic Encryption is used to further remove the limitation of NTRU i.e. reduce the file size by eliminating the white spaces from the file.

Table 4.1: Previous Approaches Comparison

Author	**Intermediate/ end-to-end encryption**	**Type**	**Technique used**	**Limitation**
Li et al.	Multilevel Encryption	Soft encryption	Encrypt AP MAC address through PMK	Decryption is easy
Jeffrey et al.		Hard encryption	Polynomial based ring cryptosystem	Increase server load, decrease throughput
Yahui et al.		Hard encryption	ID based cryptosystem	Increased processing time, authentication delay
Edward et al.	End to End encryption	Hard encryption	IP Sec function	Security threats

The structure of the chapter is organized as follows. In section 2, the taxonomy and background knowledge of the entire chapter is discussed including polynomial based ring cryptosystem, homomorphic encryption, binary operations and network architecture. Section 3 deliberates the proposed technique i.e. AEHO. Further, the performance evaluation of proposed technique in terms of encryption/decryption time and throughput is debated in section 4 and an empirical study is given in this section only. Finally section 5 concludes the chapter.

4.3 TAXONOMY

This section discusses the background knowledge, terms, concepts and additional assumptions of this chapter.

- ***Polynomial Ring Cryptosystem*** **(NRTU)**

In the designing of proposed scheme, a polynomial based ring concept i.e. NTRU algorithm [89] is being utilized. The network is divided into a number of domains. Each domain has fixed parametric values in order to encrypt the plaintext message. The message M is coded in binary and represented by polynomial p as:

$P = (Z[M])/(M^N - 1)$, Where, z is the integer and N is the number of degree.

Since NTRU eliminates the degree of data exposure at each node and security threats but the major drawback of this approach is that it may increase the file size after encryption because text may include multiple white spaces which increases the file size. The proposed approach removes this drawback by eliminating the white spaces through homomorphic operation and is able to reduce the file size during transmission.

- ***Homomorphic Encryption***

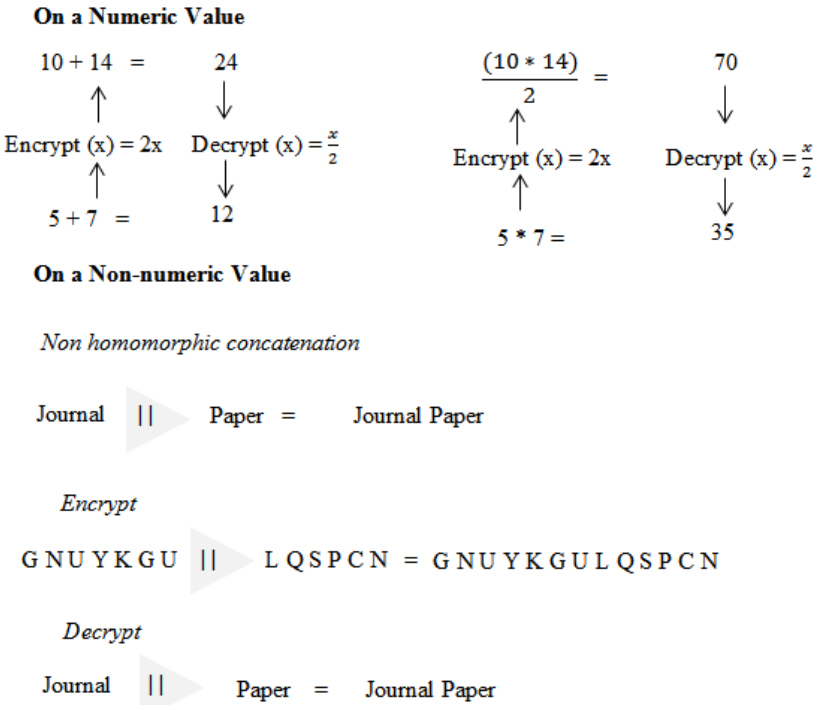


Figure 4.2 Homomorphic Encryption

Homomorphic encryption [90, 91] is defined as into and onto mapping of a specific algebraic operation performed on plaintext equivalent to another algebraic operation performed on cipher text. It can be applied on a numeric value or non-numeric value. The example of homomorphic encryption is shown in Figure 4.2. Homomorphic encryption is the one where algebraic operations are involved consistently between plaintext and cipher text. Operations applied on cipher text will change the plaintext accordingly. Let E is the encryption operation and D is the decryption operation performed over two integers x and y. The operations of the corresponding plaintext and cipher text will be shown as below:

E (algebraic operation (E(X) + E(Y)) = E (E(X+Y))

*E (algebraic operation (E(X)*E(Y)) = E (E(X*Y))*

There exist three types of homomorphic encryptions. Partial homomorphic encryption which accomplishes one operation, i.e. multiplication or addition but not both at the same time on encrypted data. Somewhat homomorphic encryption is the one which executes more than one operation, but suppers only a limited number of addition and multiplication operations. Fully homomorphic encryption sustains both addition and multiplication by computing any function.

Binary Operations used in Homomorphic Encryption

Addition operation is used to add two integer functions x and y of length l bit. Each integer's function is firstly converted in binary form and then addition operation is performed bit by bit.

$$X = x_1, X_2, X_3 \dots \dots . X_l$$

$$Y = Y_1, Y_2, Y_3 \dots \dots . Y_l$$

$$X + Y = (X_1 + Y_1 + C_{(l-1)}), (X_2 + Y_2 + C_{(l-2)}) \dots \dots . . (X_l + Y_l + C_0$$

Multiplication operation is used to multiply two integer functions x and y of length l bit. Each integer's function is added after being converted into binary form and then multiplication operation is performed using addition.

$$X = X_1, X_2, X_3 \dots \dots . X_l$$

$$Y = Y_1, Y_2, Y_3 \dots \dots . Y_l$$

$$X * Y = (X_1 * Y_1 * C_{(l-1)}), (X_2 * Y_2 * C_{(l-2)}) \dots \dots . . (X_l * Y_l * C_0)$$

In this chapter OR and XOR operations are used in order to brace the encryption process. OR operation performs addition during the process. Let integers x, y and z of length l bit, where $X = xl, \dots, x2, x1$, $Y = yl, \dots . . , y2, y1$ and $Z = zl, \dots . , z2, z1$ perform OR operation.

Every bit of x, y and z is added along with carrying on the previous stage. XOR is a universal operation. The output will be false in case of similar bits else true.

- ***Network Architecture***

In proposed model, a hierarchical architecture of WMN is considered which consists of three layers. The top most layer is of mesh servers which supply the internet service connectivity to stratum layer and TPA server which verifies the authenticity of the client nodes. The second layer consists of domain servers and mesh routers which forward the traffic to the main server and the third layer comprises of mesh clients which utilize the internet services. As shown in Figure 4.3, the network N is divided into different domains. Each domain has its own mesh server and mesh client. The purpose of dividing the network N into number of domains is to provide the services to the clients in continuous form or to reduce the load and waiting time of the clients in the network.

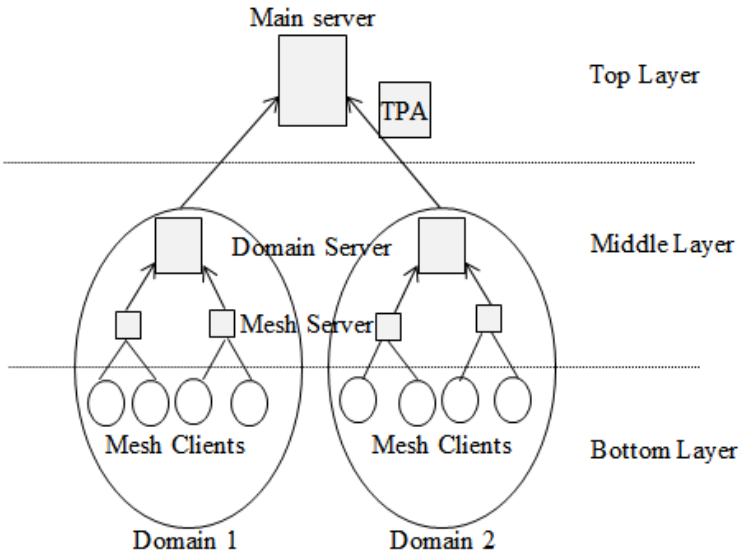


Figure 4.3 Network Architecture Model

4.4 PROPOSED APPROACH

Table 4.2: Abbreviations Meaning

Abbreviations	Meaning
TPA	Trusted Party Authority
Sr	Source
DS/d_i	Domain Server
C_i, C_j	Clients
$Auth_{rrqt}$	Authentication Request
Pu	Public keys

In this section, the proposed scheme is explained by dividing it into different number of phases. The two phases of AEHO are Authentication Verification and Encryption phase. Each phase clarifies the stepwise communication of proposed work. At last the entire working of communication is elucidated in phase three. The abbreviations used throughout the chapter are depicted in Table 4.2.

4.4.1 Authentication Verification Phase

The purpose of this phase is to identify the legitimacy of the client nodes. TPA server is responsible to check the authenticity of each client for the first time. Whenever a client makes a request of data encryption to the domain server, the primary task of the server is to check the legitimacy of the node. The following steps describe the details of authentication verification.

Step 1: Whenever a source client 'Sr' makes a communication request to its Domain Server (DS), the primary task of the domain server is to check the authenticity of the client node. For this purpose, DS will receive the source request and pass it to TPA server.

Step 2: After getting the client's request, TPA will send its address to DS which will forward the TPA's address to the client. Now, the direct communication starts between TPA and the client.

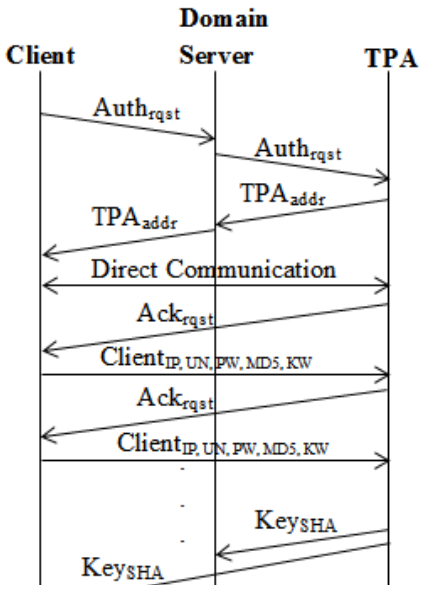


Figure 4.4 Authentication Verification Steps

Step 3: TPA server sends acknowledgement at least 10 times for checking the authenticity of the client (if TPA gets 5 or 6 replies as an average communication out of 10 that means it is authentic client otherwise not). In order to validate the legitimate client, the request has been sent 5 to 6 times to check whether the client is requesting the same message or not. If it is

legitimate client then every time the keyword=yes will be reach to the TPA server and if it is malicious client then each time the intruder may send different keywords to get the authentication**.** The Keyword=yes is a message that is sent to the remaining nodes to identify the legitimacy of the node.

Step 4: Client will respond to each request of TPA by sending its IP address, user name, password, MD5 (MAC address) and keyword (yes).

Step 5: As the client's response matches with the TPA's format, it will send SHA key as a response to both client and DS individually so that whenever the client presses encrypt button, then message with the SHA key will be sent to the domain server to cross verify the authenticity of the client. The steps discussed above are shown in Figure 4.4. An algorithm for the authentication verification process is described in Table 4.3. Now, after verifying the authenticity of the client, encryption process starts. The next phase describes the encryption steps using homomorphic operation.

4.4.2 Encryption Phase

The plaintext message M will be converted into cipher text using the steps depicted in Figure 4.5. In this, initially the message is separated into an array and typecast into decimal form in order to apply the NTRU algorithm which generates the private key 'pr' through which message will be passed from source 'Sr' to destination and OR/XOR operations are applied to cipher text the message M.

The complete process for encryption/decryption is depicted in Table 4.4 which describes how a plaintext message M is converted into cipher text and the message is transmitted to the destination node by encryption with 'pr' key and whereas destination node decrypts the message further to get the plaintext. Both clients will generate the candidate key such as public and private keys and exchange the public keys in order to generate their private keys using the NTRU algorithm. The purpose of NTRU algorithm is to generate the private keys that is used for cipher text communication and acts as a second bit during OR/XOR operation.

4.4.3 Working of above Discussed Approach

The complete working of the proposed solution is described in a number of steps.

Step 1: Whenever a client ci wants to communicate with a client cj, ci will contact to its domain server di which will further contact with the main and the TPA servers. The purpose of main server is to randomly generate two public keys and distribute them to individual

clients while the purpose of TPA server is to prove the authenticity of clients the through authentication verification phase.

Step 2: Both clients will generate the candidate key such as public and private keys and exchange public keys in order to generate their private keys using the NTRU algorithm. The purpose of NTRU algorithm is to generate the private keys and one of the Pr key is used for cipher text communication and acts as a second bit during OR/XOR operation.

Step 3: Client ci will cipher text the message by following the steps as depicted in Figure 4.5. It will send the cipher text message by encrypting it with its pr key. Destination client cj will decrypt the message M using its pr key by following the process of Figure 4.5 in reverse order.

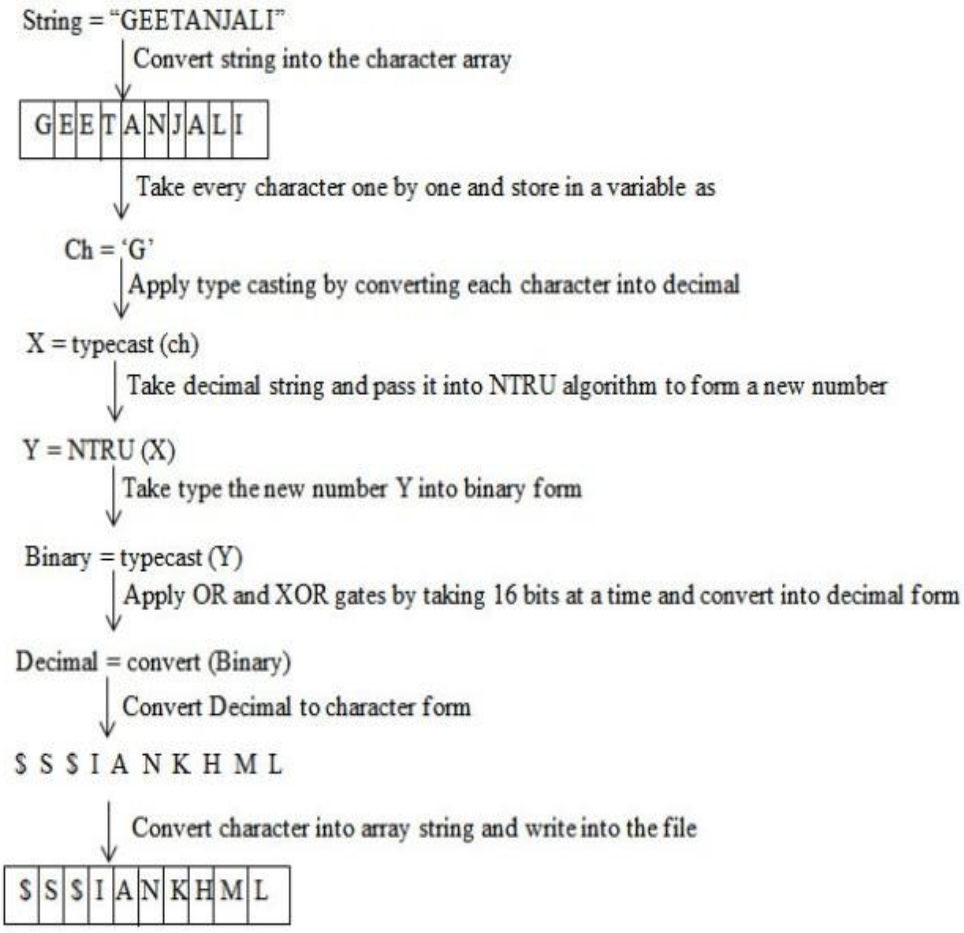


Figure 4.5 Secure Communication Steps

4.4.4 OR/XOR Operation

This section describes the OR/XOR process in detail. The private key 'pr' acts as a second bit operator in order to perform the operation which will be selected by the server. The cipher

text file generated in phase 1 is converted into binary form to perform the algebraic operations.

Table 4.3: Algorithm of Authentication Verification

Algorithm 1:Authentication Verification
1.Client c_i will send a request to its domain server di. 2.After getting the TAP address, d_i forward the TAP address to clientc_i.

//Direct communication starts between $c_i$and TAP
For (i=1 to 10)
1. TAP send acknowledge ack to c_i.
2. $c_i$will respond by sending its username, IP address, password, MD5(MAC), keyword(yes) to TAP
3. **If** (Response(c_i)>4) **then**
c_i is authentic and TAP send SHA key to c_i as well as to Domain Server d_i
End If
Else
c_i is not authentic
End Else
//whenever $c_i$contact to d_i for communication
4. d_i will verify the SHA key of its own with client SHA
If (SHA_{d_i} = =SHA_{c_i}) **then**
Authentication successful and allow encryption
End If
Else
Not Authentic
End Else
End For

Table 4.4: Homomorphic Encryption Algorithm

Algorithm 2: Homomorphic Encryption Algorithm
1. The main server will randomly generate two Pu keys and distribute to the corresponding clients. 2. On source client following homomorphic encryption algorithm will perform.
Input // Both ak and bk are the values of the selected domains Input of A; ak and Input of B ;bk Output: Lk+1

Begin
1. Ck1+1←Generate Candidate key (Lk) // Both A and B calculate their private keys through public keys generated by the main server.
For (A+1) do // loop continue till the content of the file length
2. A (plaintext) // **for encryption process**
3. W1←count(L) // *extract the string via tokenization from line*
4. T←ak and bk *// t is the cipher text*
5. α←Epk (cipher text) // *conversion of cipher text via OR and XOR operations*
6. Send to B (α) // *cipher text file send to the B*

7. B (Cipher text) // **for decryption process**
8. Wpk ←count(Dpr)
9. T←ck3(A) // *compute pr key via A pu key*
10. B←Epk(pass cipher text file)
11. T←homo comparison // *apply tokenization on file that deduct private key from content of the file*
12. Send To A(T)
13. (A)
14. R←Dsk(T) // *apply operations on content*
15. File decrypt successfully
16. End if
17. Else
18. file cannot be decrypted
End for
End

Initially, the whole file is divided into 16 bits binary form and again 16 bits are divided into 8-8 bits. The purpose of dividing 16 bits into 8-8 is to make the decryption operation complex. First 8 bits will perform OR operation using fixed 8 bit pr key generated by NTRU algorithm. The answer is then XOR with 8 bits pr key and finally the result is converted into decimal form. The operation is explained in Table 4.5.

Table 4.5: OR/XOR Operation

1. Let plaintext P is	A
2. The ASCII value of P	65
3. Let pr key generated by NTRU is	10
4. Decimal number generated after addition is	75 (65+10)
5. Let Binary form of 75 is	1101(75 in binary form)
6. A constant no. selected by the server is	1011 (constant number)
7. Number generated after OR operation is	1111(after OR operation)
8. Then XOR with constant number is	1011(constant number)
9. XOR operation result is	1010(after XOR operation)
10. Covert cipher text generated into decimal	(89)8 (cipher text)

4.5 PERFORMANCE ANALYSIS

To prove the authenticity of proposed work, the technique is analyzed using java and is compared with existing approaches through performance metrics including authentication delay, encryption/ decryption time and throughput. Authentication Delay is defined as how much time an algorithm takes to check the authenticity of the client. Encryption Time is the time taken to convert a plaintext into corresponding cipher text. Decryption Time is the time taken to convert the cipher text message into plain text and finally the Throughput is the total

time taken to transfer the number of packets to destination node. The corresponding formulas of all the mentioned parameters are defined as Encryption Time=$\sum_{i=1}^{n} \frac{\boldsymbol{Encryption\ Time}}{\boldsymbol{file\ size * number\ of\ bytes\ per\ KB}}$, Decryption Time=$\sum_{i=1}^{n} \frac{\boldsymbol{Decryption\ Time}}{\boldsymbol{file\ size * number\ of\ bytes\ per\ KB}}$ and throughput is defined in terms of file transmitted (in terms of bytes) in seconds. Let us discuss each parameter in detail with their graphical representation. The defined parameters are evaluated against Yahui for encryption/decryption timing and throughput against Jaffrey technique.

4.5.1 Encryption/Decryption Time

In order to strengthen the proposed technique, individual encryption/decryption time of different file sizes is calculated. Encryption time is evaluated as the time required converting a plain text into corresponding cipher text.

Now, it can be scrutinized from Figure 4.6 and 4.7 that encryption timing ratio of proposed approach is less as compared to Yahui. The below Figure 4.6 and 4.7 show the corresponding encryption time of both the approaches on small and large file sizes.

- ***Analysis of Encryption/Decryption***

This parameter is analyzed over Yahui technique where all the intermediate mesh routers between source and destination forward the data packets after verifying them with sender transmission key.

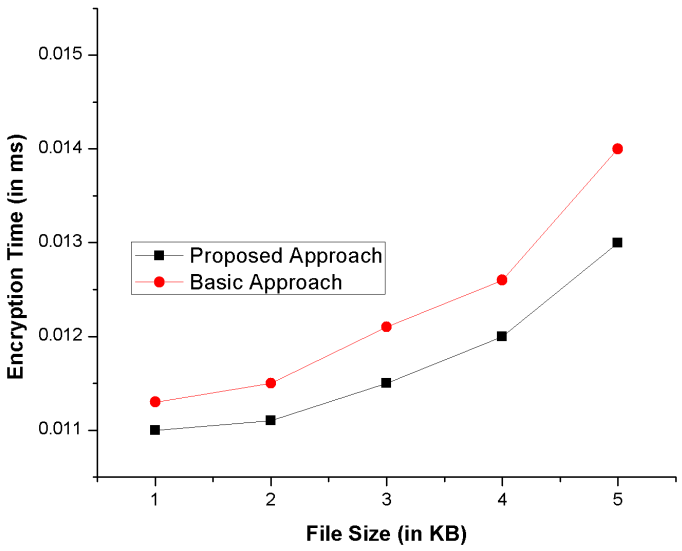


Figure 4.6 Encryption Time (Over Small File Sizes)

The encryption/decryption process is repeated at each step while in proposed approach there exists an end to end encryption which takes less processing time and improves security. Further, Figure 4.8 shows the decryption timing ratio of different file sizes over both the approaches. In proposed approach the time required for decryption is always less than encryption because cipher text needs to just follow the reverse process of encryption in order to get the plain text and there is no need to convert the strings into character and write each character in an array which is the main cause of delay.

4.5.2 Throughput

Figure 4.9 shows the throughput graph in terms of file transmission in seconds. The proposed approach outperforms basic technique because of transmitting bytes in seconds.

- *Analysis of Throughput*

The file size of proposed approach is reduced to some extent by eliminating the white spaces which are the main cause of throughput (in terms of bytes transfer in seconds) decrement. In our case as compared to existing approach, the file transmitting time is reduced in seconds.

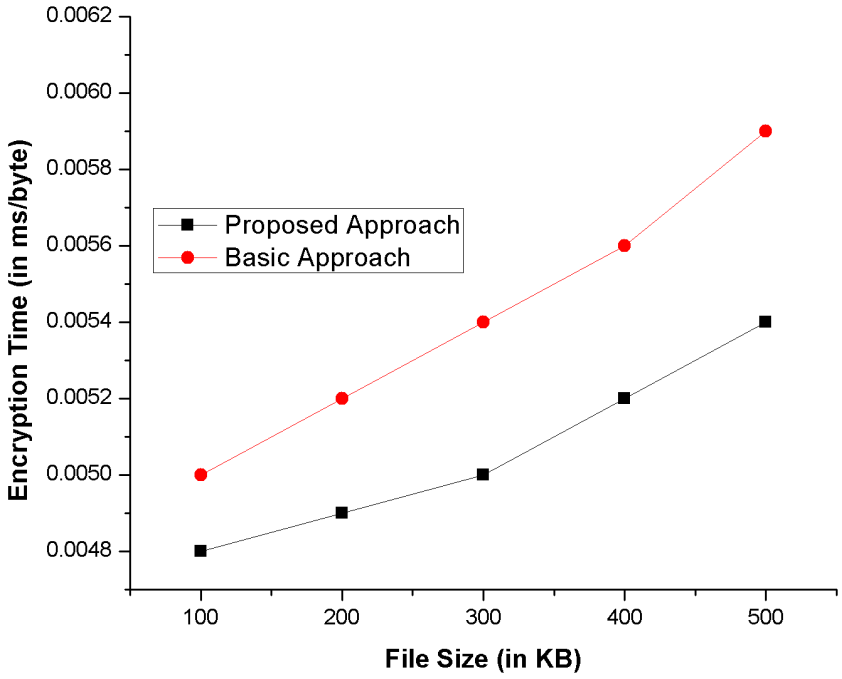


Figure 4.7 Encryption Time (Over Large File Sizes)

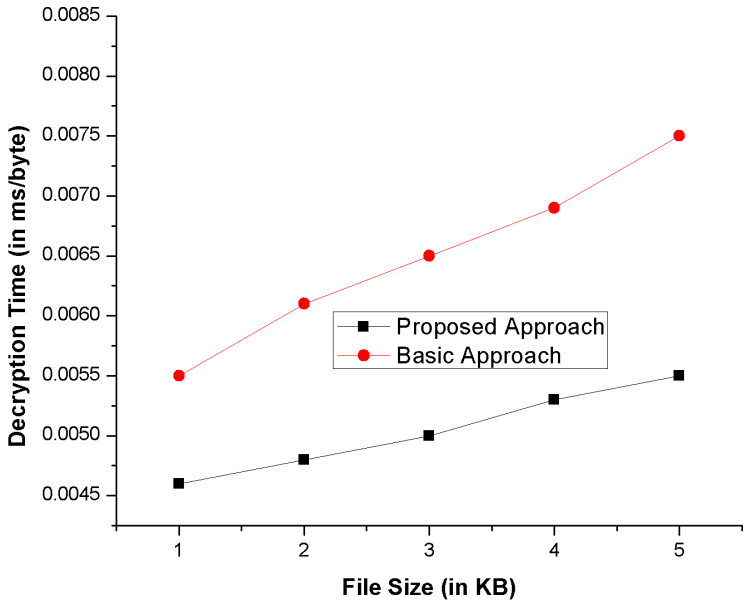


Figure 4.8 Decryption Time (Over Small File Sizes)

4.5.3 Empirical Proofs

- ***Authentication***

All the Mesh Clients authenticate them with their domain server through TPA before communicating with other nodes. To reduce the authentication latency, there exists a direct communication between the TPA and the clients. Client authentication is done by getting a key SHA from the TPA.

The Authenticity of client nodes before communication may reduce the issues of certain security threats, i.e. passive eavesdrop, traffic analysis.

Start

M_C, D_S, TPA *are the mesh clients, domain servers and Trusted Party Authority server respectively.*

Send M_C $(Xrequest \rightarrow D_S, where\ X\ request\ includes\ Authentication\ request)$

Pass $D_S(M_C(Xrequest)) \rightarrow TPA$

Send $TPA \rightarrow M_C(D_S(TPA_{addr}))$

Send M_C $(IP, UN, PW, MD5, KW) \rightarrow TPA$

$TPA \rightarrow M_C(D_S(Key_{SHA}))$

End

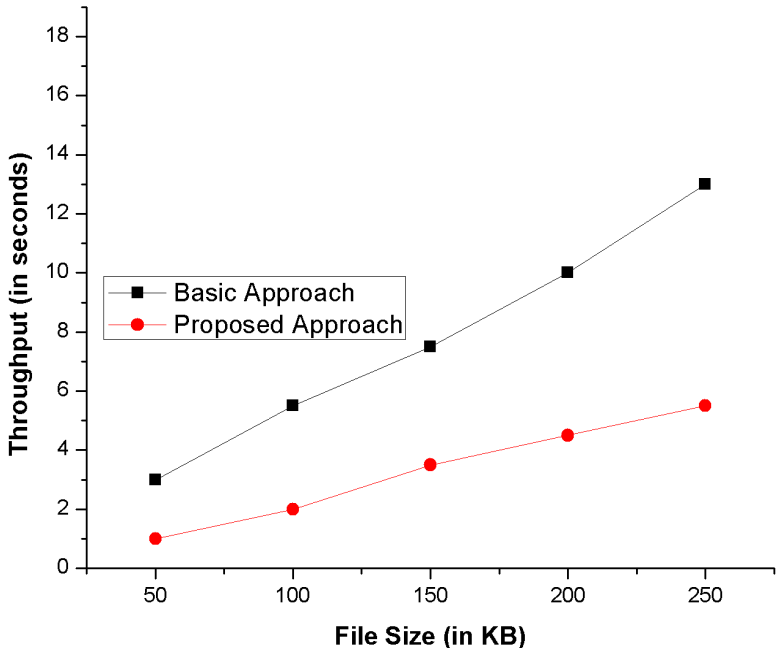


Figure 4.9 Throughput

- ***Processing Delay***

End to End encryption reduces the overall encryption/decryption process between source and destination. The proposed technique uses end to end encryption process where client node encrypts the message through algebraic operations by passing it through multiple nodes. The data will be decrypted only after reaching at destination node. There will be no multiple encryption decryption process at each node which is the main cause of processing delay as well as security threats.

- ***Attack Resistant***

The proposed technique is encrypted through OR/XOR operations. The second evaluating key for both OR and XOR operations will be selected by server only and is difficult to guess.

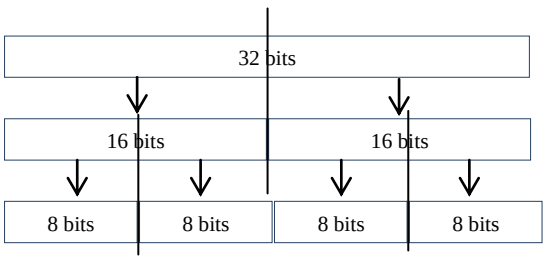


Figure 4.10 Binary Files Separation Process

Further even if the message is forged by an attacker then it will not be possible to decrypt it because it will be very difficult to guess the pairs of OR/XOR operations (i.e. in our case, firstly the file is broken into 16*16 then into 8*8 bits) (as depicted in Figure 4.10). Finally as there is no spacing in the encrypted file so it will be difficult to get the original text.

4.5 CONCLUSION AND FUTURE WORK

In this chapter, an algebraic based encryption technique is proposed which ensures the security with reduced encryption/decryption time, processing delay and increased throughput. The key idea of the proposed technique is to generate the cipher text message using OR/XOR operations and transmit it with the private key generated by NTRU algorithm. Compared with existing approaches, the proposed technique reduces the processing delay and encryption/decryption time for different file sizes. Further, the proposed technique is compared in terms of throughput. According to the experimental results, our technique outperforms better in terms of throughput and processing delay with an efficient level of security.

CHAPTER 5

WEIGHT TRUSTED ROUTING MECHANISM FOR HIERARCHICAL MESH ENVIRONMENTS

In this chapter, we have proposed a technique to detect and eliminate the malicious/misbehaving nodes involved during routing path formation in hierarchical mesh environments. In this, the Dijkstra's shortest path routing algorithm is used whose weights are deliberated using certain parameters (i.e. node distance, node's previous interactions, packet loss percentage and trust value of each node) for providing the security against routing attacks. The malicious nodes involved during route discovery process are eliminated by calculating the trust of each node using SITO. Here, we have discussed the network performance trade-off caused by secure path formation by conventional methods and have proposed a WTR mechanism for eliminating these issues (packet-loss ratio, end-to-end delay and route discovery delay). We have numerically simulated and compared the network metrics for both conventional and proposed approaches. Moreover, the proposed technique is validated (through an adversary model) by discussing an empirical study over routing attacks.

5.1 INTRODUCTION

WMN is considered as a next generation key promising technology that are attractive in the areas where infrastructure is either existing or absurdly expensive because of multi-hop, auto-configuring and dynamic features. The multi-hop characteristic of WMN extends the network scalability where numbers of nodes communicate with each other via multiple mesh routers to access or forward their data packets. The significant factor that impacts the WMN performance is the nature of fundamental routing protocols used for promoting the data packets. Presence of any malicious or misbehaving node within the routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network. The conventional routing protocols operate smoothly with an assumption that all intermediate nodes are trusted and cooperative with each other however, the dynamic and multi-hop characteristic of mesh environment invites number of internal vulnerabilities to come where attackers may launch several types of attacks either by compromising the legitimate routing nodes or by disrupting the transmitted data packets.

Therefore, one of the norm approaches to counter such attacks is secure routing. The existing routing algorithms for Mobile Ad hoc Networks (MANETs) [91] and Wireless Sensor Networks (WSNs) [92] do not perform well in mesh environments because of its unique requirements and characteristics. Further existing secure routing protocols i.e. Secure Ad hoc On-Demand Distance Vector (SAODV) [93], Security Enhanced Ad hoc On-Demand Distance Vector (SEAODV) [94], Ad hoc On-Demand Distance Vector (AODV) [95] that are basically espouse for homogenous systems does not adopt well in heterogeneous mesh environment because of its multi-hop and dynamic nature and cause copious perilous threats with a decrease in network performance metrics (i.e. end-to-end delay cost and packet delivery ratio). These protocols are vulnerable to a variety of routing threats i.e. worm hole, grey hole, jellyfish and black hole attacks [96, 97] because of an assumption of non-hostile environment where nodes are cooperative and non-malicious. However to prevent from these loop holes, an efficient secure routing protocol is needed which can successfully transmit the data packets to its intended destination node.

In this chapter, we have proposed a WTR mechanism for hierarchical mesh networks that ensures a secure path formation by detecting and eliminating the malicious nodes using trusted weight computation through SITO [117]. The SITO works on the social references of individuals where the nodes are interacting with each other to know the behavior of their neighbors. The node having low packet delivery rate would be considered as malicious node. The proposed WTR mechanism enhances the network metrics by reducing additional cryptographic operations needed to ensure the security during transmission process. Further, the proposed protocol is analyzed against reported routing protocol i.e. Secure Routing Mechanism (SRM) which overcomes routing attacks (i.e. black hole and worm hole attacks) by modifying the basic AODV protocol.

The technical contribution of this chapter is as follows:

- Dijkstra's routing algorithm is used to find the shortest path between source and destination and also reduces the overall complexity of the algorithm against reported SRM protocol.
- The weights in Dijkstra's algorithm among the nodes are computed through various factors i.e. node distance, trust of a node, residual energy and packet loss.

- An adversary model is assumed by varying the number of black hole and worm hole nodes to validate the proposed mechanism.
- Numerical simulation is performed to evaluate and analyze the network metrics and packet loss ratio parameter is considered during worm hole and black hole attacks in order to compare the proposed mechanism against reported SRM protocol.

The rest of the chapter is organized as follows. The related work section describes the literature survey done by various researchers/scientists. The proposed WTR technique along with an illustrative example is detailed in proposed approach section. An empirical study over routing attacks and numerically simulated results over different network metrics is reported in performance analysis section and finally the chapter is concluded at conclusion section.

5.2 RELATED WORK

Various researchers/scientists have proposed several routing protocols by dividing the techniques into different categories such as cryptographic computational routing [98, 99] and trust based routing [100-102] to certify a secure routing mechanism. To design a trust based model amongst WMN nodes, it is crucial to specify the interactions and norms between the nodes where a behavioral relationship is established between the entities and malformed into discrete quantity. There exist number of trust based routing protocols for WSNs and for MANETs. Similarly, many researchers have proposed cryptographic based security protocols i.e. Optimized Link State Routing Protocol (OLSR) [103], Dynamic Manet On-demand (DYMO) [104] and AODV [105] for MANETs, ad-hoc and community networks. However, none of these protocols were designed with a non-trivial security in mind and does not completely adopted well in WMN environment because of following reasons.

- The cryptographic operations in these protocols enact a huge processing delay and overhead which affects the overall performance of the routing process.
- They compact with the network as a flat network which can’t be considered for WMN nodes.

Obaidat et al, [106] have proposed an enhanced version of on-demand distance vector-based protocol which prevents the packet dropping and message tempering attacks during nodes mobility in the network. Further, Woungang et al, [107] proposed an improved version of Dynamic Source Routing (DSR) for securing the route process prior to black hole nodes. The proposed technique was proved by showing the simulation results against routing

overhead, throughput and packet delivery ratio. In addition to this, [108] have proposed a strong authentication procedure for mobility management against DOS, eavesdropping and Domain Name Server (DNS) spoofing attacks however, due to unique characteristics of WMN, prevailing routing protocols must be reconsidered to make them attuned with WMN environment by considering some important issues i.e. gateways and mesh routers are stationary, clients may be mobile or static in nature, WMN can be influential against security threats and network performance should not degrade with the involvement of security protocols. By focusing the above discussed characteristics, a number of researchers have proposed several secure routing protocols i.e. Hybrid On-demand Distance Vector Routing (HOVER) [109], a mesh routing algorithm proposed by S. Mir et al. is based upon basic AODV routing protocol. S. Mir et al. gave a routing algorithm having an optimal link selection and quality estimation capabilities. Neumann et al, [110] have proposed a decentralized secure routing mechanism by establishing a trust among individual and concurrent routing topologies. The proposed protocol protects the routed message against control plane and data plane attacks. Talawar et al [111] have proposed a secure end-to-end communication using trust node mechanism established through a shared secret key between the neighbors. The basic assumption of all these routing protocols is that all the gateways and routers are cooperative and non-malicious. Some researchers have proposed secure routing protocols but these are designed for ad-hoc networks and cannot adopt well in heterogeneous environment. Radio Aware Optimized Link State Routing (RAOLSR) [112], another secure routing mechanism implemented a combination of identity based encryption and elliptic curve digital signature algorithm to secure the messages in link state routing. Further Sbeiti et al, [113] have proposed a combination of digital signature with light weight authentication tree and symmetric block ciphers to secure the routing messages. In addition to this, S. Khan et al. [114, 115] have proposed a secure routing protocol by modifying the basic AODV routing protocol. In this, to robust against security attacks, S. Khan designed a 2-hop information and passive acknowledgement mechanism. Although the author is able to provide the security against various attacks however, it may increase the storage overhead at routers. Instead of keeping the information of 1-hop, routing table is storing the 2-hop information which may lead to extra overhead at routers.

Most of the proposed approaches use cryptographic operations to ensure the integrity and confidently of the nodes using trusted third party which seems to be infeasible in mesh environments (because of dynamic nature). Further, these methods are effective for external

attacks and are found completely infeasible to ensure security against internal attacks. So according to the best-of-author's knowledge, the potential method to ensure a secure routing during packet transmission is trust based method. Trust based methods enhance the security by degrading communication overhead and increase the network metrics in comparison of cryptographic operations because it does not require any additional computational step to ensure the security in networks.

In this work, we have proposed a trust based routing algorithm that reduces packet loss ratio in the presence of routing attacks (i.e. worm hole and black hole attacks). As the main objective of our work is to ensure a secure route discovery to securely transmit the data packets to their destination node, we have proposed a WTR mechanism which highlights some improvements in output results.

5.3 PROPOSED APPROACH

To isolate malicious nodes and to enforce cooperation among communicating entities, we have proposed a mechanism which eliminates routing attacks during path discovery process by calculating the Trust Value (TV) of each node. This section presents the hierarchical mesh architecture along with an adversary model to describe the designing methodology and proposed mechanism.

5.3.1 Proposed Network and Adversary Model

The network is assumed to be hierarchical in nature and is divided into two different Routers i.e. Probe Routers (P-Routers) which are connected with each other and serve as a backend of the network and Edge Routers (E-Routers) which directly interact with the clients.

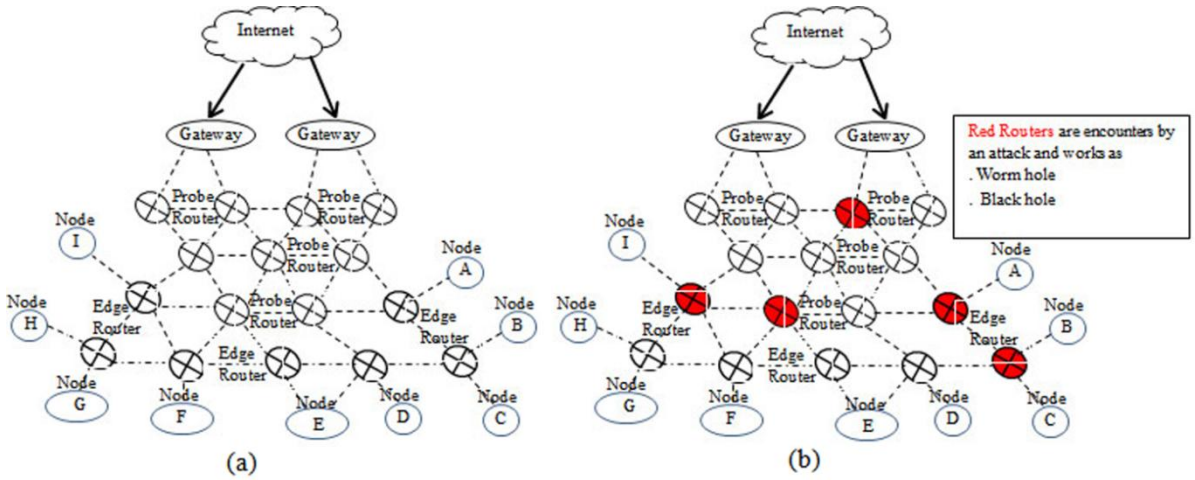


Figure 5.1 The network architectures to describe the proposed mechanism using (a) network model and (b) adversary model

The clients fall on the lowest level while E-routers are associated at a level above the clients and P-Routers above them. The network model as discussed is depicted in Figure 5.1(a). In the discussed network model, there is an assumption that nodes in WMN may duplicate, drop and selectively forward the packets. In addition to this, nodes may also indulge several unethical activities (i.e. non-optimal route selection, packet/route modification) to launch several attacks inside the network. The depicted Figure 5.1(b) shows two types of threats i.e. black hole and worm hole attacks. We have considered these two attacks as they are taken as severe threats in the network by causing a large delay, significant packet drop ratio and significant performance degradation inside the network. Black hole attack is the one in which a compromised node offers itself as the shortest route to reach the destination so that it can drop the entire packet flow going towards it and worm hole attack, where malicious node selectively forwards the packets to the destination node.

5.3.2 Proposed Weight Trusted Routing Mechanism

Dijkstra's algorithm [116] is used to calculate the shortest path and to route the packets from source (S) to destination (D). To securely transmit the data packets between S and D, the TV of each node (which is based upon previous interaction of each node) and the weights between each node (to find the shortest path) are deliberated using certain parameters. The below text discusses the basic designing of each parameter used to secure, route and forward the data packets. The proposed approach uses SITO [117] for the calculation of trust of each node. The route discovery between source and destination node is performed using Dijkstra's algorithm because it requires positive weights for the calculation of shortest route which fasten the route discovery process and found easy to implement in mesh environments. The below subsections discuss the weight computation and routing process phenomenon in detail. A flowchart is given in Figure 5.2 to clearly understand the flow of proposed approach.

- **Weight Computation**

In order to use Dijkstra's algorithm, each node must assign some weight to compute the shortest path between S and D, the weights used for routing and finding the shortest path are computed through various factors such as.

Node Distance is one in which the distance between two nodes i.e. n_i and n_j are calculated using Euclidian distance formula given as

$$d_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (1),$$

where i and j are the nodes in the network n and x and y are the coordinates.

Trust of a node is the most important parameter in weight computation. It is computed using the social impact theory optimizer which states that trust of a node depends on the number of previous interactions of each node.

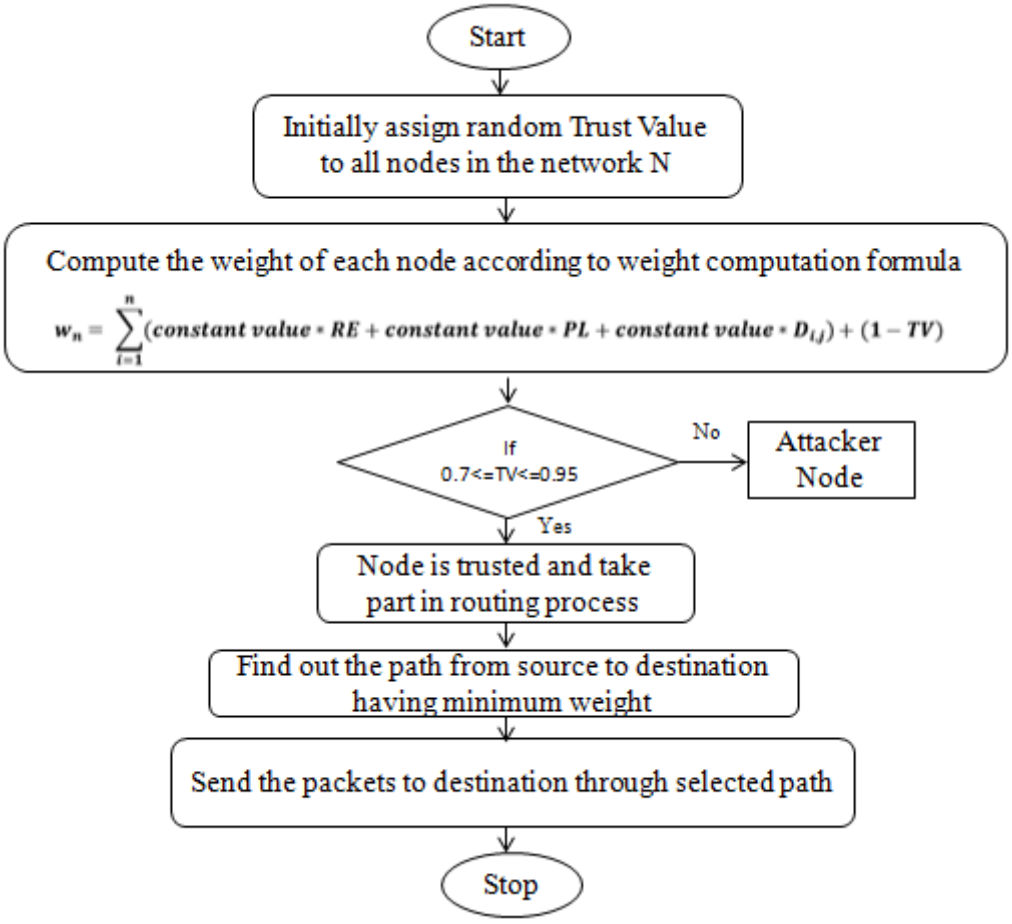


Figure 5.2 Flowchart of the proposed approach

In this, a social rank of each node is calculated using the parameters like residual energy and packets lost by the node in the network. Initially, each node is assigned some initial trust value ranging from *0.7- 0.95* with *1* as the highest trust value and then the trust of a node is increased or decreased by checking the social rank of each node by using some predefined threshold value. The initial trust value is considered between 0.7 to 0.95 (as assumed) that can be increased and decreased according to the opinions. The reason of taking this value is that the threshold will be around 30% of the maximum value, so taking initial value range will help in the further calculation instead of taking every value as simple 1. There is a disadvantage of taking this scenario also as few nodes tends to lose the trust early as compared to the other nodes. The formula for calculating the trust factor is given as

$Node\ Trust = \sum_{i=1}^{n} Previous\ interactions\ of\ node$, where, n are the number of nodes (2)

Residual Energy is the energy left with each node after the transmission of data. Here, the nodes energy is consumed with every transmission and receiving of the data and is considered for the computation of the weight as

$Residual\ Energy = Total\ Energy - (E_t + E_r)$, where E_t is the energy lost in transmitting and E_r is energy exhausted in receiving (3)

Packet Loss of each (source or intermediate) node is calculated which occurs due to some internal attacks on the node or overflow condition of packets (where each node in a network consists of a fixed length queue and if the queue of a node is full then packets start dropping and thus overflow occurs) and expiry Time to live (TTL) parameter (which is associated with each packet and decreases as the packet passes through a node).

So, the weight of each node is defined as the summation of the residual energy, packet loss and distance between the nodes multiplied by some constant value and the negation of TV (the constant value is based on the weightage given to each parameter) as given in eq. (4).

$$w_n = \sum_{i=1}^{n} (constvalue * RE + constvalue * PL + constvalue * d_{i,j}) + (1 - TV) \quad (4)$$

• Significance of negation of TV

Let there exist two paths to transmit data packets to destination node *D* i.e. *(i-D)* and *(j-D)* as depicted in Figure 5.3 and assume that the TV of node *'i'* is *0.7* and of node *'j'* is *0.9*. So, according to SITO theory, the node having maximum TV would be selected to route the data packet. Let, initially all the parameters to calculate the weights are set to be *1*. Now, the weights between *i-D* and *j-D* (according to eq. (4)) will be calculated as.

$$w_{iD} = 0.4*1 + 0.4*1 + 0.2*1 + (1 - 0.7)$$

$$= 0.4 + 0.4 + 0.2 + 0.3$$

$$= 1.3$$

$$w_{jD} = 0.4*1 + 0.4*1 + 0.2*1 + (1 - 0.9)$$

$$= 0.4 + 0.4 + 0.2 + 0.1$$

$$= 1.1$$

The weight of $node_{iD}$ is *1.3* while $node_{jD}$ is *1.1*. So, the path selected by source node would be through *j-D*. The higher is the value of trust, the lesser is the weight of a node (as depicted in equation 5).

In this way, the node having the higher trust value has a low weight and would be selected in routing path formation.

$$weight \propto {}^{1}/_{TV} \tag{5}$$

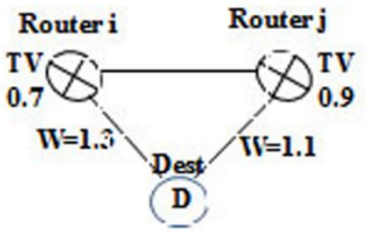


Figure 5.3 Intra-domain communication

- **ROUTING TABLE**

The routing table associated with each node contains the important information (i.e. next hop neighbor, routing weight and the destination) regarding path selection and its neighbor's as depicted in Table 5.1.

Table 5.1: Routing table of each node

Next Hop Neighbor	Weight at each node	Destination

- **ROUTE DISCOVERY**

For the discovery of a route, Dijkstra's route discovery algorithm is used as presented in Table 5.2. This algorithm works on the positive weight value and is considered in place of Bellman Ford algorithm (which is implemented in the basic approach). The Bellman Ford algorithm has a time complexity of $o(n^3)$ while the Dijkstra's algorithm has a time complexity of the order $o(n^2)$.

Table 5.2: Algorithm of minimum path selection

An algorithm to find minimum path selection	
S. No.	**Algorithm steps**
1	Dist[s] ← 0, distance/weight to source node is zero, for all $v \in V - \{s\}$
2	Do Dist[v] ← 1000, set all other distances to large value
3	S← 0, set of visited vertices is zero
4	Q← V, initially contains all vertices
5	While $Q \neq 0$, while queues is not empty

6	Do ← mindist (Q, Dist), elements of queue with min distance
7	S ←$S \cup \{u\}$, add u to vertices list, for all $v \in neighbors[u]$
8	Do if Dist[v] > Dist[u] + w(u,v), for new shortest path
9	Then d[v] ← d[u] + w(u,v)
10	Return Dist

Dijkstra's Algorithm is used to find the minimum weighted path which starts from the source and forms a tree till it reaches the destination. In this, single source minimum weighted path is find out using the weights and is added as a lowest weight to the source node and so on. According to SITO, a threshold value (i.e. 0.5) is set at each node so that if the social rank of a particular node is less than the threshold value then TV on that node would be less and if the TV is above *0.5*, the trust on that node will be satisfactory or more. The social rank of a node is calculated as.

$$Social\ Rank = \frac{Previous\ \ Interaction}{Energy + Packet\ \ Loss + Previous\ \ Interaction} \quad (6)$$

The corresponding algorithm of path selection and packet transmission is presented in Table 5.3. To clearly understand the proposed mechanism, let us consider a scenario as depicted in Figure where initially, some random TV's will be assigned to the entire network (after the first transmission, the TV's will be updated according to their previous interactions) for computing the weights between each node (as depicted in Figure 5.4 (a)). The weights of the network will be calculated using eq. (4) where the preceding node's TV will be used to find out the weights. For e.g., if node *A* wants to send some packets to node *B*, then TV of node *B* (i.e. *0.95*) will be considered for weight computation as

$$w_{AB} = 0.4 * RE + 0.4 * PL + 0.2 * D_{AB} + (1 - 0.95) \quad (7)$$

Table 5.3: Algorithm of packet transmission

An algorithm for packet transmission	
S.No.	**Algorithm steps**
Step 1	Initialize each node with trust node between *0.7-0.95*
Step 2	For i← 0 :n, n is total number of nodes
Step 3	For j ← 0:n $\forall\ j\ \neq i$
Step 4	$W_{ij} = CalWeight(S_i, S_j)$, where S is set of data required to calculate weight for node i.
Step 5	End for
Step 6	End for
Step 7	$FindRoute(n_s, n_d)$, Dijkstra's algorithm for route discovery
Step 8	Transfer $Data(n_s, n_d)$
Step 9	Go to step 2

Let us assume that RE, PL and $D_{i,j}$ is set to *1* (which will be updated according to the time as per packet transmission/receiving, packet forwarding history and mobility rate), then the corresponding weights will be calculated through eq. (4) and are shown in Figure 5.4 (b). Further, (after calculating the weight of the entire network) if source node *E* wants to send some packet to destination node *G*, packets will be transmitted by calculating the shortest routing path drawn using Dijkstra's algorithm between *E* and *G*.

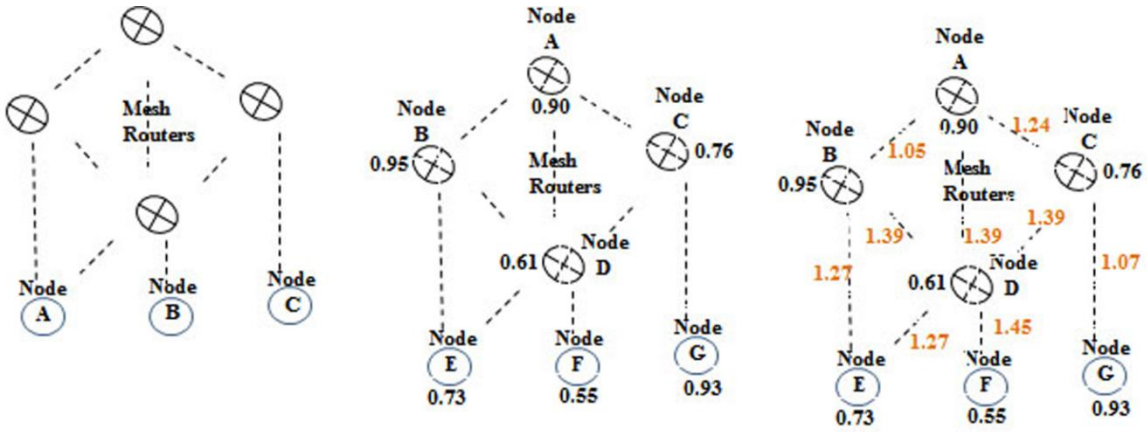


Figure 5.4 An illustrative example to describe the proposed phenomenon using (a) trust value assignment during path formation and (b) weights computation using eq. (4)

5.4 PERFORMANCE ANALYSIS

Mesh network's security is harder than sensor and ad-hoc networks because of larger coverage area and broadcasting nature. This section discusses some security aspects and advantages of proposed mechanism. The proposed mechanism minimizes the possibility of route selection using Dijkstra's algorithm which takes positive weight path for selecting the routing path.

5.4.1 Security Analysis

WTR is buoyant to many attacks such as black hole, node isolation, worm hole, grey hole, fairness reduction, packet/route modification and routing loops. Black hole attack is the one in which a compromised node offers itself as the shortest route to reach the destination so that it can drop the entire packet flow going towards it while in grey hole attack, malicious node selectively forwards the packets to the destination node. Jellyfish is similar to grey hole with an addition of packet recording and delaying the forwarding packets. Wormhole attack is used to create the routing disruption by tunneling the packet from one malicious node to another

malicious node. Further, routing loop attack is created through byzantine attack where route cannot be found to destination node and the packets keep moving in the routing paths. All the above discussed attacks can be alleviated using WTR by keeping in assessment its 2 important features i.e.TV and weight computation through TV. The theorems explained in section 4.2 with different lemmas to observe the reported results.

- **Empirical Study**

Theorem 1: The proposed mechanism is secure against routing attacks

Solution: The proposed approach calculates the trust value using the SITO and the route is calculated using those nodes which fall under the category of trusted nodes. The lemmas given below prove the validity of the theorem.

Lemma 1: Black hole Attack

In black hole attack, a fake node is created and all the data passing through that affected node is dropped or lost. The proposed approach uses social impact theory to calculate the trust of each node and the route selected for packet transmission consists of secure nodes only. So, the black hole attack is violated in proposed mechanism because the node with no previous interactions will be considered as untrusted node and will not be reflected during path formation.

Start

Initialize Trust to existing nodes N in Mesh Network M between (0.7-0.95)

If($f_n \cup M$), where f_n is a fake node appending in the existing network

Then Trust of$(f_n) = 0$ & $Interaction(f_n) = 0$, i.e. no initial trust and no interactions

Cal weight $(f_n) \rightarrow Max$

$f_n \notin FindRoute(n_s, n_d)$, f_n is not considered in the route

End If

End

Lemma 2: Wormhole Attack

In wormhole attack, the corrupted node attracts the packets at one point in the network and tunnels them to the other point or drops the entire packets at that point. The packets coming from worm hole node are lost from their path and are dropped in the network. The packet loss of a worm hole node will be increases and during the time, the trust tends towards that node would be 0 which will not be considered for path formation process.

Start

If $(N \in W_n)$, then

Receive Packet(W_n, k), where $k \in M$ is set of all nodes // Receiving packets from all the nodes

Send packet $(W_n, Null)$ // no forwarding of packets

Trust $(W_n) \rightarrow 0$ // packets lost at the node

Calweight$(W_n) \rightarrow Max$

$W_n \notin FindRoute(n_s, n_d)$,W_n is not considered in the route

End If

End

Lemma 3: Node Isolation

If a node is isolated from other nodes in the network and the receiving and sending of packets from that node tends towards zero, then the interactions of isolated node with other nodes also tend to zero. Thus, the social impact factor of that node also decreases thereby decreasing the trust value. The node with low trust value increases the weight for the routing algorithm and is not considered for route discovery.

Start

If$(I_n \in M)$, I_n is an isolated node in mesh network M

Receive packet $(I_n, Null)$ at node I_n//receiving no packets

Send packet $(I_n, Null)$ at node I_n //sending no packets

Trust $(I_n) \rightarrow 0$ & $Interaction(I_n) = 0$ // trust of I_n tends to zero with no interactions

Cal weight $(I_n) \rightarrow Max$

$I_n \notin FindRoute(n_s, n_d)$ // I_n is not considered in the route

End If

End

Theorem 2: Route discovery procedure is fast and efficient and packet loss is reduced

Solution: The lemma given below proves the validation of the theorem.

Lemma: The proposed approach uses Dijkstra's algorithm for route discovery. The algorithm works on non-negative weights only and the nodes once used cannot be used again. So the loop formation during route discovery is out of scope and the packet loss also reduces.

5.5 SECURITY ANALYSIS

The below mentioned parameters are used for the performance evaluation of proposed approach with the previous one.

Packet Delivery Ratio is the ratio of number of packets received at destination to the total number of packets transmitted by the source.

Table 5.4: Simulation parameters

Number of Nodes	Variable (30 – 70)
Dimension of Grid	400m * 400m
Radio Range	120 m (approx.)
Packet Size	512 Bytes
Simulation Period	70 sec
Physical Layer	PHY 802.11

Route Discovery Delay is the total time consumed in discovering the route from source node to destination node.

End to End Delay is the time taken by the packet generated by the source to reach to the destination.

Packet loss is the number of packets lost from the node in the presence of attack.

To evaluate the performance of proposed approach on the basis of above mentioned performance parameters, network simulator ns-2.3.5 is used. The simulation parameters are given in Table 5.4. The depicted Table 5.5 and 5.6 signifies the simulated outcomes of both the approaches (basic and proposed) on different network sizes *(i.e. 10, 20, 30, 40 and 50)* by varying the number of adversary nodes (i.e. black hole and worm hole nodes).

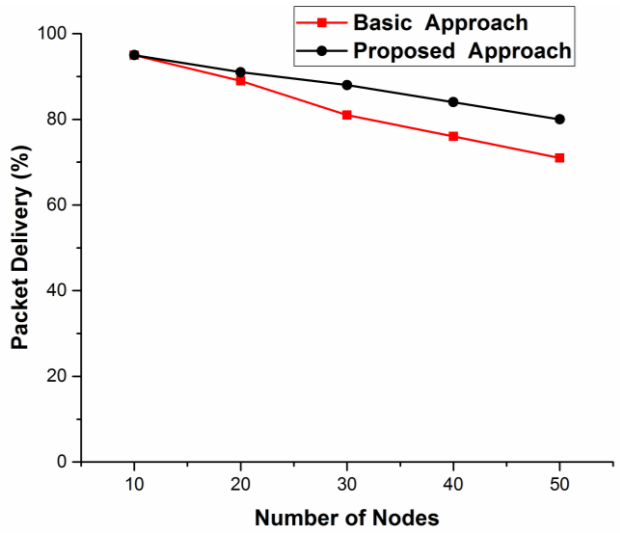


Figure 5.5 Packet delivery ratio

- **Packet Delivery Ratio**

Figure 5.5 shows the graph of packet delivery ratio plotted against number of nodes. The graph shows the comparison of basic Bellman Ford approach with Dijkstra's Algorithm approach. It is evident from the graph that the performance of proposed approach is better than basic approach by increasing the number of nodes. The reason of better Packet Delivery Ratio in proposed approach is due to the decrease in loss of packets because of trust among the communicating nodes.

Table 5.5: Simulation results values

Simulation Parameters with their Approaches		**Different Network Size (by varying the number of nodes)**				
Network Parameters	**Approach**	10	20	30	40	50
End to End Delay (Fixed node)	Basic Approach	300	420	600	780	920
	Proposed Approach	180	240	360	420	540
End to End Delay (Mobile Node)	Basic Approach	380	530	680	900	1320
	Proposed Approach	260	350	520	700	1180
Packet Delivery Ratio	Basic Approach	95	89	81	76	71
	Proposed Approach	95	91	88	84	80
Route Discovery Delay	Basic Approach	160	210	290	380	460
	Proposed Approach	90	120	170	210	260

Table 5.6: Simulation results values of black hole and worm hole attacks

Simulation Parameters with their Approaches		**Number of Nodes**				
Network Parameters	**Approach**	**1**	**2**	**3**	**4**	**5**
Black Hole Attack (Packet loss Ratio)	Basic Approach	4	7	14	19	24
	Proposed Approach	2	4	7	11	14
Worm Hole Attack (Packet Loss Ratio)	Basic Approach	7	11	14	16	18
	Proposed Approach	4	6	9	11	14

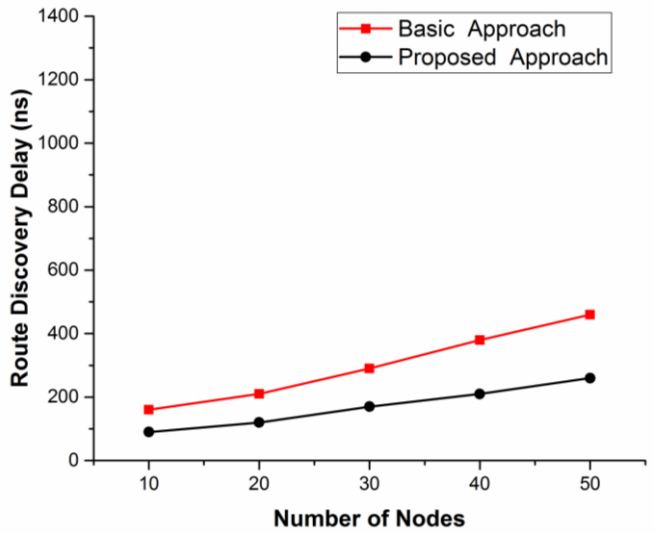


Figure 5.6 Route discovery delay

- **Route Discovery Delay**

Figure 5.6 shows the comparison graph of route discovery delay between the proposed and basic approach. It is clear from the graph that as the number of nodes in the network increase, the delay to discover the route from source to destination also increases and is more in case of basic approach. Also, the time complexity of finding the path of basic approach is of order $O(n^3)$ while in case of the proposed approach it is $O(n^2)$.

- **END-TO-END DELAY**

Figure 5.7(a) and 5.7(b) show the graph of end-to-end delay. Here two cases are considered in determining the delay.

In the first case, the network size is varied as the number of nodes are varied from 10-60. In the second case, 50% of nodes are mobile in nature by varying the number of network sizes i.e. 10, 15, 20, 25, 30, 35, 40, 45 and 50. It is evident from the graphs that as the number of mobile nodes or the size of the network increase, the end-to-end delay for the packets also increases.

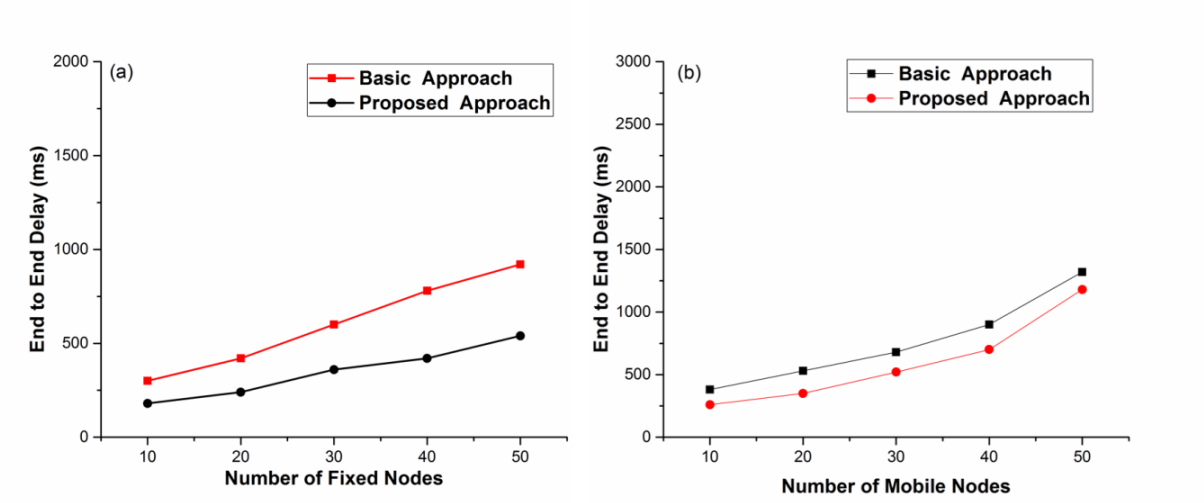


Figure 5.7 End-to-End delay over (a) fixed number of nodes and (b) mobile number of nodes

This is also due to the fact that the basic approach takes negative weights and reconsiders the same node again in the path. This may lead to the minimum weight path as the number of hops increase. So the proposed approach performs better in all the given scenarios.

The link in case of fixed number of nodes between source to destination is more stable as compared to the mobile nodes. End to End delay is the measure of the time taken by the packet to reach the destination from source. It is clearly evident from the graph that the proposed approach shows improved results as the algorithm works only on the positive

weights and forms the short paths between the source and the destination. In Figure 5.7 (a) and 5.7 (b) there is a slight decrease in the packet loss ratio as the number of faulty nodes considered is small enough for a network and the packet flow is also limited. Considering the number of packet flow in the network and the number of nodes considered the improvement is significant in the values.

PACKET LOSS

Figure 5.8 (a) shows the graph of packet loss when the network is attacked with black hole. The number of black hole nodes is varied in the graph and the packets lost from black hole nodes are considered. It is evident from the graph that in case of proposed approach, the percentage of loss of packets is less as compared to basic approach.

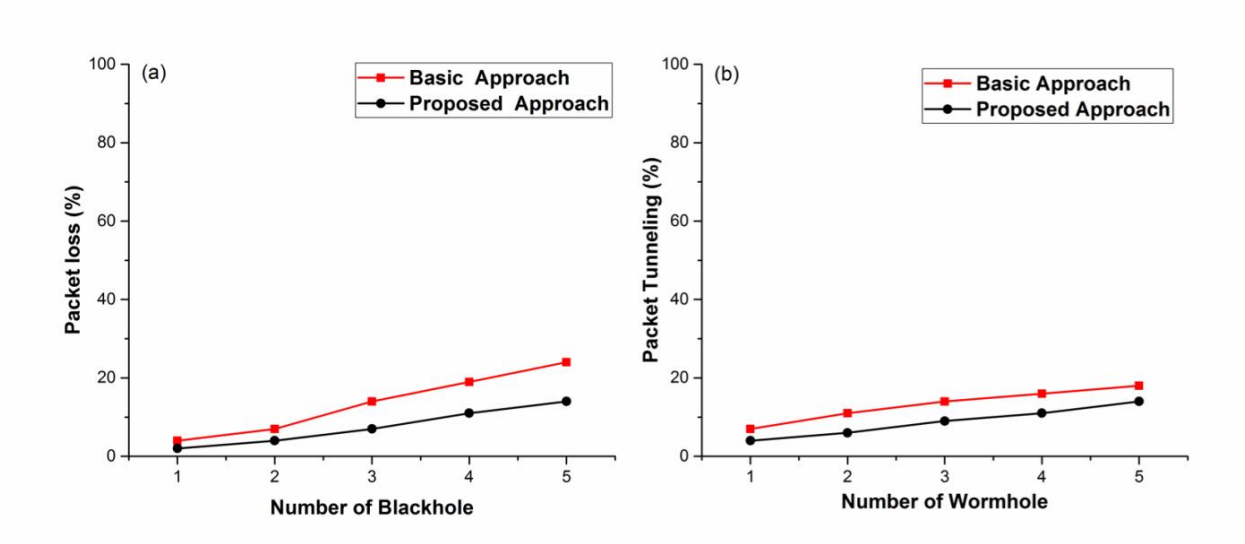


Figure 5.8 Packet loss ratio by varying the number of (a) black hole nodes and (b) wormhole nodes

Similarly to obtain the concert of WTR in presence of wormhole attack, we have presented 4 wormhole nodes as depicted in Figure 5.8(b). Approximately 16% of packets are lost in case of existing approach while numbers of packets lost in WTR are less.

5.6 CONCLUSION AND FUTURE WORK

In this chapter, the weight trusted routing mechanism for hierarchical mesh network using social impact theory optimizer mechanism has been proposed. The proposed mechanism has significantly reduced the packet loss ratio in the presence of black hole and worm hole

attacks. Hence, the weight trusted routing mechanism has enhanced the packet delivery ratio and reduced the route discovery, end-to-end delay and packet loss ratio in comparison of reported secure routing mechanism protocol. In further studies, the proposed algorithm will be tested under high packet flow and high number of attackers (by considering black hole and wormhole attacks) and then their results will be compared with the existing approaches on various performance parameters.

CHAPTER 6

ASPECTS OF TRUSTED ROUTING COMMUNICATION IN SMART NETWORKS

In this chapter, we have exploited the WTR mechanism to detect and eliminate the malevolent/malicious nodes involved during the routing path formation for smart-home environments where the routing between the communicating entities is performed through the mesh architecture. In order to provide a secure communication against malicious behavior of nodes, the proposed mechanism uses Dijkstra's shortest path routing algorithm in which the weights are deliberated using certain parameters such as node distance, packet-loss percentage and trust value of each node which is computed using SITO. Further, we have discussed the network performance trade-off caused by secure path formation with conventional method and have proposed the WTR mechanism for eliminating the potential issues such as packet-loss ratio, end-to-end delay and network throughput. The NS2 simulator is used to simulate and compare the network metrics for both conventional and the proposed approach and is validated through experimental results over end-to-end delay and message delivery ratio against reported literature.

6.1 INTRODUCTION

With the recent societal development, the demand of digital environments where humans interact smartly with their surroundings to increase their comfort zone as compared to the hard build infrastructures is accumulating day by day. Smart cities, smart homes and smart societies are potentially hot trends of intelligent environments where multiple internet-of-things (IoT) devices respond as human behavior by automatically controlling and adapting the environmental situations [118, 119]. In order to provide the interconnectivity among the communicating entities or to enhance the coverage area by introducing additional placements of devices, there is a need to use a more efficient, robust and reliable communication standard such as Zigbee, Bluetooth or Wi-Fi [120, 121]. Currently, for such systems, Zigbee is one of the most widely used wireless technology because of its mesh based architecture which allows high scalability (because of its multi-hop feature) and provides large coverage area by incorporating self-healing, self-organizing and self-configuring characteristics [122, 123].

Although, the main stream of such systems is to achieve a seamless integration of intelligent sensing and networks to provide an automated life. However, the equally important issue of handling the security in these environments is not reported in depth where the inter-connection between the devices is subject to a number of security threats either from remote attackers or from inside home area networks. The most important factor that impacts the security is the nature of fundamental routing protocols used for promoting the message signals [124-126] where the presence of any malicious or misbehaving node within the routing path may interrupt the network activities either by spoofing or reducing the data packets or by degrading the overall performance of the network. The smart devices acquire a vast amount of sensitive data whose collection and processing raises several privacy concerns regarding the secrecy of the data that would be shared only for their own good rather than being collectively or maliciously disclosed for the purpose of violating their autonomy and privacy [127, 128].

The conventional routing protocols operate smoothly with an assumption that all the intermediate nodes are trusted and cooperative with each other. However, the dynamic and multi-hop features of the mesh network invite a number of internal vulnerabilities to come where attackers may launch several types of attacks either by compromising the legitimate routing nodes or by disrupting the data packets [129-131]. Therefore, one of the norm approaches to counter such attacks is secure routing. Most of the previously proposed approaches use cryptographic operations to ensure the integrity and confidentiality of the nodes using trusted third party. The issue with these techniques is that they seems to be infeasible in mesh environments (because of its broadcasting and dynamic nature) due to certain parametric issues such as computational, communication and storage overheads. Further these techniques are effective for external attacks and are found completely infeasible to ensure the security against internal threats [132]. Recently, the trust based methods have suit an active research area as they have emerged as a viable solution to take the routing decision and overcome the above discussed issues. A number of trust based methods have been proposed for MANETs, WSNs [133, 134] and other networks [135, 136] that are basically espouse for homogenous systems and cannot be adapted well in heterogeneous mesh networks because of their multi-hop and dynamic nature [137-138]. Therefore, there is a need to provide a secure communication mechanism that overcomes the computational, communication and storage issues and ensures efficient routing procedures for establishing the communication in smart home environments.

In this chapter, a trusted weight computation through SITO mechanism is proposed for smart home communication procedures that is based on mesh architecture and ensures a secure path formation in the network by detecting and eliminating the malicious nodes. Further, the Dijkstra's shortest path routing algorithm is used to route the data packets to yield the shortest way between the communicating entities [139]. The Dijkstra's algorithm is chosen for the purpose due to its lesser computational complexity as compared to other shortest path routing algorithms such as bellman ford algorithm used by Khan et al. [140, 141] to explore their secure approach. Further, it considers positive weights to avoid the loop formation process. While the greedy algorithms like greedy parameter circuit routing (GPCR) algorithm does not provide the accurate measurements and must be tested on similar environments where their results should be compared with the existing approaches again and again. The potential contribution towards a secure routing mechanism is summarized as follows.

- The Dijkstra's shortest path routing algorithm is used to yield the shortest path between the communicating entities whose weights are assigned according to their trust factor which is computed using certain factors i.e. node distance, trust of a node, residual energy and packet loss ratio.
- The simulations are performed using commercial simulator NS2 and are experimentally validated over real environment to analyze and evaluate the network metrics against reported SRPM protocol that is considered as the basic approach of our chapter [142].
- The behavior of both the protocols is first analyzed under small network sizes and then under large network sizes having fixed number of nodes against different network metrics. Further the network metrics are measured under scalable network sizes in mobile nature where the nodes are moving at the speed of 0-25 m/s and the proposed protocol is validated under various adversary nodes having two different scenarios (metrics are measured against two severe routing attacks i.e. black hole and falsification attacks over scalable network sizes, and the performance is checked by increasing the number of black hole and falsification nodes near source and destination over small and large network sizes). A black hole attack is the one in which the compromised or malicious node offers itself as the shortest route to reach the destination so that it can drop the entire packet flow going towards it while falsification is the attack where an intruder hacks the legitimate node's address with the aim of affecting the performance metrics of the network. These two attacks are taken as two severe routing attacks because they drastically affect the

network performance. Moreover, the experimental results are shown for end-to-end delay and Message Delivery Ratio (%) for both the approaches

The remaining structure of the chapter is organized as follows. Section 2 describes the related work reported by various researchers. The proposed WTR mechanism is deliberated in section 3. The simulation and experimental measurements are presented in section 4. Further, section 5 presents the results for different cases and scenarios against reported SRPM protocol and finally, section 6 concludes the work.

6.2 RELATED WORK

Although scientists/researchers have proposed a number of routing protocols for different network environments, however, these protocols are basically espouse for homogenous systems and are designed keeping a non-trivial security in mind which are unable to perform well in heterogeneous mesh environments. Boushaba, Hafid and Gendreau have [143] proposed a gateway selection and source based routing mechanism to securely transfer the data packets to their intended destination nodes. The proposed mechanism selects the best routing path using a routing metric procedure which is basically a combination of certain networking parameters such as inter-flow, intra-flow interferences and packet loss ratio. Further the proposed protocol eliminates the issue of path changing phenomenon where the source node frequently switches to the new route in case of jitter and delays due to network congestion. The proposed mechanism eliminates this issue by computing a waiting time process where the source waits for some time before switching to the new routing path. The simulation results of proposed mechanism efficiently validate the network throughput, delay and packet loss ratio metrics over existing technique. Neumann et al. [110], have anticipated a secure decentralized routing mechanism for MANETs by ensuring the trust among concurrent and individual routing topologies. It enables a decentralized cryptographic negotiation technique among the communicating entities where the transmitted routing messages are encrypted using number of cryptographic signatures. The proposed protocol secured the routed packets against data plane attacks and control plane and validates the proposed phenomenon by analyzing the benchmark results over large number of nodes as compared to existing approach. Further, Talawar and Ramesh [111] have proposed an end-to-end secure communication through a trust based phenomenon by establishing a shared secret key between the neighbors. The generic assumption of all aforementioned routing mechanisms is that all the routers and gateways are cooperative and non-malicious during the packet

transmission. However to overcome the above discussed issues, Benitez et al. [144] projected a combination of elliptic curve digital signature and identity based encryption algorithm to secure the data packets in link state routing procedures. The elliptic curve digital signature ensures the confidentiality and integrity of routing messages while identity based encryption method prevents the routed messages from active and passive routing threats. The authors in [145-146] have proposed different schemes to quickly transfer the data packets by deriving time division multiple access (TDMA) schedule and Markov chain model is used in discrete time to enhance the performance of opportunistic routing protocols. Sbeiti and weitfeld [113] have provided a combination of digital signatures with symmetric block ciphers and light weight authentication tree to ensure the security among routing messages. The light-weight authentication reduces the computational and communication overheads of routed messages while a symmetric block cipher eliminates the issue of key storage and key management overheads. Moreover, Khan et al. [114-115] have proposed a secure protocol for hierarchical mesh networks by modifying the basic Ad-hoc On-Demand Distance Vector routing mechanism; in this protocol the authors have designed a 2-hop information and passive acknowledgement mechanism to ensure the security against various routing attacks. However, it may increase the storage overhead at routers and instead of keeping the information of single-hop neighbor, routing table is storing the 2-hop information which may lead to extra overhead at routers. To exploit the characteristics of WMN, 802.11s standard is released by IEEE in which Hybrid Wireless Mesh Protocol (HWMP) is specified, but in this protocol security in forwarding and routing is not deliberated and is vulnerable to several routing attacks like the black hole, worm hole and falsification attacks [147-148]. A wormhole attack is the one where the malicious nodes forms a tunnel between the source and destination and re-route the data packets to some other nodes rather than forwarding to their intended destinations. Further, in black hole attack, the compromised or malicious node recommends itself as the shortest route to reach the end or destination node with the aim to drop the entire packet flow going towards it while falsification is the attack where an intruder hacks the legitimate node's address with the aim of affecting the performance metrics of the network. These two attacks are taken as two severe routing attacks because they drastically affect the network performance.

Therefore, to prevent from these loopholes, an efficient secure routing mechanism is needed which can successfully transmit the data packets. From the recital point of view, the aforementioned secure routing protocols deal with flat network which are infeasible to

implement in hierarchical mesh environments and are vulnerable to a variety of routing attacks. In recent years, trust based methods have suit an active research domain as they have appeared as a viable solution to take the routing decision based on anticipated trust value of other nodes. Recently, we have reported [139] a weight trusted routing mechanism where the nodes having highest trust values would be considered during routing path formation. The trust value of each node is computed using SITO [149] and Dijkstra's shortest path routing algorithm [150] is used to formulate the path among the nodes. The weight between each node is deliberated through certain parameters such as residual energy, packet loss ratio and the distance between each node. The node having highest trust value would have the lowest weight and would be considered during routing path formation.

In this work, we have implemented the WTR mechanism in smart home communication procedures for ensuring the security against routing attacks over static and dynamic nature of nodes (consisting of small or large number of nodes). The proposed mechanism is validated by highlighting the improvements in output results over certain parameters.

6.3 PROPOSED APPROACH

Figure 6.1 depicts the network model of the proposed mechanism consisting of n number of nodes among which some are assumed as malicious nodes m, where all the nodes are connected with each other by assigning some weights (as presented in Figure 6.1(b)). To securely transmit the message signals to their intended destination nodes, the shortest path Dijkstra's routing algorithm is used where weights are assigned to each node by computing the TV of each node using certain parameters such as: 1) node distance which is calculated using Euclidian distance formula, in our proposed approach we have used Euclidian distance formula as it is used for various line of sight range applications like in sensors, which are placed in a room or in a hall to verify the range calculation. However, in case of obstacles like wall, the signals degrade by collision from the obstacles which affect the range of zigbee and hence routers are used for zigbee. 2) Node trust that is computed through social impact theory optimizer which states that trust of a node depends on the number of previous interactions of each node. In this, a social rank of each node is calculated using the parameters like residual energy and packets lost by the node in the network. Initially, each node is assigned some initial trust value ranging from 0.7- 0.95 with 1 as the highest trust value and then the trust value of a node is increased or decreased by checking its social rank using some predefined threshold value.

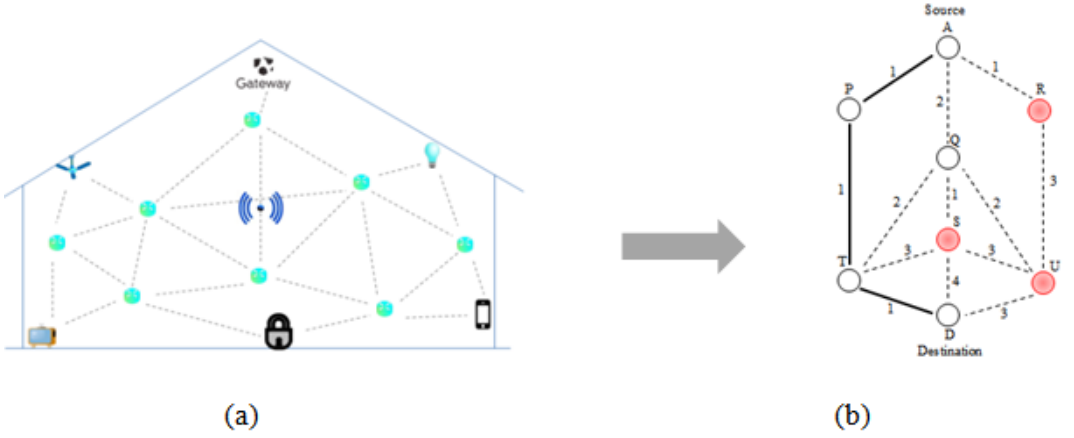


Figure 6.1 The network model of the proposed mechanism (a) mesh network in smart homes (b) path formation amongst available number of routes through trust value

The formula for calculating the trust factor is given as $\text{Node Trust} = \sum_{i=1}^{n} \text{Previous interactions of node}$, where, "n" is the number of nodes, 3) residual energy which is left after transmission of data at each node and 4) packet loss ratio that is calculated at each node depending upon the overflow condition of packets (each node in a network consists of a fixed length queue and if the queue of a node is full then packets start dropping and it encounters overflow condition) and expiry TTL parameter (which is associated with each packet and decreases as the packet passes through a node).

So, the weight of each node is defined as the summation of the residual energy, packet loss ratio, distance between the nodes multiplied by some constant value and the negation of TV (the constant value is based on the weightage given to each parameter) as given in (1).

The negation of trust value is taken to satisfy the property of Dijkstra's algorithm where the higher is the value of the trust, the lesser is the weight of each node that would be selected in routing path formation.

$$w_n = \sum_{i=1}^{n}\left(\text{constvalue} \times RE + \text{constvalue} \times PL + \text{constvalue} \times D_{i,j}\right) + (1 - TV) \qquad (1)$$

The flowchart and the corresponding algorithm of the proposed mechanism are depicted in Figure 6.2 and Table 6.1 respectively. The proposed routing mechanism is based upon two key factors i.e. network metrics and security. The dynamic and broadcasting nature of mesh network not only increases the communication or scalability range of the network but also affects the performance metrics of the network during nodes' mobility.

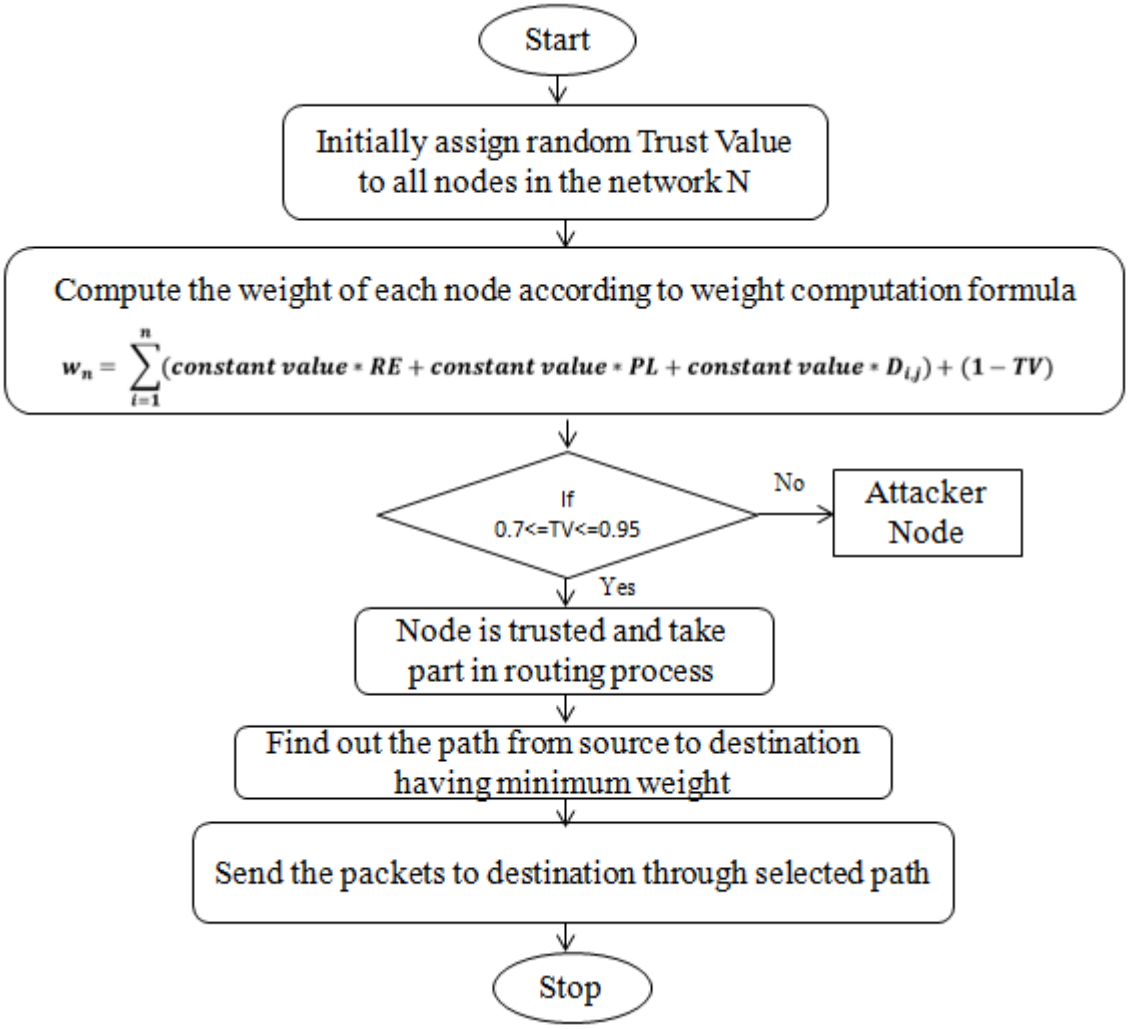


Figure 6.2 Flowchart of the proposed mechanism

Further, the multi-hop feature invites a number of internal vulnerabilities where presence of any malicious behavior during routing path formation or packet transmission may affect the security and performance metrics of the network. The proposed approach relies on the design of Dijkstra's routing algorithm and SITO optimizer.

The smart home architecture and its internal connectivity among the devices is depicted in Figure 6.1(a) and Figure 6.1(b) respectively. To clearly understand the proposed mechanism, let us take a scenario as illustrated in Figure 6.1(b) where source node '*A*' wants to transmit some packets to the intended destination node '*D*'. Initially, let '*S*','*U*'and '*R*' be assumed as three adversary nodes affected by black hole attack which simply drop the entire packet flow coming towards them. After the transmission of some messages by these malicious nodes, their TV would be very less according to SITO (as they will drop the packet flow and increase the packet loss ratio along with an increase in residual energy) and their corresponding

weights computed through the given formulas would be very high that they would never be considered during path formation process.

Algorithm 1: Packet transmission mechanism of the proposed approach

S.No.	Algorithm steps
Step 1	Initialize the process by assigning each node with a random trust value between 0.7-0.95
Step 2	For i$\leftarrow$ 0 :n; n is the total number of nodes in the network
Step 3	For j $\leftarrow$ 0:n $\forall$ j $\neq$ i
Step 4	$W_{ij} = \text{CalWeight}(S_i, S_j)$, where S is the set of data required to calculate the weight for node i.
Step 5	End for
Step 6	End for
Step 7	$\text{FindRoute}(n_s, n_d)$, Dijkstra's algorithm for route discovery
Step 8	Transfer $\text{Data}(n_s, n_d)$
Step 9	Go to step 2

As 'S' is a black hole affected node, so, the weight between '$S-T$', '$S-U$' *and* '$S-D$' is very high i.e. 3, 3 and 4 (see Figure 6.1(b)) so they would never be considered during path formation process. Similarly, the weight computed between '$U-D$' is 3 and is neglected during packet transmission process. The foremost advantage of the proposed approach is the process of computing a secure shortest routing path using Dijkstra's algorithm among available number of routes. In an ideal case where all the nodes are trusted and cooperative with each other, the available number of routes to apply the Dijkstra's algorithm between 'S' and 'D' would be $(i \times (i-1))/2$ where 'i' is the number of intermediate nodes between the communicating entities while in case of malicious behavior, if the degree of malicious nodes is 2 (i.e. each node is linked with 2 edges) and the percentage of malevolent behavior is more than 30%, then the available number of paths would be reduced to 1/3 of ideal available routes else if the degree of malicious nodes is more than 2 (means the nodes have more than two connected edges) then the available paths would be more than 50%. The reason is that the nodes selected for path formation are based on their trust values; the node having lowest trust value would never be included for the path formation and would be excluded during route generation process. So, in a network size of 8 nodes where intermediate nodes are 6 between 'S' and 'D', and if nodes 'R' and 'U' are malicious (as presented in Figure 6.1(b)), then the total number of paths would be 5 (i.e. '$A-P-T-D$', '$A-Q-S-D$', '$A-Q-T-D$', '$A-$

$Q-S-T-D$', '$A-Q-T-S-D$') while if 'P' and 'R' are malicious nodes then paths would be more than 50% of ideal case (i.e. '$A-Q-S-D$', $A-Q-T-D$', '$A-Q-U-D$', '$A-Q-S-T-D$', '$A-Q-U-S-D$', '$A-Q-T-S-D$', '$A-Q-T-S-U-D$' *and* '$A-Q-U-S-T-D$').

The possible availability of routes between 'S' and 'D'$=\left\{\begin{matrix}\frac{i\times(i-1)}{2}, & duirngidealcase \\ (i-1)andmorethan\ 50\%\ , & duringmaliciousbehavior\end{matrix}\right\}$,

where 'i' is the total number of intermediate nodes available between S and D in a network size of 'n' nodes. Table 6.2 presents the algorithm to determine the number of routes available with the increment of malicious nodes in the network.

Algorithm 2: The algorithm for computing the shortest path (using Dijkstra's algorithm) among available number of nodes with the increment of malicious nodes.

Input: Network size of 'n' nodes

Output: A single source shortest path is computed using Dijkstra's algorithm from available possible paths

Procedure:

In a network size of 'n' nodes, the total number of intermediate nodes 'i' between source 'S' and destination 'D' would be n-2 i.e. i= (n-2)

// During Ideal case where number of nodes are cooperative with each other

The available number of routes among 'S' and 'D' would be $(i*(i-1))/2$

Among $(i*(i-1))/2$ available routes, a single source shortest path is calculated between communicating entities using Dijkstra's routing algorithm

//During Attacker case where intermediate nodes among 'S' and 'D' are malicious 'm' in mature

If (percentage (%) of m >=30% and m_{degree} ==2)

Then

Available number of routes would be (i-1)

Else if (% of m >=30% and m_{degree} >2)

Then

Available number of routes would be more than 50%

End else if

End if

Therefore, the number of possible paths between the source node 'A' and destination node 'D' with their measured weights as depicted in Figure 6.1(b) are presented in the Table 6.1. According to Dijkstra's algorithm, the shortest routing path used to forward the data packets would be through route-1 i.e. '$A - P - T - D$', its nodes havethe highest computed trust value and lowest assigned weights thus are more reliable and considered for secure message transmission.

6.4 NUMERICAL SIMULATION AND MEASUREMENTS

Table 6.1: The possible available routes between source 'S'and destination 'D'.

Routes	Paths	Weights
Route 1	A-P-T-D	3
Route 2	A-Q-T-D	5
Route 3	A-Q-S-T-D	8
Route 4	A-Q-S-D	7
Route 5	A-R-U-D	7
Route 6	A-Q-U-D	7
Route 7	A-Q-S-U-D	7
Route 8	A-R-U-Q-S-D	11
Route 9	A-R-U-Q-T-D	9
Route 10	A-R-U-S-T-D	11
Route 11	A-R-U-S-D	11
Route 12	A-P-T-Q-S-D	9
Route 13	A-P-T-S-D	9
Route 14	A-P-T-Q-U-D	9
Route 15	A-P-T-S-U-D	11

The performance efficiency of WTR mechanism against reported SRPM protocol has been first investigated through simulations using NS2 and afterwards is tweaked to map the real performance using experimental outcomes. The SRPM protocol is taken as the base paper of this chapter as it ensures the security without using any cryptographic technique in hierarchical mesh networks.

6.4.1 Simulation setup

The simulation is based upon IEEE 802.11 standard in an area of 400m×400m, where the nodes are randomly distributed to execute the reported SRPM as the basic approach and WTR as the proposed protocol. In a network area of 400m×400m, constant bit rate traffic type is taken having 512 bytes of packet size where the nodes are mobile and assumed to be selfish in nature. The simulation time that we have considered is 70 seconds, it can be extended to any length as the packet generation is 512 bytes per second. The simulation time that we have used is a considerable amount of time to depict the behavior of proposed topology. The selfish nodes may drop, duplicate and selectively forward the data packets by indulging into some unethical activities (i.e. packet/route modification, non-optimal route selection etc.). Table 6.2 illustrates the entire information regarding the simulation setup.

Table 6.2: The simulation parameters for the proposed mechanism.

Parameters	Values
Number of Nodes	(10-25), (100-900)
Grid Dimension	400 m × 400 m
Routing protocol	AODV
Propagation Model	Two-ray ground
Radio Range	120m
Packet size	512 bytes
MAC Protocol	MAC 802.11
Link Bandwidth	2 mbps
Mobility Rate	0-25 m/s
PHY Layer	PHY 802.11
Antenna	Omni antenna
Simulation Period	70 sec
Protocols	WTR (proposed), SRPM (basic)

6.4.2 Experimental Setup

For the practical implementation, Zigbee wireless technology is used consisting of 8 mesh nodes to form a network. In the Zigbee network, three types of nodes can be formed, first is gateway which acts as a hub and provides the services to the end nodes, second one are routers whose task is to perform the message generation and message forwarding operations and third are the end nodes which can generate the data without forwarding capabilities. The type of data depends on the applications of the node. The embedded hardware used is a Roboard RB-110 with a vertex X86 32 bit CPU running at 1200 MHZ and 256 DRAM.

Further, the software which controls and forwards the data in Zigbee network is XCTU. The experimental results are extracted from XCTU.

6.5 RESULTS AND DISCUSSION

In this section, the reported SRPM and the proposed WTR protocol are simulated through network metrics under three different cases as discussed in section Introduction. We have considered several network sizes in fixed as well as in dynamic environments for ideal and adversary models to identify the novelty of the proposed mechanism. This section is divided into three different cases to compute the metrics of both the approaches in scalable network sizes. The first two cases show the metrics results computed through NS2 simulator over 25 and 900 number of nodes in fixed and dynamic environments while the remaining case presents the validity of the proposed mechanism by considering two routing attacks in two different scenarios.

Case 1: *Network metrics are measured against small (10-25) and large (100-900) number of nodes over fixed network sizes.*

The depicted Figure 6.3(a) presents end-to-end delay of both the approaches over increasing number of nodes which is increasing linearly with a delay difference of 80 milliseconds which means that the proposed approach is 80msec faster than the basic approach up to 25 number of nodes.

In a network size of 10 nodes, the delay of the proposed approach is 235 milliseconds and that of the basic approach is 300 milliseconds, therefore, the delay difference of basic and the proposed approach is (300-235) i.e. 65 msec. Similarly, in a network size of 15 nodes, the delay difference is 80 millisecond, therefore, the average delay difference up to 25 number of nodes between basic and the proposed approach is 80 msec (approximately) which is maintained through all the network sizes. Figure 6.3(b) shows the % of message delivery ratio (MDR) over increasing network sizes. The MDR % of both the approaches is decreasing linearly with a difference of 2.50% and is maintained up to network sizes of 25 nodes. The throughput % of the proposed approach outperforms basic approach with a difference of huge % as depicted in Figure 6.3(c). The throughput computed using basic approach (in %) is decreasing with increasing values of the network size while in the proposed approach, it is decreasing up to lower values of the network size and after network size of 15 nodes, it is decreasing at a lower rate as compared to the network size of smaller values.

Figure 6.3(d), Figure 6.3(e) and Figure 6.3(f) present the end-to-end delay, MDR and throughput % for large network sizes respectively. As depicted from the figures, the metrics of the proposed approach are increasing at a constant value after a network size of 600 nodes while the delay and % of MDR and throughput of the basic approach are increasing and decreasing significantly.

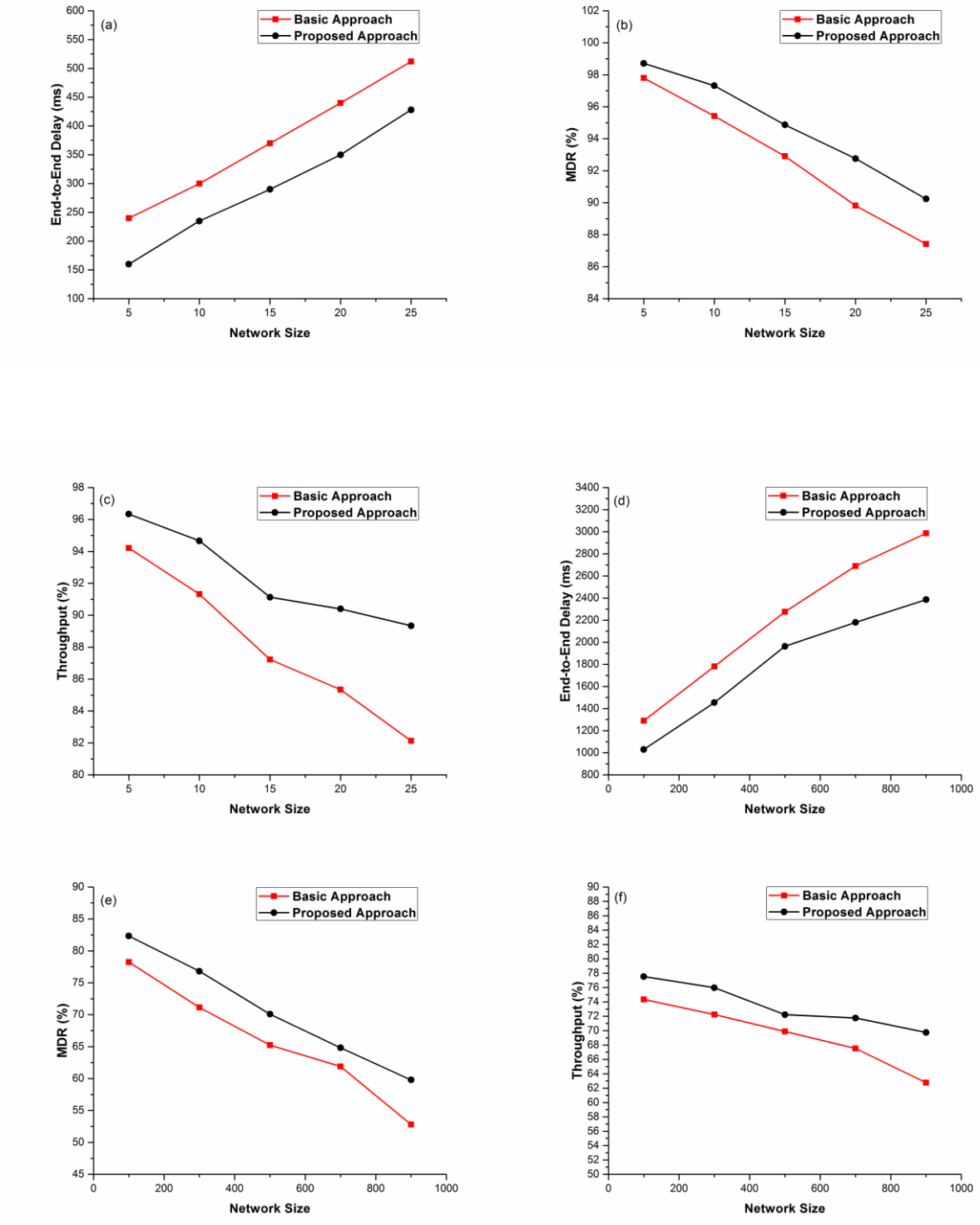


Figure 6.3 The network metrics of both basic and the proposed protocol against scalable network sizes (a) end-to-end delay over small network size (b) MDR % over small network size (c) throughput % over small network size (d) end-to-end delay over large network size (e) MDR % over large network size (f) throughput % over large network size

The proposed approach performs better against basic approach because the proposed mechanism uses Dijkstra's algorithm which has the advantage that it considers the positive weights for path formation and never chose the same path again, however in the case of basic approach, the network metrics are continuously increasing or decreasing up to 900 numbers of nodes because it considers the negative weights and same path again and again for packet transmission which delays the path formation process and affects the metrics in the network.

Case 2: *Network metrics under scalable network sizes in dynamic nature where node are mobile and moving at the speed of 0-25 m/s*

The depicted Figure 6.4(a)-(f) shows the network metrics in dynamic nature where the number of nodes are dynamic in % over all network sizes.

The dynamic environment is changing due to node placement and communication pattern including the packet generation mechanism in mobile topology which every time affects the certain network metrics such as packet delivery ratio and delay of the network. Figure 6.4(a), Figure 6.4(b) and Figure 6.4(c) show the end-to-end delay, % of MDR and throughput over increasing % of mobile nodes respectively. The delay and % of MDR and throughput is increasing and decreasing at a constant rate over small network sizes while the values are almost constant for both basic and the proposed approach in large network sizes. The delay difference and % difference of MDR and throughput of the proposed and basic approach are 594milliseconds, 7.2% and 6.4% respectively which outperforms the basic approach.

Case 3: *Network metrics are measured against black hole and falsification attacks over scalable network sizes*

In this case, the performance of the proposed protocol is measured over various adversary nodes by considering two different scenarios. Scenario-1 presents the metrics results by varying the number of black hole and falsification routing attacks while the validity of the proposed mechanism is scrutinized by increasing the number of black hole and falsification nodes near source and destination over small and large network sizes.

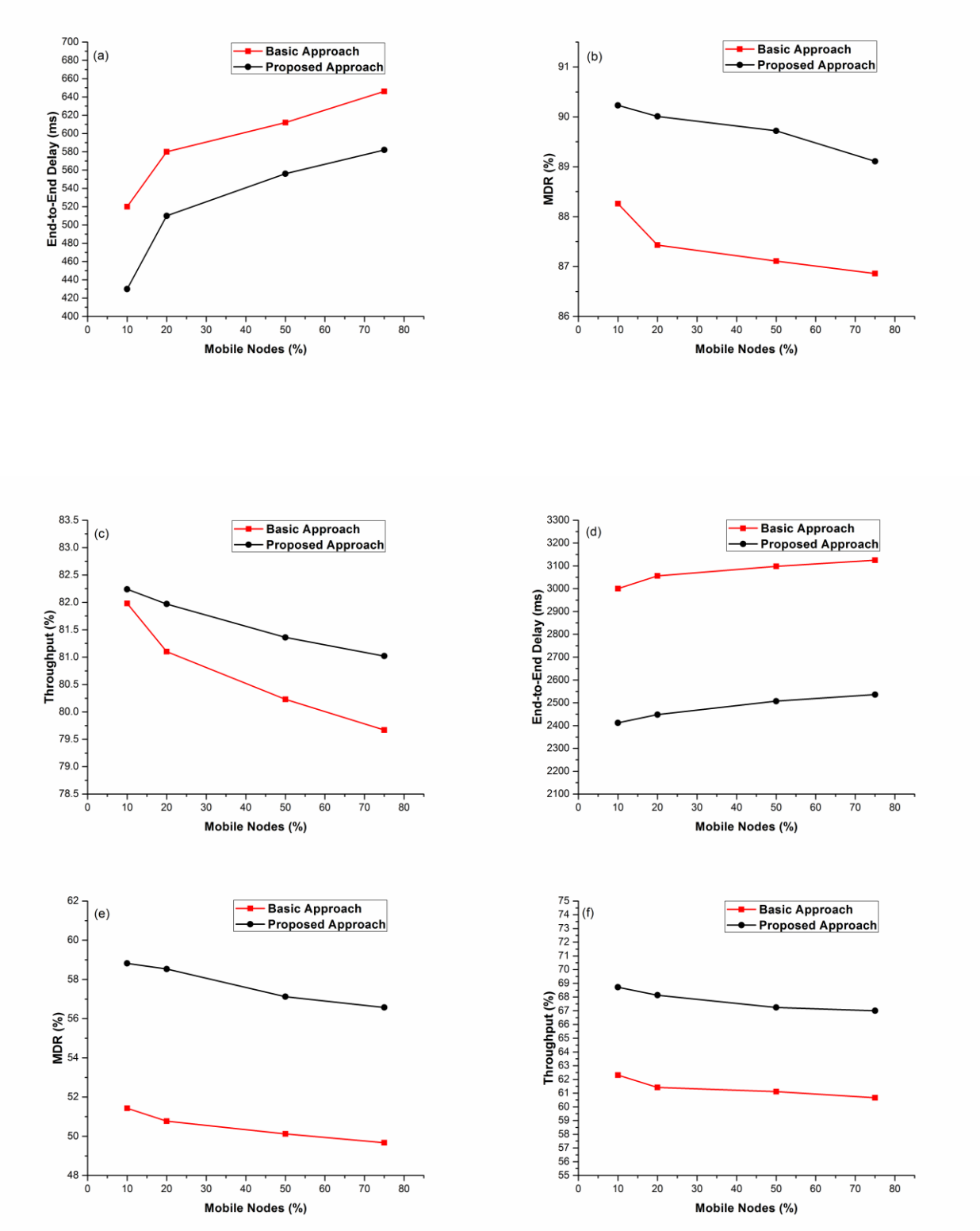
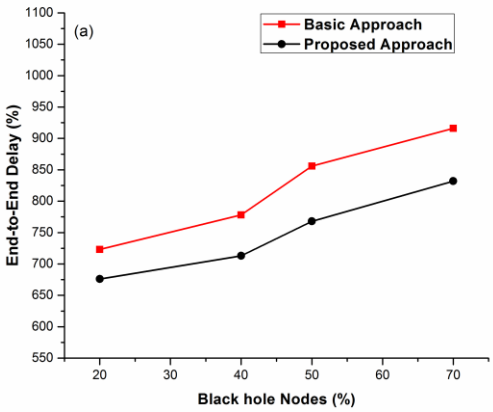
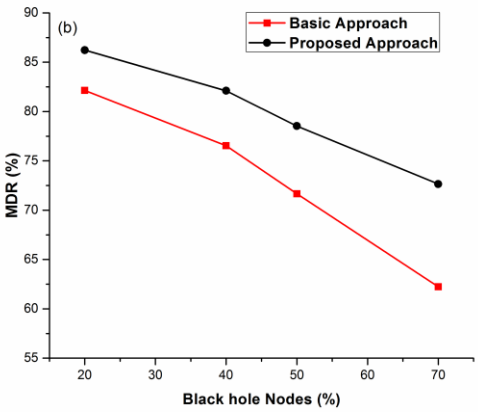
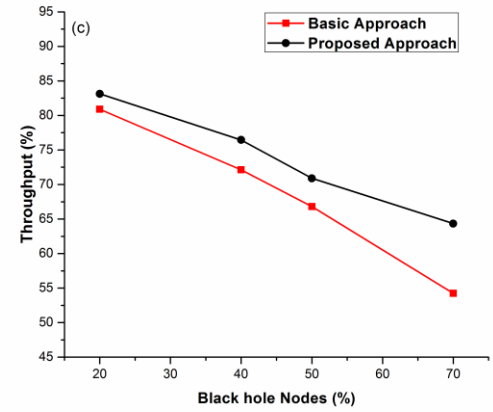
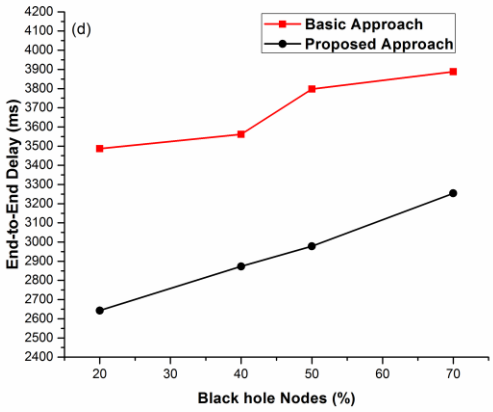


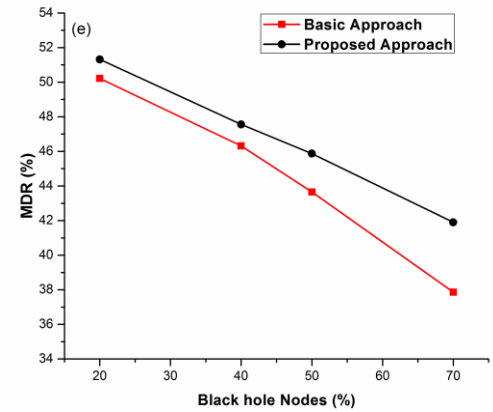
Figure 6.4 Network metrics of basic and the proposed protocol under dynamic nature (a) end-to-end delay over small network size (b) MDR % over small network size (c) throughput % over small network size (d) end-to-end delay over large network size (e) MDR % over large network size (f) throughput % over large network size.

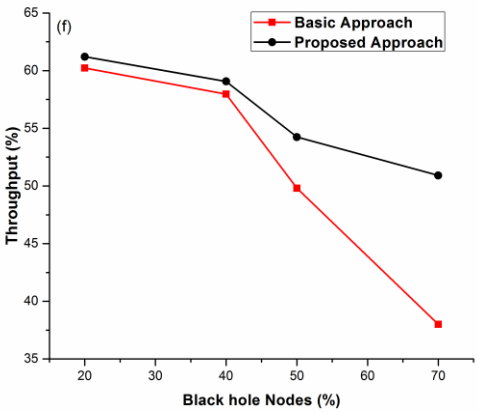

(a)
Basic Approach
Proposed Approach
End-to-End Delay (%)
Black hole Nodes (%)


(b)
Basic Approach
Proposed Approach
MDR (%)
Black hole Nodes (%)


(c)
Basic Approach
Proposed Approach
Throughput (%)
Black hole Nodes (%)


(d)
Basic Approach
Proposed Approach
End-to-End Delay (ms)
Black hole Nodes (%)


(e)
Basic Approach
Proposed Approach
MDR (%)
Black hole Nodes (%)


(f)
Basic Approach
Proposed Approach
Throughput (%)
Black hole Nodes (%)

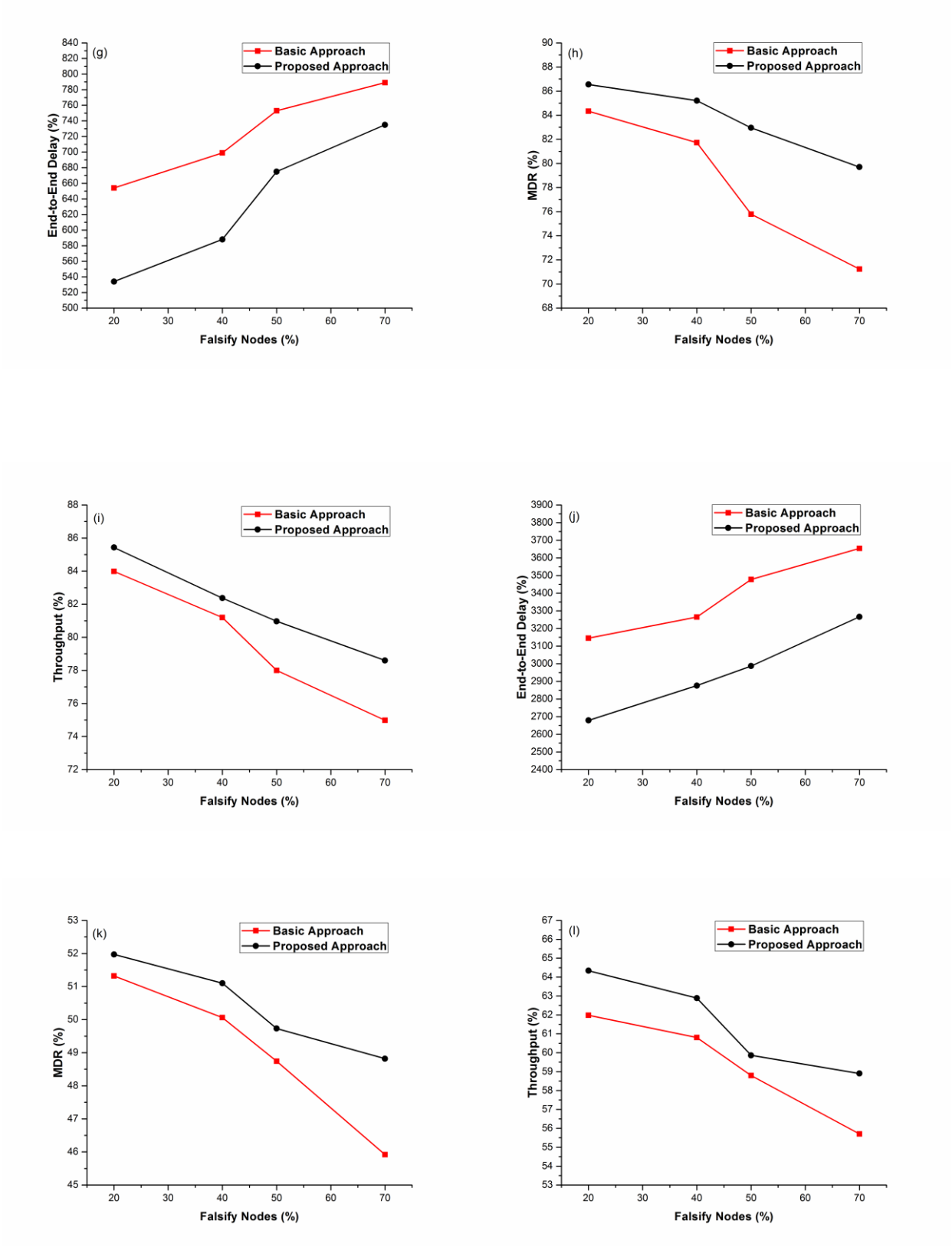


Figure 6.5 Network metrics by increasing the percentage of black hole and falsify attacks over small and large network sizes (a) end-to-end delay over small network size (b) MDR % over small network size (c) throughput % over small network size (d) end-to-end delay over

large network size (e) MDR % over large network size (f) throughput % over large network size.

Scenario-1: *Black hole and Falsification attacks are increasing at different percentage.*

To validate the proposed mechanism, numbers of nodes are increasing at the percentage of 10, 20, 50 and 70 over small and large network sizes under fixed environment. Figure 6.5 (a)-(f) shows the end-to-end delay, MDR % and throughput percentage during black hole attack. By increasing the number of black hole nodes, the proposed approach performs better as compared to the basic approach. The end-to-end delay of black hole and falsification attacks over small network sizes is increasing significantly as depicted in Figure 6.5(a) and Figure 6.5(g) while the MDR and throughput (%) is increasing linearly in both the attacks over small network sizes as depicted in Figure 6.5(b), Figure 6.5(c), Figure 6.5(h) and Figure 6.5(i). In large network sizes, the metrics results are constant after 50% of mobile nodes in the proposed approach while the values are increasing continuously in basic approach.

The good metrics results of the proposed mechanism over basic approach are because the packets are transmitted to only the nodes which are trusted and can securely transfer the packets to their destination nodes but as the number of black hole nodes increase, the basic approach results reduce drastically because firstly it considers negative weights and enters into infinite route formation and secondly the packets are transmitted without any trust value which enhances the chances of performance degradation. Further, Figure 6.5(g)-(*l*) show the results during falsification attack, the chances of falsification attacks during the proposed approach reduce due to their trust values while the basic approach may overcome the attacks through passive acknowledgement and 2-hop information but may increase the time of path formation and packet transmission process. Therefore, the values of the proposed approach are almost flat in large networks. By increasing the % of black hole and falsification attacks, in both fixed and dynamic scenarios, the path recovery and packet transmission timings of basic approach increase because firstly it identifies the attacker through passive acknowledgement process and secondly it applies the recovery process using 2-hop information while the proposed approach never allows the malicious nodes to enter during path formation process.

Scenario-2: *Increasing black hole and falsification nodes near source and sink nodes over small and large network sizes.*

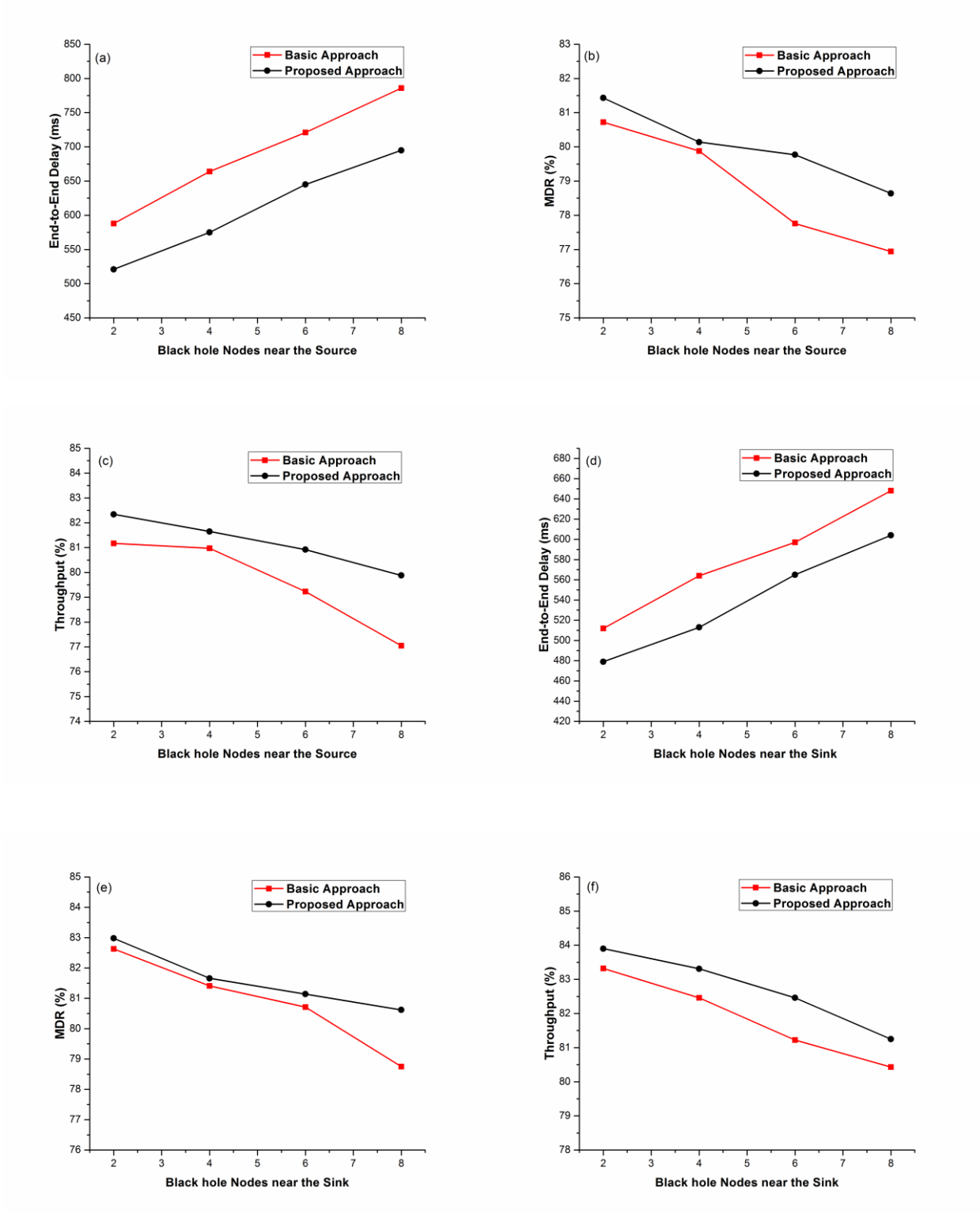


Figure 6.6 Network metrics by increasing the number of black hole and falsify nodes near the source and sink nodes (a) end-to-end delay over small network size (b) MDR % over small network size (c) throughput % over small network size (d) end-to-end delay over large network size (e) MDR % over large network size (f) throughput % over large network size

To deeply understand the proposed phenomenon, the metrics are measured against both the attacks by increasing them near the source and sink nodes. The depicted Figure 6.6(a)-(f) shows the outcomes of network metrics by increasing the adversary nodes near source and sink nodes.

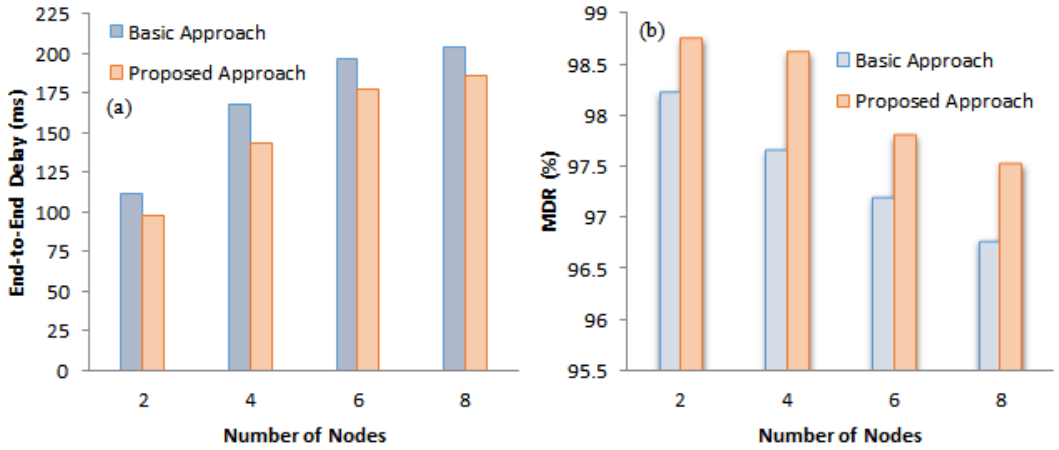


Figure 6.7 Experimental results over increasing number of nodes (a) End-to-End Delay (b) MDR %.

As the numbers of black hole nodes are increasing near the source and sink nodes, the end-to-end delay is increasing but MDR% and percentage of throughput are affected at a constant rate in the proposed mechanism. To validate the approaches, Figure 6.7(a) and Figure 6.7(b) show the experimental results of the proposed and basic approach against end-to-end delay and MDR percentage. The experimental values are same as the values simulated through NS2 simulator. In a network size of 8 nodes, the experimental end-to-end delay of the proposed approach is 186 milliseconds while through NS2 simulator the delay is 190 approximately which is same as experimental result. Similarly, the MDR % of the proposed mechanism is 97.53% through experimental and 97.50% using NS2 simulator. The proposed mechanism significantly reduces the delay because of its fastest path formation process and packet transmission through trust factors. Further, the MDR% of the proposed mechanism also shows better results because of its positive weight computation through SITO optimizer.

6.6 SECURE HANDOFF ROUTING IMPLEMENTATION IN SMART HOME ENVIRONMENTS

The secure routing mechanism is extended over handoff procedures where mesh clients or devices are mobile in nature.

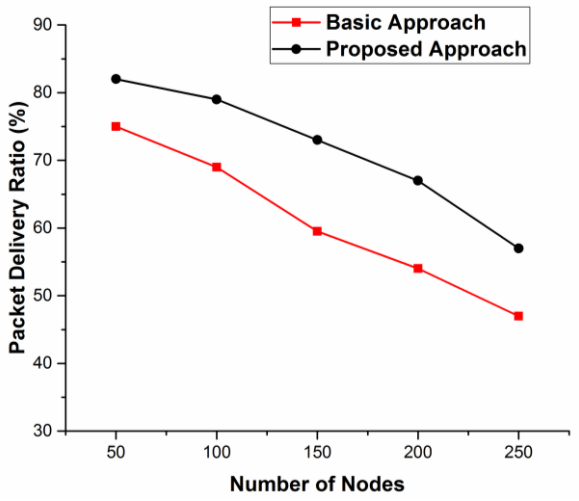


Figure 6.8 Packet delivery ratio

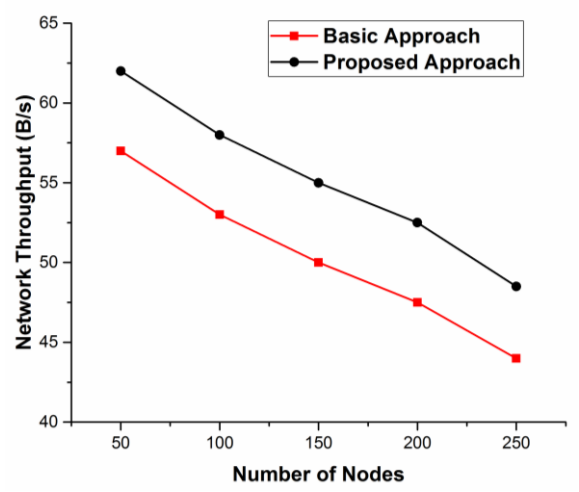


Figure 6.9 Network throughput

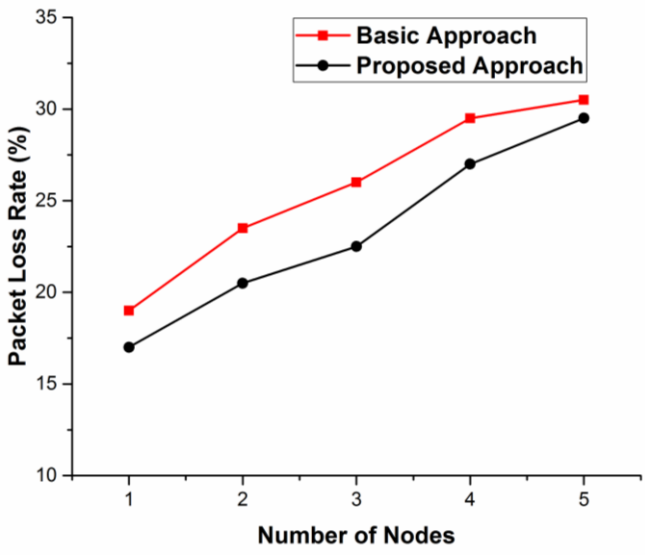


Figure 6.10 Packet loss rate (during black hole)

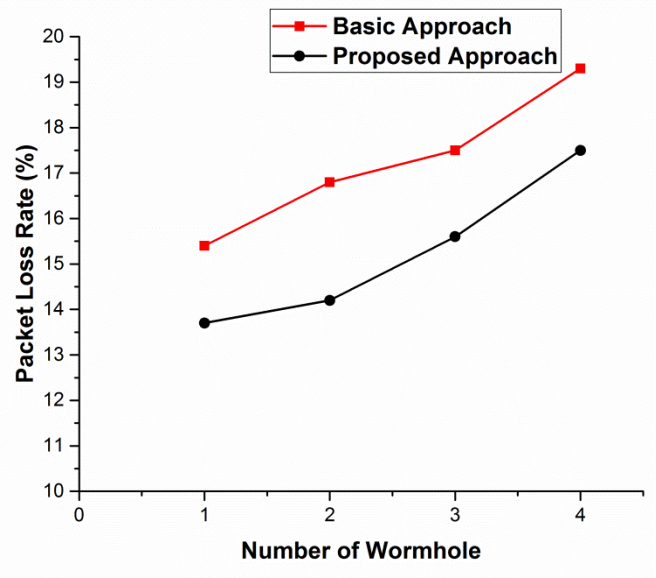


Figure 6.11 Packet loss rate (during wormhole)

During the mobility, the security is checked after authenticating the mesh clients or devices and securely routing their data transmission against a number of routing layer threats. Black hole and data falsification attacks are considered to analyze the proposed mechanism because of their severe malicious characteristics. The proposed mechanism is simulated over NS2 simulator against previously proposed handoff and routing mechanisms by measuring their certain network metrics as depicted in Figure 6.8, 6.9, 6.10 and 6.11 against packet drop ratio, network and packet loss ratio over black hole and wormhole attack.

6.7 CONCLUSION AND FUTURE WORK

In this chapter, the WTR mechanism using SITO optimizer has been exploited to perceive and eliminate the malevolent nodes concerned during the routing path formation and implemented for smart home communication procedures that are based on hierarchical mesh networks. The proposed mechanism has significantly reduced the end-to-end delay and increased the message delivery ratio and throughput percentage in presence of black hole and falsification attacks over small and large network sizes under fixed and dynamic environments. The simulation using NS2 simulator validates the proposed mechanism up to 900 numbers of nodes and illustrates that the proposed mechanism reaches up to a constant level of values against end-to-end delay, message delivery ratio and throughput percentage in comparison of the reported SRPM protocol. In addition to this, we have validated the proposed approach with experimental results at smaller values of the network sizes. However, the energy

consumption in the large network sizes during the packet transmission/reception is a potential issue which will be detailed in future communication.

CHAPTER 7
CONCLUSION AND FUTURE WORK

In this thesis, a ticket based handoff authentication, homomorphic encryption and weight trusted routing (using SITO optimizer) mechanism have been exploited to detect and eliminate the malicious nodes involved during the handoff, message transmission and routing path formation. The proposed ticket based handoff authentication is an efficient technique in terms of authentication delay and secures authentication protocol which is centralized during handoff. The mesh client authenticates itself with its new mesh router by verifying its tickets generated by the Authentication Server. The experimental analysis and empirical study confirm that the proposed protocol outperforms ticket based handoff under different probabilistic scenarios of authentication delay and request delay and is resilient against various attacks. Further, for ensuring the data security during transmission, an algebraic encryption technique is proposed which ensures the security with reduced encryption/decryption time, processing delay and increased throughput. The key idea of the proposed technique is to generate the cipher text message using OR/XOR operations and transmit it with the private key generated by NTRU algorithm. In comparison with existing approaches, the proposed technique reduces the processing delay and encryption/decryption time for different file sizes. Further, the proposed technique is compared in terms of throughput. According to the experimental results, the proposed technique performs better in terms of throughput and processing delay with an efficient level of security. Moreover, the weight trusted routing mechanism for hierarchical mesh networks using Social Impact Theory Optimizer mechanism has been proposed. The proposed mechanism has significantly reduced the packet loss ratio in the presence of black hole and wormhole attacks. Hence, the weight trusted routing mechanism has enhanced the packet delivery ratio and reduced the route discovery, end-to-end delay and packet loss ratio in comparison of reported secure routing mechanism protocol.

The proposed mechanisms have significantly reduced the authentication delay, encryption/decryption time, packet loss ratio and end-to-end delay and have increased the packet delivery ratio and throughput percentage in presence of black hole, worm hole and falsification attacks over small and large network sizes under fixed and dynamic environments.

In order to validate the proposed mechanisms, a commercial NS2 simulator is used consisting of small and large network sizes. Further, the proposed mechanisms are validated by considering a smart home application that is based on mesh architecture. The provided results depicts that the proposed mechanisms reaches up to a constant level of values against end-to-end delay, message delivery ratio and throughput percentage in comparison of reported protocols.

In further studies, the proposed algorithm will be tested under high packet flow and large number of attackers (by considering black hole and wormhole attacks) and then their results will be compared on various performances. However, the energy consumption in the large number of network sizes during the packet transmission/reception is a potential issue which will be reported in future communication. Moreover, each MC joining the network must be provided with a unique key by the AS in order to identify the MC for authentication.

REFERENCES

[1] W.A. Arbaugh, N. Shankar, Y.J. Wan & K. Zhang, "Your 80211 wireless network has no clothes", *IEEE Wireless Communications*, vol. 9, no. 6, pp.44-51, 2002.

[2] A.S.K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET, CRC press, Auerbach publications, Taylor & francis group, U.S.A, 2016.

[3] J. Kamal, "Security based on network topology against the wiretapping attack", *IEEE Wireless Communications*, vol. 11, no. 1, pp. 68-71, 2004.

[4] I.F. Akyildiz & X. Wang, A survey on wireless mesh networks, *IEEE Communications Magazine*, vol. 43, no. 9, pp. 23-30, 2005.

[5] A. Fu, Y. Zhang, Z. Zhu, Q. Jing & J. Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16 m network", *Computers & Security*, vol. 31, no. 6, pp. 741-749, 2012.

[6] J. Baek, E. Hableel, Y.J. Byon, D.S. Wong, K. Jang & H. Yeo, " How to Protect ADS-B: Confidentiality Framework and Efficient Realization Based on Staged Identity-Based Encryption", *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp.690-700, 2017.

[7] X. Du, M. Guizani, Y. Xiao & H.H. Chen, "Two tier secure routing protocol for heterogeneous sensor networks", *IEEE transactions on Wireless Communications*, vol. 6, no. 9, 2007.

[8] G. Karopoulos, G. Kambourakis & S. Gritzalis, "Survey of secure handoff optimization schemes for multimedia services over all-IP wireless heterogeneous networks", *IEEE Communications Surveys and Tutorials*, vol. 9, no. 1-4, pp.18-28, 2007.

[9] F. Guo, Y., Mu, W. Susilo, H. Hsing, D.S. Wong & V. Varadharajan, "Optimized identity-based encryption from bilinear pairing for lightweight devices", *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp.211-220, 2017.

[10] A. Anand, H. Aggarwal & R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks", *Journal of Communications and Networks*, vol. 18, no. 6, pp.938-947, 2016.

[11] R. Jain & S. Routhier, "Packet trains--measurements and a new model for computer network traffic", *IEEE journal on selected areas in Communications*, vol. 4, no. 6, pp.986-995, 1986.

[12] T. Henderson, D. Kotz & I. Abyzov, "The changing usage of a mature campus-wide wireless network", *Computer Networks*, vol. 52, no. 14, pp.2690-2712, 2008.

[13] A. Chaintreau, P.Hui, J.Crowcroft, C.Diot, R. Gass & J. Scott, "Impact of human mobility on opportunistic forwarding algorithms",*IEEE Transactions on Mobile Computing*, vol. 6, no. 6, pp. 606-620, 2007.

[14] F. Han & L. Cheng, "Stochastic user equilibrium model with a tradable credit scheme and application in maximizing network reserve capacity", *Engineering Optimization*, vol. 49, no. 4, pp.549-564, 2017.

[15] M. Boss, H. Elsinger, M. Summer & S. Thurner, "Network topology of the interbank market", *Quantitative Finance*, vol. 4, no. 6, pp.677-684, 2004.

[16] R.J. Ebersole, "Ring bus hub for a star local area network", U.S. Patent No. 4,982,400. 1 Jan., 1991.

[17] E.M. Royer & T. Chai-Keong, "A review of current routing protocols for ad hoc mobile wireless networks", *IEEE Personal Communications*, vol. 6, no. 2, pp. 46-55, 1999.

[18] S. Wang, S.M. Kim, Z. Yin & T. He, "Encode When Necessary: Correlated Network Coding Under Unreliable Wireless Links", *ACM Transactions on Sensor Networks (TOSN)*, vol. 13, no. 1, pp. 1-7, 2017.

[19] B. Daya, “Network security: History, importance, and future”, University of Florida Department of Electrical and Computer Engineering, 2013.

[20] A. Zeng, “Discussion and research of computer network security”, *Journal of Chemical and Pharmaceutical Research*, vol. 6, no. 7, pp. 780-783, 2014.

[21] M. Kumar, B. Ajay & K. Amit, “A Study of wireless Ad-Hoc Network attack and Routing Protocol attack”, *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 2, pp. 22-77, 2012.

[22] S. William, Cryptography and Network Security, 4/E. Pearson Education India, 2006.

[23] A.A. Ahmed & N.A.K. Zaman, “Attack Intention Recognition: A Review”, *International Journal of Network Security*, vol. 19, no. 2, pp.244-250, 2017.

[24] A. Mehmood, M.M. Umar & H. Song, “ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks”, *Ad Hoc Networks*, vol. 55, pp.97-106, 2017.

[25] A.A. Franklin & C.S.R. Murthy, An introduction to wireless mesh networks, Security in Wireless Mesh Networks (book chapter), CRC Press, USA, 2007.

[26] H. Skalli, S. Ghosh, S.K. Das & L. Lenzini, “Channel assignment strategies for multiradio wireless mesh networks: issues and solutions”, *IEEE Communications Magazine*, vol. 45, no. 11, 2007.

[27] M. Kodialam & N. Thyaga, “Characterizing achievable rates in multi-hop wireless mesh networks with orthogonal channels”, *IEEE/ACM Transactions on Networking* (TON), vol. 13, no. 4, pp. 868-880, 2005.

[28] S.M. Ghoreyshi, A. Shahrabi & T. Boutaleb, “Void-Handling Techniques for Routing Protocols in Underwater Sensor Networks: Survey and Challenges”, *IEEE Communications Surveys & Tutorials, 2017*. DOI: 10.1109/COMST.2017.2657881.

[29] J. Jun & L.S. Mihail, “The nominal capacity of wireless mesh networks”, *IEEE Wireless Communications*, vol. 10, no. 5, pp. 8-14, 2003.

[30] R. Behravesh & M. Jahanshahi, “Interference-Aware and Cluster Based Multicast Routing in Multi-Radio Multi-Channel Wireless Mesh Networks”, *Journal of Computer & Robotics*, vol. 10, no. 1, pp.21-30, 2017.

[31] M. Campista & M. Elias, “Routing metrics and protocols for wireless mesh networks”, *IEEE Network*, vol. 22, no. 1, pp. 6-12, 2008.

[32] J. Jun & L.S. Mihail, “MRP: Wireless mesh networks routing protocol”, *Computer Communications*, vol. 31, no. 7, pp. 1413-1435, 2008.

[33] R. Bruno, C. Marco & G. Enrico, “Mesh networks: commodity multi-hop ad hoc networks”, *IEEE Communications Magazine*, vol. 43, no. 3, pp. 123-131, 2005.

[34] S. Lall, B.T.J. Maharaj & P.J. Vuuren, “Null-frequency jamming of a proactive routing protocol in wireless mesh networks”, *Journal of Network and Computer Applications*, vol. 61, pp.133-141, 2016.

[35] Y. Andreopoulos, M. Nicholas & S. Mihaela, “Cross-layer optimized video streaming over wireless multi-hop mesh networks”, *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 11, pp. 2104-2115, 2006.

[36] T.G. Handel & T.S. Maxwell, “Hiding data in the OSI network model”, Information Hiding. Springer Berlin Heidelberg, 1996.

[37] N. Nandiraju & N. Nagesh, “Wireless mesh networks: current challenges and future directions of web-in-the-sky”, *IEEE Wireless Communications*, vol.14, no. 4, pp. 79-89, 2009.

[38] A. Shahzad, M. Lee, C. Lee, N.Xiong, S. Kim, Y.K. Lee, K. Kim, S.M. Woo & G. Jeong, “The protocol design and New approach for SCADA security enhancement during sensors broadcasting system”, *Multimedia Tools and Applications*, vol. 75, no. 22, pp.14641-14668, 2016.

[39] J. Dong, C. Reza & N.R. Cristina, “Secure network coding for wireless mesh networks: Threats, challenges, and directions”, *Computer Communications*, vol. 32, no. 17, pp.1790-1801, 2009.

[40] J. Leu, R. Lai, H. Lin & W. Shih, "Running cellular/PWLAN services: practical considerations for cellular/PWLAN architecture supporting inter operator roaming", *IEEE Communications Magazine*, vol. 44, no 2, pp. 73-84, 2006.

[41] A.D. Wood & J.A. Stankovic, "Denial of service in sensor networks", *IEEE Computer*, vol. 35, no 10, pp. 54-62, 2002.

[42] A. Naveed, S.S. Kanhere & S.K. Jha, "Attacks and security mechanisms", book chapter in: Security in Wireless Mesh Networks, pp. 111-144, Auerbach Publications, CRC Press, USA, 2008.

[43] A. Wood & A.S. John, "Denial of service in sensor networks", *Computer*, vol. 35, no. 10, pp. 54-62, 2002.

[44] C. Karlof & W. David, "Secure routing in wireless sensor networks: Attacks and countermeasures", *Ad hoc networks*, vol. 1, no. 2, pp. 293-315, 2003.

[45] Y.C. Hu, P. Adrian & B.J. David, "Wormhole attacks in wireless networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370-380, 2006.

[46] A. Prathapani, S. Lakshmi & P.A. Dharma, "Detection of black hole attack in a Wireless Mesh Network using intelligent honeypot agents", *The Journal of Supercomputing*, vol. 64, no. 3, pp. 777-804, 2013.

[47] S.B. Sanzgiri, B.N. Dahill, C. Levine & E.M. Belding-Royer, "A secure routing protocol for ad hoc networks", *Proceedings of the 10th IEEE International Conference on Network Protocols* (ICNP'02), Paris, France, pp. 78-87, 2002.

[48] S. Yi, P. Naldurg & R. Kravets, "Security-aware ad hoc routing for wireless networks", in *Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing* (MobiHoc'01), pp. 299-302, Long Beach, CL, USA, 2001.

[49] P. Papadimitratos & Z.J. Haas, "Secure routing for mobile ad hoc networks", *Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference* (CNDS'02), San Antonio, TX, USA, pp. 27-31, 2002.

[50] P. Papadimitratos & Z.J. Hass "Secure link state routing for mobile ad hoc networks", *Proceedings of the Symposium on Applications and the Internet Workshops* (SAINT'03 Workshops), pp. 379-383, Washington DC, USA, 2003.

[51] K. Sharma & G. Shrivastava, "Public Key Infrastructure and Trust of Web Based Knowledge Discovery", *International Journal of Engineering, Science and Management*, vol. 4, no. 1, pp. 56-60, 2007.

[52] A.M. Srivatsa & J. Xie, "A performance study of mobile handoff delay in IEEE 802.11-based wireless mesh networks", *Proceedings of IEEE 1st International Conference on Communications*, Beijing, 19 May, China, pp. 2485-2489, 2008.

[53] L. Xu, Y. He, X. Chen & X. Huang, "Ticket-based handoff authentication for wireless mesh networks", *Computer Networks*, vol. 73, pp. 185-194, 2014.

[54] X. Duan & X. Wang, " Authentication handover and privacy protection in 5G het nets using software-defined networking", *IEEE Communications Magazine*, vol. 53, no. 4, pp.28-35, 2015.

[55] R. Dalal, M. Khatri& Y. Singh, "Authenticity check to provide trusted platform in MANET (ACTP)", *Proceedings of Second International Conference on Computational Science, Engineering and Information Technology*, ACM, New York, 26 Oct., U.S.A., pp. 647-655, 2012.

[56] Q. Jiang, J. Ma, X. Lu & Y. Tian, "An efficient two-factor user authentication scheme with unlink ability for wireless sensor networks", *Journal of Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp.1070-1081, 2015.

[57] F. Abbas & H. Oh, "A step towards user privacy while using location-based services", *Journal of Information Processing Signals*, vol. 10, no. 4, pp.618-627, 2015.

[58] Q. Yan, F.R. Yu, Q. Gong & J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp.602-622, 2016.

[59] H. Zhang, P. Cheng, L. Shi & J. Chen, "Optimal DoS attack scheduling in wireless networked control system", *IEEE Transactions on Control Systems Technology*, vol. 24, no. 3, pp.843-852, 2016.

[60] J. Camenisch, RR. Enderlein & G. Neven, "Two-server password-authenticated secret sharing UC-secure against transient corruptions", *Proceedings of IACR international workshop on public key cryptography*, Springer Berlin Heidelberg, pp. 283-307, 2015.

[61] Q., Jiang, J. Ma, G. Li & L. Yang, "An efficient ticket based authentication protocol with un linkability for wireless access networks", *Wireless Personal Communications*, vol. 77, no. 2, pp.1489-1506, 2014.

[62] A.S. Khan, N. Fisal, Z.A. Bakar, N. Salawu, W. Maqbool, R. Ullah & H. Safdar, "Secure authentication and key management protocols for mobile multi-hopWiMAX networks", *Indian Journal of Science and Technology*, vol. 7, no. 3, pp.282-295, 2014.

[63] P. Jayaraman, R. Lopez, Y. Ohba, M. Parthasarathy & A. Yegin, Protocol for carrying authentication for network access (PANA), Framework. no. RFC 5193, 2008.

[64] Y.M. Tseng, "USIM-based EAP-TLS authentication protocol for wireless local area networks, *Computer Standards & Interfaces*, vol. 31, no. 1, pp.128-136, 2008.

[65] Y.H. Zhang, X.F. Chen, H. Li & J. Cao, "Identity‐based construction for secure and efficient handoff authentication schemes in wireless networks", *Security and Communication Networks*, vol. 5, no. 10, pp.1121-1130, 2012.

[66] C.M. Huang & J.W. Li, "A cluster‐chain‐based context transfer mechanism for fast basic service set transition in the centralized wireless LAN architecture", *Wireless Communications and Mobile Computing*, vol. 9, no. 10, pp. 1387-1401, 2009.

[67] S. Ruj, A. Nayak, I. Stojmenovic, "Pairwise and triple key distribution in wireless sensor networks with applications", *IEEE Transactions on Computers*, vol. 62, no. 11, pp.2224-2237, 2013.

[68] R. Dalal, Y. Singh & M. Khari, "A review on key management schemes in MANET", *International Journal of Distributed and Parallel Systems*, vol. 3, no. 4, pp. 165-172, 2012.

[69] H. Nguyen, P. Trudeau, A. Gupta, R.D. Sands & T.S. Stefanski, Fast roaming in a wireless network using per-STA pairwise master keys shared across participating access points, U.S. Patent 7,873,352, 2011.

[70] A. Fu, Y. Zhang, Z. Zhu & X. Liu, X., "A fast handover authentication mechanism based on ticket for IEEE 802.16m", *IEEE Communications Letters*, vol. 14, no. 12, pp.1134-1136, 2010.

[71] A. Fu, Y. Zhang, Z. Zhu, Q. Jing & J. Feng, "An efficient handover authentication scheme with privacy preservation for IEEE 802.16 m network", *Computers & Security*, vol. 31, no. 6, pp.741-749, 2012.

[72] J. Li, X. Chen, M. Li, J. Li, P.P. Lee & W. Lou, " Secure de-duplication with efficient and reliable convergent key management", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp.1615-1625, 2014.

[73] G. Pierson & J. DeHaan, Network security and fraud detection system and method. U.S. Patent 9,203,837, 2015.

[74] C.W. Lee, "Security in Wireless Mesh Networks", Wireless Network Security. Springer Berlin Heidelberg, pp. 229-246, 2013.

[75] S. Mukherjee, G. Sanyal, C. Koner, "A Novel Approach for Authentication Technique in Wireless Sensor Network", *International Journal of Communication and Networking System*, vol. 2 no. 1, 2013.

[76] S. Ravichandran, "Secured identity based approach with privacy preservation for wireless mesh networks", *International Journal of Communication and Networking System*, vol. 1, no. 2, 2012.

[77] L. Daniel, "Multi-level encryption access point for wireless network", U.S. Patent No. 6,526,506. 25 Feb. 2003.

[78] S.R. Radia. & Y.K. Elley, "Content screening with end-to-end encryption", U.S. Patent No. 6,636,838. 21 Oct. 2003.

[79] P. Narula, "Security in mobile ad-hoc networks using soft encryption and trust-based multi-path routing", *Computer Communications*, vol. 31, no.4, pp. 760-769, 2008.

[80] B. Dan & M. Franklin, "Identity-based encryption from the Weil pairing", Advances in Cryptology—CRYPTO 2001. Springer Berlin Heidelberg, 2001.

[81] X. Zhang, L. Guangsong & H. Wenbao, "Ticket-Based Authentication for Fast Handover in Wireless Mesh Networks", *Wireless Personal Communications*, vol. 85, no.3, pp. 1509-1523, 2015.

[82] J. Hoffstein, P. Jill & H. Joseph, "NTRU: A ring-based public key cryptosystem", Algorithmic number theory. Springer Berlin Heidelberg, pp. 267-288, 1988.

[83] Y. Li, X. Cui, L. Hu & Y. Shen, "Efficient security transmission protocol with identity-based encryption in wireless mesh networks", *IEEE International Conference on High Performance Computing and Simulation* (HPCS), 2010.

[84] L. Edward, P. Joseph, K.L. green, L.E. Riblett & J.M. Wisemanl, "Encryption in mobile wireless mesh networks", *IEEE International Carnahan Conference on Security Technology* (ICCST), 2012.

[85] V.D. Marten, "Fully homomorphic encryption over the integers", Advances in cryptology EUROCRYPT, Springer Berlin Heidelberg, pp.24-43, 2010.

[86] D. Boneh & M. Franklin, "Identity-based encryption from the Weil pairing", *SIAM Journal on Computing*, vol. 32 no.3, pp.586-615, 2003.

[87] I.S. Amiri, "Cryptography s cheme of an optic al switching system using pico/femto second soliton pulse", *International Journal of Advances in Engineering Technology* (IJAET), vol. 5. No. 1, pp. 176-184, 2012.

[88] Y. Mote, N. Paritosh & G. Shekhar, "Superior Security Data Encryption Algorithm (NTRU)", *International Journal of Engineering Sciences*, vol. 6, 2012.

[89] D. Van, J. Marten, "Fully homomorphic encryption over the integers", Advances in cryptology EUROCRYPT Springer Berlin Heidelberg, pp. 24-43, 2010.

[90] C. Gentry, H. Shai & P.S. Nigel, "Fully homomorphic encryption with polylog overhead", Advances in Cryptology EUROCRYPT, Springer Berlin Heidelberg, pp. 465- 482, 2012.

[91] R.H. Jhaveri & N.M. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks," *International Journal of Communication Systems*, vol. 30, no. 7, pp.1-24, 2017.

[92] N. Bendimerad & B. Kechar, B. "Rotational wireless video sensor networks with obstacle avoidance capability for improving disaster area coverage," *Journal of Information Processing Systems*, vol. 11, no. 4, pp. 509-527, 2015.

[93] S. Lu, L. Li, Y.K. Lam & L. Jia, "SAODV: A MANET routing protocol that can withstand black hole attack," *Proceedings of International Conference on Computational Intelligence and Security*, Beijing, China, pp. 421-425, 2009.

[94] C. Li, Z. Wang & C. Yang, "SEAODV: A security enhanced aodv routing protocol for wireless mesh networks," *Transactions on computational science*, XI Springer Berlin Heidelberg, pp. 1-16, 2010.

[95] I.D. Chakeres & E.M. Belding-Royer, "AODV routing protocol implementation design", *Proceedings of 24th International Conference on Distributed Computing Systems Workshops*, Tokyo, Japan, pp. 698-703, 2004.

[96] S. Choi, D.Y. Kim, D.H. Lee & J.I. Jung, J. I. "WAP: wormhole attack prevention algorithm in mobile ad hoc networks," *Proceedings of IEEE International Conference on Ubiquitous and Trustworthy Computing Sensor Networks*, SUTC, pp. 343-348, 2008.

[97] N.K. Chaitanya & S. Varadarajan, "An Implementation of Adaptive Multipath Routing Algorithm for congestion control", *International Journal of Computer Science and Network Security* (IJCSNS), vol. 16, no. 2, pp. 1-6, 2016.

[98] F. Abbas & H. Oh, "A step towards user privacy while using location-based services",*Journal of Information Processing Systems*, vol. 10, no. 4, pp. 618-627, 2014.

[99] M. Kaliappan & B. Paramasivan, "Enhancing secure routing in mobile ad hoc Networks using a Dynamic Bayesian Signalling Game model", *Computers& Electrical Engineering*, vol. 41, 301-313, 2015.

[100] H. Simaremare, A. Abouaissa, R.F. Sari & P. Lorenz, "Secure aodv routing protocol based on trust mechanism", *Wireless Networks and Security*, Springer Berlin Heidelberg, pp. 81-105, 2013.

[101] X. Wang, L. Liu & J. Su, "RLM: A general model for trust representation and aggregation", *IEEE Transactions on Services Computing*, vol. 5, no. 1, pp. 131-143, 2012.

[102] S. Konwar, A.B. Paul, S. Nandi & S. Biswas, "MCDM based trust model for secure routing in wireless mesh networks," *Proceedings of World Congress on Information and Communication Technologies* (WICT), Mumbai, INDIA, pp. 910-915, 2011.

[103] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler & D. Raffo, D, "Securing the OLSR protocol",*Proceedings of Med-Hoc-Net*, 25-27, 2003.

[104] D.W. Kum, J.S. Park, Y.Z. Cho & B.Y. Cheon, "Performance evaluation of AODV and DYMO routing protocols in MANET", *Proceedings of 7th IEEE Consumer Communications and Networking Conference* (CCNC), Las Vegas, USA, 2010.

[105] C. Perkins, E. Belding-Royer & S. Das, S, "Ad hoc on-demand distance vector (AODV) routing," (No. RFC 3561), 2003.

[106] M.S. Obaidat, I. Woungang, S.K. Dhurandher & V. Koo, "A cryptography ‐ based protocol against packet dropping and message tampering attacks on mobile ad hoc networks", *Security and Communication Networks*, vol. 7, no. 2, pp. 376-384, 2014.

[107] I. Woungang, S.K. Dhurandher, M.S. Obaidat & R.D. Peddi. " A DSR-based routing protocol for mitigating black hole attacks on mobile ad hoc networks", *Journal of Security and Communication Networks*, Wiley, vol. 9, no. 5, pp. 420-428, 2016.

[108] S. Smaoui, M.S. Obaidat, F. Zarai & K.F. Hsiao, "A new secure and efficient scheme for network mobility management", *Journal of Security and Communications Networks*, Wiley, vol. 8, no. 7, pp. 1360-1377, 2015.

[109] S. Mir, A.A. Pirzada & M. Portmann, "HOVER: Hybrid on-demand distance vector routing for wireless mesh networks", *Proceedings of the thirty-first Australasian conference on Computer science*, Australian Computer Society, Inc, 74, pp. 63-71, 2008.

[110] A. Neumann, E. Lopez, L. Cerda-Alabern & L. Navarro, "Securely-entrusted multi-topology routing for community networks", *Proceedings of 2016 12th Annual Conference on Wireless On-demand Network Systems and Services* (WONS), Italy, pp. 1-8, 2016.

[111] S.H. Talawar & C.H. Ramesh, "A protocol for end-to-end key establishment during route discovery in MANETs", *Proceedings of 29th International Conference on Advanced Information Networking and Applications* (AINA), Gwangju, Korea, pp. 176-184, 2014.

[112] Y.I. Saavedra, J. Ben-Othman & J.P. Claude, "Performance evaluation of security mechanisms in RAOLSR protocol for wireless mesh networks", *Proceedings on IEEE International Conference on Communications* (ICC), Sydney, Australia, pp. 1808-1812, 2014.

[113] M.M. Sbeiti & C. Wietfeld, "One stone two birds: On the security and routing in wireless mesh networks," *Proceedings of IEEE Wireless Communications and Networking Conference* (WCNC), Istanbul, Turkey, 2486-2491, 2014.

[114] S. Khan, K.K Loo, N. Mast & T. Naeem, "SRPM: secure routing protocol for IEEE 802.11 infrastructure-based wireless mesh networks," *Springer Journal of Network and Systems Management*, vol. 18, no. 2, pp. 190-209, 2010.

[115] S. Khan, N.A. Alrajeh & K.K Loo. "Secure route selection in wireless mesh networks," *Computer Networks*, Vol. 56, no. 2, pp.491-503, 2012.

[116] M. Tommiska & S. Jorma, "Dijkstra's shortest path routing algorithm in reconfigurable hardware," Field-Programmable Logic and Applications, Springer Berlin Heidelberg, 2001.

[117] M. Martin & L. Lhotska, Social impact theory based optimizer Advances in Artificial Life, Springer Berlin Heidelberg. pp. 635-644, 2007.

[118] L.C.D. Silva, C. Morikawa & I.M. Petra I.M. "State of the art of smart home", *Engineering Applications of Artificial Intelligence*, vol. 25, no. 7, pp. 1313-1321, 2012.

[119] J. Coutaz & J.L. Crowley, "A first-person experience with end-user development for smart homes", *IEEE Pervasive Computing*, vol. 15, no. 2, pp. 26-39, 2016.

[120] J. Domaszewicz. S. Lalis, A. Pruszkowski, M. Koutsoubelias, T. Tajmajer, N. Grigoropoulos, M. Nati & A. Gluhak, "Soft actuation: smart home and office with human-in-the-loop", *IEEE Pervasive Computing*, vol. 15, no. 1, pp. 48-56, 2016.

[121] S. Namasudra S. & P. Roy "Size based access control model in cloud computing", *Proceedings of the IEEE International Conference on Electrical, Electronics, Signals, Communication and Optimization*, Visakhapatnam, India, pp. 1-4, 2015.

[122] I. Gopalakrishnan, Wireless Mesh Routing in Smart Utility Networks. Ph.D. Thesis, Auburn University, 2011.

[123] S. Namasudra, S. Nath & A. Majumder "Profile based access control model in cloud computing environment", *Proceedings of IEEE International Conference on Green Computing, Communication and Electrical Engineering*, Coimbatore, India, pp. 1-5, 2014.

[124] C. Garzon, M. Camelo, P. Vila & Y. Donoso, "A multi-objective routing algorithm for wireless mesh network in a smart cities environment", *Journal of Networks*, vol. 10, no. 1, pp. 60-69, 2014.

[125] G. Iyer, P. Agrawal & R.S. Cardozo, "Performance comparison of routing protocols over smart utility networks: A simulation study", *Proceedings of IEEE Globecom Workshops* (GC Workshops), Atlanta, GA, pp. 969-973, 2013.

[126] A. Majumder, S. Namasudra & S. Nath "Taxonomy and classification of access control models for cloud environments", Continued Rise of the Cloud, Springer, London, pp. 23-53, 2014.

[127] T.D.P. Mendes, R. Godina, E.M.G. Rodrigues, J.C.O. Matias & J.P.S. Catalao "Smart home communication technologies and applications: Wireless protocol assessment for home area network resources", *Energies*, vol. 8, no. 7, pp. 7279-7311, 2015.

[128] S. Namasudra, P. Roy, P. Vijayakumar, S. Audithan & B. Balamurugan "Time efficient secure DNA based access control model for cloud computing environment", *Future Generation Computer Systems*, 2017, DOI: http://dx.doi.org/10.1016/j. future.2017.01.017.

[129] S.U. Rehman & S. Manickam. "A study of smart home environment and its security threats", *International Journal of Reliability, Quality and Safety Engineering*, vol. 23, no. 3, pp. 1-9, 2016.

[130] G. Iyer, P. Agrawal & R.S. Cardozo, "Analytic model and simulation study for network scalability in smart utility networks", *Proceedings of IEEE Innovative Smart Grid Technologies-Asia* (ISGT Asia), Bangalore, INDIA, pp. 1-6, 2013.

[131] S. Namasudra & P. Roy "Secure and efficient data access control in cloud computing environment: a survey", *Multiagent and Grid Systems-An International Journal*, vol. 12, no. 2, pp. 69-90, 2016.

[132] S. Bala, G. Sharma & A.K. Verma, "PF-ID-2PAKA: Pairing free identity-based two-party authenticated key agreement protocol for wireless sensor networks", *Wireless Personal Communications*, vol. 87, no. 3, pp. 995-1012, 2016.

[133] X. Anita, M.A. Bhagyaveni & J.M.L. Manickam, "Collaborative lightweight trust management scheme for wireless sensor networks", *Wireless Personal Communications*, vol. 80, no. 1, pp. 117-140, 2015.

[134] N. Labraoui, M. Gueroui & L. Sekhri, "A risk-aware reputation-based trust management in wireless sensor networks", *Wireless Personal Communications*, vol. 87, no. 3, pp. 1037-1055, 2016.

[135] C. Xi, S. Liang, M.A. Jian & M.A. Zhuo, "A trust management scheme based on behavior feedback for opportunistic networks", *China Communications*, vol. 12, no. 4, pp.117-129, 2015.

[136] C.A. Kerrache, C.T. Calafate, J.C. Cano, N. Lagraa & P. Manzoni, P. "Trust management for Vehicular Networks: An Adversary-Oriented Overview", *IEEE Access*, vol. 4, pp.1-15, 2016.

[137] S. Namasudra & P. Roy, "A new secure authentication scheme for cloud computing environment," *Concurrency and Computation: Practice and Exercise*, 2016, DOI: 10.1002/cpe.3864.

[138] S. Namasudra & P. Roy "A new table based protocol for data accessing in cloud computing", *Journal of Information Science and Engineering*, vol. 33, no. 3, pp.585-609, 2017.

[139] G. Rathee & H. Saini, "Weight trusted routing mechanism for hierarchical mesh environments", *International Journal of Distributed Systems and Technologies* (IJDST), vol. 8, no. 3, 2016. (accepted).

[140] S. Salima, M.S. Obaidat, F. Zarai & K.F. Hsiao, "A new secure and efficient scheme for network mobility management", *Journal of Security and Communications Networks*, vol. 8, no. 7, pp. 1360-1377, 2015.

[141] L. Sun, R. Pinyi, D. Qinghe & W. Yichen, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks", *IEEE Transactions on Industrial informatics*, vol. 12, no. 1, pp. 291-300, 2016.

[142] S. Sultana, G. Ghinita, E. Bertino & M. Shehab, "A lightweight secure scheme for detecting provenance forgery and packet drop attacks in wireless sensor networks", *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 3, pp. 256-269, 2015.

[143] M. Boushaba, A. Hafid & M. Gendreau, "Source-based routing in wireless mesh networks", *IEEE Systems Journal*, vol. 10, no. 1, pp. 262-270, 2016.

[144] Y.I.S. Benitez, O.J. Ben & J.P. Claude, "Performance evaluation of security mechanisms in RAOLSR protocol for wireless mesh networks". *Proceedings of IEEE International Conference on Communications* (ICC), Sydney, Australia, 1808-181, 2014.

[145] H. Wang, K. Chin & S. Soh, "On minimizing data forwarding schedule in multi transmit/receive wireless mesh networks", *IEEE Access*, vol. 4, pp. 1570-1582, 2016.

[146] A. Darehshoorzadeh, G. Robson & B. Azedine, "Towards a comprehensive model for performance analysis of opportunistic routing in wireless mesh networks", *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp.5424-5438, 2015.

[147] M.R. Babu & G. Usha, "A Novel Honey pot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET", *Wireless Personal Communications*, vol. 90, no. 20, pp. 831-845, 2016.

[148] T. Poongodi & M. Karthikeyan, "Localized secure routing architecture against Cooperative Black Hole Attack in Mobile Ad Hoc Networks", *Wireless Personal Communications*, vol. 90, no. 2, pp. 1039-1050, 2016.

[149] M. Macas & L. Lhotska, L. Social impact theory based optimizer Advances in Artificial Life. Springer Berlin Heidelberg, 635-644, 2007.

[150] T. Matti & S. Jorma, "Dijkstra's shortest path routing algorithm in reconfigurable hardware", *Proceedings of 11th international conference on Field-Programmable Logic and Applications*, Belfast, Northern Ireland, UK, 653-657, 2001

LIST OF PUBLICATIONS

Published Journal Papers

1. G. Rathee and H. Saini. "Modified AODV (MAODV) Against Black Hole in WMN", *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, DOI: 10.1007/s40010-017-0399-9.*
   [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

2. G. Rathee and H. Saini. "Aspects of Trusted Routing Communication in Smart Networks*", Wireless Personnel Communication, pp. 1-21.*
   [Major indexing: SCIE, SCOPUS, SCI mago, Google scholar, ACM digital Library]

3. G. Rathee and H. Saini. "Secure Modified Ad-hoc On-demand Distance Vector (MAODV) Routing Protocol", *International Journal of Mobile Computing and Multimedia Communications*, vol. 8, no. 1, pp. 1-18, 2017
   [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

4. G. Rathee and H. Saini. "A Secure Buffer based Routing Protocol (SBRP) for WMN", *International Journal of Business Data Communications and Networking,* vol. 13, no. 1, pp. 28-44, 2017.
   [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

5. G. Rathee and H. Saini. "Secure Handoff Technique with Reduced Authentication Delay in Wireless Mesh Network", *International Journal of Advanced Intelligence Paradigms* (in press).
   [Major indexing: SCOPUS (Elsevier), DBLP, ACM Digital Library, Academic OneFile (Gale), Educational Research Abstracts]. Online link: http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=ijaip

6. G. Rathee and H. Saini. "End-to-End Encryption by Algebraic OR/XOR", *International Journal of Control Theory and Applications*, vol. 9, no. 10, pp. 4819-4831, 2016.
   [Major indexing: SCOPUS, EBSCOhost].

7. G. Rathee and H. Saini. "A Secure Multicast Routing Protocol against Gray Hole Attack", *APRN Journal of Engineering and Applied Sciences*, vol. 11, no. 21, pp. 1-8, 2016.
   [Major indexing: SCOPUS, DBLP, Google scholar].

8. G. Rathee and H. Saini. "Security Concerns with Open Research Issues of Present Computer Network", *International Journal of Computer Science and Information Security,* vol. 14, no. 4, pp.406-432, 2016.
   [Major indexing: ESCI, IP & Science, Thomson Reuter, Web of Science].

9. G. Rathee and H. Saini. "Efficient Handoff Routing (EHR) in WMN", *International Journal of Computer Applications,* vol. 1, pp. 29-34, August 2016.
   [Major indexing: Google scholar, Proquest, EBSCO.]

10. G. Rathee and H. Saini. "Weight Trusted Routing Mechanism for Hierarchical Mesh Environments", *International Journal of Distributed Systems and Technologies*. vol. 8, no. 3, pp. 25-42, 2017.

    [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

11. G. Rathee and H. Saini. "Authentication through Elliptic Curve Cryptography (ECC) Technique in WMN", *International Journal of Information Security and Processing*, vol. 12, no. 1, pp. 42-52, 2017.
    [Major indexing: SCOPUS, ESCI, DBLP, ACM digital Library, web of sciences, Google scholar].

Published Book Chapters

12. G. Rathee and H. Saini (2016), "Mitigation Techniques for Gray Hole and Black Hole Attacks in Wireless Mesh Network", Proceedings of the International Congress on Information and Communication Technology, Springer, Singapore, pp. 383-392.
    [Major indexing: SCOPUS, DBLP, Google scholar].

13. G. Rathee, H. Saini and S.P. Ghrera (2016), "Secured Authentication and Signature Routing Protocol for WMN (SASR)", Proceedings of the Second International Conference on Computer and Communication Technologies, Springer, USA, pp. 327-336.
    [Major indexing: SCOPUS, DBLP, Google scholar].

14. G. Rathee and H. Saini (2016), "A Secure Homomorphic Routing Technique in Wireless Mesh Network (HRT for WMN)", Information Systems Design and Intelligent Applications, Springer, USA, pp. 437-444.
    [Major indexing: SCOPUS, DBLP, Google scholar].

Published Conference Proceedings

15. G. Rathee and H. Saini (2016), "A Fast Handoff Technique in Wireless Mesh Network (FHT for WMN)", *Procedia Computer Science*, vol. 79, pp.722-728.
    [Major indexing: SCOPUS, Conference Proceedings Citation Index].

16. G. Rathee and H. Saini (2015), "On Reduced Computational Cost, Efficient and Secure Routing (ESR) for Wireless Mesh Network", *Procedia Computer Science*, vol. 58, pp.333-34.
    [Major indexing: SCOPUS, Conference Proceedings Citation Index].

Communicated Journal Papers

17. *G. Rathee* and H. Saini. "Reduced Handoff Authentication Technique in Wireless Mesh Network", *Frontier of Information Technology and Electronic Engineering* (communicated)
[Major indexing: SCIE, SCOPUS, SCI mago, Google scholar, ACM digital Library].

18. G. Rathee and H. Saini. "Implementation of Secure Handoff Routing in Smart Home Environments", *Wireless Networks* (communicated)
[Major indexing: SCIE, SCOPUS, SCI mago, Google scholar, ACM digital Library].

Candidate's Signature

BIBLIOGRAPHY

GEETANJALI
Email id: geetanjali@juit.ac.in, geetanjali.rathee123@gmail.com
Mobile: (+91) 9736248186

PROFESSIONAL QUALIFICATION

Qualification	University / Institution	Duration (Year)	% Aggregate/C.G.P.A.
Ph.D. (Pursuing)	Jaypee University of Information Technology, Waknaghat	From July 2014	-
M. Tech.	Jaypee University of Information Technology, Waknaghat	2012-14	9.0
B. Tech.	BMIET, M D University	2007-11	78.56
HSC	Central Board of Secondary Education	2006-07	70.1
SC	Central Board of Secondary Education	2004-05	80.12

LIST OF PUBLICATIONS

1. **Geetanjali Rathee**, Hemraj Saini, "Secure Handoff Technique with Reduced Authentication Delay in Wireless Mesh Network", International Journal of Advanced Intelligence Paradigms, Inderscience (in production).
   *[Major indexing: **SCOPUS (Elsevier)**, Academic OneFile (Gale), ACM Digital Library, DBLP Computer Science Bibliography, Educational Research Abstracts]*
2. **Geetanjali Rathee**, Hemraj Saini, "Authentication through Elliptic Curve Cryptography (ECC) technique in WMN", International Journal of Information Security and Privacy", **IGI Global** (in production).
   *[Indexed: **SCOPUS**, DBLP, Thomson Reuters]*
3. **Geetanjali Rathee**, Hemraj Saini, "End to End Encryption by Algebraic OR/XOR", International Journal of Control Theory and Applications, vol. 9, no.10 , pp. 4819-4831, 2016.
   *[Major indexing: **SCOPUS**, DBLP, Google scholar]*

4. **Geetanjali Rathee**, Hemraj Saini, "Security Concerns with Open Research Issues of Present Computer Network", International Journal of Computer Science and Information Security, vol. 14, no. 4, p.406-432, 2016.
*[Major indexing: **ESCI - IP & Science** - Thomson Reuters - Web of Science]*

5. **Geetanjali Rathee**, Hemraj Saini, "A Secure Multicast Routing Protocol Against Gray Hole Attack", APRN Journal of Engineering and Applied Sciences, vol. 11, no. 21, pp. 1-9, 2016.
*[Major indexing: **SCOPUS**, DBLP, Google scholar]*

6. Pardeep Kumar, Kalyani, Ekta Gupta, **Geetanjali Rathee** and Durg Singh Chauhan, "Mood Swing Analyzer: A dynamic Sentiment Detection Approach", National Academy of Sciences, Springer, vol. 85, no. 1, pp. 149-157, 2015.
*[Indexed: **SCI**, **SCOPUS,** DBLP]*

7. **Geetanjali Rathee**, Hemraj Saini and S.P. Ghrera, 2016. Secured Authentication and Signature Routing Protocol for WMN (SASR). Proceedings of the Second International Conference on Computer and Communication Technologies, Springer, India, pp. 327-336.
*[Major indexing: **SCOPUS**, DBLP, Google scholar]*

8. **Geetanjali Rathee**, Hemraj Saini, 2016. A Secure Homomorphic Routing Technique in Wireless Mesh Network (HRT for WMN). Information Systems Design and Intelligent Applications, Springer India, pp. 437-444.
*[Major indexing: **SCOPUS**, DBLP, Google scholar]*

9. **Geetanjali Rathee,** Hemraj Saini, "On Reduced computational cost, Efficient and secure Routing (ESR) for Wireless Mesh Network", Second International Symposium on computer vision and internet in journal of **Elsevier**, Journal of Procedia Computer Science (Science Direct), Kochi, Kerala, June 2015, vol. 58, pp. 333-341.
[*Indexed: **SCOPUS**, DBLP]*

10. **Geetanjali Rathee**, Hemraj Saini, "Mitigation Techniques for Gray Hole and Black Hole Attacks in Wireless Mesh Network", International congress on Information and Communication Technology (ICICT), Udaipur, ASIC series of Springer, pp. 383-392, 2015.
[Indexed: SCOPUS, DBLP]

11. **Geetanjali Rathee**, Hemraj Saini, "Fast Handoff Technique in Wireless Mesh Network (FHT in WMN)", 7th international conference in computing, communication and virtualization, Journal of Procedia Computer Science (Science Direct), Mumbai, INDIA, vol. 79, pp. 722-728, 2016.
[Indexed: SCOPUS, DBLP]

12. **Geetanjali Rathee**, Ninni Singh, Hemraj Saini, "Efficient Shortest path Protocol Routing Algorithm for Multicasting in WMN Algorithm", International Journal of Wireless Network and Broadband Technology(IJWNBT 2014), vol. 6, no. 1, pp. 111-115, 2014.
[Indexed: DBLP, Google scholar, EBSCO, ProQuest]

13. **Geetanjali Rathee**, Hemraj Saini, "Efficient Handoff Routing (EHR) in WMN", International Journal of Computer Applications, vol. 1, pp. 29-34, August 2016.

[Major indexing: EBSCO, Google Scholar, Informatics, ProQuest CSA Technology Research Database, NASA]

14. **Geetanjali Rathee**, Prabhat Thakur, Ghanshyam Singh and Hemraj Saini, "Aspects of secure communication during spectrum handoff in cognitive radio networks", IEEE International Conference on Signal Processing and Communications,28-29Dec, 2016, Noida, INDIA.
[Major indexing: SCOPUS, DBLP, Google scholar]

15. L.K. Sharma, Hemraj Saini, **Geetanjali Rathee**, "Proposed Optimized Algorithm for Coverage Area with Capacity Calculations", IEEE International Conference Parallel Distributed and Grid Computing (PDGC 2014), 10.1109/PDGC.2014.7030790.
[Indexed: SCOPUS, DBLP]

16. Anum Javeed Zargar, Ninni Singh, **Geetanjali Rathee**, Amit Kumar Singh," Image Data-De duplication using block truncation coding Technique", IEEE conference on Futuristic Trends in Computational analysis and Knowledge management (FTCAKM-2015), 10.1109/ABLAZE.2015.7154986.
[Indexed: SCOPUS, DBLP]

17. Ninni Singh, Anum Javed Zargar, **Geetanjali Rathee**, Satya Prakash Ghrera, "A Novel Encryption Technique for Data De-duplication", IEEE conference on Futuristic Trends in Computational analysis and Knowledge management (ETCAKM-2015).
[Indexed: SCOPUS, DBLP]

18. Sukant Vats, **Geetanjali Rathee**, "An Image-Compression Decomposition Analysis of Sub-Bands using Threshold Implementation",3rd International conference on Image Information Processing (ICIIP), Waknaghat, Solan, INDIA, pp. 366-369, 2015.
[Indexed: SCOPUS, DBLP]

19. Abhinish Popli, **Geetanjali Rathee**, Hemraj Saini, "Advanced Autonomous Network Reconfiguration System", IOSR Journal, pp. 1-6, 2014.

20. **Geetanjali Rathee**, Ankit Mundra, Nitin Rakesh, "Buffered Based Routing and Resiliency Approach for WMN", IEEE International Conference on Human Computer Interactions (ICHCI), Chennai, INDIA, 2013, 10.1109/ICHCI-IEEE.2013.6887776.
[Indexed: SCOPUS, DBLP, ISI (Thomas Reuters)

21. Ankit Mundra**,** Bhagvan K. Gupta, **Geetanjali Rathee**, Meenu Chawla, Nitin Rakesh, Vipin Tyagi, "Validated Real Time Middle Ware for Distributed Cyber Physical Systems using HMM", International Journal of Distributed and Parallel Systems (IJDPS), Vol.4, No.2, pp. 23-33, March 2013.
*[Indexed: **SCOPUS**, DBLP]*

22. Meenu chawla, **Geetanjali Rathee**, S.P. Ghrera, Nitin Rakesh, "Performance Evaluation of Fault Tolerance Based Routing Approach for WMN", International conference on communication and computing (ICC-2014)
[Indexed: SCOPUS, DBLP]

23. Ankit Mundra**, Geetanjali Rathee**, Meenu Chawla, Nitin Rakesh, Ashutosh Soni, "Transport Information System using Query Centric Cyber Physical Systems (QCPS)", International Journal of Computer

Applications, Published by Foundation of Computer Science, New York, USA, vol. 85, no. 3, pp. 12-16, 2014.

[Index in: DBLP]

24. **Geetanjali Rathee**, Nitin Rakesh, "Resilient Packet Transmission for Buffer Base Routing Protocol", Journal of Information Processing and System (JIPS) Korea, vol. 12, no. 1, pp. 57-72, 2016.

*[Indexed: **SCOPUS**, DBLP]*

CONFERENCE ATTENDED

- 2nd IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2012), Dec 6-9, 2012, JUIT, Waknaghat, HP.
- 2nd IEEE International Conference on Image Information Processing (ICCIIP-2013), Dec 9-11, 2013, JUIT, Waknaghat, HP.
- 3rd IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC-2014), Dec - 2014, JUIT, Waknaghat, HP.
- 3rd PDGC Symposium on Security and Privacy Systems, Feb-13,14, IIIT Delhi.
- 3rd IEEE International Conference on Image Information Processing (ICIIP 2015), Dec 21-23, 2015, JUIT, Waknaghat, HP.
- Second International Conference on Computer and Communication Technologies (IC3T 2015), July 24-26, 2015, Hyderabad.
- Second International symposium on computer vision and the Internet (VisionNet'15), Aug 10-13, 2015, Kochi, Kerala.
- International Congress on Information and Communication Technology 2015 (ICICT'15), Oct 9-9, 2015, Udaipur.
- 7th annual International Conference on Communication Computing & Virtualization 2016 (ICCCV'16), 25-26, Kandiwali, Mumbai.

PROFESSIONAL ACTIVITIES AND AWARDS

- GATE 2012 qualified.
- 10th rank in National Talent Search Examination
- Bronze medal in Hindi Essay Writing

I hereby declare that all the information mentioned above is true to the best of my knowledge.

(GEETANJALI)