A MULTI-LAYER SECURITY FRAMEWORK

FOR HYBRID WIRELESS MESH NETWORKS

Thesis

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

GANESH REDDY KARRI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA,

SURATHKAL, MANGALORE - 575025

November, 2014.

Acknowledgements

I am heartily thankful to my supervisor, **Dr. P. Santhi Thilagam** for allowing me to carry out the research work under her eminent guidance and supervision. Her consistent support, positive attitude, motivation and the thought provoking suggestions enabled me to complete this thesis successfully. I also wish to express my sincere thanks to her for providing the necessary infrastructure and facilities required for the successful completion of this thesis.

I wish to express my sincere thanks to members of my assessment committee- **Dr. Ananthanarayan V.S, Dr. T.P Ashokbabu, Dr. Annappa, and Dr. Shashidhar G koolagudi** for their involvement and valuable feedback.

I would like to take this opportunity to thank my fellow scholars for their support and help and, also for sharing the joyful moments.

I thank all the faculty and staff of the department of Computer Science and Engineering, for their support and cooperation during the period of my doctoral studies.

I would like to thank NITK surathkal, for giving me an opportunity to carry out my research and also for the financial help provided.

Finally, my deep gratitude goes to my parents **(Venkata Reddy and Sri Lakshmi)** and my wife **(Anusha)** for their love, sacrifice and support during my life.

Ganesh Reddy .K

Abstract

Wireless Mesh Networks (WMNs) have emerged as a promising technology for a broad range of applications due to their self-organizing, self-configuring and self-healing capability, in addition to their low cost and easy maintenance. Hybrid Wireless Mesh Network (HWMN) is a special type of wireless mesh network, where mesh routers and mesh clients both perform routing and forwarding functionality and also mesh routers provide integration and interoperability among various heterogeneous networks. Securing HWMNs is more challenging and complex issue due to their inherent characteristics such as shared wireless medium, multi-hop and inter-network communication, highly dynamic network topology and decentralized architecture. These vulnerable features expose the HWMNs to several types of attacks in network and MAC layers. The existing standards and implementations are inadequate to secure these features and fail to provide comprehensive security solutions to protect both backbone and client mesh. Hence, there is a need for developing efficient, scalable and integrated security solutions for HWMNs. In this work, we propose a multi-layer security framework to address the security challenges in HWMNs in a holistic manner. Our framework combines a multi-level key management mechanism and a dynamic reputation-based cross-layer intrusion detection system to protect the legitimate mesh routers and mesh clients at the MAC layer and their legitimate routing paths at the network layer.

Protecting legitimate mesh routers and mesh clients from malicious nodes at the MAC layer is still a challenging issue in HWMNs. Our proposed multi-level key management mechanism supports distributed authentication scheme for backbone mesh and centralized authentication scheme for client mesh. The proposed distributed authentication scheme effectively utilizes the trusted group heads communications to secure the join and leave operations of mesh routers in backbone mesh. Our enhanced centralized authentication scheme uses the lightweight encryption to provide secure communication between the authenticator and the mesh client. Our analysis and experimental results show that the proposed mechanism mitigates the severity of malicious nodes and provides better security with less storage, communication and computation overhead than the existing key management mechanisms.

Protecting legitimate routing paths which are formed by long-distance wireless links from wormhole attacks at the network layer is an important yet challenging security issue in HWMNs. The proposed dynamic reputation-based intrusion detection system analyzes the behavior of the routing paths using cross-layer parameters to correctly isolate the wormhole malicious paths from legitimate routing paths. This isolation ensures full utilization of legitimate long-distance wireless links in HWMNs, which is not possible with the existing wormhole attack detection approaches. Our analysis and experimental results show that the proposed system increases the detection rate, decreases the false alarm rate and secures the legitimate long-distance wireless links from wormhole attacks in HWMNs.

Contents

List of Acronyms

AAA	Authentication Authorization and Accounting
AINA	Advanced Information Networking and Applications
AODV	Ad hoc Ondemand Distance Vector
AOMDV	Ad hoc Ondemand Multipath Distance Vector
ARMF	Adaptive Reputation Management Framework
ARAN	Authenticated Routing for Ad-hoc Networks
AS	Authentication Server
CEPA	Channel Ecto-Parasite Attack
CIDS	Cross-layer Intrusion Detection System
CONFIDANT	Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks
DELPHI	DELay Per Hop Indication
DFANT	Discovery Forward ANT
DOS	Denial of Service
DSDV	Destination-Sequenced Distance-Vector Routing
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
ECC	Elliptic curve cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FHSS	Frequency Hopping Spread Spectrum
GTK	Group Transient Key
IBC	Id Based Cryptography
ICCEA	In Computer Engineering and Applications
IDS	Intrusion Detection System
IKE	Internet Key Exchange
IPM	Intrusion Prevention Mechanism
ISWCS	In Wireless Communication Systems
KCK	Key Confirmation Key
KEK	Key Encryption Key
LES	Lightweight Encryption Scheme
LORA	LOw cost Ripple effect Attack
LUS	Link State Update
MA	Mesh authenticator
MAXPDR	MAXimum Packet Delivery Ratio
MC	Mesh Clients

MDS	Message Digest Scheme
MFANT	Maintenance Forward ANT
MIC	Message Integrity Check
MKD	Mesh Key Distributor
MKMM	Multi-level Key Management Mechanism
MPKM	Matrix Based Pairwise key Management
MR	Mesh Routers
MR-MC	Multi-Radio Multi-Channel
MSK	Master Session Key
NEPA	Network Endo-Parasite Attack
NPA	Neighbor Probe-acknowledge Algorithm
OLSR	Optimized Link State Routing Protocol
PCIDS	Reputation based Cross-Layer Intrusion Detection System
PCP	Per hop Collision Probability
PMK	Pairwise Master Key
PN	Pseudo Number
PREP	Path REPly
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
QOS	Quality of Service
RDP	Route Discovery Packet
REPRO	REputation based PROactive
RREP	Route REPlay
RREQ	Route REQuest
RTT	Round Trip Time
SAODV	Secure Ad-hoc On demand Distance Vector
SEAD	Secure Efficient Ad-hoc Distance Vector routing protocol
SHA	Secure Hash Algorithm
SHWMP	Secure Hybrid Wireless Mesh Protocol
SIDS	Single-layer Intrusion Detection System
SLSP	Secure Link State Routing for mobile ad-hoc networks
SNR	Signal to Noise Ratio
SRP	Secure Routing Protocol
SWAS	Secure WLAN Authentication Scheme
TG	Task Group
TPTK	Temporal Pairwise Transient Key

UFH	Uncoordinated Frequency Hopping
WFB	Wormhole attack Followed by Byzantine
WFJ	Wormhole attack Followed by Jellyfish
WFJB	Wormhole attack Followed by Jellyfish and Byzantine
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide interoperability for microwave access
WMP	Wormhole Malicious Paths
WP	Wormhole non-malicious Paths

List of Symbols

P_{Auth}	Probability of mesh router message is reachable
P_{NAuth}	Probability of mesh router message is not reachable
N_{Gw_i}	Number of keys stored by a gateway
$N_{Rgw_{ik}}$	Number of keys stored by a mesh router
$N_{RAgw_{ik}}$	Number of keys stored edge router
N_{C_k}	Number of keys stored by a mesh client
d_{C_avg}	Average degree of client mesh
d_{Gw_avg}	Average degree of backbone mesh
N_{t_d}	Number of node disjoint paths
R_{max}	Maximum transmission range
AR_{WFJ}	Affected reputation of WFJ attack
AR_{WFB}	Affected reputation of WFB attack
AR_{WFJB}	Affected reputation of WFJB attacks
α	Percentage of end-to-end packet delay increased
β	Percentage of packet drops increased
γ	Percentage of end-to-end packet delay and packet drops increased
AR_{WHP}	Affected Reputation of suspected wormhole path
$W_{q_{ij}}$	Per packet expected queuing delay
$P_{B_{ij}}$	Blocking probability
PCP	Per_hop Collision Probability
r_{min}	Minimum transmission range
$P_{SIDS_{dp}}$	SIDS detection probability
$P_{SIDS_{fa}}$	SIDS false alarm probability
$P_{CIDS_{dp}}$	CIDS detection probability
$P_{CIDS_{fa}}$	CIDS false alarm probability
$P_{RCIDS_{dp}}$	RCIDS detection probability
$P_{RCIDS_{fa}}$	RCIDS false alarm probability

Chapter 1

INTRODUCTION

In recent years, wireless mesh networks (WMNs) have become more popular because of their ubiquitous broadband wireless internet connectivity in a sizeable geographic area and cost-effective network deployment. WMNs have wide variety of applications such as commercial building automation, video surveillance, military radar sensing and emergency response. A typical WMN consists of mesh routers and mesh clients. Where, mesh routers are static, high powered devices, often equipped with multiple radio interfaces and these devices also act as internet gateways [Akyildiz et al., 2005]. These mesh routers are mainly classified into three main types namely gateways, conventional mesh routers and edge routers based on their functionalities. Gateways can access the internet links and router links, conventional mesh routers can only access router links and edge router can access router links and client links. Mesh clients are usually single-interface devices that can either be mobile or stationary. As a new networking technology, WMNs are categorized into three types such as backbone WMNs, client WMNs and hybrid WMNs [Xie and Wang, 2008]. In backbone WMNs, mesh clients gain access to mesh routers via a single wireless hop and mesh routers are involved in routing and forwarding functionality. In client WMNs, each mesh client supports multi-hop communication to form a client mesh, where mesh clients communicate with each other even if they are not within the direct transmission range. Hybrid Wireless Mesh Network (HWMN) is a special type of wireless mesh network, where both mesh routers and mesh clients provide routing and data forwarding functionality as shown in Figure 1.1. The routing capabilities of mesh clients provide improved connectivity and coverage inside the client mesh. While the backbone mesh provides seamless integration of heterogeneous wireless networks such as the Wi-Fi, cellular, ad-hoc and sensor networks. It also provides greater interoperability among these networks.

1.1 Characteristics of HWMNs

HWMNs have the following characteristics apart from multi-hop, integration and interoperability.

- Ad-hoc network: HWMNs support ad-hoc network properties such as dynamic self-organizing, self-configuring and self-healing functionalities in backbone mesh as well as client mesh. These functionalities in HWMNs improves fault tolerance and mesh connectivity, and reduces deployment and management costs.

- Multi-Radio Multi-Channel (MR-MC): Mesh routers are equipped with multiple radios and network traffic load on each radio distributed across all available channels. MR-MC increases the throughput, decreases the chance of collisions/interferences and ensures connectivity in backbone mesh.

- Long-distance wireless links: HWMNs provide long-distance wireless network connectivity over heterogeneous devices (mesh routers) for greater scalability and availability. In addition, these links reduce the delay and improve the overall throughput of the network.

- Mesh connectivity: Mesh nodes have redundant paths between each pair of nodes which increases reliability, eliminates single point failures and potential bottleneck link in HWMNs.

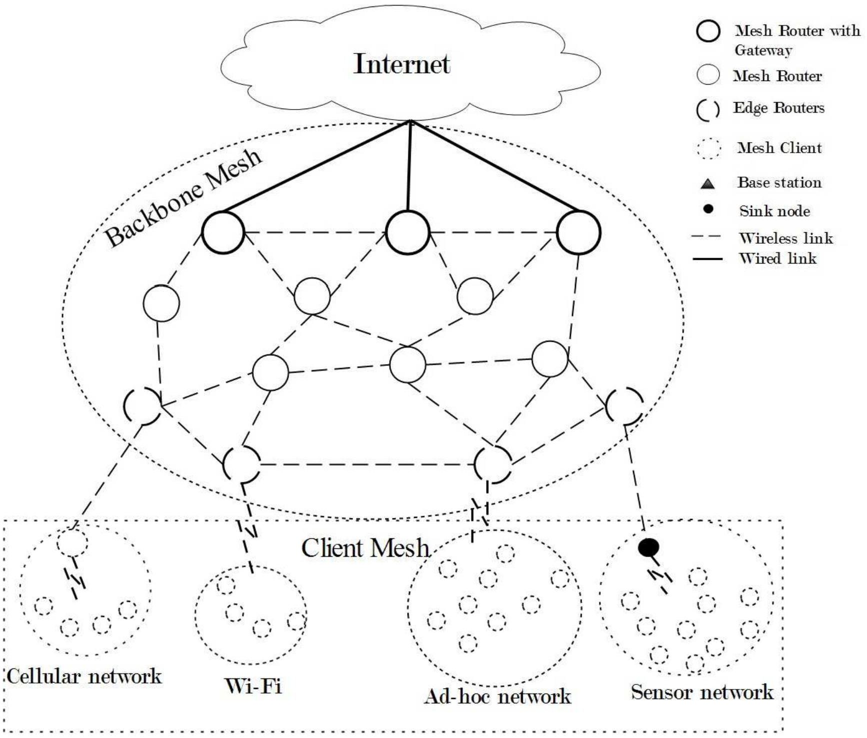


Figure 1.1: Hybrid Wireless Mesh Network Architecture

1.2 Applications

HWMNs have a wide range of potential applications, including security and surveillance, control and fine-grain monitoring of indoor and outdoor environments. Some of the application specific examples are explained below:

- High quality video streaming: In coal mines, video monitoring devices are connected in mesh to transfer high quality live video data to the central system [Srinivasan et al., 2005].

- Reliability: The 66-satellite Iridium group operates as a mesh network, with wireless links between adjacent satellites [Thomas et al., 2001].

- No need of wired or external devices: The laptops in the one laptop per child program use wireless mesh networking to enable students to exchange files and get on the Internet [Xu et al., 2010].

- No human intervention: Electric meters now being deployed on residences transfer their readings from one to another and eventually to the central office for billing without the need for human meter readers or the need to connect the meters with cables [Kumaran and Semapondo, 2010].
- QoS & Reliability: U.S. military forces are now using wireless mesh networking to efficiently connect their laptops, in field operations [Xu et al., 2010].

1.3 Security Challenges in HWMNs

The wireless mesh network standards such as 802.11s, 802.15, 802.16 (WiMAX) and 802.20 [Ricardo.C and Luiz.C, 2010, Akyildiz.F et al., 2005, Bing.W et al., 2006] have been developed in recent years. However, these standards were developed with limited characteristics of HWMN architecture, for example, 802.16 do not support the multi-hop client mesh topology, distributed Authentication, Authorization and Accounting (AAA) servers authentication etc. Existing standards restrict the scalability and availability of the network, since they support limited characteristics of HWMNs. Moreover, security protocols of these standards are still in draft stage, as these standards are adopted from other wireless networks such as mobile ad-hoc networks, sensor networks and cellular networks [Ud.S, 2009, Akyildiz.F, 2009]. Compatibility and integration are the major issues when HWMNs adopt these security solutions and this leads to several security challenges in HWMNs. In HWMNs, security is more challenging and complex issue due to their inherent characteristics which are explained below.

- Multi-hop communication: In this communication, mesh nodes in the network are able to communicate with the help of one or more intermediate nodes when they are not in the direct transmission range. The multi-hop communication improves scalability and energy efficiency in HWMNs. To optimize the performance of the multi-hop communications, routing protocols consider metrics like less delay and hop_cout, high bandwidth, low error rate etc. Attacker/ attackers take this an advantage and generate fake routing metrics to attract the mesh nodes in the network [Zhang.Y, 2008, Hoang.L and Uyen.T, 2003]. To distinguish the fake routing metrics replies and legitimate routing metrics replies is a challenging issues due to different characteristics and capacity constraints of mesh nodes. Thus, protecting multi-hop communication is still an challenging issue in HWMNs.

- Heterogeneous network environment: HWMNs usually involve integration and interoperability with heterogeneous client mesh networks [Mendonca et al., 2012]. Here, each client mesh network has different security requirements. To make all client mesh networks more secure, the first barrier that needs to be passed is to develop the interoperable security protocols without compromising security in all networks. Providing interoperable security protocols for all client mesh networks are more complex because each network has different security risks.

- Dynamic network topology: Topology of client mesh often changes due to more mobility of mesh clients. Topology change in client mesh has two security issues. The first security issue is that topology changes in client mesh are not addressed by the existing security protocols [Akyildiz et al., 2005]. If any security protocol of backbone mesh is applied to client mesh, it causes unnecessary communication and computational overhead. The second security issue is that mesh nodes update the topology based on mesh node locations, in this case attackers take an advantage and sends the false location information of mesh clients to change the network topology.

- Mesh nodes hierarchy: Mesh routers in HWMNs have different computational, communication and power resources as compared to wireless mesh clients [Bruno et al., 2005]. Thus, HWMNs need efficient security solutions that consider the difference between wireless mesh routers and mesh clients.

- Multi-channel multi-radio: Various channel assignment algorithms have been proposed for Multi-Radio Multi-Channel (MR-MC) HWMNs [Naveed et al., 2007]. All these algorithms assume that the mesh nodes are well-behaved. Therefore, a node does not verify the channel assignment information communicated by its neighbors and in fact uses the same for making a decision channel assignment about its own channel assignment. This assumed trust amongst the neighboring nodes makes these algorithms vulnerable to security attacks. Attacker takes this is an advantage and often shift its channels to create channel interference in HWMNs.

1.4 Motivation

Due to the emerging applications of WMNs, many wireless mesh network standards have been proposed. These existing standards do not support all the characteristics of HWMNs. Moreover these standards adopt the security solutions from other networks like ad-hoc or cellular etc, but these security solutions are not interoperable with each other or may have poor performance in HWMNs. Even though HWMNs have wide range of applications due to lack of the robust security solutions these applications are vulnerable to various attacks. The security challenges in HWMNs are motivated us to work in the direction of HWMNs security.

1.5 Thesis Organization

The thesis is organized as follows:

Chapter 2 presents the comprehensive study of core layer attacks and their countermeasures. In this chapter, classification of core layer attacks and their interdependencies, the analysis of existing solutions and the research directions in WMNs are presented.

Chapter 3 discusses the problem description. In this chapter, the scope of the this thesis and the proposed multi-layer security framework are presented.

Chapter 4 presents multi-level key management mechanism. In this chapter, distributed authentication scheme in backbone mesh and centralized authentication scheme in client mesh for protecting legitimate mesh nodes are presented. The effectiveness of both the authentication schemes are discussed through the analysis and simulations. Finally, storage, communication and computation costs of multi-level key management mechanism are represented in big-O notations.

Chapter 5 presents a comprehensive analysis of severity of wormhole attacks and simulation study to find the severity of the wormhole attacks and affected reputation of wormhole paths are presented.

Chapter 6 presents reputation based cross-layer intrusion detection system. In this chapter, cross-layer parameters (Network layer and MAC layer) are studied to the control unsteady state traffic. Both cross-layer parameters and affected reputation values are used in the design of RCIDS. The effectiveness of RCIDS is verified through binomial probabilistic model and simulations.

Chapter 7 summarizes the achievements of this thesis and highlights its contributions. Possible future research is also discussed in this chapter.

Chapter 2

LITERATURE REVIEW

Wireless mesh networks are more vulnerable especially in three core layers such as network layer, MAC layer and Physical layer [Zhang.Y, 2008, Hoang.L and Uyen.T, 2003,Muhammad.S and Choong.S, 2009,Ping.Y and Yue.W, 2010], due to the existing inadequate security standards/ protocols. Security vulnerabilities in these core layers lead to various types of attacks such as control plane, data plane, network security, information security, channel jamming and signal jamming attacks etc. These attacks can severely degrade the network performance by disturbing the network traffic and topology. Robust security solutions are developed to protect against these attacks. Existing security solutions can be classified into two types namely i) Intrusion Prevention System and ii) Intrusion Detection System. Intrusion prevention mechanisms ensure control and data packets authentication, integrity, confidentiality and non-repudiation in wireless mesh networks. These mechanisms can effectively prevent unauthorized nodes from the network and can provide some protection against compromised nodes (internal attackers). However, the problem of internal attackers cannot be addressed completely using the intrusion prevention mechanisms and hence the support from intrusion detection systems become mandatory. Intrusion Detection Systems (IDSs) are comprehensive to detect internal attackers. The key issue of IDSs is to set the parameters to identify the attacks such as packet drop, delay etc. These parameters values are more volatile in WMNs because radio or channel jamming, less signal strength and congestion of mesh nodes. The volatile parameters of IDSs lead to an increase of misdetection of attacks. To overcome this, reputation based IDSs are required in which, volatile parameters of IDSs can be controlled by maintaining the node independent or dependent reputation values.

The rest of the chapter is organized as follows. Section 2.1 provides classification of core layer attacks and interdependencies between them. Section 2.2 provides the analysis of security solutions with respective to core layer attacks. Section 2.3 summarizes this chapter.

2.1 Core Layer Attacks

Security attacks are possible in all protocol layers ranging from physical layer to transport layer [Ricardo.C and Luiz.C, 2010]. Usually, attacks in a upper protocol layer such as transport layer are less harmful than those in the lower layers such as network, MAC and physical layers, since the protocol stack is developed in a bottom up manner. WMNs are formed by integrating different wireless networks, thus WMNs inherit the vulnerability of the these networks. In this section, we explain about various core layer attacks and their classification and interdependencies.

2.1.1 Network Layer Attacks

Network layer is more vulnerable to various types of attacks mainly due to lack of robust standard security frameworks in multi-hop wireless networks. Figure 2.1 depicts the taxonomy of network layer attacks. Network layer attacks are classified into two types as Control plane and Data plane attacks. In control plane attacks, attacker intention is to disturb the routing functionalities and/or gain the network traffic of the target node. In data plane attacks, attacker (selfish or compromised node) intention is to create packet drops, packet delay and inject false packets on received data packets. In both cases, the attacker may either be internal or external node. Internal attacker is more harmful as compared to the external attacker because it has enough privileges to participate in routing and data forwarding phases. Whereas, all external attacker wastes more time in promiscuous mode to gain the knowledge of target node. Attacker is affective

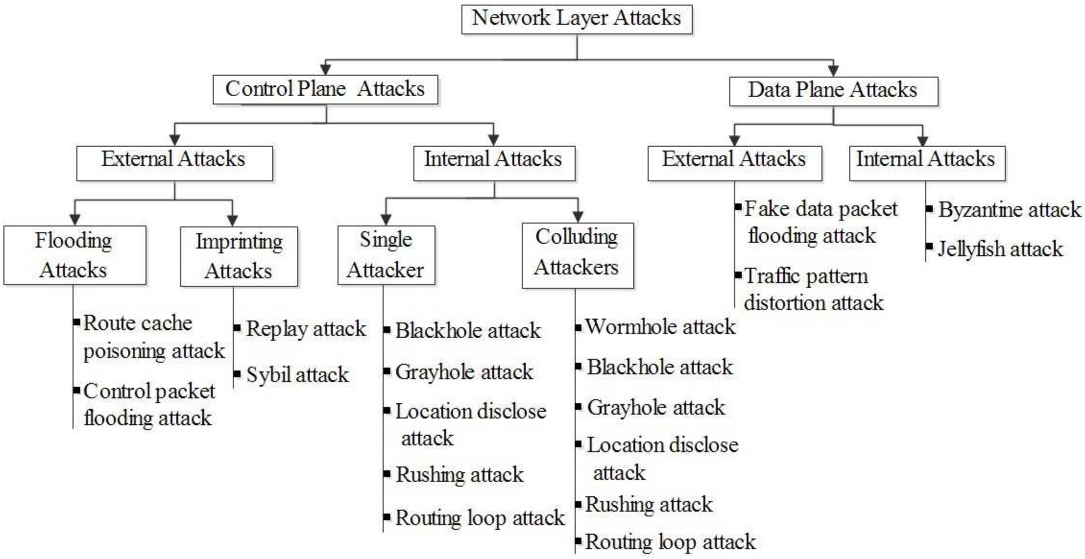


Figure 2.1: Taxonomy of Network Layer Attacks

only when the network does not prevent external attacks or loopholes on security solutions. We have classified the control plane and data plane attacks as described below.

a) Control Plane attacks

In control plane attacks, *external attackers* are the unauthorized nodes. The unauthorized nodes perform the following *flooding attacks*:

Route cache poisoning attack: In this attack, the attacker sends excessive fake route updates or error packets to all one_hop distance nodes. Upon receiving these packets, legitimate nodes replaces the important routing data with fake/error routing updates.

Control packet flooding attack: In this attack, the attacker intention is to deplete the network resource utilization like bandwidth, battery, computational power etc. This attack appears in network layer by flooding fake route reply, hello and error packets at target node or in the network [Redwan and Kim, 2008].

In*impersonation attacks*, the attacker successfully assumes the identity of one of the legitimate node. This legitimate node identity is misused in the following ways:

Replay attack: In replay attack, attacker is initially in passive mode to gain authenticated Routing REQuest(RREQ) and Route REPlay (RREP). Once, the attacker gains the authentic information of target nodes then it sends a RREQ or RREP packet on behalf target nodes to gain the network access [Zhang.Y, 2008].

Sybil attack: Sybil attack is more severe attack, in which attacker disrupts both network topology and multi-path routing protocol functionality. Attacker often changes the locations with different legitimate node ids [Sahil.S and Anil.G, 2006] to disturb network topology. The attacker appears with multiple identities in the network, which are taken from the compromised nodes and appearing in most of the node disjoint paths to disturb multi-path routing. Figure 2.2 illustrates the example scenario of sybil attack.

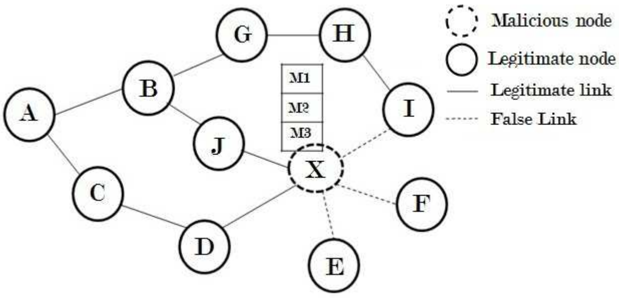


Figure 2.2: Sybil Attack

In this scenario, malicious node X has three identities M1, M2 and M3 and all these identities are spoofed in passive mode. A and F are source and destination nodes having multiple paths between them. Here, malicious node will appear in all multiple paths with different identities such as (A, C, D, M1, F),(A, B, J, M2, F) and (A, B, G, H, I, M3, F) to disturb the network performance.

In control plane attacks, *internal attackers* can do all external attacks and also can perform more severe attacks than external attacks. Preventing and detecting these attacks are more difficult. Internal attacks are mainly caused by single attacker or colluding attackers. Single attacker can do the following control plane attacks:

Blackhole attack: In this attack, malicious node drops all the packets passed through it. In order to do this, the malicious node attracts a target source node with false route reply of destination node with less hop_count and high bandwidth [Tamilselvan.L and Sankaranarayanan.V, 2007]. Once, a route is established through the malicious node then target source node starts sending packets to destination node and eventually all packets will be dropped at malicious node. This attack scenario in on-demand rout-

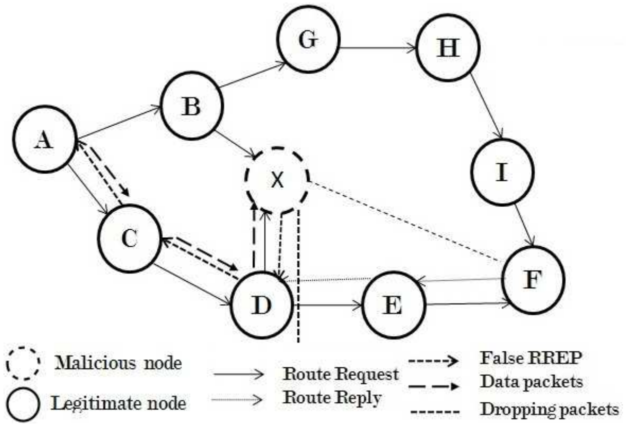


Figure 2.3: Blackhole Attack

ing protocol is depicted in Figure 2.3. Here, nodes A and F are source and destination nodes. At route discovery phase, A disseminates route request to find destination path. On-behalf of node A, RREQ packet is broadcasted by intermediate nodes until it reaches to F node. Once, RREQ received by F through I and E nodes. F sets the reverse path to A which is F, E, D, C, A (less hop_count). In Figure 2.3, this path is disturbed by the malicious node X at node D. X traps D with less hop count and high sequence number then D will drop the actual route and forwards the attacker X route (F, X, D, C, A) to A. When A starts sending data packets to F, X receives all data packets before node F and X drops them. Thus, F does not receive any data packets which are sent by A.

Grayhole attack: Grayhole attack is similar kind of blackhole attack, but more sophisticated attack as compared to blackhole attack [Gerkis.A, 2006]. In this attack, malicious node participates without any malicious functionality in the route discovery stage, but when the packets start moving through this node, it drops the packets in selective intervals. Detecting this attack is more complex than blackhole because packet drop occurs in wireless networks often occurs due to communication errors, hardware error and buffer overflow etc.

Location discloser attack: Location discloser attack is easily caused by internal network nodes, in which a internal attacker reveals the network topology or location of the nodes [khan, 2011]. This information is gained by external attacker, to deploy passive attacks or active attacks on the target nodes.

Rushing attack: Rushing attack is also called zero delay attack and more effective when the attacker is nearby to source or destination nodes. On-demand routing protocols like AODV [Trong.H and Dai.T, 2006] and DSR [Marshall, 2002] are more vulnerable to this attack, because when a source node floods the route request packet in the network, attacker receives the route request packet and sends without any delay into the network. Whenever the legitimate nodes receive the original source request packets, these packets are dropped because legitimate nodes would have already received packet from the attacker and treat them as duplicate packets. Eventually attacker is included in active route and disturbs the data forwarding phase. Figure 2.4 explains rushing attack scenario where, rushing attacker X placed at destination node. The attacker X receives the RREQ packet from J then it is broadcasted without delay (no verification process is done). This packet will be received by intermediate nodes I, E and destination node F. Intermediate nodes I and D suppress the actual RREQ packet received from nodes H and E due to their RREQ staleness or duplicity. Destination node F will receive the first RREQ packet from attacker X. Eventually, destination node F includes attacker X as an intermediate node in source to destination path.

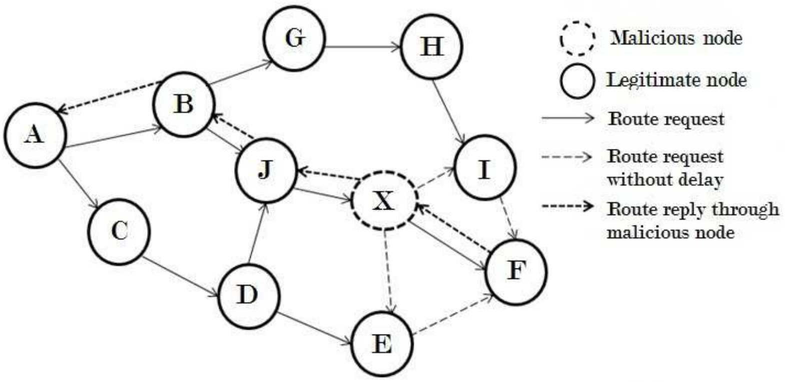

G
H
B
A
J
X
I
C
F
D
E
Malicious node
Legitimate node
Route request
Route request without delay
Route reply through malicious node

Figure 2.4: Rushing Attack

Routing loop attack: The attacker creates the loops effectively when it knows network topology at the route discovery phase. In this attack, attacker intention is to deplete the network resource by sending the duplicate packets [Shariful.Md and Hamid, 2009]. Figure 2.5. shows the routing loop attack scenario. In this scenario, source node S disseminates a RREQ packet for node I. This RREQ packet is received by attacker X and node A. Attacker X selectively sends RREQ packet to C to create X, C, D, E,

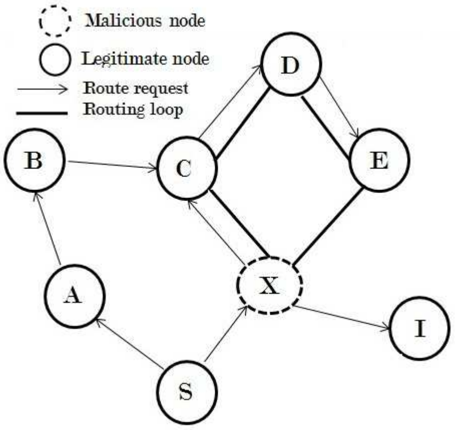


Figure 2.5: Routing Loop Attack

X loop. When node C receives RREQ packet from B and attacker X, node C drops B's RREQ packet and rebroadcasts attacker X's RREQ packet only because of less hop_cont. When node D receives RREQ from C, D rebroadcasts this packet. Eventually, this RREQ packet is received by node E then E rebroadcasts it. Once, attacker X receives RREQ packet from E then X selectively forwards RREQ packet to node I. Thus, X is able to create a loop between S and I nodes as S, X, C, D, E, X, I.

All these attacks are possible by a single attacker. Whereas, group of attackers called *colluding attackers* cooperatively can perform various attacks as well as the above attacks.

Wormhole attack: Wormhole attack is formed by two or more colluding nodes in the network. To create wormhole attack, any two mutually understanding malicious nodes form a tunnel with low latency and broadcast this information into the network. All overheard neighbor nodes send data packets through the tunnel, and then malicious nodes alter the data packets or drop the packets [Khalil et al., 2007]. This attack is more effective when these nodes have more coverage area in the network. Figure 2.6 depicts the wormhole attack scenario with two mutually understanding malicious nodes. Wormhole malicious nodes are represented as M1 and M2, M1's coverage area is a1 and M2's coverage area is a2 respectively. These two nodes form a tunnel with low latency. Moreover, these two nodes cover the entire network, thus all the neighbor nodes

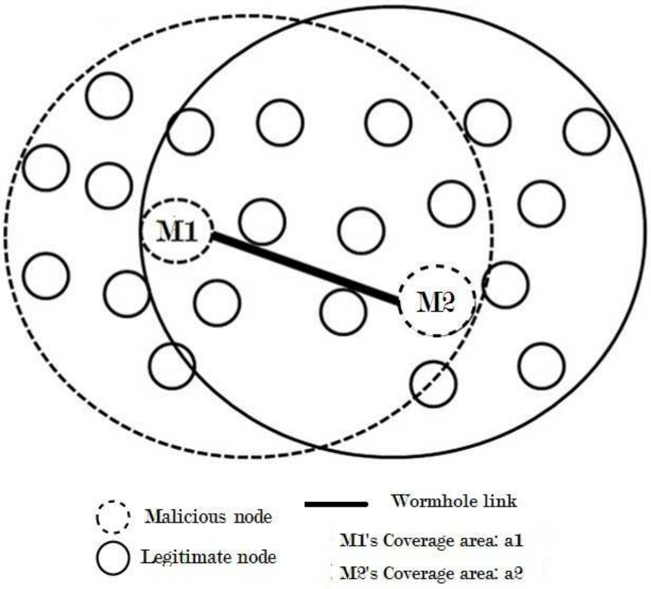


Figure 2.6: Wormhole Attack

give more priority to send their data packets through M1 and M2 tunnel.

b) Data plane Attacks

In data plane attack, attacker intention is to disturb the data traffic in the network. The following data plane attacks can be caused by *external attackers*:

Fake data packets flooding attack: In this attack, attacker depletes the network resource by using brute force mechanism. In brute force mechanism, attacker blindly injects fake or error packets into the network. These packets create the network interference when the legitimate nodes are in the data transmission phase. Existing routing paths are disturbed by this attack.

Traffic pattern distortion attack: In traffic pattern distortion attack, attacker creates the resource depletion such as channel jamming [Zhang.Y, 2008]. The attacker easily acquires the data forwarding information due to the broadcast nature of wireless communication. To do this, attacker overhears the communication channels of the neighbor nodes and analyzes the traffic patterns and sends excessive fake packets when high traffic rely on any of its two neighbor nodes. The actual data traffic is jammed by the attacker's fake data packets.

The data plane attacks can be caused by *internal attackers* and these attacks are described as follows:

Byzantine attack: In this attack, compromised node's intension is to degrade the network performance by doing malicious functionalities such as packet dropping, packet modification and injecting false packets [Zhong and Xu, 2010,Baras et al., 2007]. Here, the legitimate node is compromised by the internal/external attacker and the compromised node follows the instructions given by the attacker. This attack severely degrades the network performance when attacker takes the advantage of the control plane attacks such as blackhole, grayhole, wormhole and rushing attacks to create byzantine attack.

Jellyfish attack: In jellyfish attack, attacker intension is to decrease the goodput of selected path to near-zero [Samad et al., 2012]. To do this attack, the attacker behave as trustworthy node in route initialization phase. When the data packets of target source node are received by attacker, more delay is created for selected packets or reordered the packets. This attack severely degrades the network performance when attacker takes an advantage of the control plane attacks such as wormhole and rushing attacks to create jellyfish attack.

It is observed that there exists interdependencies among control plane and data plane attacks. Malicious node attracts the network nodes by introducing less hop_count, delay, and long coverage area to join in active route by control plane attacks. Once control plane attacker is on the active route, then it starts doing corresponding data plane or control plane attacks to create Denial of Services (DoS) attacks. For example

1. After location discloser attack, attacker can do the following control plane flooding, fake data packets flooding and traffic pattern distortion attacks.

2. After wormhole attack, the attacker can do the jellyfish and byzantine attacks.

3. After rushing attack, the attacker can do the jellyfish and byzantine attacks.

4. After grayhole attack, the attacker can do the byzantine attack.

5. After blackhole attack, the attacker can do the byzantine attack.

6. After routing loop attack, the attacker can do the jellyfish and byzantine attacks.

2.1.2 MAC Layer Attacks

In WMNs, MAC layer functionalities such as authentication and channel allocation of network nodes are more complex because of its distributive nature, multi-hop network support, resource constrains and dynamic topology. Moreover, existing security solutions are less effective to secure the MAC layer functionalities. Attacker takes this as an advantage and performs several attacks. Figure 2.7 depicts the taxonomy of MAC layer attacks. MAC layer attacks are mainly classified into two types such as network security attacks and information security attacks. In network security attacks, attacker intention is to disturb the network topology by changing the channel interfaces and isolate the target nodes from the network. In information security attacks, attacker intention is to disturb the network traffic by sending the excessive probe or authentication packets. These attacks are also called Denial of Service (DoS) attacks.

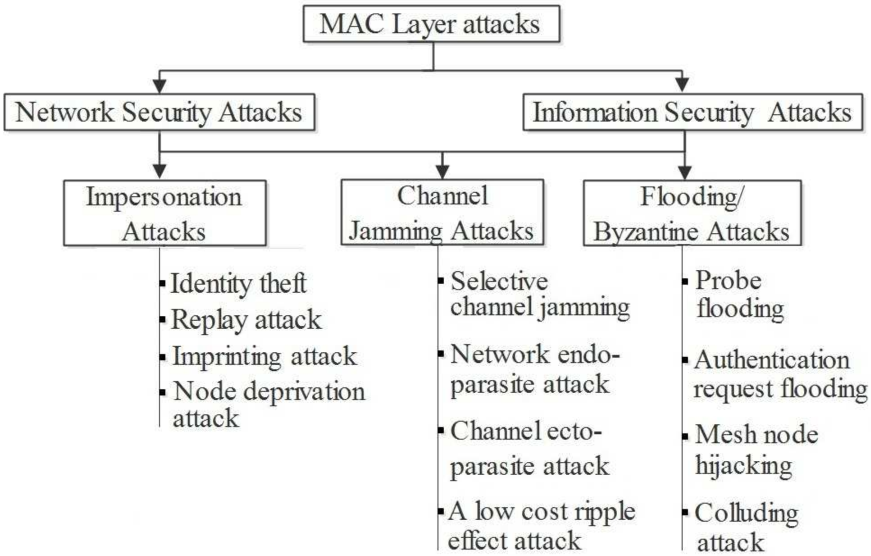


Figure 2.7: Taxonomy of MAC Layer Attacks

a) Network Security Attacks

In *impersonation attacks*, attacker successfully assumes the identity of the legitimate node. This identity of the legitimate node is misused in the following ways:

Identity theft: In identity theft attack, *id* of the legitimate node id is stolen and misused by the attacker to create different kind of attacks such as ARP packet flooding etc. [Gerkis.A, 2006]. Using this *id* attacker accesses all legitimate node privileges such as bandwidth, authentication and authorization.

Replay attack: Replay attack is mainly occurs in authentication based security protocols such as IEEE 802.11i and 802.11s(draft stage) [Zhang.Y, 2008]. In this attack, attacker records the legitimate nodes authentication messages which is nothing but a passive eavesdropping attack. Then attacker comes into active phase and replays the recorded message in the network to impersonate as the legitimate user.

Imprinting attack: The mechanism by which nodes acquire the self-signed mediator's certificate is called imprinting [Muhammad.S and Choong.S, 2009]. In wireless mesh network, any mesh node can join or leave the network at any time. If any new mesh node wants to join the client mesh or backbone mesh, then first it sends a message to the AP/gateway. AP/gateway issues the key to the new mesh node after receiving this message. The new node always selects the owner who issues the key first. In this process, attacker takes the advantage and issues the key to the new mesh node before the AP/GATEWAY.

Node deprivation attack: Node deprivation attack is similar to imprinting but targets the de-authentication part [P802.11w/D0.0, 2006]. The attacker's goal is to isolate the legitimate node from the mesh client network. IEEE 802.11s or 802.11i security protocols perform authentication and de-authentication when any node joins or leaves respectively. In this attack, attacker captures the de-authentication request message of a legitimate node and attacker misuses the captured de-authentication request message when this legitimate node re-joins the network.

b) Information Security Attacks

In information security attacks, attacker can perform the following flooding and byzantine attacks:

Probe flooding: Many intrusion detection systems propagate the probe packets among the neighboring nodes to measure their forwarding rate and receiving rate [Wang.X and Wong.J, 2007]. This parameter is useful to identify the loss probability of its neighbor nodes. But these probe packets are misused by malicious node to create DoS attack in the network by sending excessive false probe packets.

Authentication request flooding: Strong authentication mechanisms are required in order to prevent the external nodes [He and Mitchell, 2004]. To provide an authentication among mesh clients (PDAS, mobiles etc) in WMN, existing security frameworks follow the asymmetric cryptography. But, Mesh clients have major constraints such as CPU, battery, mobility, and bandwidth. Here, the attacker sends excessive fake authentication request packets to target nodes. These request packets consume more resources in the verification process at the target nodes. As consequence, resources of target nodes are depleted by authentication request flooding attack.

Mesh node hijacking: Mesh node hijacking is mainly caused by unfair greedy nodes who always look to send their traffic with high priority. Here, a greedy network owner may attempt to leverage other owners' mesh nodes for forwarding its own traffic. A hostile network owner may attempt to leverage neighbor owners' mesh nodes for forwarding its own traffic and take one step further by protecting its own mesh nodes [Zhang.Y, 2008].

Colluding attack: Colluding attack is formed by internal attackers. In which, group of attackers cooperatively work for isolating the targeted nodes in the networks [Khalil et al., 2007]. Colluding attackers drop all authentication request messages of targeted node to isolate it from the network. In addition to this, these attackers drop all de-authentication request messages of targeted nodes to deplete their resources.

c) Channel jamming attacks

Multi-Radio Multi-Channel (MR-MC) in WMNs faces severe problems in hostile environment in the channel assignment phase. Because WMNs has no centralized authority for assigns channels for each node in the network and this is chosen by node itself. Moreover, creating these attacks are more easier as compared to authentication attacks [Lazos.L and Krunz.M, 2011], [Zhang.Y, 2008]. These attacks disturb the MAC layer functionalities as well as control plane and data plane functionalities of the network layer. Moreover, these attacks comes under network security attacks and information security attacks. An attacker uses MR-MC to perform the following attacks:

Selective channel jamming: In this attack, attacker selectively targets the control channels to launch a DoS attack with fairly limited resources [Lazos.L and Krunz.M, 2011]. Initially, attacker gains the important parameters such as node locations, time slot and pseudo number code from the compromised node or by network layer location discloser attack. The attacker transmits fake control frames (MAC without payload) selectively to prevent the use of all channels during the data transmission phase.

Network Endo-Parasite Attack (NEPA): In this attack, compromised node disturbs heavily loaded channels [Zhang.Y, 2008]. To disturb heavily loaded channel, the compromised node switches its interface to heavily loaded highest priority channel. Then compromised node allots same channel to other neighbor nodes without any prior information. Thus, the neighboring node channels are always disturbed by the attacker which leads to the DoS attacks.

Channel Ecto-Parasite Attack (CEPA): The channel ecto-parasite attack is a similar kind of network endo-parasite attack [Parker et al., 2006]. Here, attacker changes the channel assignments to heavy loaded channels without informing to same domain neighbours. The effect of this attack is to hide the usage of the most-heavily loaded channels, which increases the interference considerably, resulting in poor performance. channel, which increases the interference considerably, resulting in poor performance.

A LOw cost Ripple effect Attack (LORA): In this attack, attacker disturbs the channel interface of neighbor nodes to send misleading channel assignment information. Here, the attacker transfers false channel assignment information about its interfaces to the neighboring nodes without actually changing the channel assignment [Zhang.Y, 2008]. This false channel assignment information changes affects the neighbor domain channel assignment. This attack increases the interference in the neighbor domain.

2.1.3 Physical Layer Attacks

Physical layer has many communication systems such as directional antennas, multi-antenna etc. All the existing systems mainly focus on optimizing the bit error rate and improve transmission rate in wider area networks. However, these systems are vulnerable to various attacks due to the shared frequency band. Once the security in the physical layer is broken due to jamming, the entire wireless network just does not work anymore, no matter what security schemes are adopted in upper layers. Physical layer is often attacked with signal jamming which continuously emits RF signals to fill the wireless channel, so that legitimate traffic will be completely blocked. Physical layer signal jamming attacks are mainly classified into two types such as non-sophisticated signal jamming and sophisticated signal jamming attacks as shown in Figure 2.8.

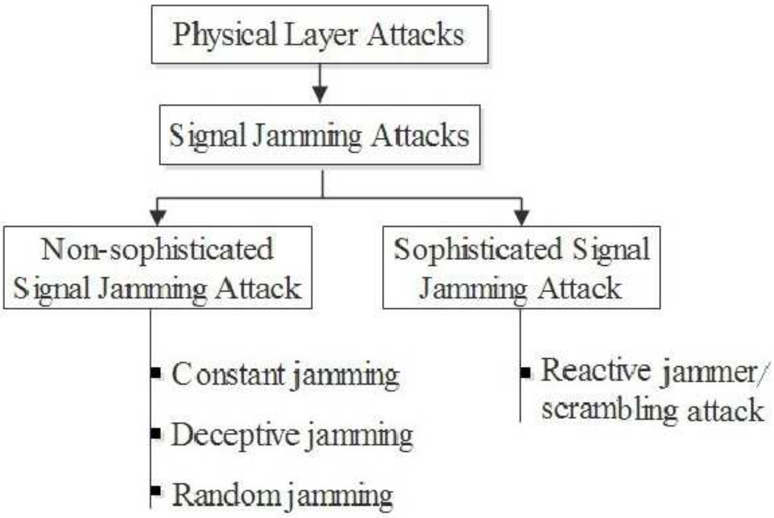

Physical Layer Attacks
Signal Jamming Attacks
Non-sophisticated Signal Jamming Attack
Sophisticated Signal Jamming Attack
Constant jamming
Deceptive jamming
Random jamming
Reactive jammer/ scrambling attack

Figure 2.8: Taxonomy of Physical Layer Attacks

a) Signal Jamming Attacks

Non-sophisticated signal jamming attack is also called brute force attack and attacker needs more resource to create this attack. The attacker can perform the following jamming attacks.

Constant jammer: In constant jammer, compromised node intention is to block the wireless medium and prevent the other devices to communicate [Fragkiadakis.G et al., 2010]. Here, compromised node uses signal strength stronger than any other node in the wireless medium and continuously sends random bits to create DoS attack. **Deceptive jamming:** In deceptive jamming, attacker continuously sends excessive packets to abort wireless communication of its neighbor [Xu.W et al., 2003]. This attack occurs in each layer differently with powerful transmitters such as Syn flooding in transport layer, RREQ flooding in network layer and authentication flooding in MAC layer.

Random jamming: In random jamming, attacker alternates between sleeping and jamming mode [Xu.W et al., 2003, Zhang.Y, 2008]. Here, the attacker sets the timers to generate radio frequency (RF) signals randomly in between sleep and jamming in wireless medium. Attacker gains better results than constant jamming or deceptive jamming because jamming is done with less signal strength and detection of this attack is a bit difficult.

Sophisticated signal jamming attack is more effective and intellectual and it is explained below:

Reactive jammer/scrambling attack: Reactive jamming/scrambling attack is more sophisticated attack than the random jamming. Here, attacker starts its transmission as soon as network traffic is detected on the channel [Sahil.S and Anil.G, 2006, Xu.W et al., 2003]. Attacker targets the reception of a message because it stays silent when the channel is idle, but starts generating a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of a message. Detecting this attack is more difficult than the random jamming because attacker acts as normal node.

2.2 Security Solutions

To study the existing security solutions for WMNs, we first investigate the intrusion prevention and detection solutions in several wireless networks that are closely related to WMNs, i.e., IEEE 802.11 wireless LANs, IEEE 802.16 wireless Metropolitan Area Networks (MANs), sensor, mobile ad hoc networks etc [Akyildiz.F et al., 2005]. Security solutions for these wireless networks have become building blocks for WMNs. Investigating security solutions of these wireless networks will help us to find out what existing solutions can be used and what are the remaining issues to be resolved for WMNs.

2.2.1 Intrusion Prevention Mechanisms (IPMs)

In this section, we analyse the existing intrusion prevention mechanisms for core layer attacks.

2.2.1.1 Network Layer Intrusion Prevention Mechanisms

To protect against network layer attacks many secure routing protocols have been proposed. The secure routing protocols and their effects on various control plane attacks are explained below:

Secure Ad-hoc On demand Distance Vector (SAODV) protocol: SAODV is secure variant of AODV protocol which uses self-organized key management system to protect the routing metric from the internal and external attacks. SAODV depends on IPv6 protocol to select unique IDs of each and every node in the network [Marina and Das, 2006]. In SAODV, source node generates route request packet which contains mutable (hop_count) and non-mutable fields (control message). Mutable field is protected by the hash chain and non-mutable field is protected by digital signature of each intermediate node in the route discovery path. Every time a node wants to send a Route REQuest (RREQ) or a Route REPly (RREP) packet packet, it selects the maximum hop_count seed in equation 2.1.

$$Top\_Hash = h^{Max\_Hop\_Count}(seed) \tag{2.1}$$

Every time a node receives a RREQ or a RREP packet, it will verify the hop_count of the message. Before rebroadcasting a RREQ or forwarding a RREP packet, it creates hash of hashes for the signature extension in equation 2.2.

$$Top\_Hash = h^{Max\_Hop\_Count-Hop\_Count}(seed) \tag{2.2}$$

When a node has a route to the destination, it generates a RREP packet with double signatures (RREP packet is signed by intermediate node and destination node).

The double signature verification of each request/ reply packet needs more CPU time. Moreover, self-organized key management mechanism is more vulnerable to colluding attacks such as blackhole, grayhole, wormhole attacks etc., because no centralized authority to control the internal colluding attackers. For example, colluding attackers are able to create blackhole attack by forwarding a RREQ or a RREP packet without increase the hop_count.

Secure Routing Protocol (SRP): SRP is secure variant of DSR protocol uses secret sharing mechanism to prevent external DoS attacks. Prerequisite shared secret key (K_{sd}) is required between source and destination nodes before route discovery starts [Ertaul.L and Ibrahim.D, 2009]. This process has less communication and computational overhead because intermediate authentication is required only when route reply is generated for destination node. In the process of SRP, route request packet contains $<$ Soure IP, Destination IP, ID, SN $>$ and it is signed by shared secret key K_{sd}. Source node disseminates the RREQ packet which will be forwarded by intermediate nodes until it reaches to destination node. Destination verifies the route request with K_{sd} and verifies the sequence number (SN) to confirm whether this packet is new or old . Once the verification is done, destination node creates route replay (RREP) which contains <Source IP, Destination IP, ID, SN, intermediate nodes> and it is signed by K_{sd} then unicast RREP in reverse route to source node. Source node verifies RREP packet with shared secret key to detect alteration in RREP packet by malicious node. SRP is more vulnerable than SAODV, because single attacker can forward the RREP packet without incrementing/ decrementing the hop_cont to create blackhole attack. In addition, all attacks which are possible in SAODV also possible in SRP.

Secure Link State Routing Protocol (SLSP): SLSP protects link state update (LSU) and topological maintenance information about nodes which are in the same zone [Papadimitratos.P and Haas.J, 2003]. It prevents from authentication attacks such as IP forging attack, masquerading attack and detects the flooding attacks such as hello packet flooding by using threshold parameter. Self-organized public key cryptosystem is used here to authenticate the neighboring nodes i.e., to do this every node has to select its own public key and disseminate periodically to its neighbors. Each node public key is certified by its neighbors therefore each of the link state updates(LSU) are signed by this certified public keys. It calculates a one-way hash chain to make sure LSU are propagated within the zone of origin. To prevent the DoS attacks, each node broadcasts its (IP, MAC) in the form of signed hello messages. SLSP is vulnerable to group of internal attackers. For example, group of internal attackers can isolate the legitimate node from the network by sending false LSU to other group members. Other internal control plane attacks are also easily possible when group of attackers work together.

Secure Efficient Ad-hoc Distance vector (SEAD) routingprotocol: SEAD protocol is mainly focused on four functionalities such as i) metric and sequence number authentication, ii) neighbor authentication iii) preventing same-distance fraud and iv) bounding verification overhead [Yih-Chun.H and Johnson.D.B, 2003]. To provide confidentiality, integrity and authenticity, SEAD protcol uses one-way hash chains, merkle hash trees and shared secret key mechanisms. Authenticator (source node) uses one-way hash function to protect against multiple uncoordinated attackers. To prevent same-distance fraud attack, authenticator uses merkle hash tree chains. Any two neighboring nodes authentication is done by shared secret key. In SEAD protocol, attacker can attempt or reduce the amount of routing information available to other nodes by not advertising certain routers or by destroying routing paths. In addition, this protocol is vulnerable to all internal colluding attackers.

Secure Hybrid Wireless Mesh Protocol (SHWMP): SHWMP is secure variant of HWMP which uses hop-by-hop authentication on the mutable fields using a Merkle tree [Shariful.Md and Hamid, 2009]. This protocol assumes the availability of keys via IEEE 802.11s security framework and utilizes IEEE 802.1X for initial authentication. SHWMP protects control plane packets such as path request (PREQ), path reply(PREP) and route announcement (RANN). These packets have routing information elements in which mutable and non-mutable elements exist. All the mutable elements of PREQ, PREP, and RANN are protected by authenticated one way-hash using the concept of mekrle tree. Non-mutable elements of PREQ, PREP, and RANN protected by using symmetric key cryptosystem. In SHWMP colluding attackers affect all mutable fields, and all attacks possible in SAODV are possible in SHWMP because these two are work-ing on same principle called mutable fields and non-mutable fields security.

AntSec: It is a proactive, probabilistic, multipath, stigmatic-based, distributed and non-broadcast based secure routing algorithm in WMN security framework. Antsec discovery forward ant (DFANT) contains registration certificate and public key to authenticate source node [Parag and Kalman.G, 2010]. Each intermediate node requests the registration certificate and public key of the destination on forwarding route. Maintenance forward ant (MFANT) message is used for update the current routes. Backward ant (BANT) message is generated by destination node which contains its registration certificate and the public key of this node. BANT message guarantee the integrity by being signed by destination node which will verify by the intermediate nodes on backward path. Moreover, WMN security framework uses intrusion detection (watchant) and reputation (antrep) solutions which are explained in next section. In AntSec, hop_count field is vulnerable to internal attackers when the nodes are failed to receive routing updates in a timely manner.

Authenticated Routing for Ad-hoc Networks (ARAN): Authenticated Routing for Ad-hoc Networks (ARAN) protocol objective is to provide end-to-end authentication [Papadimitratos.P and Haas.Z.J, 2002]. It is a secure variant of AODV and DSR protocols. The prerequisite condition of ARAN is to have trusted centralized certification server to distribute certificates. These certificates are revoked when they expire. In the process of renewing these certificates, ARAN protocol creates more network overhead. In ARAN, authenticated route discovery process is initiated by source node *S* for a particular node *D* (destination). Here, source broadcasts Route Discovery Packet (RDP) which contains the following fields: IP address of the destination (IP_D), *S* certificate ($Cert_S$), nonce (N_S), and the current time *t* signed with *S* private key K_S. The receiving node *A* of RDP uses *S* public key, which it extracts from *S* certificate, to validate the signature and verify that *S* certificate has not expired and on *A's* private key K_A, appends its certificate CertA. This process continues until RREQ message reaches to the destination. Once it reaches to destination node *D*, it verifies the intermediate node certificates and signatures then it forms a reverse route called REply Packet (REP). The destination node *D* signs on the REP packet and follows similar process of RDP to forward REP to source node *S* along with the reverser path. ARAN is more vulnerable to colluding attackers as compared to any other security routing protocols because every intermediate node first authenticates by its neighboring nodes. Here, all neighboring nodes can act as colluding attackers to isolate the target nodes from the network.

A secure on-demand routing protocol for Ad-hoc networks (Ariadne): Ariadne is secure variant of DSR and protects using TESLA [Hu et al., 2005]. TESLA is a broadcast authentication protocol for authenticating routing messages. Every message has message authentication code (MAC) to provide a secure authentication in point-to-point communication. To prevent other nodes from forging MAC, each node needs time synchronization and delayed key discloser. The prerequisite conditions of Ariadne initializes pairwise secret keys, shared keys between all source and destination pairs and their clocks must be synchronized. In Ariadne, source node computes delayed key also called TESLA key to encrypt MACs of sending messages. Destination node buffers all messages until source node release the delayed key and then verifies it by using the key. Time synchronization is required to protect the MAC and delayed key. It can protect the wireless network from internal rushing attack because it provides time synchronization for packet verification at the destination node irrespective of source information. However, the major problem of Ariadne is not being integrated with decentralized systems.

Table 2.1. shows the analysis of secure routing protocols against control plane attacks. Whereas blackhole, wormhole, grayhole, routing loop, rushing and location discloser attacks are the internal attacks which are discussed in section 2.1.1. All these attacks have enough privileges to participate in the routing functionalities. To participate in active route, single attacker can create blackhole and grayhole attacks by not incrementing the hop_count in SRP, SEAD, SHWMP, SAODV, and SLSP protocols because hash of the mutable field only look at the modification of hop_count. AntSec, ARAN, and Ariadne is less vulnerable to blackhole and grayhole attacks because destination node verifies the certification of all intermediate nodes in the active route but these security protocols are not adequate to block blackhole and grayhole attacks. Wormhole attack by colluding attackers can gain the active route by broadcasting very low latency routes in the network. However, existing secure routing protocols do not consider

Table 2.1: Analysis of Secure Routing Protocols Against Control Plane Attacks

Attacks/Security protocols	SAODV	SHWMP	AntSec	ARAN	Ariadne	SEAD	SRP	SLSP
Blackhole	NO	NO	NO	NO	NO	NO	NO	NO
Wormhole	NO	NO	NO	NO	NO	NO	NO	NO
Grayhole	NO	NO	NO	NO	NO	NO	NO	NO
Location discloser	NO	NO	NO	NO	NO	NO	NO	NO
Sybil	NO	NO	NO	NO	NO	NO	NO	NO
Rushing	NO	NO	NO	YES	YES	YES	NO	NO
Routing loop	YES	YES	YES	YES	YES	YES	YES	YES
Replay	YES	YES	YES	YES	YES	YES	YES	YES
Flooding	YES	YES	YES	YES	YES	YES	YES	YES
Routing cache poisoning	YES	YES	YES	YES	YES	YES	YES	YES

the packet delay between two nodes. Location discloser attack cannot be prevented because any internal node intentionally can broadcast the topology information in the network. Rushing attack is prevented by ARAN, Ariadne, and SEAD because it follows the time synchronization between nodes. However, ARAN, Ariadne and SEAD do not have countermeasure for blackhole, wormhole, grayhole, sybil and location discloser attacks. Routing loop attack, replay, flooding, route cache and sybil attack are the external attacks of the control plane. To prevent external attacks, all the security routing protocol provides robust security services by using long keys and strong encryption algorithms. Due to this reason, replay attack is not possible and route looping attack is avoided because of protected sequence number and TTL by all secure routing protocols. Sybil attacker steals the legitimate user identities or uses the stale identities of legitimate user to participate in different routes of inter-network. This attack is also not addressed by any secure routing protocols. Route cache poisoning and flooding external attacks can be avoided because authorized nodes participate in route discovery and route maintenance phase. Existing IPMs are inadequate to protect against internal attacks which leads to data plane attacks in the network layer.

2.2.1.2 MAC Layer Intrusion Prevention Mechanisms

MAC layer attacks are caused by internal/ external (unauthorized) nodes. Network security attacks can be prevented by using strong authentication and key distribution mechanisms. Information security attacks can be prevented by securing the management frames. However, colluding attacks are still possible in WMNs because these attacks are caused by internal attackers and they have enough privileges to block the messages. We analyze the existing MAC layer security standards and security mechanisms with respect to four different security characteristics of WMNs such as protecting against unauthorized nodes, protecting against colluding attacks, securing heterogeneous devices/ networks and providing security at gateway level, router level and client level.

Mobisec is a centralized key distribution scheme in backbone mesh [Martignon et al., 2008]. In Mobisec, Key Server (KS) issues the keys to the newly joining routers. Once new router acquires of its private key, then it starts sending authentication request message. If this request message is received by its authenticated neighborhood routers, then checks the received request message. If it is valid then this request message is rebroadcasted in backbone mesh network. This process is continued until it reaches to the KS. When KS receives this request, first it authenticates by private key, which is issued at joining time. If this authentication is valid then the KS forwards secure communication key encrypted with private key to the request initiated router. To prevent stale authentication request messages, this secure communication key is periodically updated. This process creates additional communication and computational overhead. Mobisec can isolate the unauthorized nodes from WMNs by using legitimate mesh nodes public keys. However, Mobisec does not support heterogeneous networks, and colluding attacks are still possible because of single server authentication.

DSA-Mesh is an enhanced version of Mobisec, it could overcome the scalability problem at backbone by introducing distributed security architecture [Martignon et al., 2011]. In DSA-Mesh, backbone nodes (routers) are divided into two groups such as generic nodes and core nodes. This architecture mainly works on distributed proactive request protocol and session secret agreement protocol. In distributed proactive request protocol, initially any generic node M_i broadcasts the authentication message. When this packet is received by core nodes, they first verify the M_i certificate. Then they reply back to the M_i with its key K_i. M_i wait until it receives the 't' replies. Once it receives 't' replies then it forms the group key with t^{th} reply. Eventually it verifies the resultant key with known public key K_k. If this key is valid, it can be used to obtain the next session secret key after t_s seconds. This mechanism has problem of constructing public key when M_i gets only t-1 responses. Second, session secret agreement protocol in which key exchange mainly has taken place among core nodes. Initially all core nodes selects peer master of the session then peer master broadcasts a message. When a core node receives this message, it verifies the authentication and authorization of the message. Then, it chooses a random number to reply to the peer master. Peer master waits for the n-1 replies, and after verification of all received messages integrity and sender's identity. Eventually, peer master derives the public key and broadcast among core nodes. This public key is used to isolate the unauthorized nodes. On the other hand, each generic node requires 'n' number of core node signatures to join/ leave the network, which increases the severity of colluding attacks in this mechanism. DSA-Mesh does not address the heterogeneous client mesh networks security issues.

Mi Wen et al. proposed an Adaptive Key Management (AKM) mechanism [Wen et al., 2010]. This mechanism is mainly designed for wireless mesh and sensor network security. MPKM, MGKM, and TKM protocols are used to distribute the keys among sensor and mesh networks. Out of three protocols, Matrix Based Pairwise key Management (MPKM) protocol is essential to handle pairwise key establishment for the resource limited sensor nodes. In MPKM, Base Station (BS) acts as a trusted server and issues the seed (s_i) value to the cluster head. Then BS creates row seed matrix D based on prime number q and it creates column seed matrix B based on GF(q). The matrix B is public while the matrix D is kept secret by the base station. Since D was symmetric, the key matrix K = AB can be written as:

$$\text{K} = (DB)^T\text{B}=B^T D^T\text{B}=B^T \text{ DB} =(AB)^T=K^T$$

Thus K is also a symmetric matrix and K_{ij}=K_{ji}, where K_{ij} is the element of K at i^{th} row and j^{th} column. K_{ij} (or) K_{ji} is the pairwise key between node N_i and node N_j. The same technique is used to derive Matrix Based Group Key Management (MGKM) among cluster heads. In Threshold Key Management (TKM), the group keys of the WSNs will be calculated as a secret key shared by 'n' mesh nodes. The secret key can be recovered by a coalition of 't' mesh nodes. This mechanism can prevent unauthorized nodes based on MPKM, MGKM and TKM protocols. Each node requires 't' number of signatures to join/ leave the network, which increase the colluding attacks severity in this mechanism. Moreover, this mechanism does not consider multi-hop communication in client mesh.

SeGroM mechanism has proposed by Jing Dong [Dong et al., 2009]. The main objective of this mechanism is to reduce the communication and computation overhead of secure group communication. To achieve this, SeGroM-Hop was developed, in which each head members of the group encrypt the secret key (K_d) with each hop key of their downstream members instead of both upstream and downstream members. This K_d values prevents loss of forward and backward secrecy of each data packet. SeGroM works only on single group communication not for multi group communication. SeGrom framework does not discuss the security issues of client mesh networks.

Distributed IEEE 802.16j-2009 multi-hop relay security standard follows three level hierarchies [Peters and Heath, 2009]. Top-level master Base Station (BS) authenticates all two level hierarchy nodes called Relay Station (RS) and Mobile Station (MS). Initially these RS is formed Security Association (SA) with BS. Once, MS sends authentication request to RS, it forms security association with MS and then RS forwards to next subordinate RS, if the BS is not within the rage. The subordinate RS then establish SA with MS. This process will continue until request reaches to base-station. This process suffers from unauthorized nodes, for example, if a MM sends wrong request, it has to forward by intermediate RS until master BS recognizes the fraud id MM, means all the RS and SA association process had taken place before it is wasted. Due to single base station, colluding attacks are more severe in IEEE 802.16j security standard. This standard supports heterogeneous devices communication but not the heterogeneous networks. This security standard cannot be adapted to ad-hoc and sensor networks due to its high communication and computational overhead.

Zhang Yanchao et al. proposed Attack-Resilient Security Architecture (ARSA) for multihop wireless mesh networks [Zhang and Fang, 2006]. ARSA consists of two levels such as backbone mesh and client mesh. Id Based Cryptography (IBC) is used to authenticate backbone mesh and client mesh. In each node certification process, communication and computational overhead can be reduced because ARSA follows IBC instead of X.509 certification. To provide the operator service, each operator (O_i) needs to authenticate each mesh client (C_{ij}) by broker (B_i) and mesh router (R_{ij}) by session key (K_{ij}). O_i issues the temporary keys when each C_{ij} needs operator service. The temporary keys of mesh client is used to prevent unauthorized nodes. When a mesh client needs to send an authentication request to router (R_{ij}), it increases the communication range to establish a direct communication with R_{ij} if mesh client is not within the radio range of R_{ij}. This process can isolate colluding attacks in client mesh. On the other hand, Colluding attacks in backbone mesh are not addressed because ARSA supports multi-hop communication in client mesh, but not in backbone network. In addition to this, it does not address the heterogeneous networks security and fails to address the security of all the three level mesh nodes.

IEEE 802.11i security standard was approved in june 2004 as the standard for security of the MAC layer of the wireless network and it adapts various wireless networks security protocols such as WAP, WAP2, and 802.11r, 802.11s and 802.15 standards. The objectives of 802.11i are to provide data confidentiality, data integrity and authentication [802.11i 2004 Amendment6, 2004]. It uses robust security network association (RSNA) for data confidentiality, integrity and 802.1X for authentication. RSNA is used to establish authentication or association between supplicant and access point includes the four-way handshake protocol. In 802.1X extensible authentication protocol (EAP) is used generate pairwise Master key (PMK) between authenticator and supplicant. 802.11i authentication scheme contains 5-phases [802.11i 2004 Amendment6, 2004].

Phase 1: Access Point (AP) receives the Mobile Node (MN) station authentication request which contains RSN Information Element (RSNIE) in open authentication phase and then the Mobile Node (MN) is associated with AP.

Phase 2: 802.1X authentication is used to establish Pairwise Master Key (PMK) between Authentication Server (AS) and mobile node after this AS shared this PMK with AP.

Phase 3: A four-way handshake protocol is used between the MN and the AP to derive,

bind, and verify a Pairwise Transient Key (PTK). The PTK is a collection of operational keys: Key Confirmation Key (KCK), as the name implies, is used to prove the possession of the PMK and to bind the PMK to the AP. Key Encryption Key (KEK) is used to distribute the Group Transient Key (GTK).
Phase 4: Protected data transfer happens based on PTK and GTK. PTK is used to encrypt the unicast messages and GTK for broadcast and multicast messages.
Phase 5: Mobile node connection termination or de-authentication is necessary when the mobile node leaves the access point.
802.11i authentication scheme is used as Wi-Fi Protected Access (WPA2) in Wi-Fi networks. WPA2 uses counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to provide authentication, confidentiality and integrity of each message in Wi-Fi networks.

802.11s is a standard for wireless mesh network certified by Task Group (TG) in 2006 [Akyildiz.F, 2009, Islam et al., 2009]. The security framework of 802.11s uses the 802.11i authentication scheme with small amendments and provides cryptographic functionalities such as authentication, integration and confidentiality. To justify these functionalities, 802.11s framework is organized hierarchically as authentication server (AS), mesh key distributor (MKD) at upper level, Mesh Authenticator (MA), Mesh Point (MP) at lower level. Here, the mesh node hierarchy changes based on security keys it holds, if the MP has both MKD and MA functionalities it is called portal or gateway, else if MP has neither MKD nor MA then it called as supplicant. In this security framework, MA and MP are with in the range of MKD. To create PTK and GTK at MP between MA, Authentication Server (AS) derives Pair-wise Master Key (PMK) at MKD by using either Pre-Shared Key (PSK) or Master Session Key (MSK). Then MKD issues the pair-wise master key to MP and MA. Based on pair-wise master key, MA and supplicant initialize a PTK and GTK by using using four-way handshake protocol as shown in Figure 2.9. Since, the mesh clients are directly communicated to the authentication server, colluding attacks are not possible (NP) in WPA2 and 802.11s. However, 802.11s and WPA2 only support client mesh authentication and also not consider the backbone mesh and heterogeneous networks security. In addition to this, both

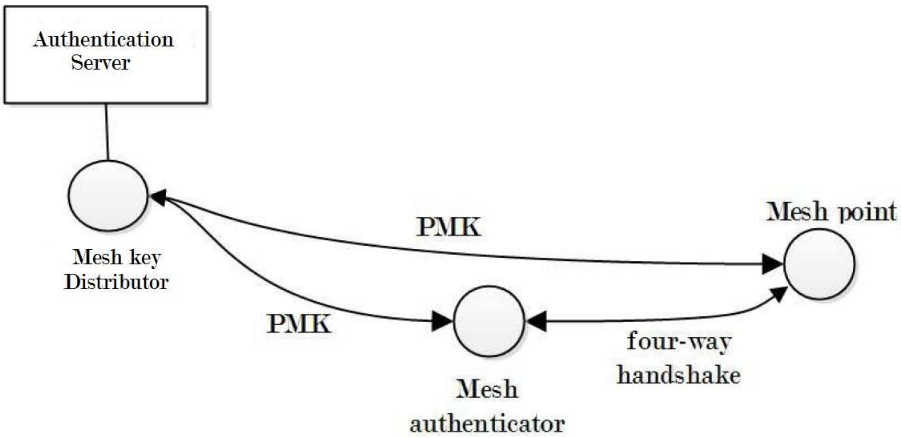


Figure 2.9: 802.11s Security Framework

security standards suffer form unauthorized node due to inherent flaw in their four-way handshake protocol [Altunbasak and Owen, 2004].

Analysis of existing security mechanisms (ESM) with respect to all four different characteristics (FDC) of WMNs is shown in Table 2.2. All these mechanisms are only able to protect unauthorized attacks and/ or colluding attacks from either backbone mesh or client mesh. In addition, these mechanisms do not consider the security of heterogenous client mesh networks. Thus, security of three level mesh nodes is incomplete. Based on the analysis study, we can conclude that existing security mechanisms are inadequate to support all four characteristics of WMNs. On the other hand, channel jamming attacks which we described in section 2.1.2 create DoS attacks. To prevent channel jamming attacks, we need centralized authentication channel assignment system, but it not possible due to dynamic channel allocation in large scale networks. Several anti-jamming methods are available such as Group based management of multichannel allocation algorithm, Hyacinth Model, assignment of unique a pseudo-noise codes [CHI.Y and RONG.J, 2007], [Haq.A and Naveed.A, 2007]. However none of the prevention technique guarantees the complete security.

2.2.1.3 Physical Layer Intrusion Prevention Mechanisms

Physical layer attacks are explained in section 2.1.3 can simply jam the entire network operations no matter how secure the upper layer protocols such as MAC, network layer and transport layer. These radio jamming attacks are created by either internal or ex-

Table 2.2: Analysis of MAC layer Intrusion Prevention Mechanisms

ESM / FDC	MobiSec *Martign 2008*	DSA-Mesh *Martign 2011*	AKM *Mi Wen 2010*	SeGroM *Dong.J 2009*	802.16j *IETF group 2009*	ARSA *Zhang.Y 2006*	WPA2 *IETF group 2004*	802.11s *TG 2006*
Protect against unauthorized nodes	Backbone mesh	Backbone mesh	Backbone mesh	Backbone mesh	Backbone mesh	Client Mesh	Client Mesh	Client Mesh
Protect against colluding internal attacks	NO	NO	NO	NO	NO	Client Mesh	Client Mesh	Client Mesh
Heterogeneous devices and networks security	NO	NO	NO	NO	NO	NO	NO	NO
Three level security	Gateway & Router levels	Gateway & Router levels	Gateway & Router levels	Gateway & Router levels	Gateway & Router levels	Client level	Client level	Client level

ternal attackers in WMNs. Here, internal attackers can attack easily because they have secret information about neighborhood channels, on the other hand external attackers have to use brute force method. To protect against these radio-jamming attacks WMNs need strong jamming resistance techniques are needed. The well-known jamming resistance techniques are spread spectrum techniques such as Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). These techniques use a shared secret key between communication parties. The problem of these techniques is that, the attacker can learn the keys of target nodes and disturb the target nodes communication [Haq.A and Naveed.A, 2007]. Many anti-jamming techniques have been proposed without using shared secret key. Baird proposed a coding approach to encode data to be transmitted into ”marks” (e.g., short pulses at different times) that can be decoded without any prior knowledge of keys (UDSSS), which avoids jamming by randomly selecting a spreading code sequence from a pool of code sequences [Baird.L and Bahn, 2007]. RD-DSSS relies completely on publicly known spreading codes and it does not require any shared key among the sender and the receiver. Uncoordinated Frequency Hopping (UFH) communication is the one in which the sender and the receiver choose the frequency channels uniformly at random from a set of common frequency channels. However these techniques are still suffering from isolating the physical layer jamming-attacks.

2.2.1.4 Research Directions

A number of intrusion prevention mechanisms have been discussed which are aimed at solving core layer attacks. However, the IPMs of WMN have number of research issues that require a considerable attention.

- New secure routing protocols needs to be developed to prevent/ mitigate the internal colluding attacks such as blackhole, gryhole, sybil, wormhole, jellyfish and byzantine attacks.
- The secure routing protocols need to be adaptive in backbone mesh as well as client mesh. In addition to this, these routing protocols needs to have minimum communication and computational overhead.
- Enhancing the efficiency of existing key management mechanisms or developing the new key managements mechanisms are needed to prevent colluding attacks and unauthorized nodes at MAC layer.
- The key management mechanisms needs to address the heterogeneous devices/ network security issues for improving scalability and high availability of WMNs.
- The key management mechanisms needs to ensure the gateway level, router level and client level authentication in WMNs. These mechanisms do not incur unacceptable overheads to cater for mobility or robust in an effort to accommodate the trade-off between available resources.
- New secure distributed channel allocation algorithms need to be developed to prevent channel jamming attacks in multi-radio multi-channel wireless backbone mesh networks.
- New efficient physical layer encryption mechanisms needs to be developed for preventing signal jamming attacks such as random jamming and reactive jamming attacks.

2.2.2 Intrusion Detection Systems (IDSs)

We have discussed Intrusion Prevention Mechanisms (IPMs) with respect to core layer attacks in previous section. The existing IPMs are inadequate to prevent the internal attacks because internal attackers (compromised nodes) have enough privileges to join the network. To overcome this drawback, the Intrusion Detection Systems (IDSs) are introduced. IDS is an analysis engine and goal of IDS is to have high detection rate and low false alarm rate. In recent years, many IDSs have been proposed to identify the internal attackers in wireless networks. Wireless Mesh Networks (WMNs) adopts IDSs from other wireless networks such as MANETs, sensor networks and wireless LAN [Wang, 2006], [Zonghua.Z et al., 2008]. All these existing IDSs are mainly classified into three types such as misuse-based IDS, anomaly-based IDS and specification-based IDS.

Misuse-based or Signature-based IDS compares the current activities by using the pre-computed attack signatures or patterns. It should sustain signature database, which is built based on past experience of known anomalies. These anomalies have been confirmed when the activity matches with any signature in the database otherwise this activity has confirmed normal behaviour.

In **Anomaly-based IDS**, database contains the information about the normal behaviour of the protocol. To obtain the normal behaviour, it uses statistical analysis of training data. This training data is periodically updated to detect all anomalies (known and unknown) which are significantly deviated from the normal behaviour.

In **Specification-based IDS**, manually specified program behavioral specifications are used as a basis to detect anomalies. At run time, automata-based IDS is used to detect known and unknown attacks of its verification phase. Known attacks are identified based on specified vulnerabilities and unknown attacks are identified by deviation from the normal behaviour.

Based on these consepts, many IDSs have been proposed in recent years. Most of the IDSs are proposed for network layer due to increasing number of vulnerabilities in routing and data forwarding functionalities, and followed by MAC layer and physical layer. All IDSs fall-into three categories such as Single-layer IDS (SIDS), Cross-layer IDS

(CIDS) and reputation based IDS. SIDS considers layer independent paraments, CIDS considers the layer dependent paraments and reputation based IDS considers reputation of the nodes to detect the core layer attacks. Most of the detection systems are proposed under network layer because this layer has more vulnerabilities as compared to MAC and physical layer. In network layer, we mainly study the IDS for wormhole attacks because this attack severely affects the long-distance wireless links in wireless mesh networks.

2.2.2.1 Single-layer IDSs (SIDSs)

a) Network layer IDS

Hao yang et al. proposed a specification-based self-organized network-layer security in mobile ad-Hoc networks (SCAN) which uses collaborative mechanism [Hao.Y and James.S, 2006] to detect blackhole attackers. In collaborative mechanism, local area nodes collaboratively monitor each other to detect the individual blackhole attackers. Local monitoring nodes set threshold value (t) to protect against t colluding attackers. However, local monitoring nodes can only detect one_hop distance blackhole attacks by cross-verification with their neighbours.

S.Marti et al. proposed a specification-based watchdog IDS. In this IDS, each node (n_i) is monitored by their neighbours (monitor nodes) in promiscuous mode to calculate the incoming and outgoing packet ratio of n_i. If this ratio is 1 then n_i has normal behaviour otherwise n_i has malicious behaviour [Marti.S et al., 2000]. This IDS has less communication overhead because no extra packets are used to know the behaviour of n_i. Watchdog IDS can detect only one hop byzantain, blackhole and grayhole attacks.

Parag S. et al. proposed WatchAnt which uses challenge-response based IDS for detecting packet forwarding misbehaviour of neighbouring nodes in WMNs [Parag and Kalman.G, 2010]. In packet forwarding path, if a node wants to verify one hop node packet forwarding behaviour, it is depending on next to next hop (two hop) node received packets information. WatchAnt IDS can detect only one hop byzantain, blackhole, grayhole and routing loop attacks.

Yi-an Hung and Wenke proposed a cooperative anomaly-based IDS in ad-hoc networks and it uses cross-feature analysis approach. This approach explores the correlations between each feature and all other features [Huang and Lee, 2003]. Here, cooperative intrusion detection works to generate these features (training data). Once, this approach calculates the average probability of input values of a particular node with trained data then these values are compared with it threshold value. In this approach, 141 features have been derived to identify the known attacks such as blackhole and maximum sequence and rushing and flooding and routing loop attacks. This approach is not effective in WMNs because it does not take physical layer or MAC layer parameters such as collisions or queueing delays into the consideration. Thus, cooperative anomaly-based IDS has high false alarm rate when it is adapted by WMNs.

Hu et al. have proposed a technique based on the concept of geographical and temporal leashes to prevent the wormhole attacks from active paths [Hu et al., 2003]. The geographical leashes are used to restrict the long-distance communication between nodes. In this approach, each node has to know its current location and maintains loosely coupled synchronized clocks with all other nodes in the network. The temporal leashes are used to restrict the maximum time difference between any two communicating nodes. This time value must be known by all nodes in the network. All the above approaches require additional mechanisms to synchronize the clocks of all nodes. Jane Zhen and Sampalli Srinivas have tried to detect wormhole attacks using RTT between one-hop nodes [Zhen and Srinivas, 2003]. All the nodes in the network calculate RTT of their neighbours. If the neighbouring nodes have higher RTT then these nodes are treated as wormhole attackers. Jane Zhen et al. consider that RTT between two fake neighbours is always higher than two real neighbours [Zhen and Srinivas, 2003]. This approach is not able to detect wormhole attacks because long-distance communication nodes may have higher RTT value.

Tran Van Phuong et al. proposed a transmission time based mechanism to detect wormhole attacks by computing RTT between every two successive nodes along the established path during route setup procedure [Van Phuong et al., 2007]. Maximum threshold of RTT is set at runtime in the network to detect the wormhole attacks. Khabbazian et al. have proposed a timing-based solution to detect the wormhole attacks [Khabbazian et al., 2009]. They use hello packets to calculate each link delay and each node has to calculate one-hop neighbours delay followed by two-hop neighbours delay and so on. All the one hop and two hop delays are compared with the maximum transmission range delay. Wormhole attacks are detected when the delay is higher than the maximum transmission range delay. Jie Zhou et al. proposed a neighbor-probe-acknowledge algorithm (NPA) to detect wormhole attacks by identifying the occurrence of large standard deviation of round trip time (stdev(RTT)) [Zhou et al., 2012].

Chiu et al. proposed Delay Per Hop Indication (DELPHI) for wormhole attack detection. They observe the delay and hop count of different paths between source to destination to fix the maximum $\frac{delay}{hop}$ value [Chiu and Lui, 2006]. If any path $\frac{delay}{hop}$ value is more than maximum $\frac{delay}{hop}$ then this path is detected as wormhole malicious path. Xia Wang et al. proposed an End-to-end Detection of Wormhole Attack (EDWA) [Wang and Wong, 2007]. To detect the wormhole attack, EDWA estimates the smallest hop count between source and destination. If the hop count of a received shortest route is much smaller than the estimated value then wormhole attack is detected on the route.

Dezun Dong et al. proposed topology based method to detect the wormhole attacks [Dong et al., 2011]. Based on network topology, they set the maximum transmission range of a node. This predefined maximum transmission range is used by mesh nodes to detect wormhole attackers in rouging paths. Hayajneh et al. proposed a DeWorm protocol to detect wormhole attacks [Hayajneh et al., 2009]. In DeWorm protocol, each source node is to find alternative paths to a target node such that does not pass through the wormhole path. These alternative paths will be significantly different in length compared to the wormhole path, then this path is detected as wormhole malicious path.

b) MAC layer IDS

Stephen glass et al. present a MAC layer based intrusion detection mechanism which uses a secure positive acknowledgement message between a sender and receiver to detect the malicious wormhole attacks [Glass et al., 2009]. This positive acknowledgement is protected by a shared secret key and message digest of sender and receiver. The adversary cannot predict which frames are acknowledged or not without the knowledge of the shared key. Consequently, sender and receiver can identify the wormhole attackers based on false acknowledgements sent by the adversary.

Loukas L. et al. proposed control channel architecture and control channel maintenance scheme [Lazos.L and Krunz.M, 2011]. In control channel architecture, to mitigate the impact of jamming, it uses a dynamic control channel allocation strategy, whereby each cluster establishes and maintains its own control channel. In control channel maintenance scheme, each node of the cluster hop between channels in a pseudo-random fashion, following a unique hopping sequence not known to other nodes. If the jammer captures the hopping sequence of a compromised node, this node can be uniquely identified. This mechanism can detect MAC layer channel jamming attacks. This mechanism is not effective in client mesh due to mobility and energy constraints.

c) Physical layer IDS

Fragkiadakis et al. proposed anomaly-based detection algorithms for detecting jamming attacks in 802.11 networks [Fragkiadakis.G et al., 2010]. Based on signal to noise ratio (SNR) value, these algorithms are classified into two types namely simple threshold algorithms and cumulative sum algorithms. Simple threshold algorithms have better performance in terms of the detection rate and false alarm rate when applied to measurements collected at node *close* to the jammer. On the other hand, cumulative sum algorithms have better performance when measurements collected at node from the jammer. This IDSs can detect the periodic jamming effectively.

All these SIDSs suffer from high false positive and false negative rate as layer independency parameters are more volatile to analyse the anomalies of each layer in WMNs. For example packet drops occur for various reasons such as congestion, jamming, channel interferences, TTL packet expired, and duplicate packets. Hence, SIDSs need other layer support to improve the intrusion detection rate.

2.2.2.2 Cross-Layer IDSs (CIDSs)

Cross-layer Intrusion Detection Systems (CIDSs) consider multi-layer interactions such as such as network plus MAC or physical plus MAC plus network layer layers etc. to analyze the malicious behavior of nodes. For example, channel allocation collisions in MAC layer affects the routing performance in network layer, thus MAC layer performance is considered in network layer to effectively judge the anomalies. CIDSs receive more attention than SIDSs because of their comprehensive ability to judge the anomalies in WMNs.

a) Network plus MAC layer IDS

Xia wang proposed cross-layer based anomaly detection in wireless mesh networks in which routing layer intrusion detection depends on network plus MAC layer trained data and it is limited to local system [Wang.X and Wong.J, 2007]. This cross-layer IDS can detect probe flooding attack at MAC layer, and blackhole and grayhole attacks at network layer.

Jim parker proposed cross-layer IDS for detecting wireless misbehaviour [Parker et al., 2006]. In cross-layer IDS, number of RTS packets at MAC layer is used to detect network layer grayhole and blackhole attacks and to reduce the false alarm rate. Moreover, the number of RTS packets generated by a node is fixed.

Geethapriya proposed cross-layer IDS for wireless mesh networks. This CIDS follows two methods of intrusion detection namely CIDS-I and CIDS-II. In CIDS-I, malicious node data is collected from different layers to identify the truly malicious nodes in the network [Thamilarasu.G et al., 2005]. In CIDS-II, malicious node data collection and detection occurs on same layer. Any detection found on CIDS-II, it passes to CIDS-I for further analysis. It detects blackhole and grayhole attacks at network layer.

b) MAC layer plus physical layer IDS

Xu el at. proposed cross-layer IDS that works based on jamming detection with consistency checks [Xu.W et al., 2003]. The main goal of this approach is to discriminate jamming attacks from normal congested scenarios and other cases caused by poor link quality and sudden failures of nodes. To do this, two enhanced detection algorithms are proposed which employ signal strength for a consistency check, and location information for a consistency check. Signal strength consistency check is performed to see whether the low MAXimum Packet Delivery Ratio (MAXPDR) values are consistent with signal strength and the signal strength measurements. This mechanism mainly addresses the random jamming, constant jamming, deceptive jamming, and reactive jamming. Moreover, this mechanism is effective only when the network has less mobility, and less number of nodes.

Mishra et al. proposed MAC plus physical layer distributed monitoring scheme to perform multiple phases of detection namely phase-I and phase-II detection. In phase-I, a monitoring node seems to find the malicious behaviour such as jamming and collision [Sudip.M et al., 2011] of its neighboring node (n_j). Once monitoring node finds an attack, it will pass to phase-II detection in which channel utilization value of n_j is calculated. If this value exceeds the threshold value then monitoring node conforms n_j has jamming attacker otherwise n_j has non-malicious node. In analysis part, it can detect physical jamming, MAC layer packets (RTS/CTS) flooding and interference attacks in 802.11.

2.2.2.3 Reputation based IDSs

Both SIDSs and CIDSs are effective in steady-state traffic. In unsteady-state traffic, these IDSs suffer from low detection rate and high false alarm rate because the detection parameters such as number of packet drops and delay can be affected. To overcome this problem, reputation based IDSs allow the suspected node until the reputation of this node reaches to the threshold value. Repuation based IDSs consider the number received and forward packets of a node to find the reputation of the nodes. Reputation based IDSs can be classified into two types such as node independent (self-organized) and node dependent (collaborative). These IDSs protect against network layer attacks because the received and forward packets of a node are considered at network layer. In node independent mechanism, all nodes independently assess their neighbour's reputation based on direct interactions. In node dependent mechanism, cooperative nodes exchange reputation tables among themselves. We explain these two types of reputation mechanisms below:

a) Node independent (self-organized) reputation based IDSs

M. Tamer Refaei et al. proposed a reputation based IDSs for isolating selfish nodes in ad-hoc networks [Tamer.M and Vivek.S, 2005]. In this mechanism, nodes do not depend on monitoring of neighbours in promiscuous mode and exchange reputation information in group of nodes. Instead of depending on other nodes in the network, this mechanism works autonomously. Every node identifies and isolates selfish nodes based on reputation value. Each node maintains reputation table which stores all one-hop neighbouring reputation values. Reputation of each node value (r_0) in the routing path has been incremented/ decremented based on the destination information. If a node r_0 value falls below the threshold value then this node is treated as selfish and it is blacklisted. This mechanism has less communication overhead due to its self-organized reputation management. On the other hand, it can only detect one-hop distance malicious nodes.

Parag S. mogre et al. proposed AntRep for isolating all detected attackers from active routes [Parag and Kalman.G, 2010]. The reputation management is implemented on a distributed and decentralized fashion. Moreover, AntRep represents all information gathered by WathAnt which is explained in section 2.2.1.1. Here, each node maintains reputation table of neighbor's and these table values are not shared with any other nodes in the WMN. For normal behaviour, of a node reputation value lies between [-25, 25] and for selfish node behaviour, it lies between [-26, -40]. If a node reputation value falls under -40 then this node is revoked from active routes. Advantages of WathAnt are that it is more accurate and faster to isolate the known attacks and easy to maintain in one hop distance nodes and it has less network overhead. On the other hand, it can only detect one-hop distance malicious nodes.

Xiu-feng et al. proposed MTSR to isolate the wormhole attacks. In MTSR, each node calculates trust values of neighbour nodes by monitoring their incoming and outgoing packets [Xiu-feng et al., 2010] . If a node in the network finds the trust value of neighboring node which falls below the threshold value then neighboring node is isolated from the data-forwarding path.

b) Node dependent (collaborative) reputation based IDSs

Buchegger Sonja et al. proposed Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT) protocol [Buchegger and Le Boudec, 2002]. It empowers DSR IDSs with watchdog and pathrater by adding a reputation model. CONFIDANT framework consists of four major components such as reputation system, trust manager, monitor and path manager. If a node detects its neighbouring node's malicious behaviour, then this node reduces the reputation value of its neighboring nodes. On the other hand, trust manger sends and receives alarm messages from it local neighboring nodes. When a node receives alarm from a trust manager of a particular node then reputation of that node decreases in its reputation table. Path manger takes care of two functionalities i.e 1) isolate a node from the path when the node's reputation goes below the threshold value and 2) find a new path with highest reputation. Malicious nodes can be isolated by trust manager from locally and globally.

Qing ding et al. proposed a REputation based PROactive (REPRO) routing protocol for the wireless mesh Backbone [Ding.Q and Jiang.M, 2009]. In this protocol, the Adaptive Reputation Management Framework (ARMF) consists of four major functionalities such as reputation model, reputation context manger, adaptation manager and application context subscription manger. The reputation model defines the process of raw data and explores the metrics such as link quality, queue length of the nodes. The reputation context manger collects the raw data from different sensors and data process through standard-based process models. The adaptation manager performs cross-layer context monitoring with the reputation context manger. The application context subscription manger manages the QoS, overload balance and other constraints of these applications. REPRO results are effective only when sensors are not compromised and these results are affected by colluding attacks. It takes much time to decide an attack.

Francesco et al. proposed AODV Reputation Extension (AODV-REX) protocol [Franscesco.O and Simon.P, 2008]. It considers most trustworthy path, instead of shortest path in AODV. In AODV-REX, each node maintains local and global reputation levels of its neighbours. Each node (monitor) calculates its neighbour node (n_g) local reputation value by using watchdog mechanism. Monitor disseminates n_g IP address and its reputation value by using Route REQuest (RREQ). Once any neighbouring node receives this RREQ , first it extracts the n_g reputation value and constructs the global reputation value of n_g. The local and global reputations are used to estimate the actual behaviour of n_g. Route REPlay (RREP) process in AODV-REX considers the hop-count plus reputation metric of each link on the route selection path.

Khalil et al. proposed a behaviour based SIDS (LiteWorp) to detect and isolate the wormhole attacks in MANET [Khalil et al., 2007]. LiteWorp approach collects statistical information from the monitored nodes of in and out packets of their neighbouring nodes. Each link is monitored by several monitoring nodes and stores this information. In addition, the monitoring nodes check whether both packets transmitted by the monitored nodes are identical or not to detect the wormhole attacks. This approach is inadequate to protect against wormhole attacks when the wormhole attacker intentionally increases the delay for all the received packets since monitoring nodes only check whether the received packets are identical or not. In this approach, each monitored node stores '*t*' number of packets per unit time to monitor one neighbouring node behaviour. To monitor all neighbouring nodes, each monitored node requires *t * number of neighboring nodes*. Hence, storage overhead of each monitored node increases as its number of neighboring nodes increases. It is difficult for each monitored node to monitor all links of its neighboring nodes because each node uses multiple channels to communicate with its neighbouring nodes.

Zhang et al. proposed a novel anomaly detection approach, called RADAR, to detect and isolate malicious mesh nodes in WMNs by fully exploring the spatio-temporal properties of mesh node behaviour [Zhang et al., 2008]. In this cooperative anomaly detection approach, neighbors change the node's reputation value based on its received and forwarded packets. This reputation value is used to calculate the trust value of a node. RADAR isolates the attackers from WMNs based on node's trust values. However, node dependent reputation based IDSs take more time to declare a node as malicious node. In additions to this, these IDSs suffers from high false alarm rate and more communication overhead.

Existing node independent or dependent reputation based IDSs do not consider the cross layer parameters, instead they only consider the single layer paraments. Due to inadequate layer parameters to judge the malicious nodes, reputation based IDSs may have low detection rate and high false alarm rate. Table 2.3 show the analysis of existing IDSs with respect to core layer attacks.

2.2.2.4 Research Directions

We have analyzed various intrusion detection systems with respect to core layer attacks. Based on the our analysis, there is a need to develop IDSs for both backbone mesh and client mesh.

- Resource constraint client mesh networks such as sensor and mobile ad-hoc networks need effective IDSs in terms of detection speed and less storage overhead. Whereas, monitoring cross-layer parameters or maintaining reputation of mesh clients need more time to detect the attacks and create more overhead in these networks. Thus, single layer IDSs are still essential for client mesh networks to isolate the network layer attacks such as jellyfish, sybil attacks, MAC layer authentication flooding, mesh node hijacking attacks and physical layer reactive jamming attacks.

- Backbone mesh routers have less resource and less mobility as compared to mesh clients. Thus, the advantages of CIDSs can be used in backbone mesh for detecting more severe colluding attacks such as wormhole attacks, jellyfish attacks and sybil attacks.

- In node independent reputation based IDSs, mesh nodes only able to isolate the attacks from its one-hop neighbours. On the other hand, these reputation based IDSs are more accurate and take less time to detect attacks as compared to node independent reputation based IDSs. Thus, enhanced node independent reputation based IDSs need to consider the drawbacks of these IDSs.

Table 2.3: Analysis of Existing IDSs with Respect to Core Layer Attacks

Types of IDSs	Author name/ year	Detection	Approach
Network Layer	[Hao.Y and James.S, 2006]	Blackhole attack	Specification-based
Network Layer	[Marti.S et al., 2000]	Byzantine, blackhole, grayhole attacks	Specification-based
Network Layer	[Parag and Kalman.G, 2010]	Replay, Blockhole, flooding, Routing loop attacks	Misuse-based
Network Layer	[Huang and Lee, 2003]	Rushing,flooding,routing loop, balckhole and grayhole attacks	Anomaly-based
Network Layer	[Hu et al., 2003], [Zhen and Srinivas, 2003], [Van Phuong et al., 2007], [Khabbazian et al., 2009], [Chiu and Lui, 2006], [Wang and Wong, 2007], [Dong et al., 2011], [Hayajneh et al., 2009]	Wormhole attacks	Misuse-based
MAC Layer	[Glass et al., 2009], [Lazos.L and Krunz.M, 2011]	Channel jamming attacks	Misuse-based
Physical Layer	[Fragkiadakis.G et al., 2010]	Radio Jamming attacks	Anomaly-based
Network + MAC Layers	[Wang.X and Wong.J, 2007]	Blackhole, Grayhole, RTS flooding attacks	Anomaly-based
Network + MAC Layers	[Parker et al., 2006]	blackhole and grayhole attacks	Misuse-based
Network + MAC Layers	[Thamilarasu.G et al., 2005]	balckhole and grayhole attacks	Specification-based
MAC + Physical Layers	[Xu.W et al., 2003]	random jamming, constant jamming and deceptive jamming, and reactive jamming	Anomaly-based
MAC + Physical Layers	[Sudip.M et al., 2011]	Radio jamming Collision, RTS/CTS flooding attacks	Specification-based
Reputation based Node Independent	[Tamer.M and Vivek.S, 2005], [Parag and Kalman.G, 2010], [Xiu-feng et al., 2010]	Blackhole, Grayhole, fake control or data flooding attacks	Specification-based
Reputation based Node Dependent	[Buchegger and Le Boudec, 2002], [Ding.Q and Jiang.M, 2009], [Francesco.O and Simon.P, 2008], [Khalil et al., 2007], [Zhang et al., 2008]	Blackhole, Grayhole, wormhole, fake control or data flooding attacks	Specification-based

- New reputation based cross-layer intrusion detection systems need to be developed for detecting the core layer attacks in unsteady-state network traffic.

Based on the literature, existing prevention or detection solutions are able to address the security issues either in backbone mesh or client mesh. These solutions are inadequate to provide complete solution for hybrid wireless mesh network because it needs the security solution which works on both backbone mesh and client mesh.

2.3 Summary

We have discussed the various attacks and their classification at the core layers. The countermeasures of these attacks are mainly classified into two main types namely intrusion prevention and intrusion detection solutions. The both of these security solutions are legacy to protect from the malicious nodes in hostile network. Moreover, very few frameworks have been proposed which includes both of the intrusion prevention and intrusion detection solutions. However, all these frameworks are inadequate to protect the unique characteristics of WMNs. Hence, future security frameworks of wireless mesh networks should support both the prevention and detection solutions for protecting unique characteristics of WMNs from internal and external attacks. On the other hand, these solutions need to be developed in both backbone mesh and client mesh for HWMNs.

Chapter 3

PROBLEM DESCRIPTION

The research issues and challenges in the area of backbone mesh and client mesh security have been discussed in the previous chapter. In this chapter, we describe the problem which is addressed in this thesis and the objectives of the proposed multi-layer security framework.

3.1 Problem Description

Problem Description The unique characteristics of HWMNs, like integration, interoperability and long-distance links are more vulnerable to various network layer and MAC layer attacks. Few existing security prevention and detection solutions address both network layer and MAC layer attacks in wireless mesh networks. However, these prevention and detection solutions protect the HWMNs either in backbone mesh or client mesh. These solutions are inadequate to address the most severe network layer and MAC layer colluding attacks. In this thesis, we have developed a multi-layer security framework for HWMNs to protect the legitimate mesh routers and mesh clients at the MAC layer and their legitimate routing paths at the network layer.

3.1.1 Objectives of Multi-layer Security Framework

The proposed security framework consists of two objectives which address the unsolved security issues in HWMNs.

Objective 1: A multi-level key management mechanism is developed to secure both legitimate mesh routers and mesh clients from malicious nodes by using the centralized and distributed authentication schemes.

Objective 2: A dynamic reputation-based cross-layer intrusion detection system is developed to secure the legitimate routing paths from wormhole attacks by using dynamic reputation and behavior based cross-layer Parameters.

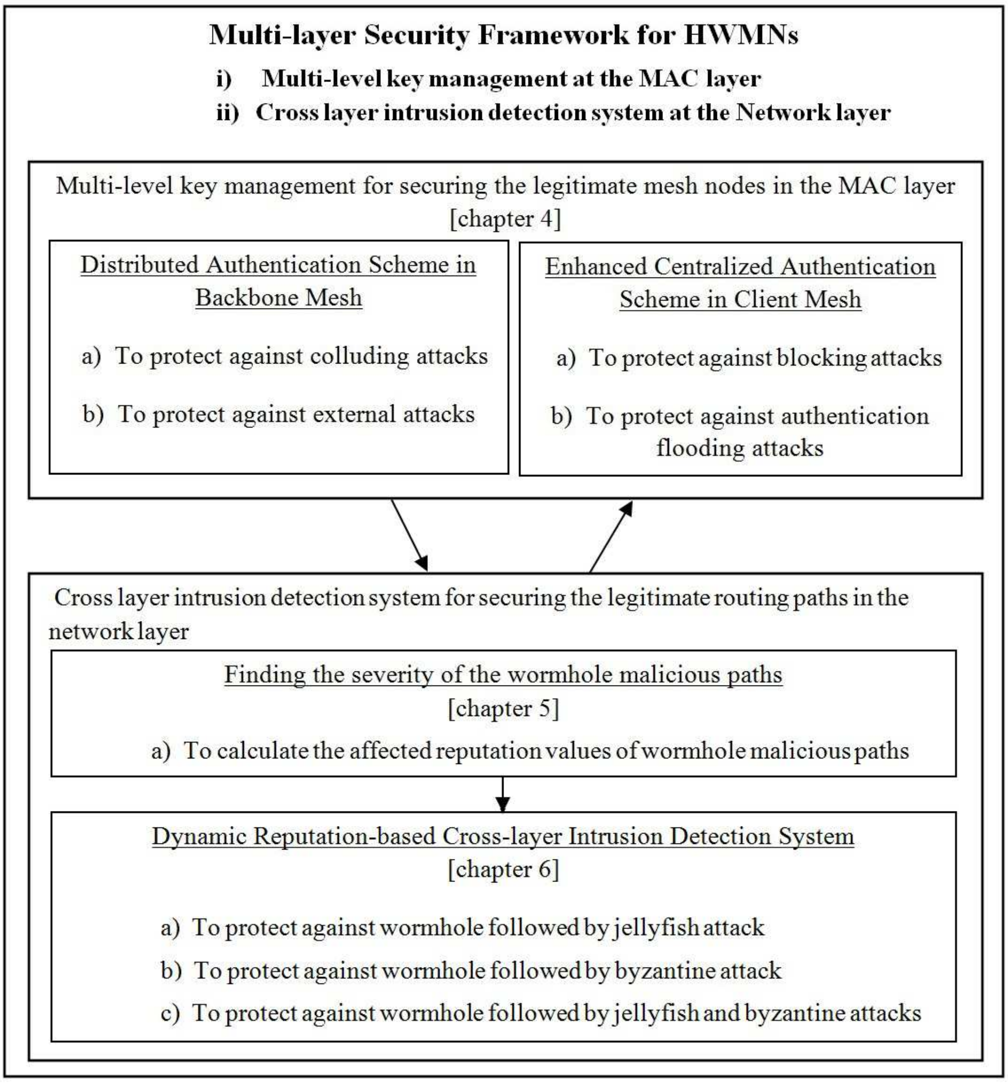

Multi-layer Security Framework for HWMNs
i) Multi-level key management at the MAC layer
ii) Cross layer intrusion detection system at the Network layer
Multi-level key management for securing the legitimate mesh nodes in the MAC layer [chapter 4]
Distributed Authentication Scheme in Backbone Mesh
a) To protect against colluding attacks
b) To protect against external attacks
Enhanced Centralized Authentication Scheme in Client Mesh
a) To protect against blocking attacks
b) To protect against authentication flooding attacks
Cross layer intrusion detection system for securing the legitimate routing paths in the network layer
Finding the severity of the wormhole malicious paths
[chapter 5]
a) To calculate the affected reputation values of wormhole malicious paths
Dynamic Reputation-based Cross-layer Intrusion Detection System
[chapter 6]
a) To protect against wormhole followed by jellyfish attack
b) To protect against wormhole followed by byzantine attack
c) To protect against wormhole followed by jellyfish and byzantine attacks

Figure 3.1: Multi-layer Security Framework for HWMNs

Based on the objective 1 and 2 the proposed security framework protects both backbone mesh and client mesh. It includes

- Distributed authentication scheme and Enhanced centralized authentication scheme for protecting against MAC layer information security and network security attacks.
- Dynamic Reputation based Cross-layer IDS (RCIDS) for protecting against network layer wormhole attacks.

Figure 3.1 gives an overview of the structure of our framework. In the proposed framework, digital authentication scheme secures the legitimate mesh routers from colluding and external attacks in backbone mesh. On the other hand, enhanced centralized authentication scheme secures the mesh clients from blocking and authentication flooding attacks. Based on distributed and enhanced centralized authentication schemes, legitimate mesh nodes are able to initialize the certified authentication keys in both backbone and client mesh. These authentication keys are used for protecting the network layer packets. However, authentication schemes need a support from intrusion detection system since, internal attackers are still able to perform wormhole attacks in the network layer. The proposed dynamic reputation based cross-layer intrusion detection system secures the routing paths from wormhole attacks such as wormhole, jellyfish and byzantine attacks in the network layer. When the internal wormhole attackers are detected by the dynamic RCIDS, the authentication keys (created by distributed and enhanced centralized authentication schemes) of these internal attackers are revoked by the mesh nodes authentication tables.

Chapter 4

MULTI-LEVEL KEY MANAGEMENT MECHANISM FOR HWMNS

4.1 Introduction

In chapter 2, we have discussed various MAC layer network security and information security attacks performed by malicious nodes. Protecting legitimate mesh routers and mesh clients from malicious nodes at the MAC layer is still a challenging issue in HWMNs. The existing key management mechanisms are broadly classified into main types namely centralized and distributed key mechanisms to protect against these attacks. Centralized key management mechanisms used in backbone mesh such as adaptive key management, SeGroM and Mobisec [Bettahar et al., 2002], [Martignon et al., 2008], [Dong et al., 2009] are not effective due to their high communication overhead and non-fault tolerant nature. Whereas, distributed mechanisms such as DSA-Mesh [Martignon et al., 2011] and IEEE 802.16j multi-hop relay security architecture [Dai and Xie, 2010] are fault tolerant mechanisms but their unicast and broadcast communications are still vulnerable to MAC layer attacks.

Centralized key management mechanisms used in client mesh such as 802.11i and 802.11w are also widely used in Wi-Fi (802.11b/g) and multi-hop (802.11s mesh) wire-

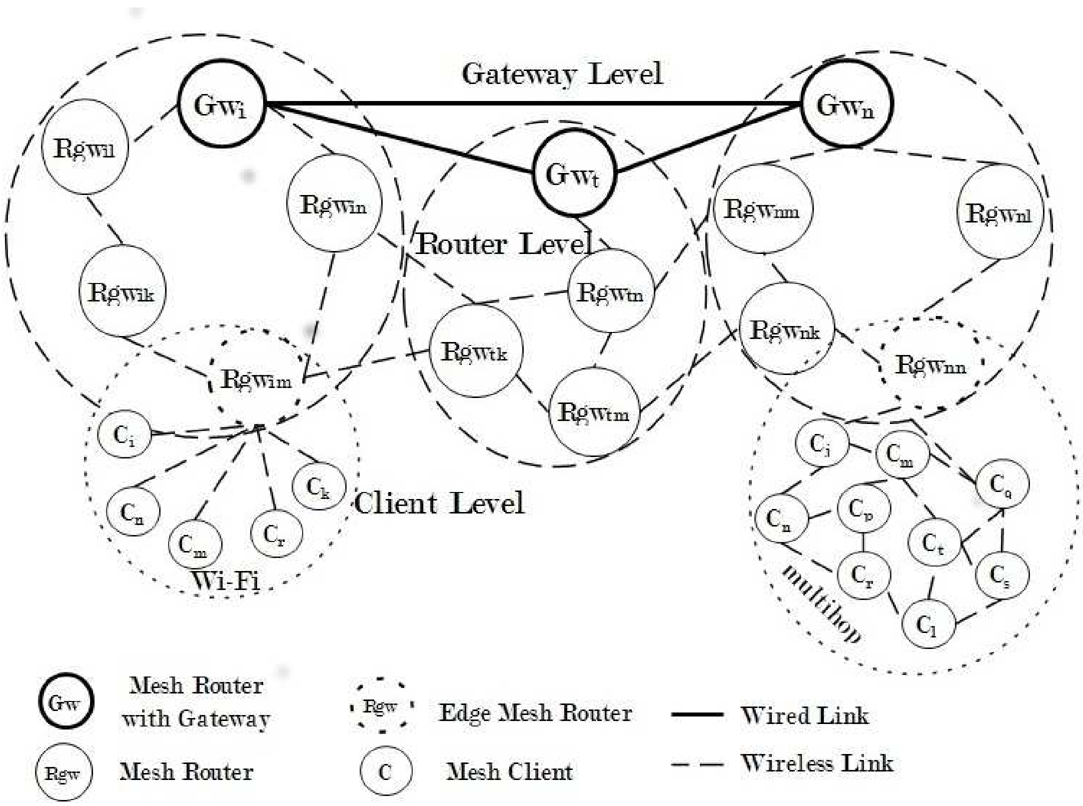


Figure 4.1: Example of HWMNs Three Level Architecture

less networks. However, these key management mechanisms have an inherent flaw in four-way handshake protocol which allows malicious nodes to create various attacks in the client mesh networks. When a mesh router integrates with client mesh networks, both backbone mesh and client mesh become vulnerable to malicious nodes. This shows that the single-level key management mechanisms are insufficient to address the security issues of both backbone mesh and client mesh. Hence, efficient multi-level key management mechanisms are essential to protect the legitimate mesh nodes from malicious nodes in HWMNs.

In this chapter, we develop a Multi-level Key Management Mechanism (MKMM) which uses a distributed public key authentication scheme and a centralized symmetric key authentication scheme to secure the legitimate mesh nodes in HWMNs. The proposed mechanism effectively utilizes the trusted group heads communications in backbone mesh and uses the lightweight encryption in client mesh networks such as Wi-Fi and multi-hop wireless networks to secure the legitimate mesh nodes.

4.1.1 Security Challenges of MKMM

The main security challenges of MKMM are explained below.

1. Protecting against unauthorized nodes: Unauthorized (external) mesh nodes do not have network access. However, these nodes may misuse network resource by illegal network access. Hence, HWMNs need proper authentication schemes to protect against unauthorized nodes from whole network.

2. Protecting against colluding attacks: Two or more attackers work together to isolate the legitimate mesh node from HWMNs. Here, colluding attackers isolate legitimate mesh node by blocking its data or authentication request messages. Colluding attacks severely affect the backbone mesh due to lack of distributed key management mechanisms. Hence, HWMNs need distributed key management mechanism to protect against colluding attacks from backbone mesh.

3. Heterogeneous devices/networks security: Backbone mesh supports heterogenous device communication and these devices provide access to heterogeneous networks such as Wi-Fi and ad-hoc networks. Construction of key management mechanisms for wireless heterogeneous devices/networks are critical and mandatory in hybrid wireless networks development.

4. Three-level security: HWMNs follow the three level architecture namely gateway level, router level and client level. The HWMNs three level architecture is depicted in Figure 4.1. Gateways are placed at top level and these nodes are stable nodes. Mesh routers have less mobility and these nodes are authorized by gateways at the second level. Mesh clients are placed at third level have more resource constrains such as memory, computational power and bandwidth. Existing security mechanisms address the security issues in gateway level, router level or client level. Thus, HWMNs three-level architecture is vulnerable to different type of attacks. HWMNs need three-level security key management mechanism to protect the legitimate mesh nodes.

4.1.2 Preliminaries

In MKMM, we use conventional IPsec for key exchange between gateways and SHA-2 for providing integrity of the messages. In addition to this, we use Elliptic curve cryptography (ECC) for mesh router authentication and one time pad for providing authentication and confidentiality of the messages.

IPsec: IPsec mainly operates at two modes such as transport mode (host to host) and tunnel mode (gateway to gateway). IPSec transport mode is used for end-to-end communications, for example, for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host). Tunnel mode provides security association between gateways in which internet key exchange (IKE) takes place by using diffie-hellman key exchange algorithm. These keys are used to provide authentication and confidentiality between gateways [Doraswamy and Harkins, 2003, Seth et al., 2010].

Secure Hash Algorithm(SHA): SHA-256 is one of the successor hash functions to SHA-1 (collectively referred to as SHA-2), and is one of the strongest hash functions available [Dix, 2009]. While SHA-1 has not been compromised in real-world conditions, SHA-256 is not much more complex to code. In addition to this, SHA-2 is called secure because it is designed to be computationally infeasible to recover a message corresponding to the message digest. If attacker modifies the original message, there is a very high probability that it results in a different message digest. Thus, this message digest will not match with original message digest.

Elliptic curve cryptography (ECC): ECC devices require less storage, less power, less memory, and less bandwidth than other systems. Moreover, it takes less time in the authentication verification process and more efficient than RSA. For example, to achieve the security level of a 1024-bit RSA, ECC requires only 160-bit key length. Elliptic Curve Digital Signature Algorithm (ECDSA) is used to generate public and private keys, and for signature generation and signature verification [Johnson et al., 2001a].

Public and private keys generation: The domain parameters for ECDSA consist of a suitably chosen elliptic curve E defined over a finite field F_p of characteristic p and a base point G $\in$ Ep(a,b) with order n. Each mesh router uses the following steps to create public and private keys

1. Mesh router chooses a point on curve, $e_1(x_1, y_1)$.
2. Mesh routers selects a pseudo-random integer d, between 1 and n-1.
3. Mesh router calculates another point on curve $e_2(x_2, y_2)$ = d * $e_1(x_1, y_1)$.
4. Mesh router consider E(a, b), $e_1(x_1, y_1)$ and $e_2(x_2, y_2)$ as its public key, and d as its private key.

Signature generation: To generate mesh router's signature on message (m), mesh router use domain parameters (p, Ep(a, b), e_1, e_2, n) along with its private key.

1. Mesh router chooses secret random number r, between 1 and n-1.
2. Mesh router selects third point on the curve r * $e_1(x_1, y_1)$ = (x_1', y_1').
3. Mesh router calculates S_1 = x_1' mod n. If r = 0 then go to step 1.
4. Mesh router calculates SHA-2(m) and then convert this string to an integer H(m).
5. Mesh router calculates S_2 = (H(m)+ d*S_1)*r^{-1} mod n. If s = 0, then go to step 1.
6. Mesh router's signature for message m is (S_1, S_2).

Signature verification: To verify mesh router's signature (S_1, S_2) on message (m), mesh router$_1$ obtains an authentic copy of mesh router's domain parameters (p, Ep(a, b), e_1, e_2, n).

1. Mesh router$_1$ verifies that whether S_1 and S_2, are integers in the interval [1, n-1].
2. Mesh router$_1$ calculates SHA-2(m) and then convert this string to an integer H(m).
3. Mesh router$_1$ calculates A = H(m)* S_1^{-1} mod n and B = S_2^{-1} S_1 mod n.
4. Mesh router$_1$ calculates T(x, y) = A * $e_1(x_1, y_1)$ + B * $e_1(x_2, y_2)$.
5. If x = S_1 mod n signature is verified.

6. Otherwise, message is rejected.

One Time Pad: The One Time Pad (OTP) encryption algorithm is a binary additive stream cipher, where a stream of truly random keys is generated and then combined with the plain text for encryption or with the ciphertext for decryption by an 'exclusive OR' (XOR) addition [Deng and Long, 2004]. This is the first and only encryption algorithm that has been proven to be unbreakable. The OTP encryption and decryption examples are given below:

Example a: OTP Encryption

Key = 0010010010

$\oplus$

Plain text = 1101010101

Cypher text = 1111000111

Example b: OTP Decryption

Key = 0010010010

$\oplus$

Cypher text = 1111000111

Plain text = 1101010101

Since true random key is very essential to provide confidentiality in our work, we use true random number generator based on embeddable ADC-based true random number generator [Callegari et al., 2005]. OTP needs to generate very big key's when plain text size is big. However, the proposed MKMM uses OTP to secure 128-bit random number.

The rest of this chapter is organized as follows. Section 4.2 presents the MKMM. Section 4.3 describes performance analysis of MKMM in HWMNs. Section 4.4 summarizes this chapter.

4.2 Multi-level Key Management Mechanism

The proposed multi-level key management mechanism uses a distributed authentication scheme and a centralized authentication scheme to update status of mesh node authentication key's when it leaves or joins the network. Both of these schemes make use of two level trust nodes such as gateways for backbone mesh and edge routers for client mesh. Gateways are the special type of mesh routers which support both wired and wireless communication. Edge routers are the backbone routers which connect with mesh clients. These trust nodes ensure the authentication among mesh routers and mesh clients in HWMNs.

4.2.1 Distributed Authentication Scheme

The proposed distributed authentication scheme follows two level authentication namely gateway-level and router-level to secure the legitimate mesh routers in backbone mesh. Description of distributed authentication scheme notations shown in Table 4.1 are explained below: The Gw_n represents the n^{th} gateway in backbone mesh. Each gateway (Gw_n) use its private key (Gwq_n) to sign the messages (M_{gw_n}) and public key (Gwp_n) to authenticate these messages. A mesh router is represented as Rgw_{nk} and neighboring mesh router is represented as ($Rgwn_{st}$) where s is group id and t is mesh router id. Mesh router uses their public key ($Rgwp_{nk}$) and private key ($Rgwq_{nk}$) for authentication and secure communication. Mesh router stores all authenticated public keys in authentication table (At_{nk}).

Gateway issues unique r_{id} to mesh router with its signature and issues a 128-bit session key ($Krgw_{nk}$) for secure communion between gateway and mesh router. Gateway and mesh router uses the message time out value ($T_{Rgw_{nk}}$) to drop the stale messages. Mesh router creates authentication request ($AReq_{Rgw_{nk}}$) and de-authentication request ($DAReq_{Rgw_{nk}}$) messages to join or leave the backbone mesh. Gateway issues authentication reply ($ARep_{Rgw_{nk}}$) to authenticate the mesh router (Rgw_{nk}) in backbone mesh. Gateway and mesh router uses t_d number of node disjoint paths where t_d is minimum degree of gateway (Gw_n) + number of gateways supported to forward the authentication request ($AReq_{Rgw_{nk}}$). These nodes use message digest $H(M)_{Krgw_{nk}}$ for message integrity check.

Table 4.1: Distributed Authentication Scheme Notations

Gw_n	gateway
Gwp_n & Gwq_n	public key and private keys of Gw_n
M_{gw_n}	message singed by Gw_n
Rgw_{nk}	mesh router belongs to Gw_n
$Rgwn_{st}$	neighboring mesh router
$Rgwp_{nk}$ & $Rgwq_{nk}$	public and private keys of Rgw_{nk}
At_{nk}	authentication table of Rgw_{nk}
r_{id}	mesh router key identifier
$Krgw_{ik}$	session key
$T_{Rgw_{nk}}$	message timeout of Rgw_{nk}
$AReq_{Rgw_{nk}}$	authentication request of Rgw_{nk}
$DAReq_{Rgw_{il}}$	de-authentication request of Rgw_{nk}
$ARep_{Rgw_{nk}}$	authentication reply for Rgw_{nk}
t_d	node disjoint paths
$H(M)_{Krgw_{nk}}$	message digest of Rgw_{nk}

4.2.1.1 Gateway-level Authentication

Gateways (group heads) trust each other and are connected through conventional wired network in backbone mesh. As compared to wireless networks, wired networks are more secure due to the availability of standard security protocols [Redwan and Kim, 2008, Seth et al., 2010]. We have considered the standard wired security protocol (IPsec) to establish mutual authentication between group heads (Gw_is). Based on IPsec, group heads provide authentication, integrity, confidentiality and non-repudiation for every mesh router in backbone mesh. Each group head authenticates/ de-authenticates their corresponding mesh routers (group members) and exchanges their group members (Rgw_{ik}s), information with other group heads. This information is authenticated by the corresponding group head's public key (Gwp_i).

4.2.1.2 Mesh Router-level Authentication

In this section, we present the authentication and de-authentication algorithms for securing join and leave operations of mesh routers. Both the algorithms are explained below.

Mesh Router Authentication

When a new mesh router (Rgw_{ik}) requests with its router identity (r_{id}) to join in a group, group head (Gw_i) decrypts r_{id} with it's public key (Gwp_i's). If r_{id} is valid then Gw_i issues a signed message (M_{gw_i}) with r_{id} and expiration time ($T_{Rgw_{ik}}$) and a session key ($Krgw_{ik}$) to mesh router (Rgw_{ik}).

Once Rgw_{ik} is placed in backbone mesh, it generates its own public key ($Rgwp_{ik}$) and private key ($Rgwq_{ik}$) by using elliptic curve cryptography and creates an authentication request message. This message consists of M_{gw_i}, r_{id}, $T_{Rgw_{ik}}$, $Rgwp_{ik}$ and $H(M)_{Krgw_{ik}}$, where $H(M)_{Krgw_{ik}}$ is a message digest of whole message created by session the key $H(M)_{Krgw_{ik}}$=$\{M_{gw_i}, \{r_{id}, T_{Rgw_{ik}}\}, Rgwp_{ik}\}_{Krgw_{ik}}$.

Rgw_{ik} disseminates this authentication request message in backbone mesh. When this message is received by a neighboring mesh router ($Rgwn_{ij}$) belonging to same group, $Rgwn_{ij}$ decrypts the M_{gw_i} with group head's public key (Gwp_i's) and verifies r_{id} and $T_{Rgw_{ik}}$. If r_{id} is not stored in the authentication table and $T_{Rgw_{ik}}$ is valid then mesh router ($Rgwn_{ij}$) stores r_{id} and then rebroadcasts the authentication request message. Otherwise, this request message is dropped by the mesh router. This process continues until it reaches to its group head (Gw_i).

When this message is received by a neighboring mesh router ($Rgwn_{nj}$) belonging to other group, $Rgwn_{nj}$ decrypts the M_{gw_i} with corresponding group head's public key (Gwp_i) and verifies r_{id} and $T_{Rgw_{ik}}$. If r_{id} is not stored in the authentication table and

$T_{Rgw_{ik}}$ is valid then $Rgwn_{nj}$ stores r_{id} and then forwards (unicast) the authentication request message to their group head (Gw_j) through the known path. Upon receiving the authentication request message, Gw_j directly unicast this message to the corresponding group head (Gw_i).

If Gw_i receives the authentication request message then it verifies the received message by its public key (Gwp_i) and their session key ($Krgw_{ik}$). If this message is valid then group head stores Rgw_{ik}'s public key ($Rgwp_{ik}$) in its authentication table and creates a reply message which consists of r_{id}, $T_{Rgw_{ik}}$ and certified $Rgwp_{ik}$'s public key. Then Gw_i signs the reply message with its private key (Gwq_i) and sends this authentication reply message through 't_d' node disjoint paths (multicast) to overcome the colluding attacks. When a mesh router ($Rgwp_{ij}$) receive this reply message, it decrypts this message by known corresponding group head's public key (Gwp_i). If $Rgwp_{ij}$ is able to decrypt this message then certified Rgw_{ik}'s public key is added to their authentication table. Then, they forward this message to their next mesh router in the path and this process will repeat until it reaches to Rgw_{ik}. All the mesh routers use their public keys and private keys for authentication and secure communication. Mesh router authentication is explained in algorithm 4.1.

Mesh router de-authentication

When a mesh router (Rgw_{il}) leaves the backbone mesh, it creates a de-authenti- cation request message with r_{id} and $T_{Rgw_{ik}}$. Rgw_{il} signs this message with its private key ($Rgwq_{il}$) and sends this message to Gw_i through 't_d' number of node disjoint paths. When this message is received by a neighboring router ($Rgwn_{ij}$), it decrypts this message by the mesh router's public key ($Rgwp_{il}$). If this message is valid, then it deletes the $Rgwp_{il}$ from its authentication table and forward this message to the next router in the path. Otherwise, this request message is dropped by $Rgwn_{ij}$. This process will repeat until it reaches to the group head (Gw_i). Upon receiving the de-authentication request message, Gw_i verifies this message by $Rgwp_{il}$. If this message is valid then delete the $Rgwp_{il}$ from its authentication table and disseminates this message to other group heads (Gw). Eventually, Rgw_{il} is completely isolated from the backbone network.

Algorithm 4.1 : Mesh Router (Rgw_{ik}) Authentication

```
When the new node $\mathrm{Rgw_{ik}}$ sends a join request with $\mathrm{r_{id}}$ to $\mathrm{Gw_i}$
$\mathrm{Gw_i}$ disseminates $\mathrm{r_{id}}$ to all Gw nodes
$\mathrm{Gw_i}$ issues $\mathrm{M_{gw_i}, Krgw_{ik}}$to $\mathrm{Rgw_{ik}}$
$\mathrm{Rgw_{ik}}$ generates its own public and private keys $\mathrm{Rgwp_{ik},\ Rgwq_{ik}}$
$\mathrm{Rgw_{ik}}$ creates and disseminates authentication request $\mathrm{AReq_{Rgw_{ik}}}$
$\mathrm{AReq_{Rgw_{ik}}}$is received by its neighbour $\mathrm{Rgwn_{nj}} \,||\, \mathrm{Gw_t}$
Extract $\mathrm{M_{gw_i}}$ from $\mathrm{AReq_{Rgw_{ik}}}$
 if $\mathrm{Rgwn_{nj}} \in \mathrm{Gw_i}$
     If $\mathrm{T_{Rgw_{ik}}}$ = valid & $\mathrm{r_{id}} \notin \mathrm{At_{nj}}$
          Stores $\mathrm{r_{id}}$ & Broadcasts $\mathrm{AReq_{Rgw_{ik}}}$
     Else  Drops $\mathrm{AReq_{Rgw_{ik}}}$
Else if $\mathrm{Rgwn_{nj}} \notin$  $\mathrm{Gw_i}$
     If $\mathrm{T_{Rgw_{ik}}}$ = valid & $\mathrm{r_{id}} \notin \mathrm{At_{nj}}$
          Stores $\mathrm{r_{id}}$ & Forwards $\mathrm{AReq_{Rgw_{ik}}}$to $\mathrm{Gw_t}$
     Else  Drops $\mathrm{AReq_{Rgw_{ik}}}$
Else if $\mathrm{Gw_t}$ receives $\mathrm{AReq_{Rgw_{ik}}}$
     If $\mathrm{T_{Rgw_{ik}}}$ = valid & $\mathrm{r_{id}} \in \mathrm{At_{nj}}$
          Forwards $\mathrm{AReq_{Rgw_{ik}}}$to $\mathrm{Gw_i}$
     Else  Drops $\mathrm{AReq_{Rgw_{ik}}}$
Else if $\mathrm{Gw_i}$ receives $\mathrm{AReq_{Rgw_{ik}}}$
     If $\mathrm{T_{Rgw_{ik}}}$ = valid & $\mathrm{r_{id}} \in \mathrm{At_{nj}}$
          If $\mathrm{H'(M)_{Krgw_{ik}} = H(M)_{Krgw_{ik}}}$
            flag = 1
            Stores the public key and drops $\mathrm{Krgw_{ik}}$
            $\mathrm{Gw_i}$ creates authentication reply ($\mathrm{ARep_{gw_{ik}}}$)
            $\mathrm{ARep_{gw_{ik}}}$Forwards to $\mathrm{Rgw_{ik}}$by using node disjoint paths
            $\mathrm{Gw_i}$ disseminates $\mathrm{Rgwp_{ik}}$ to all Gw nodes
     Else  flag = 0
            Drop $\mathrm{AReq_{Rgw_{ik}}}$
```

Mesh router de-authentication is explained in algorithm 4.2. When Rgw_{il} re-joins the backbone mesh, the mesh router authentication process will take place for Rgw_{il} secure key authentication.

Algorithm 4.2 : Mesh Router(Rgw_{il}) De-authentication

```
$\mathrm{Rgw_{il}}$ sends a leave request (signed $\mathrm{DAReq_{Rgw_{il}}}$)
through the node disjoint paths to $\mathrm{Gw_i}$
If $\mathrm{DAReq_{Rgw_{il}}}$ received by its neighbour $\mathrm{Rgwn_{nj}} \,||\, \mathrm{Gw_k}$
  $\mathrm{Rgwn_{nj}} \,||\, \mathrm{Gw_k}$ decrypts $\mathrm{DAReq_{Rgw_{il}}}$with $\mathrm{Rgwp_{il}}$
   If $\mathrm{T_{Rgw_{il}}}$ & $\mathrm{Rgw_{il}}$ authentication $=$ valid
    $\mathrm{Rgwn_{nj}} \,||\, \mathrm{Gw_k}$ forwards $\mathrm{DAReq_{Rgw_{il}}}$to $\mathrm{Gw_i}$
    $\mathrm{Rgwn_{nj}} \,||\, \mathrm{Gw_k}$ deletes $\mathrm{r_{id}}$ & $\mathrm{Rgwp_{il}}$ from $\mathrm{At_{nj}} \,||\, \mathrm{At_k}$
Else if $\mathrm{Gw_i}$ receives $\mathrm{DAReq_{Rgw_{il}}}$
  $\mathrm{Gw_i}$ decrypts $\mathrm{DAReq_{Rgw_{il}}}$with $\mathrm{Rgwp_{il}}$
   If $\mathrm{T_{Rgw_{il}}}$ & $\mathrm{Rgw_{il}}$ authentication $=$ valid
    $\mathrm{Gw_i}$ deletes $\mathrm{r_{id}}$ & $\mathrm{Rgwp_{il}}$ key from $\mathrm{At_i}$ &
    the backbone mesh by sending $\mathrm{DAReq_{Rgw_{il}}}$ to all other Gw nodes
```

4.2.1.3 Security Analysis

A security analysis of the proposed distributed authentication scheme is performed using MAC layer network security and information security attacks which are explained in chapter 2.

Imprinting attack: When a mesh router (Rgw_{nk}) joins the backbone mesh network, Rgw_{nk} sends a authentication request message to gateway (Gw_n). Imprinting attacker overhears this request message and sends forged authentication reply message to Rgw_{nk} on behalf of Gw_n to capture the Rgw_{nk} network traffic. Trusted gateways in the proposed scheme use 256-bit elliptic curve cryptography public keys to generate their digital signature. In this case, imprinting attacker needs 2^{128} computations to forge (imprinting) a trusted gateway's digital signature, which is computationally infeasible for an attacker.

Identity theft: When an attacker know the public key of a gateway, attacker is able to capture the legitimate mesh router id's (r_{id}). However, attacker cannot generate fake messages with this r_{id} because attacker fails to create legitimate mesh router signature on these messages.

Replay attack: The attacker records the legitimate mesh router's (Rgw_{nk}) authentication request message also called passive eavesdropping attack. Then attacker comes into active phase and replays recorded request message to get the illegal access in backbone mesh on behalf of Rgw_{nk}. In the proposed scheme, timeout value of every authentication request message is secured by its private key ($Rgwq_{nk}$) and DES-128 bit session key. Thus, attacker needs 2*2^{128} computations to change the timeout value and break the AES-128 bit session key of a authentication request message, which is computationally infeasible for an attacker.

Node Deprivation attack: The attacker records the legitimate mesh router (Rgw_{nk}) de-authentication request message. When Rgw_{nk} re-join the backbone mesh, attacker replays the recorded request message to isolate the Rgw_{nk} from backbone mesh. In the proposed scheme, timeout value of every de-authentication request message is secured by its private key ($Rgwq_{nk}$). Thus, attacker needs 2^{128} computations to change the timeout value of a de-authentication request message, which is computationally infeasible for an attacker.

Authentication flooding: Upon receiving the same authentication request messages multiple times, mesh routers either broadcast or multicast the first message and remaining all messages will be dropped. The process of preventing duplicate messages in our proposed scheme mitigates the severity of authentication flooding attack.

Colluding attack: Group of attackers isolates target (legitimate) mesh router (Rgw_{nk}) by dropping Rgw_{nk} authentication request messages. Thus, Rgw_{nk} authentication request message does not reach gateway (Gw_n). In our proposed scheme, mesh routers can comprehensively join / leave the backbone mesh because the proposed scheme resists up to 't_d-1' colluding malicious paths between the mesh router and the gateway, where 't_d' is the number of disjoint paths selected by Gw_n.

Our analysis confirms that the proposed authentication scheme effectively prevents various MAC layer attacks such as imprinting attacks, replay attacks, node deprivation attacks and colluding attacks in the backbone mesh because of its robust cryptographic functionalities.

4.2.1.4 Mesh Router Message Reachability

HWMNs are suffering from colluding (group of selfish or compromised) attackers. These attackers affect the scalability of network by blocking the legitimate mesh routers join/leave operations in backbone mesh. This is because of colluding attackers in backbone mesh drop all received authentication requests from their neighbours. Colluding attackers are severe when

- A single authentication system authenticates/ de-authenticates mesh routers in backbone mesh.
- A new mesh router authentication/ de-authentication request is sent only to the selected neighbouring routers.
- A new mesh router needs to authenticated by two or more number of group heads to join/leave the backbone mesh.

The proposed distributed authentication scheme effectively utilizes the unicast, multicast and broadcast communications among mesh routers and group heads instead of sending only to specific routers. In the proposed scheme, when a mesh router joins or leaves a group, other group mesh routers also cooperate in order to forward its message to the corresponding group head and a mesh router is able to authenticated/ de-authenticated by single group head. The cooperative behavior of mesh routers mitigates the severity of colluding attackers and increases the message reachability in backbone mesh.

4.2.1.5 Connectivity Probability Model in Hostile Network

C Bettstetter proposed a connectivity probability model for homogeneous and heterogeneous radio range wireless devices [Bettstetter, 2002]. This model reflects the relations among the coverage and the number of nodes, the communication ranges of nodes, and the network size. We have made amendments to this model to find the message reachability in hostile network. The updated connectivity probability model is used to compare the proposed scheme with other selected centralized and distributed authentication schemes. In this model, the malicious mesh routers vary from 0 to 100% to create hostile backbone mesh. The notations used in this model are defined as follows:

1. Network coverage area is A.
2. Total number of gateways in the HWMN is n_{gw}.
3. Total number of mesh routers in the HWMN is n_r.
4. Total number of backbone nodes n= n_{gw} + n_r.
5. Total number of gateways authenticate or de-authenticate to join a router in backbone mesh is n_{gws}.
6. n backbone nodes consist of J different node types, i.e., there are n_j nodes of type j with range r_j , such that n = $\sum_{j=1}^{J} n_j$ for j = 1. . .J.
7. Define the density ρ = n_j/A. These n nodes consist of J different node types.
8. Each router coverage area is πr_j^2 where j= 1,2......N;
9. Each router neighborhood connectivity (degree of a router) is $d_{min}^{(k)}$ where k= 1,2......N.
10. Number of malicious nodes m = $\sum_{j=1}^{J} m_j$ for j = 1. . .J.

The probability of mesh router message is not reachable (P_{NAuth}) or reachable (P_{Auth}) at Gw_i is mainly reflected by affected colluding attackers, also by the degree of the network, the communication ranges of backbone nodes, the network size and number of gateways in the network. The P_{NAuth} and P_{Auth} are calculated using the equations 4.1 and 4.2.

$$P_{NAuth} = exp(-\sum_{m=1}^{J} d_{min}^{(k)} * \rho_m * \pi r_e^2) \tag{4.1}$$

where k is the minimum degree of each node and the ”effective range” r_e = min{ r_j , r_e }. Thus,

$$P_{Auth} = (1 - (P_{NAuth}))^{(n_r - m) * \frac{n_{gws}}{n_{gw}}} \tag{4.2}$$

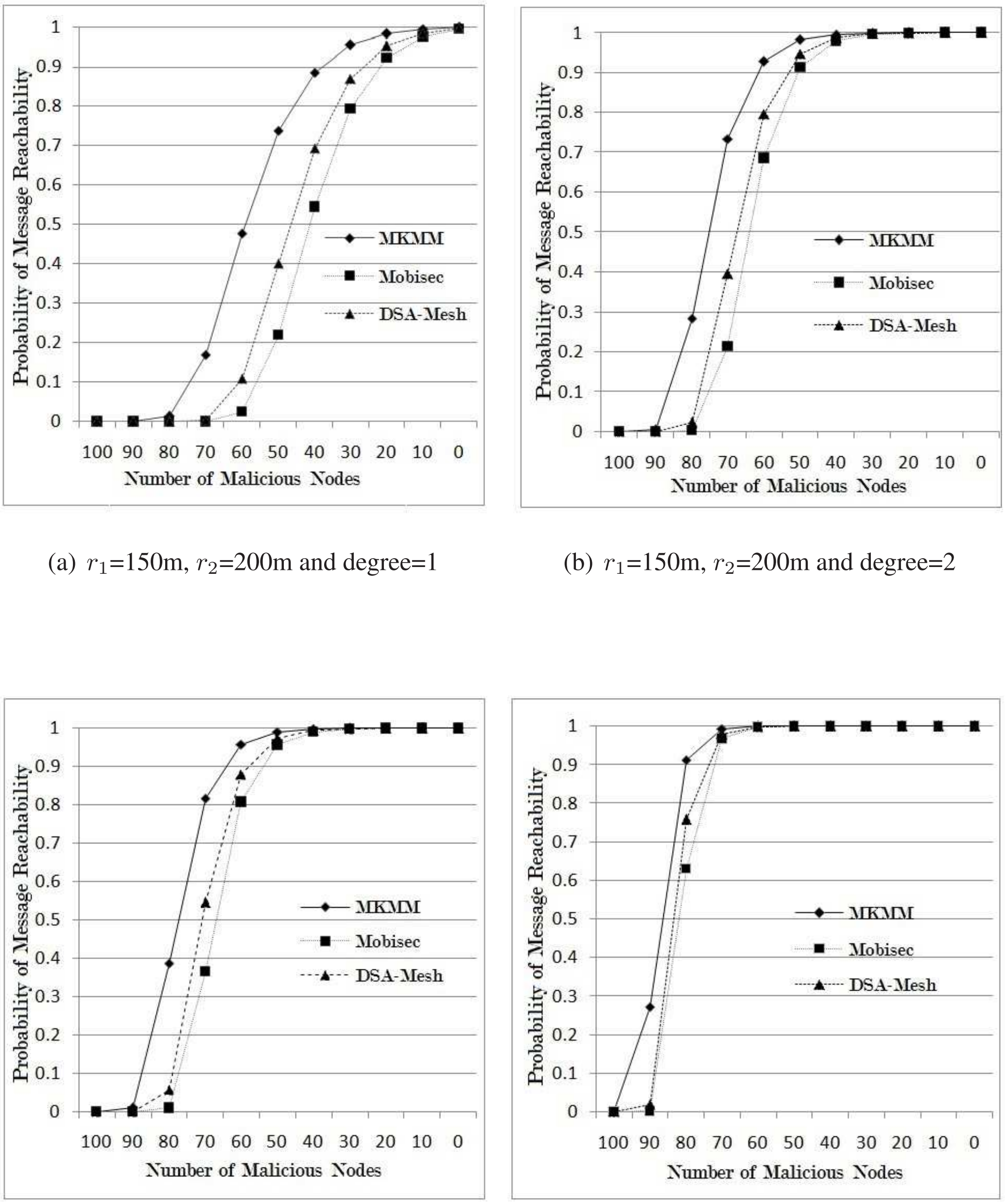
From equations 4.2, the message readability of a mesh router to Gateway (Gw_i) is determined by the backbone nodes communication range, mesh router density, and number of gateway nodes. The main difference of proposed distributed authentication scheme (MKMM-DA) and DSA-Mesh [Martignon et al., 2011] and mobisec [Martignon et al., 2008] is the number of gateway's required to authenticate each mesh router. Thus, we analyze the performance of proposed and existing schemes by varying the number of gateways.

In Figure 4.2(a), 4.2(b), 4.3(a) and 4.3(b), we consider r_1 as 150m, r_2 as 200m with $d_{min}^{(k)}$ as 1 and 2. In Figure 4.2(c), 4.2(d), 4.3(c) and 4.3(d), we consider r_1 as 200m, r_2 as 250m with $d_{min}^{(k)}$ as 1 and 2. Figure 4.2 and 4.3 show that probability of mesh router message reachabilities of proposed scheme (MKMM-DA), DSA-mesh and mobisec schemes with n_{gw} value as 5 and 10.

For n_{gw} value as 5 and 10, the proposed MKMM-DA scheme message reachability at group head is better than that of DSA-mesh and mobisec schemes in all scenarios. This is because out of n_{gw} group heads, the mesh router message needs to reach any one of the group head to authenticate or de-authenticate the mesh router in the proposed MKMM-DA scheme. On the other hand, the mesh router message needs to reach minimum of ($\frac{n_{gw}}{2}$)+1 group heads to authenticate or de-authenticate the mesh router in DSA-Mesh. Mobisec is less effective as compared to the proposed MKMM-DA scheme and DSA-Mesh because the mesh router message needs to reach a specific group head.

From Figure 4.2, average message reachability of proposed scheme has 69% reachability, DSA-mesh 60% reachability and mobisec has 57% reachability in hostile network (0-100% malicious nodes) for n_{gw} value as 5. The proposed MKMM-DA has 9% better performance than DSA-mesh, and 12% better performance than mobisec.

From Figure 4.3, average message reachability of proposed scheme has 76% reachability, DSA-mesh 60% reachability and mobisec has 57% reachability in hostile network (0-100% malicious nodes). The proposed MKMM-DA has 16% better perfor-



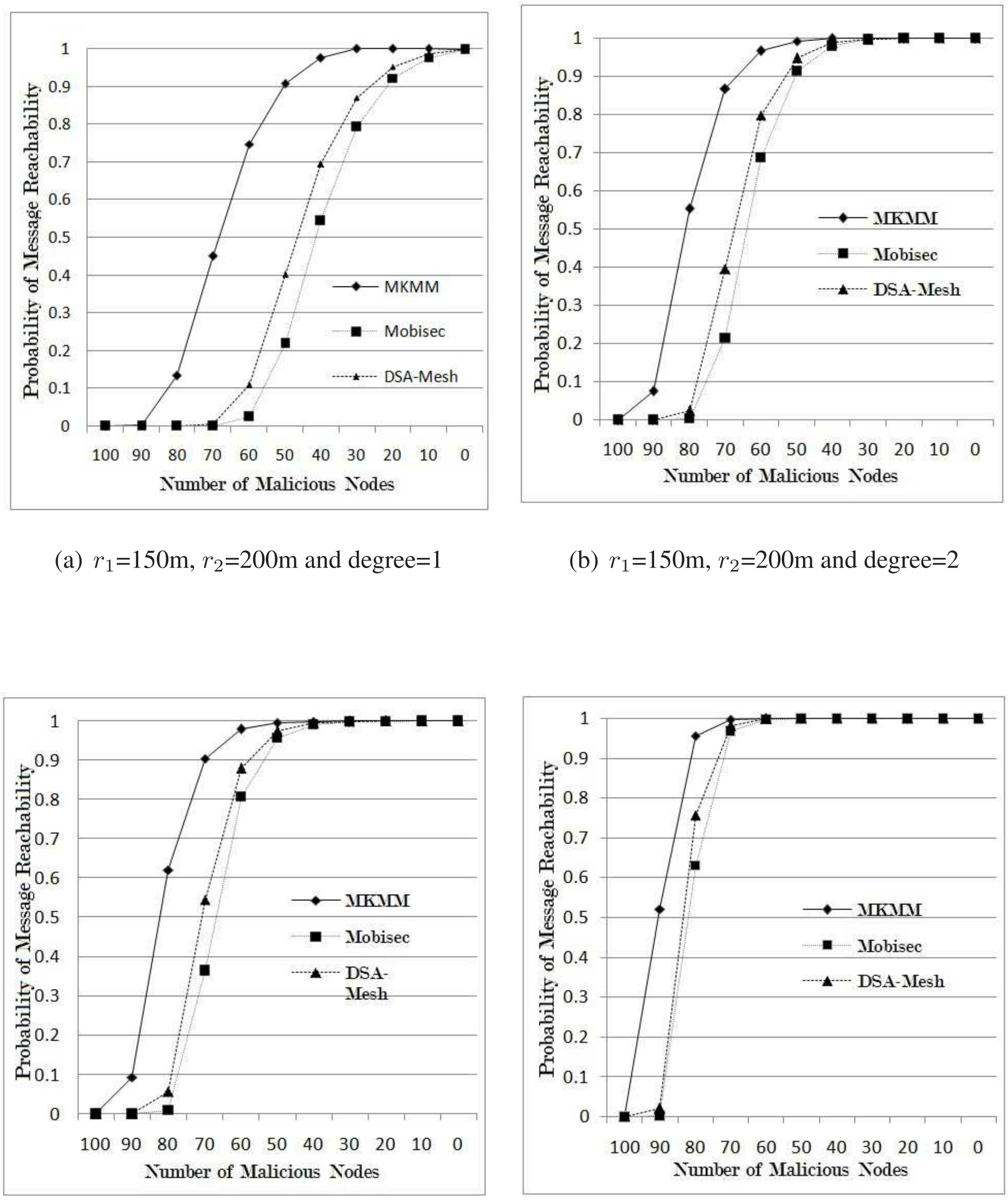
(a) r_1=150m, r_2=200m and degree=1

(b) r_1=150m, r_2=200m and degree=2

(c) r_1=200m, r_2=250m and degree=1

(d) r_1=200m, r_2=250m and degree=2

Figure 4.2: Mesh Router Message Reachability with n_{gw}=5



(a) r_1=150m, r_2=200m and degree=1

(b) r_1=150m, r_2=200m and degree=2

(c) r_1=200m, r_2=250m and degree=1

(d) r_1=200m, r_2=250m and degree=2

Figure 4.3: Mesh Router Message Reachability with n_{gw}=10

mance than DSA-mesh, and 19% better performance than mobisec for n_{gw} value as 10. This performance difference further increases when the number of gateways increase in backbone mesh. In addition to this, the proposed MKMM scheme can mitigate the hostile network severity by increasing the transmission range or minimum degree of each router in backbone mesh.

Based on heterogeneous device connectivity probability model, the proposed MKMM-DA scheme outperforms DSA-mesh and mobisec in hostile network. We also conduct the simulation study to compare the proposed MKMM-DA scheme with the DSA-mesh and mobisec schemes by varying n_{gw} value.

4.2.1.6 Simulation Results

We implement the proposed MKMM-DA scheme, DSA-mesh and mobisec schemes in NS2 simulator. In our simulation environment, we consider simulation parameters mentioned in section 4.2.1.5. A uniform random generator chooses the x and y coordinates of n_r = 100 mesh routers on a 1000m X 1000m area. Out of 100 mesh routers, 50 mesh routers transmission range set as 150m, other mesh routers transmission rage as 250m. We consider 802.11 MAC layer protocol and AOMDV path discovery protocol in network layer, and create 100bytes of message for mesh router authentication and de-authentication. The pause time is set to 2ms to simulate the HWMN. We set up communication range vary between long-distance and short-distance wireless links from 50m and 250m. In this simulation setup, we have conducted 10000 simulations by varying the number of malicious nodes from 0-100%. All the legitimate mesh routers cooperate by forwarding this message.

We measure the performance of MKMM-DA scheme, DSA-mesh and mobisec schemes by considering n_{gw} value as 5 in one scenario and n_{gw} value as 10 in another scenario. For each scenario, we conduct 1000 simulations by varying the number of malicious nodes from 0-100%. The malicious nodes present in the network to drop the legitimate mesh router messages. We evaluate the performance of by average of 1000 simulations where each simulation time is 100s. For n_{gw} value as 5, the performance of MKMM-DA scheme, DSA-mesh and mobisec schemes are shown Figure 4.4. The

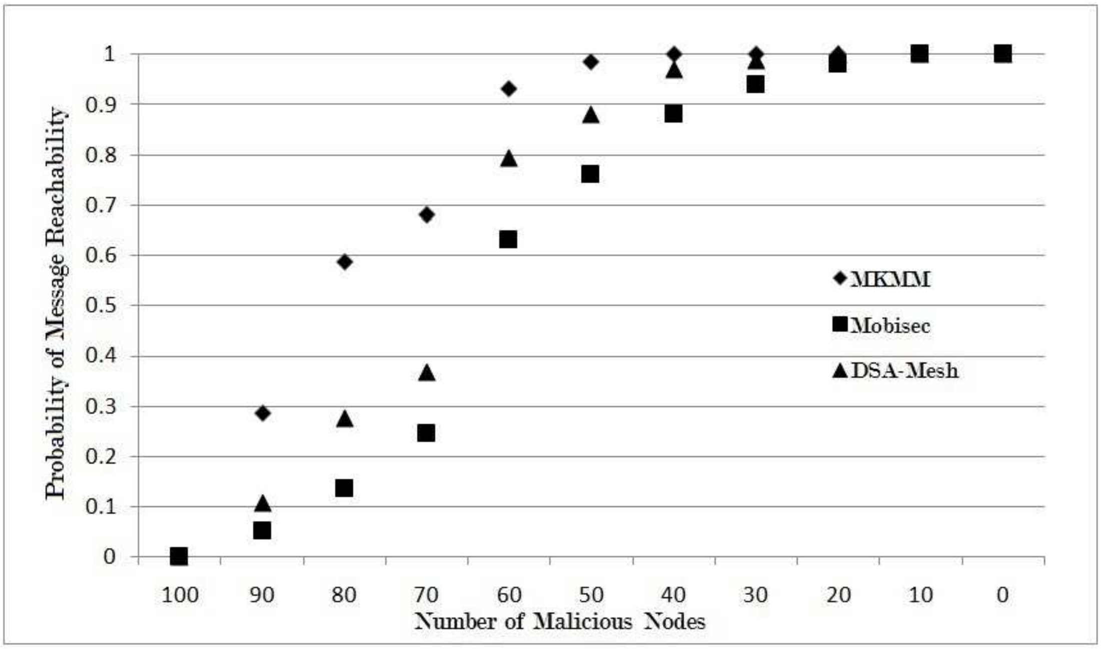


Figure 4.4: Message Request Reachability with n_{gw}=5

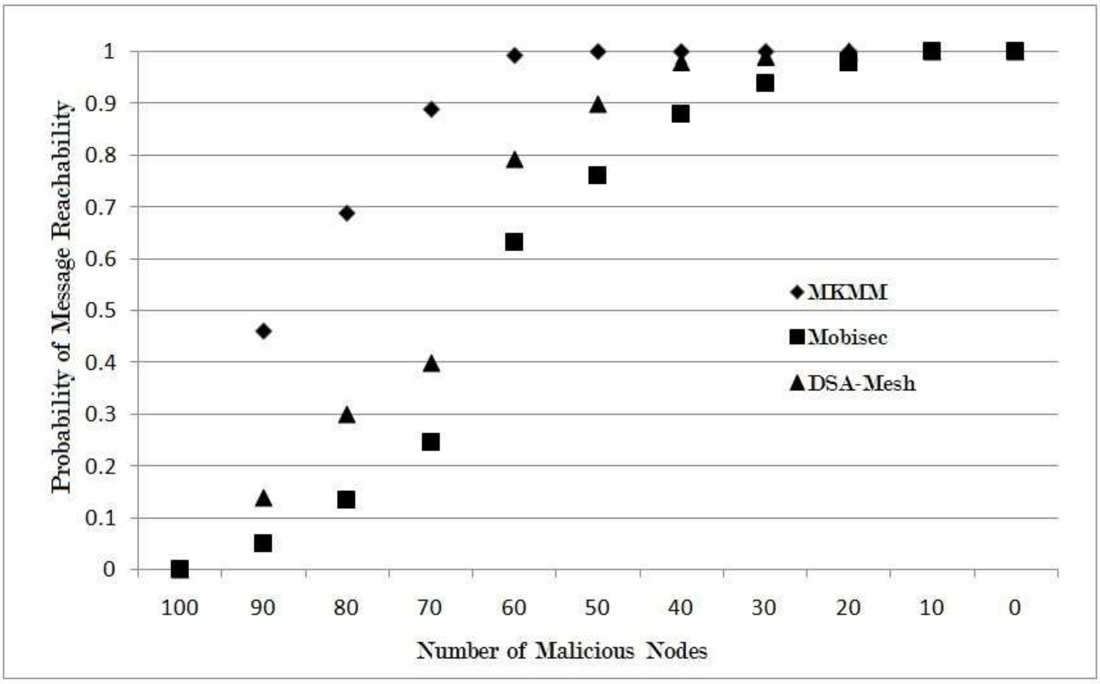


Figure 4.5: Message Request Reachability with n_{gw}=10

average message reachability of MKMM-DA scheme is 77% , 67% for DSA-mesh and 60% for mobisec.

For n_{gw} value as 10 the performance of MKMM-DA scheme, DSA-mesh and mobisec schemes as shown in Figure 4.5. The average message reachability of MKMM-

DA scheme is 82%, 68% for DSA-mesh and 60% for mobisec. In both the scenarios, the proposed MKMM-DA scheme outperforms DSA-mesh and mobisec schemes.

The proposed authentication scheme has greater message reachability in hostile backbone mesh. Our security analysis and simulation results show that proposed authentication scheme out performance the other existing schemes.

4.2.2 Enhanced Centralized Authentication Scheme

In this section, we present the enhanced centralized authentication scheme for securing the client mesh against various attacks. Edge routers in backbone mesh connect to different client mesh networks such as Wi-Fi (802.11b/g), multi-hop (802.11s) networks, ad-hoc networks, sensor networks and cellular networks. Providing security for different client mesh networks is very complex and challenging issue. In this work, MKMM supports two types of client mesh networks such as Wi-Fi (802.11b/g) network and multi-hop (802.11s) network. These two client mesh networks adapt the 802.11i authentication scheme to secure their mesh clients. 802.11i authentication scheme uses the centralized authentication server (edge router) to authenticate/de-authenticate the mesh clients (supplicants). Initially, authenticator and supplicant is to derive Pairwise Master Key (PMK) using Pre-Shared Key (PSK) or Mater Session Key (MSK). PMK is alive until the connection is completely terminated. Authenticator and supplicant use the four-way handshake protocol to derive a Pairwise Transient Key (PTK) and an Group Transient Key (GTK) as shown in Figure 4.6.

4.2.2.1 802.11i Four-way Handshake Protocol

In four-way handshake protocol, to secure single-link communication and group communication, supplicant needs two session keys called PTK and GTK [802.11i 2004 Amendment6, 2004]. In the process of deriving PTK and GTK keys, authenticator sends Anonce and Authenticator MAC address (AA) in Message-1. Upon receiving Message-1, supplicant generates PTK by concatenating (Anonce, AA, Snonce and Supplicant MAC address (ASP)) then supplicant creates Message Integrity Check (MIC) using PTK. Supplicant sends PTK and MIC_{PTK} to authenticator in Message-2. Use of

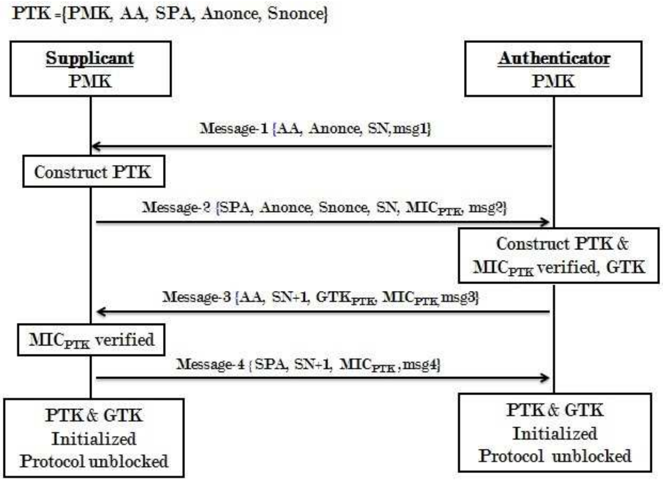

PTK ={PMK, AA, SPA, Anonce, Snonce}
Supplicant
PMK
Authenticator
PMK
Message-1 {AA, Anonce, SN,msg1}
Construct PTK
Message-2 {SPA, Anonce, Snonce, SN, MIC$_{PTK}$, msg2}
Construct PTK &
MIC$_{PTK}$ verified, GTK
Message-3 {AA, SN+1, GTK$_{PTK}$, MIC$_{PTK}$ msg3}
MIC$_{PTK}$ verified
Message-4 {SPA, SN+1, MIC$_{PTK}$,msg4}
PTK & GTK
Initialized
Protocol unblocked
PTK & GTK
Initialized
Protocol unblocked

Figure 4.6: Four-way Handshake Protocol

Snonce, Anonce, AA, and ASP, authenticator will generate PTK of Message-2. The generated PTK is used to create MIC_{PTK} which matches to the MIC_{PTK} of Message-2. Then authenticator constructs GTK and sends to supplicant in Message-3. After receiving Message-3, supplicant generates MIC_{PTK} using stored PTK. If this MIC_{PTK} same as Message-3 MIC_{PTK}, supplicant uses this PTK to encrypt Message-4. This four-way handshake of 802.11i is vulnerable to various DoS attacks such as blocking and flooding attacks [Gharavi and Hu, 2013].

Blocking attacks on four-way handshake protocol: In blocking attack, the authenticator sends Message-1 (not encrypted) to the supplicant [Meng et al., 2013], [Li and Yang, 2012]. Upon receiving, for every new Message-1 from authenticator, supplicant generates PTK and MIC_{PTK} and responds with the Message-2. This will be taken as an advantage by the attacker and sends fake Message-1' with the spoofed MAC address of the authenticator in three different levels which is shown in Figure 4.7. In each level, supplicant calculates PTK'(different from PTK and overwriting PTK) based on the Anonce' sent by the attacker and sends Message-2' again which is encrypted using PTK'. In level 1, after Message-1 is received by supplicant, attacker sends Message-1' to supplicant. Attacker cannot send legitimate Message-3 to supplicant. Hence, supplicant is blocked. In level 2, the authenticator responds to the Message-2 of the supplicant by sending the Message-3 which is encrypted using PTK. However, attacker sends fake

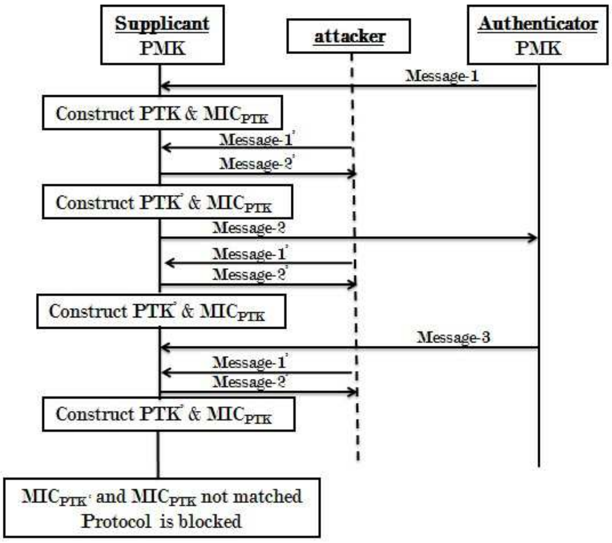


Figure 4.7: Blocking Attack in Four-way Handshake Protocol

Message-1' in between Message-1 & 3. Integrity check performed by the supplicant is failed on Message-3 because the supplicant is using PTK' to generate MIC_{PTK} but the authenticator generate MIC_{PTK} using PTK. Consequently, the supplicant is blocked. In level 3, attacker sends Message-1' after PTK is derived at supplicant, in which supplicant drops the current PTK and derive the new PTK' and sends Message-2' to attacker. Since, attacker is not sending legitimate Message-3 to supplicant, supplicant is blocked.

Flooding attack on four-way handshake protocol: Flooding attack can be taken place at any level in four-way handshake protocol as shown in Figure 4.8. In client mesh, supplicant has more resource constrains such as memory and CPU than authenticator [Li and Yang, 2012]. Thus, supplicant resource are mainly depleted by flooding attack. Upon receiving each new Message-1, supplicant needs to compute PTK and MIC_{PTK}, and store Anonce, PTK, and Snonce. If no attack has been performed on four-way handshake, supplicant needs to compute PTK and MIC_{PTK} at most once and store only one set of Anonce, PTK, and Snonce.

However, four-way handshake protocol is vulnerable to flooding attack which is shown in Figure 4.8. Thus, supplicant needs to compute PTK and MIC_{PTK} 'n' times and store 'n' sets of Anonce, PTK, and Snonce where 'n' is the number of fake messages

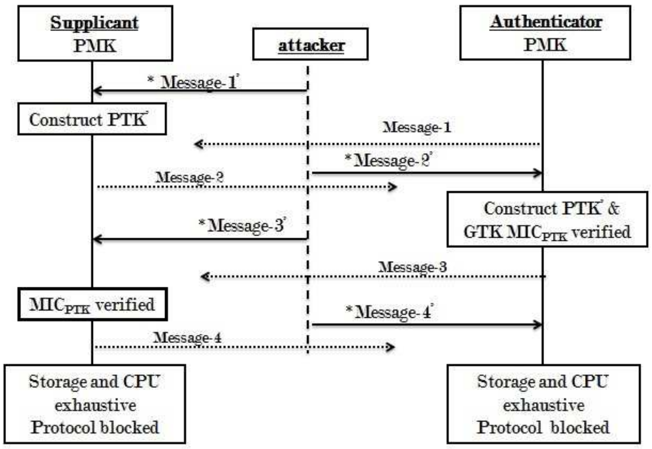


Figure 4.8: Flooding Attack in Four-way Handshake Protocol

sent by attacker. Memory and CPU exhaustion take place at supplicant if attacker floods the Message-1'.

After receiving of every Message-2, authenticator needs to compute PTK and MIC $_{PTK}$, verifies MIC_{PTK} with Message-2 MIC_{PTK}. If attacker floods the Message-2', CPU exhaustion takes place at authenticator.

After receiving of every Message-3, supplicant needs to compute MIC_{PTK} of Message-3 and verifies MIC_{PTK} with Message-3 MIC_{PTK}. If attacker floods the Message-3', CPU exhaustion takes place at supplicant.

Similarly, after receiving of every Message-4, authenticator needs to compute MIC $_{PTK}$ of Message-4 verifies MIC_{PTK} with Message-4 MIC_{PTK}. If attacker floods the Message-4', CPU exhaustion takes place at authenticator. Supplicant is severely suffer from CPU exhaustion attack as compared to authenticator because supplicant has less CPU resource in client mesh network.

4.2.2.2 Enhanced 802.11i Authentication Schemes

In 802.11i four-way handshake, authenticator does not secure the Message-1. An adversary can easily forge Message-1 by spoofing authenticator MAC address and sends this message to supplicant. This case supplicant cannot distinguish whether the received Message-1 is forged or not. For every new Message-1, supplicant creates a new PTK. Adversary takes this is an advantage and sends forged Message-1 between the legitimate Messages-1 and 3. Upon receiving Message-3, supplicant drops this message when the current PTK is not matched with stored PTK. Thus, four-way handshake is blocked by sending one adversary message. Existing schemes use different mechanisms to overcome this problem.

Temporal PTK (TPTK) mechanism is introduced to mitigate affect of the adversary false *Message-1' in 802.11i four-way handshake. Supplicant creates TPTK and PTK when it receives Message-1 and PTK will not update until Message-3 is received and verified. TPTK will be updated when supplicant receives new Message-1. However, this mechanism cannot prevent message forgery attack as it can only prevent those attacks which send forged Message-1' after supplicant has installed and updated PTK.

He and Mitchell propose two possible mechanisms. One is authenticating Message-1 with common secret (PMK) shared between the authenticator and the supplicant, and the second is SNonce Re-use [He and Mitchell, 2004] to enhance the security of 802.11i four-way handshake protocol. In the first approach, authenticator uses PMK to generate a MIC to Message-1. Second approach reuses the SNonce and need not store PTK and ANonce at supplicant. When the Message-1 one is received by supplicant, it only stores SNonce and reuse this SNonce until the Message-3 is received and verified. Supplicant recompute PTK to verify the MIC when it receives Message-3. Once the MIC is verified, Message-4 is sent out and the corresponding PTK can be used as the session key. This approach can overcome the four-way handshake blocking problem and memory exhaustion, but still suffers from CPU exhaustion attack when adversary floods stale Message-3 because for each receiving Message-3 supplicant needs to recompute the PTK to verify MIC [Meng et al., 2013], [Li and Yang, 2012]. Rango, F. et.al analyze in detail of reusing SNonce approach proposed by He and Mitchell. They proposed a resource-aware variant approach which is proposed to get a tradeoff between memory and CPU exhaustion [De Rango et al., 2006]. Rajeev Singh et.al proposed a Secure WLAN Authentication Scheme (SWAS) for wireless LANs [Singh and Sharma, 2013]. In this scheme, authenticator and supplicant make use of four-way handshake protocol to initialize PTK value. Both authenticator and supplicant derive asymmetric keys based on elliptic curve cryptography. The asymmetric keys are used to authenticate the legitimate messages and protect the four-way handshake protocol from blocking and flooding attacks. However, asymmetric key verification consumes more CPU resource than symmetric key verification. Thus, targeted supplicant suffers from CPU exhaustion attack when malicious nodes flood the fake authentication request messages in SWAS.

Existing schemes are inadequate to eliminate the inherent flaw of 802.11i four-way handshake protocol because they still suffer from CPU exhaustion attacks when the malicious nodes flood fake Messages'(1-4). This inherent problem creates more vulnerabilities in Wi-Fi and multi-hop networks. We propose a lightweight encryption scheme to overcome the CPU exhaustion attacks in 802.11i four-way handshake protocol.

4.2.2.3 Lightweight Encryption Scheme

We propose a lightweight encryption scheme to address the security issues of 802.11i four-way handshake protocol as shown in Figure 4.9. Lightweight encryption scheme provides confidentiality and authentication for Message-1, 2, 3 and 4 by using one time pad in four-way handshake protocol to prevent the blocking and false packet flooding attacks. In lightweight encryption scheme, PTK and GTK are initialized between authenticator and supplicant as follows:

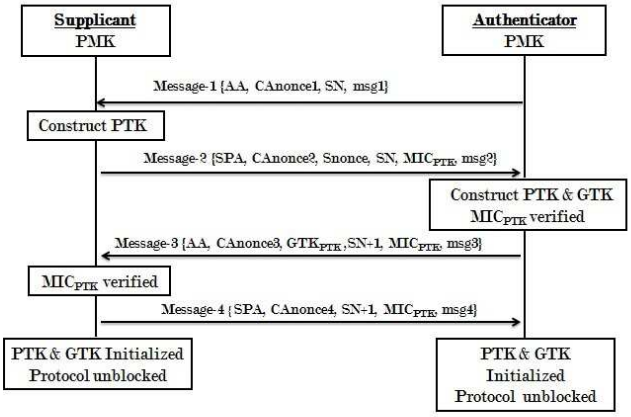

Supplicant
PMK
Authenticator
PMK
Message-1 {AA, CAnonce1, SN, msg1}
Construct PTK
Message-2 {SPA, CAnonce2, Snonce, SN, MIC_{PTK}, msg2}
Construct PTK & GTK
MIC_{PTK} verified
Message-3 {AA, CAnonce3, GTK_{PTK} ,SN+1, MIC_{PTK}, msg3}
MIC_{PTK} verified
Message-4 {SPA, CAnonce4, SN+1, MIC_{PTK}, msg4}
PTK & GTK Initialized
Protocol unblocked
PTK & GTK
Initialized
Protocol unblocked

Figure 4.9: Lightweight Encryption in Four-way Handshake Protocol

To initialize the PTK, authenticator creates the 128-bit Cipher ANonce (CAnonce1) by XORing Anonce with Pairwise Master Key (PMK) least significant 128-bit. After creation of the CAnonce1, authenticator sends Message-1 to supplicant.

Message-1: A->S: AA, CANonce1, SN, msg1;

Supplicant gets Anonce by XORing CAnonce1 with known PMK. It derives PTK from the stored SNonce and received ANonce, and then computes a Message Integrity Check (MIC) from the derived PTK. In addition, supplicant creates the CAnonce2 by XORing the Anonce1 with the Anonce. After creation of the CAnonce2, supplicant sends Message-2 to authenticator.

Message-2: S->A: SPA, CAnonce2, Snonce, SN, MIC_{PTK}, msg2.

Upon receiving the Message-2, authenticator decrypts the CAnonce2 by using stored Anonce. If it is able to decrypt then authenticator generates a PTK by using stored Anonce and received SNonce. The resultant PTK is used to verify MIC of the Message-2. If MIC is valid, authenticator creates CAnonce3 by XORing stored Anonce1 with Anonce2 and sends GTK in Message-3 to supplicant.

Message-3: A->S: AA, CAnonce3, SN+1, GTK_{PTK}, MIC_{PTK}, msg3.

Upon receiving the Message-3, supplicant decrypts the CAnonce3 by using stored Anonce1. If supplicant is able to decrypt then it uses stored PTK to verify MIC of the Message-3. If MIC is valid, supplicant will install PTK and GTK, and creates CAnonce4 by XORing stored Anonce2 with Anonce3 and sends Message-4 to authenticator.

Message-4: S->A: SPA, CAnonce4, SN+1, MIC_{PTK}, msg4.

Upon receiving the Message-4, authenticator decrypts CAnonce4 by using stored Anonce2. If authenticator is able to decrypt then it uses stored PTK to verify MIC of the Message-4. If MIC is valid, authenticator will install PTK. Supplicant uses PTK for de-authentication and secure data communication in Wi-Fi and multi-hop (802.11s) client mesh networks.

4.2.2.4 Security Analysis

Our lightweight encryption scheme prevents blocking attack on four-way handshake by responding only to legitimate messages. In this scheme, supplicant updates Anonce, Snonce and PTK only on the received Message-1 can be decrypted by PMK. Otherwise, supplicant drops the received Message-1.

Fake Message-1' can be sent to block the four-way handshake as shown in Figure 4.7. Supplicant drops all three fake messages because supplicant cannot decrypt these fake messages by using PMK. Moreover, CAnonce is encrypted by 128-bit random number and attacker needs 2^{128} computations to break the CAnonce. Since, authentication server takes very less time (1 or 2s) to authenticate each mesh client in 802.11i four-way handshake protocol, malicious nodes cannot compute 2^{128} computations in this short period of time.

Flooding attack severely depletes the supplicant resource such as memory and CPU. Our light weight encryption scheme mitigates the flooding attack severity on four-way handshake protocol. Flooding attack can be done by sending excessive fake *Messages-1' to supplicant. Upon receiving every fake Message-1', supplicant computes new PTK' and stores Anonce, PTK', Snonce and stores every set {Anonce, PTK', Snonce} values till the completion of PTK initialization. It will take more storage and computation overhead. To overcome this problem, in our proposed scheme, supplicant only responds to legitimate Message-1 in which CAnonce1 is decrypted by PMK. Here, supplicant needs only 128-bit XOR operation for every fake Message-1' and stores only one set {Anonce, PTK', Snonce} legitimate Message-1. This process will take less computation and storage overhead as compared to other existing mitigation schemes such as digital signature and message digest schemes.

If attacker sends excessive *Message-2', authenticator needs to compute PTK and MIC_{PTK}, verify MIC_{PTK} for every Message-2'. This process will need more computation overhead. On other-hand, lightweight encryption scheme the computation and verification are done only for the legitimate Message-2 in which CAnonce2 is decrypted by stored Anonce. Our approach mitigates the severity of CPU exhaustion(*Message-2's) attack by only computing 128-bit XOR operation to isolate the fake Message-2'.

If attacker sends excessive *Message-3's, supplicant needs to compute MIC_{PTK} and verifies with Message-3' MIC_{PTK}. If generated MIC_{PTK} is not matched with stored MIC_{PTK} then supplicant drops the Message-3'. Supplicant needs to use more resource to compute MIC_{PTK} for every Message-3'. Hence, CPU exhaustive attack occurs on four-way handshake protocol. In the proposed scheme, upon receiving each message, supplicant checks CAnonce3 can be decrypted or not by using Anone1. If supplicant is unable to decrypt CAnonce3 then supplicant drops the Message-3'. Similarly, authenticator drops Message-4' when it is unable to decrypt CAnonce4 of Message-4' with stored CAnonce2. Decrypting CAnonce takes very less time instead of computing and verifying $MIC\ _{PTK}$ [He and Mitchell, 2004] or verifying digital signature [Singh and Sharma, 2013].

We have analyzed the performance of Lightweight Encryption Scheme (LES), Digital Signature Scheme (DSS) and Message Digest Scheme (MDS) [Singh and Sharma, 2013] [He and Mitchell, 2004] on four-way handshake protocol using NS-2 network simulator. We consider a scenario with 100 mesh clients, out of which 50 mesh clients are connected to Wi-Fi edge router (R/A) and remaining 50 mesh clients are connected to multi-hop (802.11s) edge router (R/A). To create hostile client mesh network traffic, a group of 30 malicious mesh clients flood 10000 to 1 million fake messages' at targeted mesh client which is going to initialize PTK and GTK in Wi-Fi and multi-hop client networks. Targeted mesh client needs to process all received messages until it is initialized PTK and GTK. Targeted mesh client processing time varies at target mesh client with respect to type of encryption used by security schemes. Since, Wi-Fi and multi-hop client networks follow the same four-way handshake protocol to initialize PTK and GTK the targeted mesh client processing time is same for both the networks. We run this scenario in four different types of processing speeds such as A1 mesh clients with i7-processor-3.40GHz, A2 mesh clients with i5-processor-2.53GHz, A3 mesh clients with Dual core processor-2.8GHz and A4 mesh clients with Single core processor-2.79GHz to find the severity of the blocking and CPU exhaustion attacks with respect to the security schemes.

4.2.2.5 Simulation Results

Table 4.2: Comparison Study of Security Schemes on A1 & A2 Mesh Clients

Wi-Fi/ Multi-hop	**A1 Mesh Client** **Processing time in Sec**			**A2 Mesh Client** **Processing time in Sec**		
Messages	DSS	MDS	LES	DSS	MDS	LES
10000	0.47	0.0406	0.00109	0.734	0.05163	0.0011
20000	0.93	0.0796	0.00203	1.467	0.10115	0.0022
30000	1.41	0.1203	0.00312	2.184	0.156	0.0033
40000	1.87	0.1609	0.00406	2.917	0.2074	0.0044
50000	2.34	0.2015	0.00515	3.65	0.2574	0.0055
60000	2.82	0.239	0.00593	4.353	0.3088	0.0066
70000	3.28	0.2781	0.00718	5.07	0.3588	0.0077
80000	3.75	0.3203	0.00812	5.818	0.4102	0.0088
90000	4.22	0.3609	0.00906	6.583	0.4586	0.0099
100000	4.69	0.4	0.0109	7.34	0.561	0.011
500000	23.43	2.015	0.0512	36.441	2.574	0.055
1000000	46.72	4	0.1	72.946	5.116	0.11

Digital signature scheme (ECC 224-bit): A1 mesh client processing time is 0.47s for 10000 verification messages and 46.72s for 1 million verification messages as shown in Table 4.2. A4 mesh client processing time is 1.688s for 10000 verification messages and 169.28s for 1 million verification messages as shown in Table 4.3.

Message digest scheme (SHA-2 256-bit): A1 mesh client processing time is 0.0406s for 10000 verification messages and 4.00s for 1 million verification messages shown in Table 4.2. A4 mesh client processing time is 0.129s for 10000 verification messages and 12.297s for 1 million verification messages as shown in Table 4.3. Message digest scheme shows better performance than Digital signature scheme.

Lightweight encryption scheme (OTP 128-bit): A1 mesh client processing time is 0.00109s for 10000 verification messages and 0.1s for 1 millon verification messages as shown in Table 4.2. A4 mesh client processing time is 0.00219s for 10000 verification messages and 0.219s for 1 million verification messages as shown in Table 4.3.

Table 4.3: Comparison Study of Security Schemes on A3 & A4 Mesh Clients

Wi-Fi/	**A3 Mesh Client**			**A4 Mesh Client**		
Multi-hop	**Processing time in Sec**			**Processing time in Sec**		
Messages	DSS	MDS	LES	DSS	MDS	LES
10000	0.78	0.0609	0.00124	1.688	0.129	0.00219
20000	1.56	0.1217	0.00234	3.36	0.2438	0.00437
30000	2.294	0.1825	0.00359	5.031	0.3672	0.00641
40000	3.105	0.2418	0.00483	6.719	0.4938	0.00891
50000	3.806	0.3042	0.00593	8.422	0.6141	0.01344
60000	4.571	0.365	0.00718	10.094	0.7328	0.0141
70000	5.367	0.4259	0.00827	11.719	0.8563	0.01563
80000	6.225	0.4852	0.00952	13.563	0.9828	0.01781
90000	6.832	0.546	0.01076	15.25	1.1016	0.02
100000	7.68	0.609	0.01201	16.828	1.219	0.0219
500000	38.06	3	0.0593	83.444	6.141	0.141
1000000	76.06	6.068	0.125	169.28	12.297	0.219

Based on the observations as shown in Table 4.2 and 4.3, processing time of proposed lightweight encryption scheme in the mesh client is more effective and efficient than the digital signature and message digest schemes.

From Table 4.2 and 4.3 results, we study the blocking attack possibility in the security schemes. We consider timeout value as 1s for all four legitimate messages in four-way handshake protocol.

The digital signature scheme is inadequate to mitigate blocking attack in the four-way handshake protocol because the legitimate message is not processed in 1s when A4 mesh client receives 10000 fake messages and when A1 mesh client receives 30000 fake messages.

The message digest scheme is inadequate to mitigate blocking attack in the four-way handshake protocol because the legitimate message is not processed in 1s when A4 mesh client receives 90000 fake messages and when A4 mesh client 250000 fake messages.

The proposed lightweight encryption scheme is capable of handing fake messages without blocking the four-way handshake protocol because the legitimate message is processed in 1s even if A1, A2, A3 and A4 mesh clients receives 1 million fake messages.

Our proposed scheme mitigates the severity of CPU exhaustion attacks because A1 and A4 mesh clients tack 1s to process 1 million fake messages which is not possible in Digital Signature Scheme (DSS) [Singh and Sharma, 2013] and Message Digest Scheme (MDS) [He and Mitchell, 2004]. Thus, our proposed scheme performs much better than digital signature and message digest security schemes in the four-way handshake protocol.

802.11i centralized authentication scheme is widely used in Wi-Fi (802.11b/g) and multi-hop (802.11s mesh) wireless networks. However, this authentication scheme has an inherent flaw in four-way handshake protocol which allows malicious nodes to create various attacks in the client mesh networks. When a edge router (R/A) integrates with Wi-Fi (802.11b/g) and multi-hop mesh networks client mesh becomes more vulnerable to malicious nodes. Our lightweight encryption scheme uses one time pad to efficiently prevents the blocking attacks and memory exhaustive attacks, and mitigates the severity of CPU exhaustive attacks formed by malicious nodes in 802.11i four-way handshake protocol. Our security analysis and simulation results show that the proposed lightweight encryption scheme effectively protect the centralized key management mechanism from various MAC layer attacks. Thus, edge router (R/A) effectively integrates with Wi-Fi (802.11b/g) and multi-hop mesh networks in enhanced centralized authentication scheme.

4.3 Performance analysis of MKMM

In this section, we analyze the storage cost, computation cost, and communication cost of the proposed MKMM. We represent these costs in terms of big-O notation.

4.3.1 Storage Cost

In HWMNs, MKMM has four levels of mesh nodes such as Gateway (Gw_i), mesh router(Rgw_{ik}), edge routers ($RAgw_{ik}$) and mesh client (C_i) levels to store the keys. Storage overhead of a mesh node varies based on the level in which it is placed in the network.

In level 1, each gateway (Gw_i) stores all routers public keys (N_{Rgwp} = $\sum_{i=1 k=1}^{n,m}$ $N_{Rgwp_{ik}}$) and their gateway public keys (N_{Gwp} = $\sum_{i=1}^{n} N_{Gwp_i}$) where 'N' value is started with 0 and increased by 1 on each iteration. The total number of keys stored by a gateway is N_{Gw_i}. N_{Gw_i} = N_{Rgwp} + N_{Gwp}, where ($N_{Rgwp} >> N_{Gwp}$). Level 1 gateway (Gw_i) storage cost is O(N_{Rgwp}).

In level 2, each mesh router (Rgw_{ik}) stores all group members public keys ($N_{Rgwp_{ik}}$ = $\sum_{i=1,k=1}^{1,m}$ $N_{Rgwp_{ik}}$) in Gw_i and neighboring mesh routers public keys ($N_{Rngwp_{tk}}$) and gateways public keys (N_{Gwp} = $\sum_{i=1}^{n} N_{Gwp_i}$). The total number of keys stored by level 2 mesh router is $N_{Rgw_{ik}}$. $N_{Rgw_{ik}}$= $N_{Rgwp_{ik}}$ + $N_{Rngwp_{tk}}$ + N_{Gwp}, where ($N_{Rgwp_{ik}}$ > $N_{Rngp_{tk}}$, N_{Gwp}). Level 2 mesh router (Rgw_{ik}) storage cost is O($N_{Rgwp_{ik}}$).

In level 3, edge router ($RAgw_{ik}$) acts as both mesh router as well as Access points. The storage cost of a $N_{RAgw_{ik}}$ is more than mesh routers in backbone mesh by N_{C_k} (number of mesh clients under $RAgw_{ik}$) in client mesh network. This N_{C_k} value is equal or more than to $N_{Rgwp_{ik}}$. Usually, N_{C_k} value is more than $N_{Rgwp_{ik}}$ value. Total number of keys stored by level 3 mesh router ($RAgw_{ik}$) is $N_{RAgw_{ik}}$. $N_{RAgw_{ik}}$ = $N_{Rgwp_{ik}}$ + N_{C_k}. Where N_{C_k} is 't' time greater than $N_{RAgw_{ik}}$. Level 3 mesh router ($RAgw_{ik}$) storage cost is O(N_{C_k}).

In level 4, each mesh client (C_k) is connected to $RAgw_{ik}$ and its one-hop neighbours. Total number of keys stored by level 4 mesh client is N_{C_k}. N_{C_k}= d_{C_avg} + group key + public key of $RAgw_{ik}$ where d_{C_avg} average degree (average number of neighbouring nodes) of client mesh network. Level 4 mesh client (C_k) storage cost is O(d_{C_avg}).

4.3.2 Communication Cost

When a mesh router broadcasts authentication request message to join in the backbone mesh. The received backbone routers of Rgw_{ik} rebroadcasts this message until it reaches to corresponding Gw_i. In the process of rebroadcasting authentication request message, for each time k number of neighboring routers (node degree) receive this message. This k value lies in between 1 and maximum degree of the Gw_i. We consider average degree of Gw_i is d_{Gw_avg}. Then the total number of communication messages generated is $N_{Rgw_{ik}}$ * d_{Gw_avg}. If this request is received by other group mesh router ($Rgwn_{tk}$) then authentication request message is unicasted to its corresponding gateway (Gw_t) which requires 't+1' communications, where 't' is a number of intermediate mesh routers between Gw_t and ($Rgwn_{tk}$) node. Then the total number of communications required when a mesh router joins in the network is $N_{Rgw_{ik}}$ * d_{Gw_avg} + d_{Gw_avg} * (t+1), where $N_{Rgw_{ik}}$ * $d_{avg} > d_{Gw\_avg}$ * (t+1). The communication cost of Rgw_{ik} authentication request message is O($N_{Rgw_{ik}}$ * d_{Gw_avg}). The communication cost of Rgw_{ik} de-authent- ication request message is O(N_{t_d}) where N_{t_d} is number of nodes in t_d node disjoint paths.

When a mesh client broadcasts authentication/de-authentication request message in the multihop client mesh network, it will need 1 + d_{C_avg} communications to get authenticated by access point and one-hop mesh clients. The communication cost of C_k authentication / de-authentication request message is O(d_{C_avg}). In case of Wi-Fi (one_hop communication) network, new client unicasts a authentication request to get authenticated by access point. Hence, the communication cost of C_k authentication/de-authentication request message is O(1).

4.3.3 Computation Cost

When a mesh router(Rgw_{ik}) broadcasts authentication request message to join in the backbone mesh. All $N_{Rgw_{ik}}$ nodes check the corresponding Gw_i is signed on received authentication request message. Any mesh router receives same authentication requests from different mesh routers, it only verifies for one request message and remaining requests messages are dropped without signature verification which reduces the computation cost on mesh routers. Hence, Rgw_{ik} creates O($N_{Rgw_{ik}}$) computations in its group (Gw_i). If this request message is received by other group mesh routers ($N_{Rgwn_{tk}}$) then the authentication request message is unicasted to its corresponding gateway (Gw_t) which requires 't+1' computations, where 't' is the number of intermediate mesh routes between Gw_t and mesh router ($Rgwn_{tk}$). The computational cost of Rgw_{ik} authentication request message is O($N_{Rgw_{ik}}$). The computation cost of Rgw_{ik} de-authentication request message is O(N_{t_d}) because this request message is passed through t_d number of node disjoint paths to reach Gw_i.

When a mesh client broadcasts authentication/de-authentication request message in the multi-hop client mesh network, all its one-hop mesh clients need to verify this request message along with access point. Thus, this request message will need 1 + d_{C_avg} computations. The computation cost of C_k authentication/ de-authentication request message is O($d_{C_{avg}}$). In case of Wi-Fi network, new client unicasts a authentication request to get authenticated by access point. Hence, the computation cost of C_k authentication/de-authenticati- on request message is O(1).

4.4 Summary

In this chapter, a multi-level key management mechanism has been proposed for HWMNs. The major components of this mechanism are distributed authentication scheme and an enhanced centralized authentication scheme to secure the legitimate mesh nodes. The distributed authentication scheme protects heterogeneous devices communication in backbone mesh. The enhanced centralized authentication scheme provide security for two different networks such as Wi-Fi and multi-hop networks in client mesh. Both the schemes protects the three level mesh nodes such as gateways, mesh routers and mesh clients from various MAC layer network security and information security attacks. Our security analysis and simulation results show that MKMM outperforms the existing DSA-mesh, mobisec schemes in backbone mesh, and digital signature and message digest schemes in client mesh.

Chapter 5

SEVERITY OF WORMHOLE ATTACKS

5.1 Introduction

HWMNs are susceptible to broad variety of attacks particularly in network layer. In chapter 2, we have classified the network layer attacks into two broad categories such as internal and external attacks. All the internal and external attacks are performed either by a single (individual) node or by a group of colluding nodes. Individual attackers are causes less damage to the network than the colluding attackers because colluding attacks are more severe and it is difficult to identify and isolate them from HWMNs. Wormhole attacks are the most severe security attacks formed by colluding attackers. In wormhole attacks, colluding attackers form wormhole malicious tunnel (i.e., malicious long-distance wireless link) with low latency to capture the huge network traffic. These attackers could perform the severe attacks on the captured network traffic by dropping, altering and delaying packets. Most of the existing intrusion detection systems protect HWMNs from single adversary node, but failed to protect from colluding attackers [Glass et al., 2009] [Hu et al., 2003] [Zhen and Srinivas, 2003]. Single-layer Intrusion Detection Systems (SIDSs) consider only layer independent parameters to detect the wormhole attacks [Malkani et al., 2011] [Muhammad Sharif, 2012] [Khabbazian et al., 2009]. SIDSs generally use predefined measures such as maximum distance or Round Trip Time (RTT) of any two communicating nodes to isolate the wormhole attacks. These mechanisms effectively isolate the wormhole attacks in client mesh networks since mesh clients have same transmission range. The predefined measures of SIDSs are inadequate to isolate the wormhole attacks in backbone mesh, because routers are capable of communicating through different transmission ranges. In addition to this, existing SIDSs fails to study the severity of wormhole attacks on routing paths which leads to isolate the legitimate wormhole paths from the backbone mesh. In this chapter, we study the severity of the wormhole paths to find the affected reputation based on the behaviour of the wormhole malicious paths in backbone mesh. These reputation values are used to detect wormhole attacks in our proposed dynamic reputation based cross-layer intrusion detection system in the next chapter 6.

The remainder of this chapter is organized as follows. Section 5.2 discusses the wormhole attacks. Section 5.3 presents impact of the wormhole attacks on HWMN. Section 5.4 describes the severity of the wormhole attacks. Finally, section 5.5 summarizes this chapter.

5.2 Wormhole Attacks

Based on literature survey, wormhole attacks occur in two phases. In first phase, colluding attackers attract their neighbours by forming wormhole malicious tunnel with low-latency. The second phase, attacker receives data packets from its neighbours and ”tunnels” them to another attacker which leads to various attacks.

Phase 1: The wormhole malicious tunnel can be established in different ways, such as through a long-distance wireless/wired link or packet encapsulation [Cagalj et al., 2007] [Pelechrinis et al., 2008]. The routing protocols such as DSDV [Perkins and Bhagwat, 1994], AODV [Chakeres and Belding-Royer, 2004], DSR [Johnson et al., 2001b], HWMP [Bahr, 2007], OLSR [Baras et al., 2007] etc. for wireless mesh networks find paths with the minimum hop count and delay. Out of these protocols, AODV and AOMDV are the most popular on-demand ad hoc routing protocols studied in the research community and the Internet Engineering Task Force (IETF) [Chakeres and Belding-Royer, 2004] and [Marina and Das, 2001]. However, all these protocols are vulnerable to wormhole malicious tunnel [Xiu-feng et al., 2010] [Baras et al., 2007] [Poovendran and Lazos, 2007] [Awerbuch et al., 2002]. We exemplify how the Ad-Hoc On-demand Multi-path Distance Vector (AOMDV) [Marina and Das, 2001] routing protocol is vulnerable to malicious wormhole tunnel.

Wormhole Attacks on AOMDV Protocol: AOMDV is an extension of AODV routing protocol which computes multiple disjoint paths, these paths are either link disjoint or node disjoint. Each node maintains a monotonically increasing sequence number to determine freshness of routing and to prevent routing loops. In AOMDV, a source node initiates a route discovery to destination node by broadcasting a route request (RREQ) packet. Other than source and destination addresses, this RREQ packet contains important fields such as a known destination sequence number field for loop-free routing and a hop count field for finding shortest routes between source and destination. When an intermediate node receives the RREQ packet from the source node, it increases RREQ packet hop count by one. It stores reverse route entry to source node as last_hop before rebroadcasting the RREQ packet to find destination node. If an intermediate node receives duplicate RREQ packets from different nodes, it stores all last_hops information, but it only rebroadcasts single RREQ packet. This process is continued until the RREQ packet reaches the destination. Destination node generates route replay (RREP) packet for each received RREQ packet and it sends back to source in reverse path. Upon receiving RREP packet, intermediate node stores the forward route entry to destination node as next_hop. To form link disjoint paths between source and destination, all intermediate nodes must have unique next_hops as well as unique last_hops. In addition to this, each intermediate node forwards RREP packet to only one last_hop node in reverse path. Source node will choose the best path with respect to less hop count and delay from existing multiple paths. However, we explain how AOMDV routing protocol fails in a wormhole malicious tunnel environment with the help of scenario a and b.

Scenario a: *Wormhole malicious tunnel through long-distance wireless/ wired link*

In Figure 5.1, if Source(S) node broadcasts the route request (RREQ) packet to find the route to Destination(D) node, neighboring nodes M1 and R1 receive the RREQ packet. If nodes M1 and M2 form a wormhole malicious tunnel by using long-distance wireless

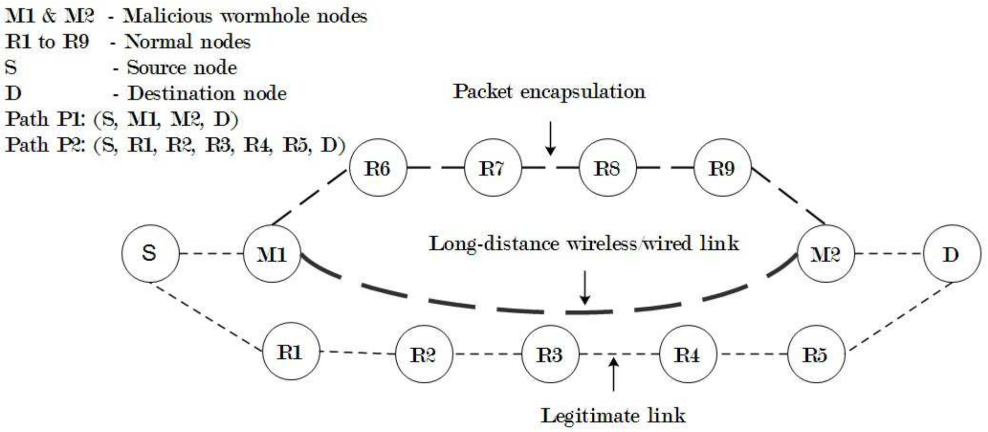


Figure 5.1: Example of Wormhole Attacks

/ wired link then node M1 forwards the RREQ packet directly to node M2 with less delay instead of rebroadcasting the RREQ packet. Upon receiving RREQ, M2 rebroadcasts the RREQ packet. Nevertheless, all other legitimate nodes follow the protocol by rebroadcasting the received RREQ packet. Node D first receives RREQ packet from M2 because of wormhole malicious tunnel. Later D receives RREQ packet from R5 because RREQ packet was passed through nodes R1, R2, R3 and R4 before reaching node R5. Destination first sends a route replay (RREP) packet to S through M2 and then R5. Node S has two paths, first path P1:(S, M1, M2, D) is three hops long and second path P2:(S, R1, R2, R3, R4, R5, D) is six hops long. Node S selects path P1:(S, M1, M2, D) to forward the data packet to D, due to low latency and less hop count.

Scenario b:*Wormhole malicious tunnel through packet encapsulation*

In Figure 5.1, M1 and M2 use packet encapsulation to form wormhole malicious tunnel. M1 encrypts the RREQ packet with known shared secret key of M1 and M2. Node M1 forwards this packet to M2 via R6, R7, R8 and R9 nodes. After decryption of received packet from M1, M2 gets RREQ packet. Node M2 rebroadcasts the RREQ packet to get the reply from node D. When M2 receives RREP packet from node D, it follows to send RREP packet to M1 as the same procedure as M1 has followed to forward the RREQ packet to M2. The resultant path at node S is P1:(S, M1, M2, D). On the other hand, all legitimate nodes follow the protocol and form P2:(S, R1, R2, R3, R4, R5, D). Node S selects path P1:(S, M1, M2, D) to forward the data packets to D due to less hop count.

In packet encapsulation, delays of intermediate nodes (From Figure 5.1 nodes R6, R7, R8 and R9) are added to both RREQ and RREP packets to form a path P1:(S, M1, M2, D), which is less vulnerable, since HWMNs provide long-distance wireless/wired links communications.

Phase 2: Wormhole malicious tunnel attackers are able to capture their neighbors network traffic. When an attacker receives data packets from its neighbors, it ”tunnels” them to another attacker which allows them to perform various attacks.

In Figure 5.1 node S selects path P1:(S, M1, M2, D) to send the data packet to D. When attacker M1 receives data packets from S, M1 ”tunnels” them to another attacker M2. Then attacker M2 can perform jellyfish or byzantine attack or both attacks of received data packets.

In **jellyfish attack**, attacker intends to decrease the goodput by *increasing delay* of received data packets before forwarding them to target node which leads to Denial of Service (DoS) attack [Samad et al., 2012]. In Figure 5.1, attacker M2 can *increase delay* of received data packets from M1 in two different ways: M2 intentionally keeps them for longer time in its queue or replays them locally (between M1 and M2) before forwarding them to node D. This attack is called as Wormhole attack Followed by Jellyfish (WFJ) attack.

In **byzantine attack**, attacker intends to decrease the goodput by doing malicious functionalities such as *packet dropping, packet modification* and *injecting false packets* of received data packets before forwarding them to target node [Zhong and Xu, 2010] [Baras et al., 2007]. In Figure 5.1, attacker M2 can implement malicious functionalities of received packets from M1 before forwarding them to node D. This attack is called as Wormhole attack Followed by Byzantine (WFB) attack. If *jellyfish* and *byzantine attacks* are simultaneously performed by M2 on received packets then this attack is called as Wormhole attack Followed by Jellyfish and Byzantine (WFJB) attacks.

A single attacker can also create malicious long-distance wireless communications to attract its neighbour nodes to send data packet to other neighbour nodes via this attacker [Azer et al., 2009] [Dong et al., 2011]. However, when the wormhole attacks are launched by single attacker, attacker itself implements these attacks of received packets, instead of tunneling them to any other attackers. These attacks can be easily detected by local monitoring intrusion detection systems [Marti et al., 2000] [Han and Poor, 2009] [Khalil et al., 2010] [Yi et al., 2009]. On the other hand, wormhole attacks are more powerful and difficult to identify if it is launched by more than one attacker.

5.3 Impact of the Wormhole Attacks on HWMN

Mesh clients have same transmission range in client mesh networks. Wormhole attack in client network is more affective when the attackers use long transmission range than the existing transmission rage. In this case, existing security solutions [Van Phuong et al., 2007] [Chiu and Lui, 2006] [Glass et al., 2009] and [Zhen and Srinivas, 2003] effectively isolate wormhole attacks by fixing the maximum RTT or distance values between any one-hop communication nodes. Thus, we use the maximum transmission range (R_{max}) between two mesh clients to isolate wormhole attacks in client mesh networks.

Mesh routers have different transmission ranges in backbone mesh. Wormhole attack severity in backbone mesh increases as wormhole attackers transmission range increases. The existing security solutions [Khalil et al., 2007] and [Zhang et al., 2008] detect or isolate legitimate long-distance wireless links (non malicious wormholes) due to lack of wormhole attacks analysis and their predefined measures such as RTT and transmission range (distance). Thus, legitimate long-distance wireless link communications are still vulnerable in backbone mesh. To overcome this, first we study the severity of wormhole attacks and develop a dynamic reputation-based cross-layer intrusion detection system to protect the legitimate long-distance wireless links from wormhole attacks.

5.4 Severity of Wormhole Attacks

The experimental study is conducted to analyse the behaviour of Wormhole Malicious Paths (WMP) and Wormhole non-malicious Paths (WP) using ns2 simulator. Without loss of generality, our simulation scenario as shown in Table 5.1 considers IEEE 802.11

MAC protocol, AOMDV routing protocol in the network layer and CBR data traffic in the application layer. HWMN consists of 80 nodes which are uniformly distributed in the area of 1500m X 1500m and initially all these nodes have the same transmitting range 150m. We observe the goodput (actual data in the network traffic) of the wormhole malicious and non-malicious paths. To find the severity of attack, we calculate the percentage of affected goodput(gp_{aff}) in equation 5.1.

$$Percentage\ of\ gp_{aff} \ = \ \frac{WP\ goodput\ -\ WMP\ goodput}{WP\ goodput} \ * \ 100. \tag{5.1}$$

We consider 40 nodes as backbone Mesh Routers (MR) and 40 nodes as Mesh Clients (MC). Out of 40 backbone mesh routers, we have chosen five sets of Source (S) and Destination (D) routers. These routers have both Router as well as Access point (R/A) functionalities and each of these routers connects to four mesh clients. Each S and D routers maintain 1250m distance. All mesh clients have random mobility within their corresponding R/A nodes area. In AOMDV routing protocol, source selects the best path among the multiple paths based on minimum hop_count and delay. Since, all nodes have same transmission range (150m), each S and D nodes require minimum 8 intermediate nodes to form a path. Wormhole paths have minimum hop_count and delay because each node has long-range transmission in the path. Hence, nodes S and D select the wormhole path to forward the data packets. We create 6-node, 4-node and 2-node wormhole paths by altering the nodes transmission rage from 150m to 200m, 320m and 950m at physical layer. Each individual path covers all source and destination nodes.

We examine the individual wormhole path behaviour with three different CBR packet sizes as 500, 1000 and 1500 bytes. For each CBR packet size, we run the simulation for 1000s and calculated the goodput. Here, all mesh clients of source nodes send the these data packets to mesh clients of destination nodes. Based on the observation, 2-node wormhole non-malicious path(WP_1) has higher goodput than 4-node and 6-node wormhole non-malicious paths(WP_2 & WP_3) as shown in Table 5.2 and also we observe that the average goodput of the wormhole path increases as packet size increases.

Wormhole attacks are created on the above three wormhole non-malicious paths to observe the wormhole malicious paths ($WMP_{1,\ 2\ \&\ 3}$) behaviour.

Table 5.1: Network Parameters

Network area	1500m X 1500m
Placement of MR	Uniform
MAC protocol	IEEE 802.11
Routing protocol	AOMDV
Network traffic	CBR
Packet size	500, 1000 and 1500 bytes
Number of nodes	80 (40 MR + 40 MC)
# gateway nodes in MR	2
# wormhole nodes in MR	12
# wormhole paths in MR	3 (2-node, 4-node and 6-node)
# S and D nodes(R/A) in MR	10
Node mobility	Random (40 MC)
Simulation Time	1000s

Table 5.2: Wormhole Non-malicious Paths Average Goodput in Kbps

	Avg goodput(Kbps)		
Wormhole nodes / Packet size	**2-nodes**	**4-nodes**	**6-nodes**
500 bytes	1884	1372	1172
1000 bytes	1944	1482	1255
1500 bytes	1970	1554	1348

To create Wormhole Followed by Jellyfish (WFJ) attack, we set that 50% of the attackers on wormhole path increase the path delay and remaining 50% of the attackers support the above attackers by forwarding the data packets to them. We observe the behaviour of the each wormhole malicious path by varying the initial path delay (D') to 2D', 4D' and 8D'. We observe the average goodput of $WMP_{1,\,2\,\&\,3}$ as shown in Table 5.3. As a result, increase in number of malicious nodes and delay on wormhole malicious paths ($WMP_{1,\,2\,\&\,3}$) leads to increase the percentage of affected goodputs of these paths from 50% to 100%.

Table 5.3: Wormhole Malicious (WFJ) Paths Average Goodput in Kbps

	Avg goodput(Kbps)									
WFJ Attackers /	**2-node**			**4-node**			**6-node**			% gp_{aff}
Packet size	2D'	4D'	8D'	2D'	4D'	8D'	2D'	4D'	8D'	Min — Max
500 bytes	876	86	0	331	0	0	25	0	0	53 — 100
1000 bytes	947	88	0	445	0	0	39	0	0	51 — 100
1500 bytes	984	104	0	545	0	0	59	0	0	50 — 100

To create Wormhole Followed by Byzantine (WFB) attack, we set that 50% of the attackers on the wormhole path disturb the network traffic by dropping all/selectively the packets or altering the packets and remaining 50% of the attackers support these attackers by forwarding data packets. Here, the attackers on the $WMP_{1,\ 2\ \&\ 3}$ disturb the network traffic by 5%, 10% and 20%. We observe the average goodput of $WMP_{1,\ 2\ \&\ 3}$ is shown in Table 5.4. As a result, increase in number of attacking nodes, packet size and percentage of affected traffic wormhole malicious paths ($WMP_{1,\ 2\ \&\ 3}$) leads to increase the percentage of affected goodputs of these paths from 75% to 100%.

Table 5.4: Wormhole Malicious (WFB) Paths Average Goodput in Kbps

	Avg goodput(Kbps)									
WFB Attackers /	**2-node**			**4-node**			**6-node**			% gp_{aff}
Packet size	5%	10%	20%	5%	10%	20%	5%	10%	20%	Min — Max
500 bytes	470	22	0	110	0	0	160	0	0	75 — 100
1000 bytes	349	9	0	22	0	0	0	0	0	81 — 100
1500 bytes	243	0	0	0	0	0	0	0	0	88 — 100

To create Wormhole Followed by Jellyfish and Byzantine (WFJB) attacks, we set that 50% of the attackers on the wormhole path disturb the network traffic by performing both the attacks, remaining 50% of the attackers support these attackers by forwarding data packets. We observe the average goodput of $WMP_{1,\ 2\ \&\ 3}$ is shown in Table 5.5. As a result, increase in number of attacking nodes, packet size and percentage of affected traffic wormhole malicious paths ($WMP_{1,\ 2\ \&\ 3}$) leads to increase the percentage of affected goodputs of these paths from 85% to 100%. From the above experimental results, we can infer that the severity of the each attack is known by the affected goodput of any suspected wormhole path. Hence, we use the Affected Reputation (AR) to fix the range of Affected Reputation of suspected wormhole path (AR_{WHP}). Initially, AR_{WHP}

Table 5.5: Wormhole Malicious (WFJB) Paths Average Goodput in Kbps

	Avg goodput(Kbps)									
WFJB Attackers / Packet size	**2-node**			**4-node**			**6-node**			% gp_{aff} Min — Max
	2D’ 5%	4D’ 10%	8D’ 20%	2D’ 5%	4D’ 10%	8D’ 20%	2D’ 5%	4D’ 10%	8D’ 20%	
500 bytes	278	14	0	28	0	0	0	0	0	85 — 100
1000 bytes	172	2	0	3	0	0	0	0	0	92 — 100
1500 bytes	56	0	0	0	0	0	0	0	0	97 — 100

value is set by the source and destination nodes. The affected reputation of WFJ attack (AR_{WFJ}), WFB attack (AR_{WFB}) and WFJB attacks (AR_{WFJB}) are calculated using the following equations 5.2, 5.3 and 5.4.

$$AR_{WFJ} = (1 - \alpha) * AR_{WHP} \qquad 0 \leq \alpha \leq a \tag{5.2}$$

$$AR_{WFB} = (1 - \beta) * AR_{WHP} \qquad 0 \leq \beta \leq b \tag{5.3}$$

$$AR_{WFJB} = (1 - \gamma) * AR_{WHP} \qquad 0 \leq \gamma \leq c \tag{5.4}$$

Where *a* is 0.5, *b* is 0.75 and *c* is 0.85 from Table 5.3, 5.4 and 5.5. AR_{WFJ} does not include the packet size to set the α value because affected goodput of the wormhole path is relatively same for all packet sizes. In contrast, affected goodput on the wormhole path increases as the packet size increases in WFB and WFJB attacks. Thus, AR_{WFB} and AR_{WFJB} consider the packet size to set the corresponding β and γ value. We use the affected reputation values to punish the wormhole paths when they are suspected for wormhole attacks. As per the results, we can say that wormhole attacks severely affect the network performance in HWMNs.

5.5 Summary

Most of the existing single layer intrusion detection systems detect all the wormhole paths as attacking paths without analysing the behaviour of wormhole paths. This leads to non-utilization of long-distance wireless links in backbone mesh networks. To overcome this problem, we analyse the behaviours of the routing paths to find the severity of the wormhole malicious paths in backbone mesh network. The severity values of the wormhole malicious paths are used to detect wormhole attacks in our proposed dynamic Reputation-base Cross-layer Intrusion Detection System (RCIDS) which is discussed in the chapter 6. On the other hand, pre-defined measures such as maximum RTT or distance values between any one-hop communication nodes are effective to isolate wormhole attacks in client mesh networks because all mesh clients have same transmission capacity.

Chapter 6

DYNAMIC REPUTATION BASED CROSS-LAYER INTRUSION DETECTION SYSTEM

Cross-layer Intrusion Detection Systems (CIDSs) consider multi-layer interactions to analyze the anomalies. CIDSs receive more attention because of comprehensive ability to judge the anomalies in HWMNs [Paris et al., 2011] [Thamilarasu.G et al., 2005] [Wang et al., 2009]. However, no CIDSs have been proposed to protect against wormhole attacks and CIDSs also suffer from false alarms due to misdetection of failure of a node/path as malicious node/path. Reputation based IDSs empower the CIDSs by varying the reputation value of a node/path in the network. However, existing reputation IDSs do not consider the behavior based cross-layer parameters to isolate the wormhole attacks [Refaei et al., 2005] [Ding.Q and Jiang.M, 2009].

In this chapter, we propose a dynamic Reputation based Cross-layer Intrusion Detection System (RCIDS) to detect and isolate wormhole attacks in backbone mesh. RCIDS uses the behaviour based cross-layer (network layer and MAC layer) parameters with reputation to detect nodes involved in the wormhole attacks. It provides a countermeasure security solution that isolates the wormhole malicious nodes from all the monitoring nodes thereby removing their ability to cause future damage.

The rest of this Chapter is organized as follows. Section 6.1 describes RCIDS and its defenses against the various wormhole attacks. Section 6.2 presents the performance analysis of RCIDS. Finally, section 6.3 summarizes this chapter.

6.1 Dynamic Reputation based Cross-Layer Intrusion Detection System

In this section, we describe the process for wormhole attacks detection in RCIDS followed by the process for isolation of the wormhole malicious nodes.

6.1.1 Cross-layer Parameters

The proposed RCIDS uses cross-layer (network layer and MAC layer) parameters to develop a behaviour-based intrusion detection system to mitigate the wormhole attacks. Since wireless mesh routers in backbone mesh have finite buffer size, packet drops occur when the arriving packets find the buffer is full and queuing delay of a packet is more when the number of packet arrivals are more in queue per unit time. RCIDS evaluates these packet drops and delays on the wormhole paths by considering packet blocking probability and per packet expected queuing delay. To define these values in backbone mesh, group heads (gateways) monitor the network traffic of their group members (mesh routers) to evaluate each member per packet expected queuing delay ($W_{q_{ij}}$) and blocking probability ($P_{B_{ij}}$), where 'i' represents group head and 'j' represents group member. Since group heads know their group members finite buffer and transmission capacities, M/M/1/K queuing model [Bunday, 1986] [Pourbabai, 1988] [Capdehourat et al., 2012] [Gupta and Shroff, 2009] is used to calculate $W_{q_{ij}}$ and $P_{B_{ij}}$. The following equations are used by group heads to calculate the $W_{q_{ij}}$ and $P_{B_{ij}}$ values of their corresponding group members:

When a group member queue size is N_{ij}, and packet arrival rate is λ_{ij}, packet departure rate is μ_{ij}, then utilization factor is $\rho_{ij} = \frac{\lambda_{ij}}{\mu_{ij}}$. In M/M/1/K queuing model, per packet expected waiting time in queue ($W_{q_{ij}}$) = $\frac{Average\ queue\ size}{packet\ arrival\ rate}$.

$$W_{q_{ij}} = \begin{cases} \frac{1}{\lambda_{ij}}(\frac{\rho_{ij}}{1-\rho_{ij}} - \frac{N_{ij}+1}{1-\rho_{ij}^{N_{ij}+1}}\rho^{N_{ij}+1} - \rho_{ij}) & \rho_{ij} \neq 1 \\ \\ \frac{1}{\lambda_{ij}}(\frac{N_{ij}}{2} - \rho_{ij}) & \rho_{ij} = 1 \end{cases}$$

In M/M/1/K queuing model, if the arriving packets find that the queue is full then packet loss occurs. It is called blocking probability ($P_{B_{ij}}$)

$$P_{B_{ij}} = \begin{cases} \frac{(1-\rho_{ij})\rho^{N_{ij}}}{1-\rho_{ij}^{N_{ij}+1}} & \rho_{ij} \neq 1 \\ \\ \frac{1}{N_{ij}+1} & \rho_{ij} = 1 \end{cases}$$

Each group head waits over a period of time to update $W_{q_{ij}}$ and $P_{B_{ij}}$ values and sends to corresponding group members. Here, $W_{q_{ij}}$ and $P_{B_{ij}}$ values are signed by public-key of group head and encrypted with public-key of corresponding group member to provide authentication and confidentiality between group member and group head. To handle the volatile network traffic in backbone mesh, group heads consider maximum arrival packets per unit time of their group members to calculate these values.

To handle the collisions from MAC and routing layers, each group head periodically calculates the number of collisions and active hops of its group members. These values are shared with other group members to find the total number of collisions and the total number of active hops in backbone mesh. Based on these values, we define Per_hop Collision Probability (PCP) = $\frac{Total\ number\ of\ collisions}{Total\ number\ of\ active\ hops}$ which is calculated periodically at each group head and distributed in backbone mesh in order to update the group members. RCIDS excludes $W_{q_{ij}}$, $P_{B_{ij}}$ and PCP values from total affected packets on wormhole path to find the actual wormhole path behaviour. In backbone mesh, group members have different transmission ranges. Each group head selects minimum transmission range of its group and sends to other group heads to find the minimum transmission range in backbone mesh. Once all group heads minimum transmission ranges are found then they select minimum transmission range (r_{min}). This r_{min} value is broadcasted into backbone mesh.

Table 6.1: Notations Used

D_{SD}	Distance between S and D
R_{SD}	S and D shared malicious nodes revocation list
I_{SD}	Ideal end-to-end packet delay between S and D
T	Threshold value
A_S	Average end-to-end packet delay at S
A_D	Average end-to-end packet delay at D
W_S	Worst case average end-to-end packet delay at S
W_D	Worst case average end-to-end packet delay at D
EPDR	Expected Packet Delivery Ratio
E_D	Current average end-to-end packet delay at D
E_S	Current average end-to-end packet delay at S
Dl_{max}	Maximum expected wormhole path delay
AR_{PS}	Change of AR for different packet sizes

6.1.2 Notations used in RCIDS

Description of notations shown in Table 6.1 are explained as follows:

The location information of Source (S) and Destination (D) nodes helps to find the distance measures such as D_{SD}. Shared revocation list consists of public keys of wormhole attackers and R_{SD} is used by S and D to isolate previously known attackers from the new path. Nodes S and D use the control (routing) packets to find and maintain paths between them. Control packets have high priority in mesh routers priority queue so that control packets have negligible queuing delay. Thus, we define ideal end-to-end packet delay (I_{SD}) = control packet arrival time at node D $-$ control packet start time at node S of each path. We set the Threshold (T) value on both S and D to find whether the existing wormhole path is malicious or not. To find average end-to-end packet delay (A_D) at node D, node S sends 'n' packets to D. Since, packet drops can occurre due to $P_{B_{ij}}$ and PCP in wireless networks, we define EPDR = 1 - (($\sum_{k=1}^{n\_hops-1} P^{k}_{B_{ij}}$) + n_hops * PCP), where EPDR $>$ 0 and n_hops is a number of hops in a wormhole path. Node D excludes these packet drops from 'n' value and considers 'n^p' as $\lfloor n * EPDR \rfloor$ to calculate A_D. We define $A_D = \frac{n}{n^p} * \sum_{k=1}^{n^p} t_k$ ($n^p \geq 1$) at D, where t_k = arrival time at D - start time at S of each packet. A_D value is sent to S by using reply packet. This packet may have less end-to-end delay than A_D. Thus, the average end-to-end packet delay A_S at node S, we define $A_S = \frac{(A_D * n^p)\ +\ destination\ reply\ packet\ end-to-end\ Delay}{n^p+1}$.

Since, A_S and A_D values are average end-to-end packet delays, D will wait for a extra time to monitor path behavior of 'n^p' packets. As this waiting time at node D increases, the wormhole malicious paths affected goodput also increases. Thus, we define W_S = 1.5 * A_S and W_D = 1.5 * A_D, where node D waits 50% extra time for each packet. D will wait for minimum of (n*W_S, n*W_D) time to start observing the wormhole path behaviour. In addition, W_S and W_D values change when A_S and A_D values change.

Node D calculates CPDR = $\frac{number\ of\ packets\ received\ by\ D}{number\ of\ packets\ sent\ by\ S}$ in minimum of (n*W_S, n*W_D) time. D considers 'n^p' packets to calculate current average end-to-end packet delay (E_D) when EPDR greater than or equal to CPDR, we define $E_D = \frac{\sum_{k=1}^{n^p} t_k}{n}$ ($n^p \geq 1$).

D will send this value to S then $E_S = \frac{(E_D * n)\ +\ destination\ reply\ packet\ end-to-end\ delay}{n+1}$. The packet delays increase on wormhole path when intermediate nodes per unit packet arrivals increase on this path. Thus we define maximum expected wormhole path delay (Dl_{max}) = I_{SD} + $\frac{data\ packet\ size}{control\ packet\ size} * n\_hops * t_{strans}$ + $\sum_{k=1}^{n\_hops-1} W_{q_{ij}}^k$, where t_{strans} is source node rate of transmission (bits for second). Based on $W_{q_{ij}}$ and $P_{B_{ij}}$ PCP periodic updates of a wormhole path, nodes S and D update Dl_{max} and EPDR. Since size of the packet increases the affected goodput increases (from Table 5.4, 5.5 in section 5.4), thus we define AR_{PS} value is 1 for 500bytes packet, 2 for 1000bytes packet and 3 for 1500bytes packet. All notations are sustained by nodes S and D and each intermediate node only sustains its $W_{q_{ij}}$ and $P_{B_{ij}}$ values on the wormhole path. In addition to this, mesh clients need not know the RCIDS parameters because mesh clients prevent the wormhole attacks by fixing maximum transmission range (R_{max}) between two nodes in client mesh. Edge router (R/A) sets the R_{max} value and disseminates in the client mesh. Hence, RCIDS parameters have no impact on mesh clients.

6.1.3 Detection and Isolation of Wormhole Malicious Paths

In the proposed approach, wormhole path behaviour is observed based on I_{SD}, A_S, A_D, W_S, W_D delays and EPDR value. Initial threshold (T) and affected reputation (AR_{WHP}) values are set by S and D at route initialization phase. Affected reputation values AR_{WFJ}, AR_{WFB} and CPDR are initially set to zero. The proposed approach works in two phases such as path initialization phase and path behaviour phase.

In path initialization phase, nodes S and D select the best path (minimum hop_count and delay) in which none of the intermediate node in the path is an element of R_{SD}. Here, we assume that the S and D nodes trust each other and share their malicious nodes revocation list R_{SD}. These nodes calculate D_{SD} value. If D_{SD} value is greater than r_{min}*Hop_Count value where Hop_Count>1 then selected path is a wormhole path. When the wormhole path is established between nodes S and D, intermediate nodes on wormhole path send their $W_{q_{ij}}$, $P_{B_{ij}}$ values to them. In addition, they have PCP value which is received from corresponding group head. Initially, node S sends 'n' number of test packets to D. The value of 'n' is kept secret between nodes S and D to protect RCIDS from play back attacks. Node D calculates the average end-to-end packet delay (A_D) for 'n^p' packets and sends A_D value to S using reply packet in the same path. Upon receiving reply packet, S calculates A_S. If minimum value of (A_S, A_D) is less than Dl_{max} value then node S sends this minimum value to D. Otherwise, S will set to minimum value of (A_S, A_D) value as Dl_{max} and sends this value to D. Nodes S and D calculate their respective values W_S and W_D based on A_S and A_D values.

In path behaviour phase, node D will wait until minimum of (n*(W_S), n*(W_D)) time to receive the 'n^p' packets from node S. If CPDR is greater than or equal to EPDR then node D calculates current average end-to-end packet delay (E_D) of the 'n^p' packets and this value is sent to S using reply packet. Node S also calculates E_S value based on received reply packet. Nodes S and D consider minimum of (A_S, A_D), (W_S, W_D) to verify the maximum of current average end-to-end packet delay (E_S, E_D). If 'n^p' packets current average end-to-end packet delay value lies between ideal and average end-to-end packet delays, then there is no attack on that wormhole path. If the current average end-to-end packet delay value lies between average and worst case average end-to-end packet delays then affected reputation AR_{WFJ} becomes AR_{WFJ} + (1-α)* AR_{WHP}, where α is $\frac{I_{SD}}{max(E_S,E_D)}$ and 1-α is a percentage of I_{SD} increased in the wormhole path. If updated affected reputation AR_{WFJ} becomes more than threshold value then this wormhole path is treated as WFJ attack. If CPDR is below than the EPDR (number of received packets at D is less than n'), then affected reputation AR_{WFB} becomes AR_{WFB} + (1-β)* AR_{WHP}, where β is $\frac{1}{AR_{PS} * number\ of\ packet\ drops}$, and 1-$\beta$ is percentage of packet drops in the wormhole path. If updated affected reputation AR_{WFB} is more than threshold value then this wormhole path is treated as WFB attack. On the other hand, if WFJ attack is suspected and AR_{WFB} value greater than zero then AR_{WFJ} is updated by adding (1-γ)* AR_{WHP}, where γ is $\frac{I_{SD}}{max(E_S,E_D) + AR_{WFB}}$. If WFB attack is suspected and AR_{WFJ} value greater than zero then AR_{WFB} is updated by adding (1-γ)* AR_{WHP}, where γ is $\frac{1}{(AR_{PS} * number\ of\ packet\ drops) + AR_{WFJ}}$. In both the cases 1-$\gamma$ is percentage of I_{SD} increased and packet drops in the wormhole path. If the summation of affected reputations of both the attacks is more than the threshold value then the wormhole path is treated as WFJB attacks.

In RCIDS, for each iteration nodes S and D wait minimum of (n*W_S, n*W_D) time to observer wormhole path behaviour is explained in algorithm 6.3. When a wormhole path is suspected to one of the wormhole attacks in present iteration, Min (A_S, A_D) value of this path is updated for next iteration as shown in Figure 6.1. If updated Min (A_S, A_D) value is less than Dl_{max} value then node S and D set this Min (A_S, A_D) value. Otherwise, S and D will set Min (A_S, A_D) value as Dl_{max}.

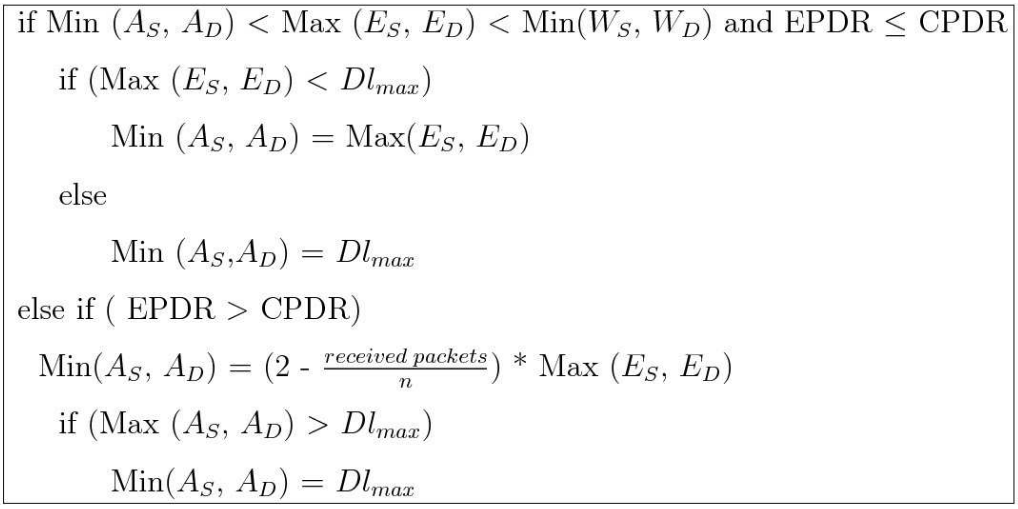
When a wormhole path is suspected to one of the wormhole attacks in present iteration, 'n' value of this path is changed for next iteration as shown in Figure 6.2. If updated 'n' value is grater than 2*$\lceil n * (1 - EPDR) \rceil$ value then node S and D set this 'n' value. Otherwise, S and D will set 'n' value as 2*$\lceil n * (1 - EPDR) \rceil$.

If any one of the attack is detected on the wormhole path, immediately S and D drop this path and update their malicious nodes revocation list R_{SD}. These nodes select the new path (minimum hop_count and delay) in which no single intermediate node belongs to updated R_{SD}. If this new path is a wormhole path, all the reputation parameters are

Algorithm 6.3 : Wormhole path behaviour in RCIDS

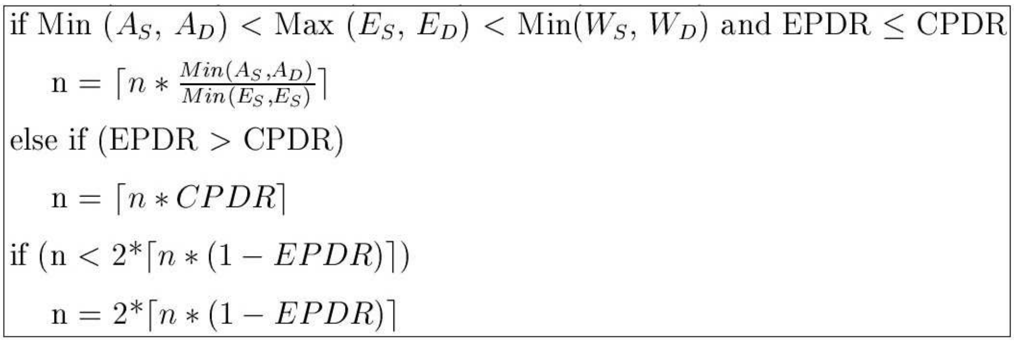
```
if $I_{SD} \leq$ Max ($E_S$, $E_D$) $\leq$ Min ($A_S$, $A_D$) and EPDR $\leq$ CPDR
    No attack has performed
else if Min ($A_S$, $A_D$) $<$ Max ($E_S$, $E_D$) $<$ Min ($W_S$, $W_D$) and EPDR $\leq$ CPDR
  if $AR_{WFB}$ = 0
   $AR_{WFJ}$ = $AR_{WFJ}$ + (1-$\alpha$) * $AR_{WHP}$
    if T $\geq$ $AR_{WFJ}$
      Wormhole attack followed by jellyfish attack is suspected
    if T $<$ $AR_{WFJ}$
      Wormhole attack followed by jellyfish attack is found
      Drop the path & Update $R_{SD}$
      S and D go for new path (which does not contain adversaries)
  if $AR_{WFB}$ $>$ 0
   $AR_{WFJ}$ = $AR_{WFJ}$ + (1-$\gamma$) * $AR_{WHP}$
    if T $\geq$ ($AR_{WFJ}$ + $AR_{WFB}$)
      Wormhole attack followed by jellyfish and byzantine attacks are
      suspected
    if T $<$ ($AR_{WFJ}$ + $AR_{WFB}$)
      Wormhole attack followed by jellyfish and byzantine attacks are
         found
      Drop the path & Update $R_{SD}$
      S and D go for new path (which does not contain adversaries)
else if EPDR $>$ CPDR
  if $AR_{WFJ}$ = 0
   $AR_{WFB}$ = $AR_{WFB}$ + (1-$\beta$)* $AR_{WHP}$
    if T $\geq$ $AR_{WFB}$
      Wormhole attack followed by byzantine attack is suspected
    if T $<$ $AR_{WFB}$
      Wormhole attack followed by byzantine attack is found
      Drop the path & Update $R_{SD}$
      S and D go for new path (which does not contain adversaries)
  if $AR_{WFJ}$ $>$ 0
   $AR_{WFB}$ = $AR_{WFB}$ + (1-$\gamma$)* $AR_{WHP}$
    if T $\geq$ ($AR_{WFB}$ + $AR_{WFJ}$)
      Wormhole attack followed by jellyfish and byzantine attacks
      are suspected
    if T $<$ ($AR_{WFB}$ + $AR_{WFJ}$)
      Wormhole attack followed by byzantine attack is found
      Drop the path & Update $R_{SD}$
      S and D go for new path (which does not contain adversaries)
```

re-initialized and this path is observed by RCIDS. Time required to select the new path is protocol dependent which is explained in section 6.2.2.



```
if Min $(A_S, A_D)$ < Max $(E_S, E_D)$ < Min$(W_S, W_D)$ and EPDR $\leq$ CPDR
    if (Max $(E_S, E_D) < Dl_{max}$)
        Min $(A_S, A_D)$ = Max$(E_S, E_D)$
    else
        Min $(A_S, A_D) = Dl_{max}$
else if ( EPDR > CPDR)
    Min$(A_S, A_D)$ = (2 - $\frac{received\,packets}{n}$) * Max $(E_S, E_D)$
    if (Max $(A_S, A_D) > Dl_{max}$)
        Min$(A_S, A_D) = Dl_{max}$
```

Figure 6.1: Updated Min (A_S, A_D) Value for Next Iteration



```
if Min $(A_S, A_D)$ < Max $(E_S, E_D)$ < Min$(W_S, W_D)$ and EPDR $\leq$ CPDR
    n = $\lceil n * \frac{Min(A_S,A_D)}{Min(E_S,E_S)} \rceil$
else if (EPDR > CPDR)
    n = $\lceil n * CPDR \rceil$
if (n < 2*$\lceil n * (1 - EPDR) \rceil$)
    n = 2*$\lceil n * (1 - EPDR) \rceil$
```

Figure 6.2: Updated the Number of Packets (n) Value for Next Iteration

Cross-layer Intrusion Detection System considers network layer and MAC layer parameters to monitor the wormhole path behaviour and assigns affected reputation to wormhole paths to improve the detection accuracy. In this approach, source and destination nodes tolerate the packet drop or delay until the affected reputation value reaches to the threshold value set by these nodes.

6.1.4 Study of RCIDS in Hostile Backbone Mesh

We exemplify the RCIDS in the context of AOMDV routing protocol. Each route discovery of AOMDV routing protocol finds multiple paths between source and destination. These multiple paths are either node disjoint or link disjoint. RCIDS considerers node disjoint paths because source and destination can easily select an alternative path when a present path is detected as wormhole malicious path. Source and destination nodes need intermediate nodes IDs of each path and their locations which are not included in AOMDV. In order to provide this information at source and destination, we add two fields to AOMDV such as location and inter_nodelist to the route request (RREQ) and route reply (RREP) packets.

The proposed approach is described using the scenario as shown in Figure 6.3. The wormhole nodes (*M1*, *M2*, *M3*, *M4*, *M5*) are communicating through long-distance wireless links. Initially, Source (S) and Destination (D) nodes affected reputation values AR_{WFJ} and AR_{WFB} values are set zero, and R_{SD} is empty.

In path initialization phase, node S broadcasts route request (RREQ) packet to find the route to node D at 0.0s. Intermediate nodes rebroadcast this RREQ packet until it reaches to D. Node D receives RREQ packets from *M2*, *M5* and R4 at 0.3s, 0.5s and .75s. Node D generates route reply (RREP) packet to S and this packet is forwarded through *M2*, *M5* and R4. Each RREP packet includes arrival time of RREQ packet at node D. These RREP packets are received by S in the reverse paths. Based on number of hops on each received RREP packet and distance (D_{SD}), S checks whether RREQ packet passed through wormhole path or not. Now, S selects 3-hop wormhole path (S, *M1*, *M2*, D) to forward the data and set ideal end-to-end packet delay (I_{SD}) as 0.3s of this path. Wormhole nodes (*M1*, *M2*) per packet expected waiting time in queue (0.06s, 0.06s) and blocking probabilities (0.03, 0.03) are signed by corresponding Gw and these values send to nodes S and D. Each Gw broadcasts per-hop collision probability PCP as 0.01. Based on these values S and D calculate Dl_{max} as 0.42, and EPDR as 0.91. These nodes set T value as 5, AR_{WHP} value as 1. S sends 10 test packets size of 500bytes to D.

Based on EPDR, D calculates expected receiving packets from S as 9. After D receives 9 test packets in 3.6s then it calculates A_D as .4s which is less than 0.42 of Dl_{max}. Thus, node D sends A_D value to S by using reply packet. This packet delay as .38s at node S. Now S calculates A_S as ((3.6 + .38) / 10) = .398s. Nodes S and D calculate W_S as .597s, W_D as .6s. Once path initialization process is over then S and D

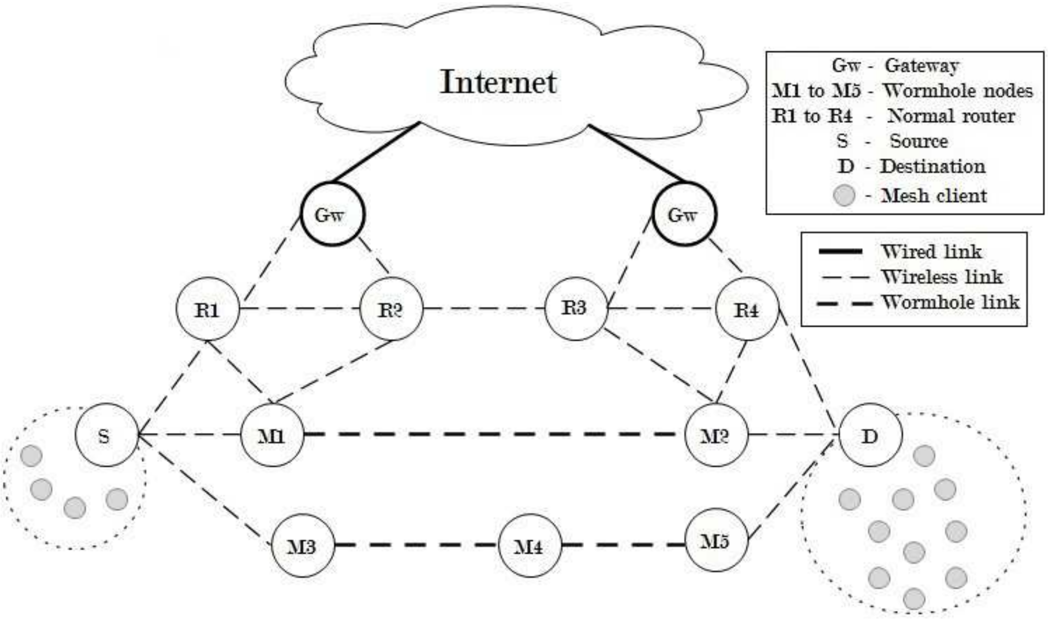


Figure 6.3: Example Scenario of Wormhole Paths

find minimum of (A_S, A_D) as .398s and (W_S, W_D) as .597s. In path observation phase, D will wait for 5.97s to receive 9 data packet and also calculates current PDR.

Case 1: RCIDS on Jellyfish attack

If D receives 9 data packets in 5.5s and the CPDR is greater than or equal to 0.91 then it calculates E_D as .55s. This value is sent to S by using reply packet. This packet delay is .38s at node S. Now S calculates E_S as ((5.5 + .38) / 11) = .534s. Nodes S and D consider maximum of (E_S, E_D) which is .55s. Here, wormhole nodes *M1* and *M2* are suspected to WFJ attack because wormhole path maximum of (E_S, E_D) is between minimum of (A_S, A_D) and (W_S, W_D). Thus, AR_{WFJ} value becomes 0.545 (AR_{WFJ} + (1-α)* AR_{WHP}). Nodes S and D update their minimum of (A_S, A_D) as 0.42, (W_S, W_D) as 0.63 and 'n' as 8 for next iteration. For each WFJ attack is suspected on wormhole path the corresponding AR_{WFJ} value is updated. Data packets are continued to flow in the same path, if updated AR_{WFJ} value is between 1 and 5. If this value is more than 5 then wormhole nodes *M1* and *M2* on wormhole path are detected as WFJ attackers.

Case 2: RCIDS on Byzantine Attack

If D receives 6 data packets in 5.97s and the EPDR (0.91) is greater than the CPDR (0.6), then wormhole nodes *M1* and *M2* are suspected to perform wormhole attack followed by byzantine attack. The affected reputation AR_{WFB} value becomes 0.75 (AR_{WFB} + (1-β)* AR_{WHP}). Nodes S and D update their minimum of (A_S, A_D) as 0.42, (W_S, W_D) as 0.63 and 'n' as 6 for next iteration. For each WFB attack is suspected on wormhole path the corresponding AR_{WFB} value is updated. Data packets are continued to flow in the same path, if updated AR_{WFB} value is between 1 and 5. If this value is more than 5 then wormhole nodes *M1* and *M2* on wormhole path are detected as WFB attackers.

Case 3: RCIDS on Jellyfish and Byzantine Attacks

If the wormhole nodes *M1* and *M2* are suspected as performing wormhole attack followed by jellyfish or byzantine attack, RCIDS checks current AR_{WFJ}, AR_{WFB} value. If both the current AR_{WFJ} and AR_{WFB} values are greater than zero then affected reputation (1-γ)* AR_{WHP} value is added to either AR_{WFJ} or AR_{WFB} value. When WFJB attacks are suspected on wormhole path the corresponding AR_{WFJ} or AR_{WFB} value is updated. Data packets continue to flow in the same path, if the updated AR_{WFJ} or AR_{WFB} value between 1 and 5. If one of the updated value is more than 5 then wormhole nodes *M1* and *M2* on wormhole path are detected as WFJB attackers.

In all above three cases, when a path is detected as a wormhole malicious path, S and D drop the current path immediately and update their revocation lists R_{SD} by adding *M1* and *M2*. Then node S selects the next best path from the list of node disjoint paths.

6.2 Performance Analysis

6.2.1 Binomial Probability Model

We have developed a binomial probability model to study the detection and false alarm probabilities of Single-layer IDS, Cross-layer IDS, and RCIDS. In this model, each IDS detects N wormhole malicious paths in order to detect a wormhole malicious path which is independent of each other. The probability of each detected path as a malicious path is (P) and non-malicious path is (1-P).

The probability of number of correctly identified malicious paths 'k' in N number of detected malicious paths is calculated as below:

$$P_S(N,k,P) = \binom{N}{k} P^k (1-P)^{N-k} \tag{6.1}$$

The probability of number of wrongly identified malicious paths 'k' in N number of detected malicious paths is calculated as below:

$$P_F(N,k,P) = \binom{N}{k} (1-P)^k (P)^{N-k} \tag{6.2}$$

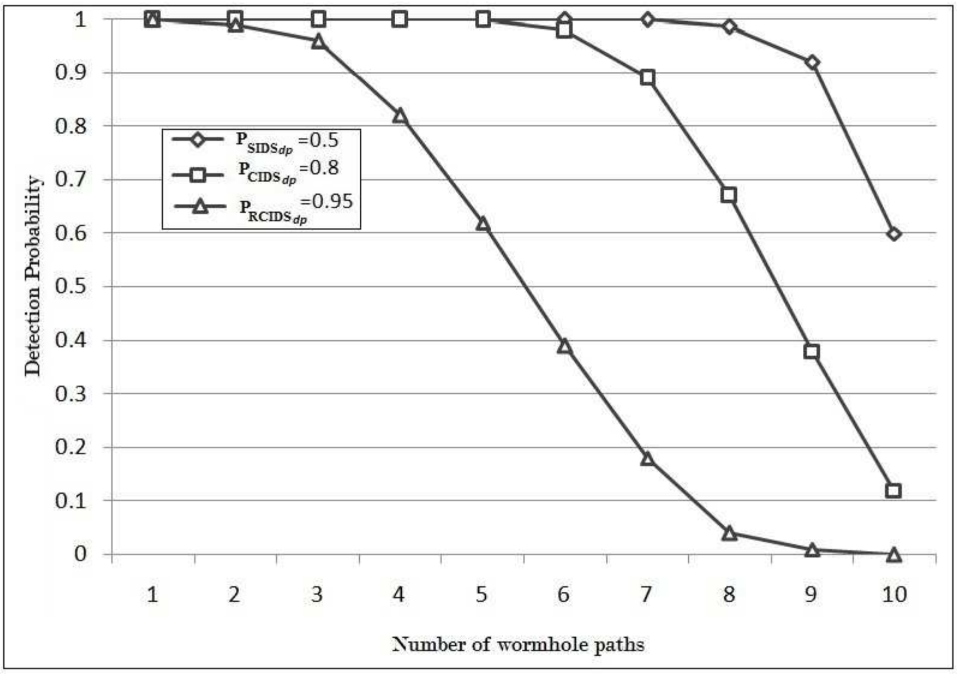


Figure 6.4: Detection Probability of Three Approaches

The selected source and destination find the detection probability using SIDS is $P_{SIDS_{dp}}$ for each 't' number of wormhole attack paths as given in equation 6.3 where t value additively increases from 1 to N, where 'P' is the probability of detected wormhole paths affected by wormhole attacks. SIDS does not consider behaviour of the node,

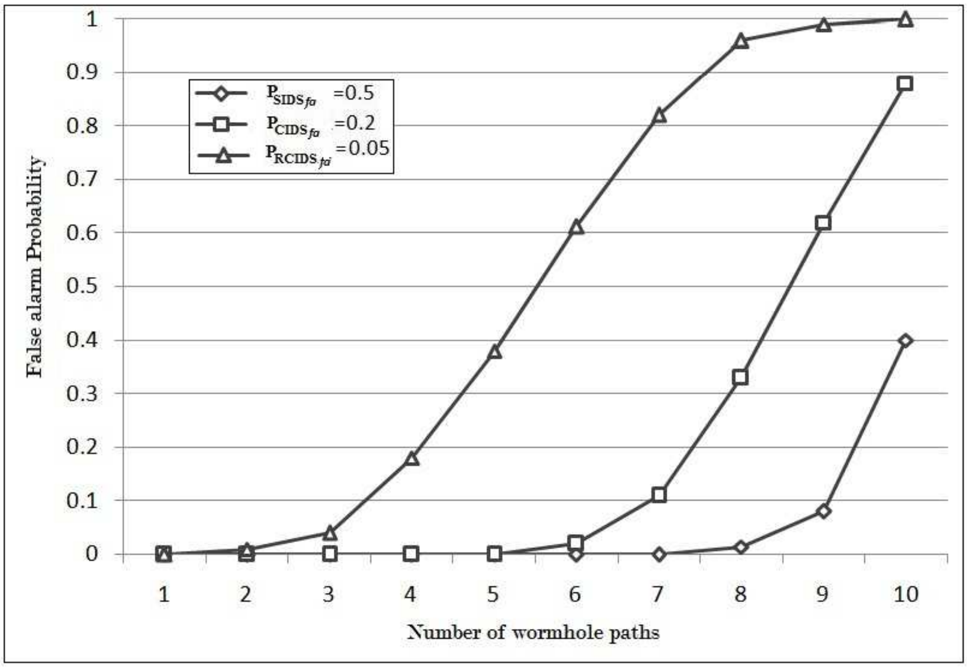


Figure 6.5: False Alarm Probability of Three Approaches

instead it considers only predefined distance or RTT value to define the wormhole attacks. Thus, probability (P) of a detected path has 50 percent chances to become a malicious path and thus increases the false alarm detection. SIDS false alarm probability ($P_{SIDS_{fa}}$) is given in equation 6.4 which is inversely proportional to $P_{SIDS_{dp}}$.

$$P_{SIDS_{dp}} = \sum_{K=t}^{N} \binom{N}{k} (P)^k (1-P)^{N-k} \tag{6.3}$$

$$P_{SIDS_{fa}} = \sum_{K=t}^{N} \binom{N}{k} (1-P)^k (P)^{N-k} \tag{6.4}$$

Since Cross-layer IDS (CIDS) supports both the path metrics and path behaviour to improve the detection performance, the probability of detected wormhole paths affected by wormhole attacks which is 1-(P_C + P_D), where P_C is the probability of number of wormhole paths CPDR value less than EPDR value and P_D is the probability of number of wormhole paths $Max(E_S, E_D)$ value greater than Min(A_S, A_D) value. P_C and P_D values are existed when more $W_{q_{ij}}$, $P_{B_{ij}}$ and PCP have occurred on wormhole paths than what source and destination were expected. Detection probability of Cross-layer IDS ($P_{CIDS_{dp}}$) is given in equation 6.5. $P_{CIDS_{dp}}$ value decreases as P_C and P_D values increase in the network. The false alarm probability of Cross-layer IDS ($P_{CIDS_{fa}}$) is inversely proportional to $P_{CIDS_{dp}}$ which is given in equation 6.6. In behavior based SIDS the P_C and P_D values are more than CIDS, this is because SIDS considers all packet drops and packet delays (i.e do not exclude affects of $W_{q_{ij}}$, $P_{B_{ij}}$ and PCP of different layers) due to malicious behaviour. As a result, SIDS detection probability is less than CIDS and false alarm probability is more than CIDS.

$$P_{CIDS_{dp}} = \sum_{K=t}^{N} \binom{N}{k} (1 - (P_C + P_D))^k (P_C + P_D)^{N-k} \tag{6.5}$$

$$P_{CIDS_{fa}} = \sum_{K=t}^{N} \binom{N}{k} (P_C + P_D)^k (1 - (P_C + P_D))^{N-k} \tag{6.6}$$

Reputation based cross-layer IDS (RCIDS) considers the threshold (T) value to improve the CIDS detection probability and reduce the false alarm probability. In RCIDS, the probability of detected wormhole paths affected by wormhole attacks, which is (1-(P_C + P_D)/T), where T is threshold value which is set by source and destination. Each time suspected wormhole path affected reputation increases based on severity, this value increases until it reaches to T. Detection probability of reputation based cross-layer intrusion detection system $P_{RCIDS_{dp}}$ is given in equation 6.7. In worst-case, RCIDS acts as CIDS when source and destination nodes do not allow if wormhole path is suspected once. False alarm probability of reputation based cross-layer intrusion detection system ($P_{RCIDS_{fa}}$) is inversely proportional to the detection probability of ($P_{RCIDS_{dp}}$) and is given in equation 6.8. All above three IDSs detection and false alarm probabilities are shown in Figure 6.4 and 6.5.

$$P_{RCIDS_{dp}} = \sum_{K=t}^{N} \binom{N}{k} (1 - (P_C + P_D)/T)^k ((P_C + P_D)/T)^{N-k} \tag{6.7}$$

$$P_{RCIDS_{fa}} = \sum_{K=t}^{N} \binom{N}{k} ((P_C + P_D)/T)^k (1 - (P_C + P_D)/T)^{N-k} \tag{6.8}$$

6.2.2 Simulation Results

The performance of RCIDS is observed in steady-state traffic and unsteady-state traffic on wormhole paths. Steady-state traffic is considered to define how the RCIDS isolates wormhole malicious paths from backbone mesh and improves the network performance such as goodput and packet delivery ratio using wormhole non-malicious paths. Unsteady-state traffic is considered to study the RCIDS detection probabilities of wormhole malicious paths and false alarm probabilities of wormhole non-malicious paths. Initially all wormhole paths R_{SD} are empty, EPDR, CPDR, Dl_{max} as 0, r_{min} as 150m and min(W_S, W_D) is calculated for 40 packets. Affected reputation of wormhole paths (AR_{WHP}) as 2 and A_{WFJ}, A_{WFB} as 0. In backbone mesh, $W_{q_{ij}}$, $P_{B_{ij}}$ and PCP values are updated in every 3. Mesh routers (R/As) restrict the maximum transmission range (R_{max}) between two mesh clients as 150m to isolate the wormhole attacks in multi-hop client mesh network. We describe all the simulation parameters in section 6.1.2.

6.2.2.1 Validation of RCIDS in Steady-state Traffic

To maintain steady-state traffic in backbone mesh, each node S sets interval between sending of any two packets from 0.02s and this value is stable for all wormhole paths. Since, all wormhole paths have steady-state traffic, Dl_{max} and EPDR values of each wormhole path are also stable. In Steady-state traffic, RCIDS is tested on AODV (single-path) and AOMDV (multi-path) routing protocols. Backbone mesh consists of 14 wormhole nodes out of which 12 wormhole nodes act as malicious nodes by forming three different wormhole malicious paths ($WMP_{1,\,2\,\&\,3}$) (2-node, 4-node & 6-node) and two nodes act as non-malicious by forming 2-node wormhole non-malicious path (WP_1). In the path initialization phase, four node-disjoint wormhole paths (WP_1, $WMP_{1,\,2\,\&\,3}$) are formed between all five sets of Source(S) and Destination(D) nodes. We conduct our experiments with packet size of 1000bytes for 400s. Each node S changes the path after every 100s such as 0-100s WP_1, 100-200s WMP1, 200-300s WMP2 and 300-400s WMP3 to send data traffic to corresponding node D. Each S and D set threshold value (T) as 5. All other network parameters are same as given in Table 5.1. The following results show that how the RCIDS protects backbone mesh against WFJ, WFB and WFJB attacks on wormhole paths in steady-state traffic:

Case 1: RCIDS on Jellyfish Attack

Wormhole Path delay is (D'). We have varied the delay between 2D' to 8D' to create jellyfish attack on other three wormhole malicious paths ($WMP_{1,\,2\,\&\,3}$). As a result, the percentage of affected goodput increases as number of attackers increases in the wormhole malicious path. In Figure 6.6, it is between 54-100% in WMP_1, 38-100% in WMP_2, and 29-100% in WMP_3. Since, goodput is not decreased by the delay, CPDR is more than or equal to EPDR and AR_{WFJ} value is less than T in WP_1, no false alarm has been trigged for the first 100s in AODV and AOMDV protocols. On the other hand, these protocols start detecting the wormhole malicious paths $WMP_{1,\,2\,\&\,3}$ at 122s, 216s and 312s because AR_{WFJ} value is more than T in all paths.

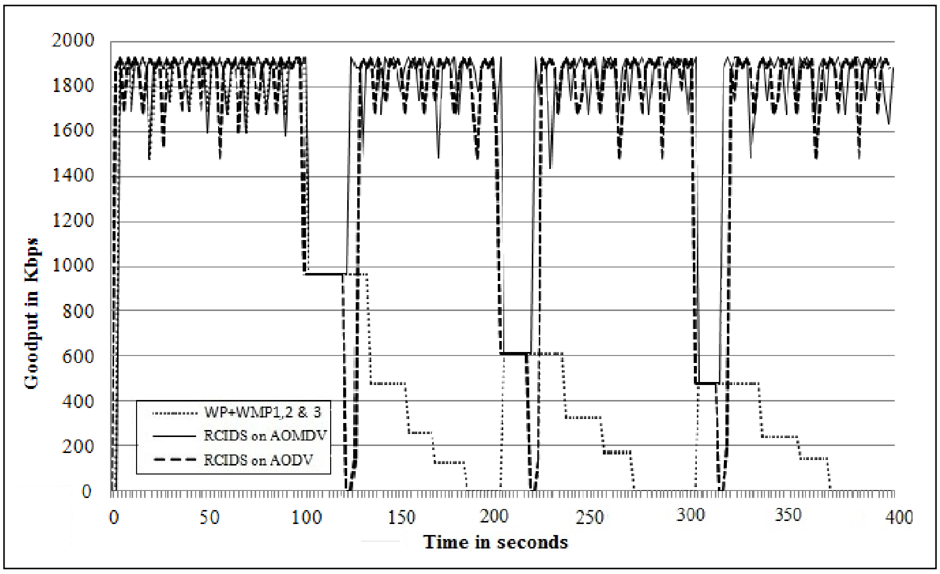


Figure 6.6: Goodput comparison (WFJ attack)

Case 2: RCIDS on Byzantine Attack

We disturb the network traffic by altering and dropping packets from 5% to 20% to create byzantine attack on three wormhole malicious paths ($WMP_{1,\,2\,\&\,3}$). As a result, the percentage of affected goodput increases as number of attackers increases in the wormhole malicious path. In Figure 6.7, it is between 24-100% in WMP_1, 19-100% in WMP_2, and 12-100% in WMP_3. Since, CPDR is more than EPDR and AR_{WFJ} value is less than T in WP_1, no false alarm has been trigged for first 100s in AODV and AOMDV protocols. On other hand, these protocols start detecting wormhole malicious

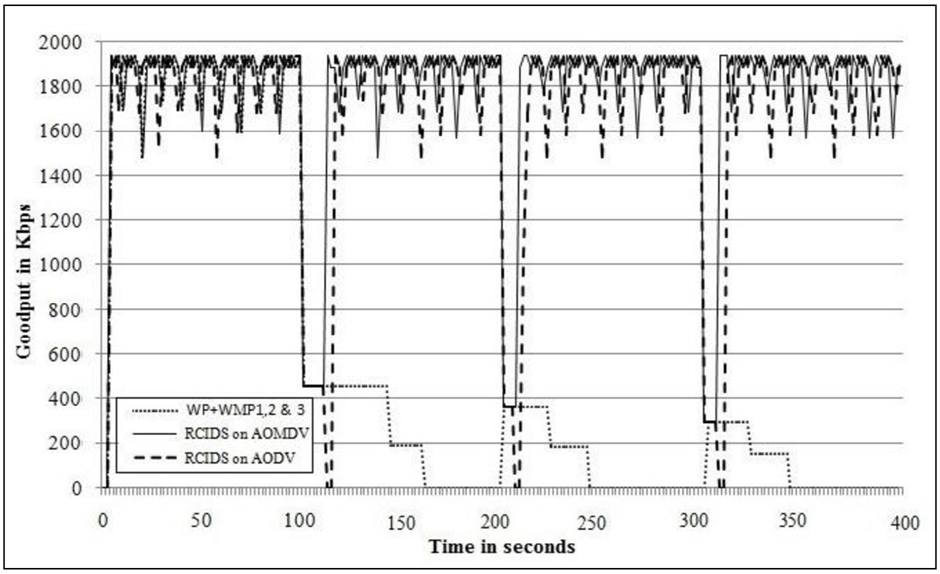


Figure 6.7: Goodput Comparison (WFB attack)

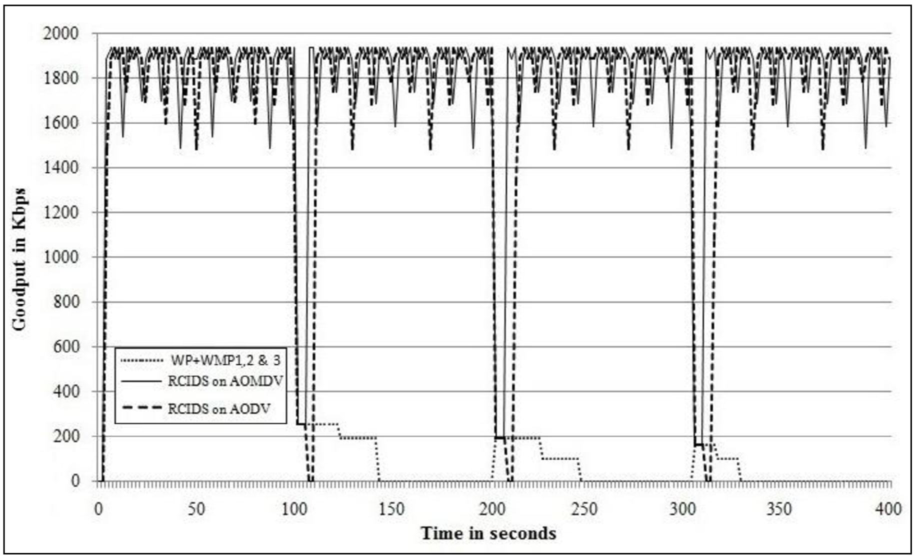


Figure 6.8: Goodput Comparison(WFJB attack)

paths $WMP_{1,\ 2\ \&\ 3}$ at 112s, 208s and 306s because AR_{WFB} value is more than T in all the paths.

Case 3: RCIDS on Jellyfish and Byzantine Attacks

We also perform both the attacks at the same time on $WMP_{1,\ 2\ \&\ 3}$. As a result, the percentage of affected goodput increases as number of attackers increases in the wormhole malicious path. In Figure 6.8 it is between 13-100% in WMP_1, 10-100% in WMP_2,

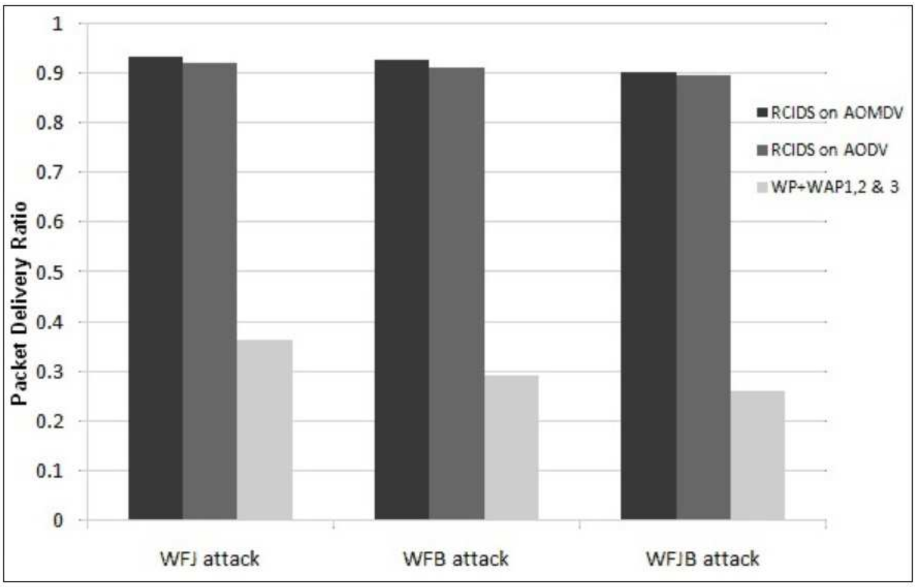


Figure 6.9: PDR Comparison of Wormhole Attacks

and 8-100% in WMP_3. In both the protocols, no false alarm has been trigged in WP_1. These protocols start detecting wormhole malicious paths $WMP_{1,\,2\,\&\,3}$ at 108s, 206s and 306s because sum of AR_{WFJ} and AR_{WFB} value is more than T in all the paths.

RCIDS detects wormhole attackers faster as their attacking severity increases in all the above cases which is shown Figure 6.6, 6.7 and 6.8. Each S and D drop the wormhole malicious paths, update their revocation list R_{SD} by adding attackers. After isolating each wormhole malicious path, AODV and AOMDV perform differently to select a new path. In AODV, each node S drops all cached data packets and initiates route request again. Upon receiving each route request, corresponding node D will check the R_{SD} list with intermediate nodes on the request packet. If the received request matches with R_{SD} then D drops the packet, otherwise forwards the route reply in reverse path (WP_1) to the corresponding node S. During this process, goodput is zero which is shown Figure 6.6, 6.7 and 6.8. In AOMDV, each node S selects immediately the best path (WP_1) from the stored data to send remaining data packets. Hence,the goodput of the path remains high as shown in Figure 6.6, 6.7 and 6.8. We observe the similar performance in packet delivery ratio which is shown in Figure 6.9.

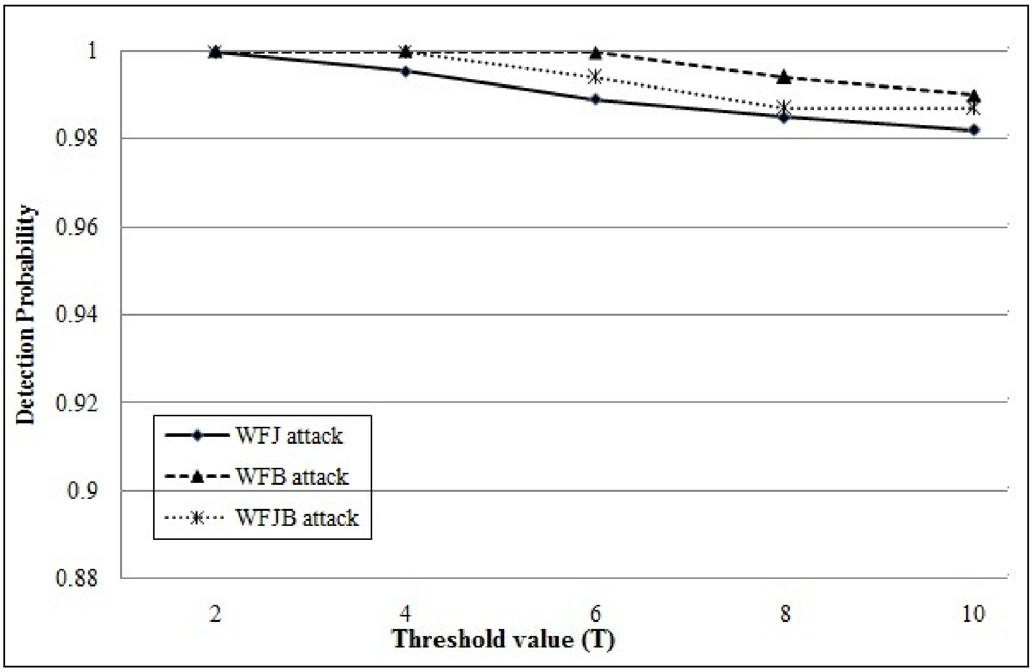
In steady-state traffic, Reputation based Cross-layer IDS (RCIDS) has shown a clear distinction of all three wormhole attacks in the detection process. As a result, RCIDS isolates all the wormhole malicious paths and no false alarm raises in wormhole non-malicious path.

6.2.2.2 Validation of RCIDS in Unsteady-state Traffic

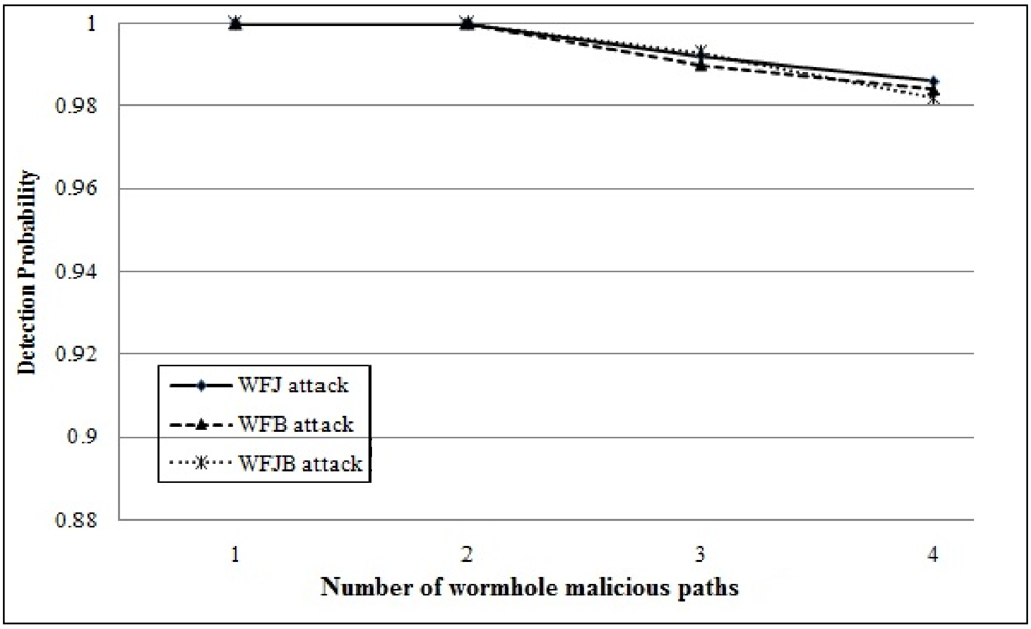
To create unsteady-state traffic in backbone mesh, each node S varies interval between sending of any two packets is 0.02s to 0.002s. Here, unsteady-state traffic can be varied ten times of steady-state traffic on the wormhole paths. Since, all wormhole paths have unsteady-state traffic, Dl_{max} and EPDR values of each wormhole path are unstable. If the increase or decrease of these values on wormhole paths are not updated by corresponding S and D then there is a possibility of misdetection and false alarm on wormhole paths. To improve the detection and decrease the false alarm probabilities, RCIDS considers Threshold (T) value which is maintained by each set of S and D to find the wormhole malicious paths. The following results show that the detection and false alarm probabilities of RCIDS in unsteady-state traffic.

In Figure 6.10(a) and Figure 6.11(a), we observe the wormhole malicious paths detection and false alarm probabilities with respect to wormhole attacks by varying T value from 2 to 10, at simulation time of 1000s. In unsteady-state traffic, RCIDS is tested on AOMDV (multi-path) routing protocol. We consider all four wormhole paths act as wormhole malicious paths, to find the detection probabilities of WFJ, WFB and WFJB attacks on these paths. To create WFJ attack on each wormhole malicious path, we have varied the path delay between Dl_{max} to 1.5*Dl_{max} and to create WFB attack on each wormhole malicious path, we have disturbed the network traffic by altering and dropping packets from 1% to 20%. We have performed both WFJ and WFB attacks on wormhole malicious paths simultaneously to create WFJB attacks. To detect the wormhole attacks on wormhole malicious paths, each S and D initially considers 40 packets to observe the wormhole path. This value is decreased by S and D, when any one of the attack is suspected on wormhole malicious paths. Thus, even T value increases from 2 to 10 at S and D, the detection probabilities of wormhole attacks on wormhole malicious paths slightly decrease from 1 to 0.982 which is shown in Figure 6.10(a).

We consider all four wormhole paths act as wormhole non-malicious paths, to find



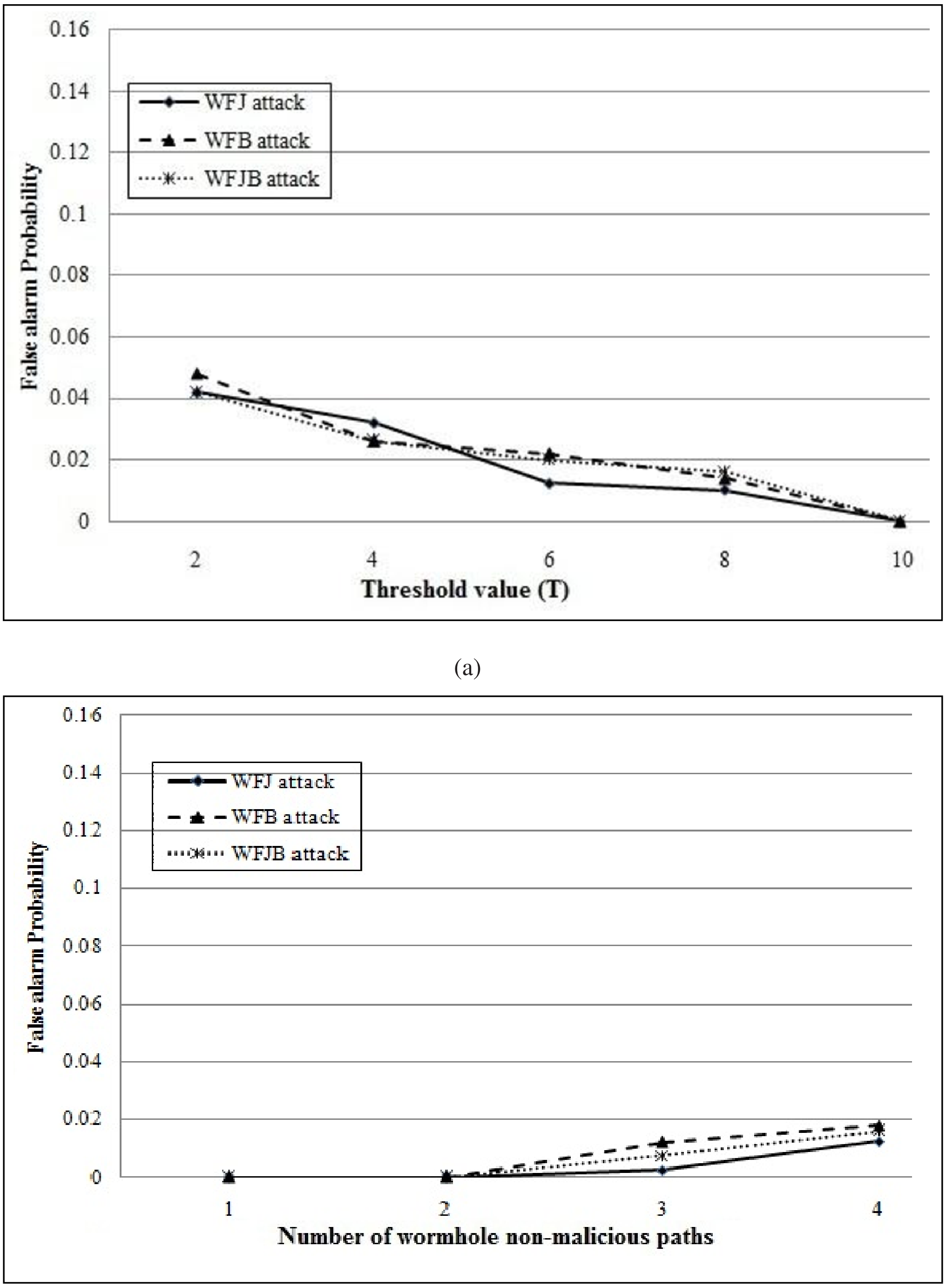
(a)



(b)

Figure 6.10: Wormhole Malicious Paths Detection Probability

the false alarm probabilities of WFJ, WFB and WFJB attacks on these paths. Figure 6.11(a) shows that false alarm probabilities of wormhole attacks on wormhole non-malicious paths decrease from 0.05 to 0 as T value increases from 2 to 10. From Figure 6.10(a) and Figure 6.11(a), the wormhole attacks on wormhole malicious paths



(a)

(b)

Figure 6.11: Wormhole Non-malicious Paths False Alarm Probability

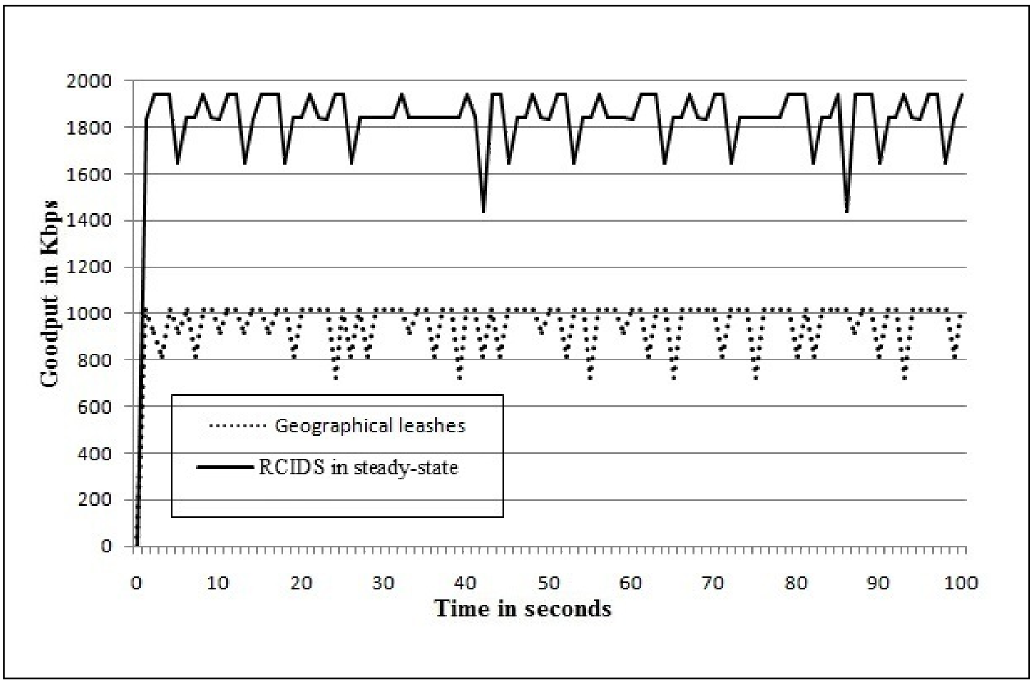
detection probability is insensitive to the change of T, while the wormhole attacks on wormhole non-malicious paths false alarm probability increase as the decrease of threshold value. The reason is that each set of S and D tolerates any wormhole path until the path affected reputation reaches to T. However, when T becomes too large, the detection probabilities of wormhole attacks on wormhole malicious paths decrease. As observed good tradeoff between Figure 6.10(a) and Figure 6.11(a), is achieved when T is 5. In unsteady-state, we fix the T as 5 and observe the detection and false alarm probabilities with respect to number of wormhole paths which are shown in Figure 6.10(b) and Figure 6.11(b).

6.2.2.3 Comparison Study

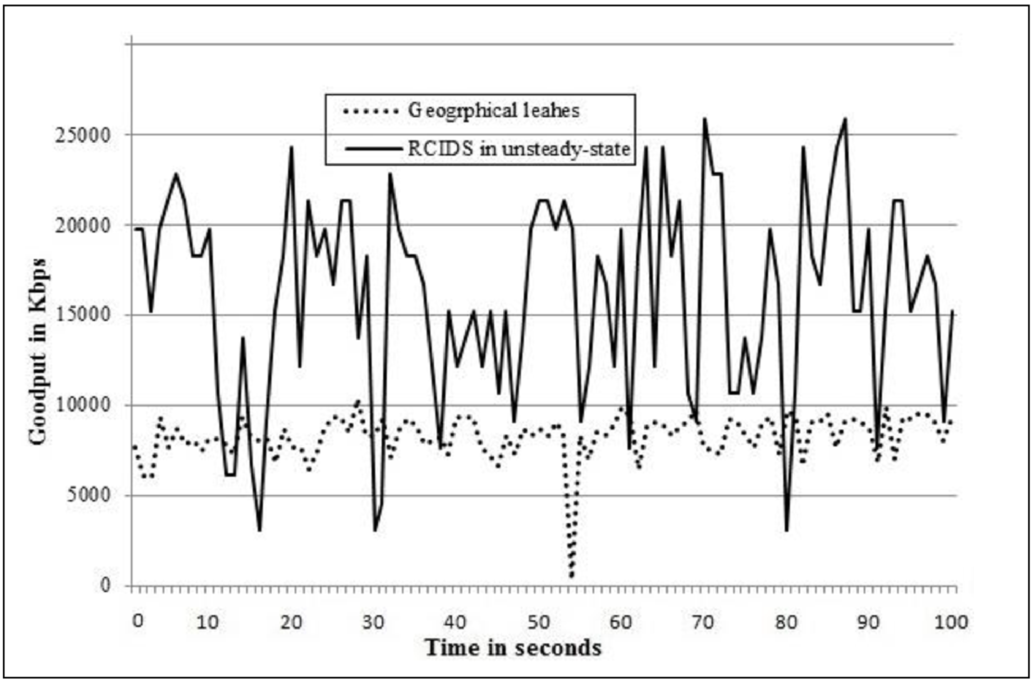
We have compared the performance of RCIDS and geographical leashes on AOMDV protocol. Since geographical leashes approach [Hu et al., 2003] is not allowing wormhole nodes (even if they are non-malicious), it requires more number of intermediate nodes (8 nodes) to forward the data from each S to D. More number of nodes in a path incurs large delay and more number of drops due to collisions. Hence, goodput decreases as number of nodes increase in the communication. The goodput of geographical leashes is shown in Figure 6.12(a) and Figure 6.12(b). RCIDS overcomes this drawback by allowing wormhole non-malicious paths in the communication of each S and D. From Figure 6.12(a), the average goodput of RCIDS is 1854 Kbps, which is more than 50% of average goodput of geographical leashes which is 913 Kbps in steady-state traffic. From Figure 6.12(b), the average goodput of RCIDS is 10570 Kbps, which is more than 50% of average goodput of geographical leashes which is 4873 Kbps in unsteady-state traffic. The average goodput of geographical leashes further gets reduced as number of intermediate nodes are increased in communication path. Based on Figure 6.12(a) and Figure 6.12(b), our proposed approach greatly improves the network performance because it uses wormhole non-malicious paths for long-distance wireless communications.

6.2.2.4 Cost Analysis

In this section, we analyse the RCIDS approach with respect to storage and communication overheads. In RCIDS, only mesh routers(R/As) maintain path behaviour parameters T, AR_{WHP}, AR_{WFJ}, AR_{WFB}, I_{SD}, Min (A_S, A_D) , Min (W_S, W_D), EPDR, AR_{PS}, Dl_{max}, r_{min} each of 4-bytes. Each R/A requires only 44 bytes of memory space



(a)



(b)

Figure 6.12: Performance Evaluation of RCIDS and Geographical Leashes

for all path behaviour parameters in case of single path routing protocols since each source R/A has one path to destination R/A. However, it varies for multi-path routing protocols because each source R/A has multiple paths (N) to destination R/A. Hence, each R/A requires N*44-bytes for multi-path routing protocols. For example, a source R/A maintains 10 multiple paths for a destination R/A, they only need 440-bytes which is less than 4Kb.

In path behaviour phase, destination R/A sends one reply message for every minimum of (W_S, W_D) time. Hence, RCIDS needs $\frac{path\ observation\ time}{W\ time}$ additional communication messages. Path behaviour phase communication overhead is same for single-path and multi-path routing protocols. In path isolation phase, R/A drops the current path and selects a new path in case of single-path routing protocols and selects a new path from a list of paths in multi-path routing protocols. In single-path routing protocol, source R/A re-initiates the route, so it will generate minimum 2*n number of packets where n is the number of nodes in the network. The communication overhead for t number of wormhole paths isolation is minimum of t*(2*n) for single-path routing protocols and minimum of 2*n for multi-path routing protocols.

6.3 Summary

In this chapter, the proposed dynamic reputation based cross-layer intrusion detection system ensures the complete utilization of these links in backbone mesh by isolating the wormhole attacks. It uses the affected reputation to punish the suspected wormhole paths based on behaviour of cross-layer parameters. It also exploits reputation and cross-layer parameters to increase the detection probability and reduce the false alarm probability. The analysis of RCIDS, CIDS and SIDS is performed by using binomial probability model in backbone mesh. Based on the analysis, RCIDS outperforms CIDS and SIDS in steady-state and unsteady-state traffic. On the other hand, edge router (R/A) in RCIDS sets maximum transmission range between two nodes to isolate the wormhole attacks in client mesh. Simulation study is conducted by considering the behaviour based cross layer parameters and maximum transmission range parameter in ns2 network simulator. Simulation results have confirmed that the RCIDS has protected the HWMNs from wormhole attacks.

Chapter 7

CONCLUSIONS AND FUTURE SCOPE

In this thesis, we have developed the multi-layer security framework to address the security issues of the network layer and MAC layer attacks from both backbone mesh and client mesh. Our framework combines a multi-level key management mechanism and a dynamic reputation-based cross-layer intrusion detection system to provide secure communication among mesh routers and mesh clients.

Multi-level key management mechanism consists of the distributed authentication scheme and enhanced centralized authentication scheme. Distributed authentication scheme is used to authenticate and de-authenticate the mesh routers. In this scheme, the cooperative behavior of gateways and mesh routers mitigates the severity of the internal attackers and robust cryptography functionalities isolate the external attackers. Our analysis and simulation results show that distributed authentication scheme has higher message reachability than existing the DSA-mesh and mobisec authentication schemes in hostile network traffic. Enhanced centralized authentication scheme uses lightweight encryption to the secure the 802.11i four-way handshake protocol which is used in Wi-Fi and multi-hop (802.11s) client networks. The security analysis and simulation results show that lightweight encryption on 802.11i four-way handshake protocol prevents blocking and flooding attacks. In MKMM, authentication keys of mesh nodes effectively isolate various MAC layer attacks and use these keys to authenticate and encrypt the network layer packets. The process of authentication and encryption of network layer packets provides some security against internal attackers. However, internal attackers can still perform severe wormhole attacks on those packets.

RCIDS uses the predefined maximum transmission range between two communicating nodes to isolate wormhole attacks in client mesh networks. On the other hand, RCIDS uses affected reputation and cross-layer parameters to effectively detect and isolate the wormhole attacks in backbone mesh. Cross-layer parameters such as number of packet collisions, number of packet drops and delays on wormhole path are used to find the behavior of the wormhole paths. For fast detection of wormhole attackers, affected reputation values are changed with respect to the type of attack and its severity on the wormhole malicious path. In addition, the number of monitoring packets on wormhole malicious paths is dynamically reduced by monitoring nodes. Our analysis and experimental results show that the proposed system increases the detection rate and decreases the false alarm rate in hybrid wireless mesh networks.

Future Scope

The research work presented in this thesis provides a foundation to explore several research avenues in the area of HWMNs security. We summarize several research directions, in which our work can be pursued.

- Dynamic channel assignment algorithms are more vulnerable due to the mesh node independent decision making and non-verification of the mesh node decision. The proposed distributed authentication scheme effectively isolate various internal and external colluding attacks in backbone mesh. This scheme can be further enhanced by securing dynamic channel assignment algorithms in backbone mesh network.

- Client mesh network security can be further enhanced by addressing the security issues of edge routers while integrating with other wireless networks such as sensor networks, ad-hoc networks and cellular networks.

- The proposed reputation based cross-layer intrusion detection systems performance can be further studied by considering physical layer performance, such as bit error rate and signal to noise ratio for detecting wormhole attacks. The reputation based cross-layer intrusion detection systems needs to be implemented for other internal/ external attacks such as sybil and rushing attacks.

- Gateways and edge routers may perform mesh node hijacking attacks in HWMNs. The proposed multi-level key management mechanism can be further improved by considering misbehavior (mesh node hijacking) detection of compromised gateways in backbone mesh and edge routers in client mesh.

Appendix I

Wireless Mesh Networks (WMNs) :WMNs consist of two types of nodes: mesh routers and mesh clients. Other than the routing capability for gateway/repeater functions as in a conventional wireless router, a wireless mesh router contains additional routing functions to support mesh networking. To further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. Compared to a conventional wireless router, a wireless mesh router can achieve the same coverage with much lower transmission power through multihop communications. Optionally, the medium access control protocol in a mesh router is enhanced with a better scalability in a multihop mesh environment. Based on multihop communication wireless mesh networks are three types: Backbone wireless mesh networks, Client wireless mesh networks and Hybrid wireless mesh networks [Ud.S, 2009, Akyildiz.F, 2009].

Backbone Wireless Mesh Networks: Backbone WMN includes mesh routers that form an infrastructure for clients that connect to them. The WMN infrastructure/backbone can be built using various types of radio technology, in addition to the heavily used IEEE 802.11 technology. The mesh routers form a mesh of self configuring, self healing links among themselves. With gateway functionality, mesh routers can be connected to the Internet. This approach, also referred to as infrastructure meshing, provides backbone for conventional clients and enables the integration of WMNs with existing wireless networks, through gateway/bridge functionalities in mesh routers. Conventional clients with Ethernet interface can be connected to mesh routers via Ethernet links. For conventional clients with the same radio technologies as mesh routers, they can directly communicate with mesh routers [Ud.S, 2009, Akyildiz.F, 2009].

Client Wireless Mesh Networks: Client meshing provides peer-to-peer networks among client devices. In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end-user applications to customers. Hence, a mesh router is not required for this type of network. In Client WMNs, a packet destined to a node in the network hops through multiple nodes to reach the destination. Client WMNs are usually formed using one type of radio on devices. Moreover, the requirements on end-user devices is increased when compared to infrastructure meshing, since, in Client WMNs, the end users have to perform additional functions such as routing and self-configuration [Ud.S, 2009, Akyildiz.F, 2009].

Hybrid Wireless Mesh Networks: This architecture is the combination of infrastructure and client meshing. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet,Wi-Fi, WiMAX, cellular, and sensor networks, the routing capabilities of clients provide improved connectivity and coverage inside the WMN. The hybrid architecture will be the most applicable case in our opinion [Ud.S, 2009, Akyildiz.F, 2009].

Bibliography

[802.11i 2004 Amendment6, 2004] 802.11i 2004 Amendment6, I. (2004). Medium access control (mac) security enhancements. In *http://standards.ieee.org/getieee802/download/802.11i-2004.pdf*.

[Akyildiz et al., 2005] Akyildiz, I. F., Wang, X., and Wang, W. (2005). Wireless mesh networks: a survey. *Computer networks, Elsevier*, 47(4):445–487.

[Akyildiz.F, 2009] Akyildiz.F (2009). *Wireless Mesh Networks*. WILEY.

[Akyildiz.F et al., 2005] Akyildiz.F, Xudong.W, and Weilin.W (2005). Wireless mesh networks: a survey. *Computer Networks*, 47:445–487.

[Altunbasak and Owen, 2004] Altunbasak, H. and Owen, H. (2004). Alternative pairwise key exchange protocols for robust security networks (ieee 802.11 i) in wireless lans. In *SoutheastCon, 2004. Proceedings. IEEE*, pages 77–83.

[Awerbuch et al., 2002] Awerbuch, B., Holmer, D., Nita-Rotaru, C., and Rubens, H. (2002). An on-demand secure routing protocol resilient to byzantine failures. In *Proceedings of the 1st ACM workshop on Wireless security*, pages 21–30.

[Azer et al., 2009] Azer, M., El-Kassas, S., and El-Soudani, M. (2009). A full image of the wormhole attacks-towards introducing complex wormhole attacks in wireless ad hoc networks. *arXiv preprint arXiv:0906.1245*.

[Bahr, 2007] Bahr, M. (2007). Update on the hybrid wireless mesh protocol of ieee 802.11 s. In *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on*, pages 1–6.

[Baird.L and Bahn, 2007] Baird.L and Bahn (2007). Keyless jam resistance. In *In Proceedings of the IEEE Information Assurance and Security Workshop*, pages 143–150.

[Baras et al., 2007] Baras, J. S., Radosavac, S., Theodorakopoulos, G., Sterne, D., Budulas, P., and Gopaul, R. (2007). Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in olsr. In *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pages 1–7.

[Bettahar et al., 2002] Bettahar, H., Bouabdallah, A., and Challal, Y. (2002). Akmp: an adaptive key management protocol for secure multicast. In *Computer Communications and Networks, 2002. Proceedings. Eleventh International Conference, IEEE*, pages 190–195.

[Bettstetter, 2002] Bettstetter, C. (2002). On the minimum node degree and connectivity of a wireless multihop network. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, pages 80–91.

[Bing.W et al., 2006] Bing.W, Jianmin.C, Jie.W, and Mihaela.C (2006). *WIRELESS/MOBILE NETWORK SECURITY*.

[Bruno et al., 2005] Bruno, R., Conti, M., and Gregori, E. (2005). Mesh networks: commodity multihop ad hoc networks. *Communications Magazine, IEEE*, 43(3):123–131.

[Buchegger and Le Boudec, 2002] Buchegger, S. and Le Boudec, J.-Y. (2002). Performance analysis of the confidant protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*, MobiHoc '02, pages 226–236.

[Bunday, 1986] Bunday, B. D. (1986). *Basic queueing theory*, volume 522. Edward Arnold London.

[Cagalj et al., 2007] Cagalj, M., Capkun, S., and Hubaux, J.-P. (2007). Wormhole-based antijamming techniques in sensor networks. *Mobile Computing, IEEE Transactions*, 6(1):100–114.

[Callegari et al., 2005] Callegari, S., Rovatti, R., and Setti, G. (2005). Embeddable adc-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos. *Signal Processing, IEEE Transactions*, 53(2):793–805.

[Capdehourat et al., 2012] Capdehourat, G., Larroca, F., and Belzarena, P. (2012). Minimum queue length load-balancing in planned wireless mesh networks. In *Wireless Communication Systems (ISWCS), 2012 International Symposium, IEEE*, pages 781–785.

[Chakeres and Belding-Royer, 2004] Chakeres, I. D. and Belding-Royer, E. M. (2004). Aodv routing protocol implementation design. In *Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference, IEEE*, pages 698–703.

[Chiu and Lui, 2006] Chiu, H. S. and Lui, K.-S. (2006). Delphi: wormhole detection mechanism for ad hoc wireless networks. In *Wireless Pervasive Computing, 2006 1st International Symposium, IEEE*, pages 1–6.

[CHI.Y and RONG.J, 2007] CHI.Y and RONG.J (2007). Sa mac protocol for multi-channel multi-interface wireless mesh network using hybrid channel assignment scheme. 23:1041–1055.

[Dai and Xie, 2010] Dai, X. and Xie, X. (2010). Analysis and research of security mechanism in ieee 802.16 j. In *Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference, IEEE*, pages 33–36.

[De Rango et al., 2006] De Rango, F., Lentini, D. C., and Marano, S. (2006). Static and dynamic 4-way handshake solutions to avoid denial of service attack in wi-fi protected access and ieee 802.11 i. *EURASIP Journal on Wireless Communications and Networking*, 2006(2):1–19.

[Deng and Long, 2004] Deng, F.-G. and Long, G. L. (2004). Secure direct communication with a quantum one-time pad. *Physical Review APS*, 69(5):519–23.

[Ding.Q and Jiang.M, 2009] Ding.Q and Jiang.M (2009). Repro:a reputation-based proactive routing protocol for the wireless mesh backbone. In *IEEE Fifth International Joint conference on INC, IMS and IDC*, pages 516–521.

[Dix, 2009] Dix, A. (2009). *Human-computer interaction*.

[Dong et al., 2011] Dong, D., Li, M., Liu, Y., Li, X.-Y., and Liao, X. (2011). Topological detection on wormholes in wireless ad hoc and sensor networks. *IEEE/ACM Transactions on Networking (TON)*, 19(6):1787–1796.

[Dong et al., 2009] Dong, J., Ackermann, K., and Nita-Rotaru, C. (2009). Secure group communication in wireless mesh networks. *Ad Hoc Networks, Elsevier*, 7(8):1563–1576.

[Doraswamy and Harkins, 2003] Doraswamy, N. and Harkins, D. (2003). *IPSec: the new security standard for the Internet, intranets, and virtual private networks*. Prentice Hall Professional.

[Ertaul.L and Ibrahim.D, 2009] Ertaul.L and Ibrahim.D (2009). Evaluation of secure routing protocols in mobile ad hoc netowks(manets). In *In Proceedings of Security and Management*, pages 663–639.

[Fragkiadakis.G et al., 2010] Fragkiadakis.G, Vasilios.A, and Nikolaos.P (2010). Anomaly-based intrusion detection algorithms for wireless networks. In *WWIC 2010,springer*.

[Franscesco.O and Simon.P, 2008] Franscesco.O and Simon.P (2008). A reputation-based metric for secure routing in wireless mesh networks. In *Global Telecommunications Conference, 2008. IEEE GLOBECOM*, pages 1–5.

[Gerkis.A, 2006] Gerkis.A (2006). A survey of wireless mesh networking security technology and threats. In *OTM workshops*, pages 1–17.

[Gharavi and Hu, 2013] Gharavi, H. and Hu, B. (2013). Dynamic key refreshment for smart grid mesh network security. In *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, pages 1–6.

[Glass et al., 2009] Glass, S. M., Muthukkumarasamy, V., and Portmann, M. (2009). Detecting man-in-the-middle and wormhole attacks in wireless mesh networks. *Advanced Information Networking and Applications, International Conference on*, 0:530–538.

[Gupta and Shroff, 2009] Gupta, G. R. and Shroff, N. (2009). Delay analysis for multi-hop wireless networks. In *INFOCOM 2009, IEEE*, pages 2356–2364.

[Han and Poor, 2009] Han, Z. and Poor, H. V. (2009). Coalition games with cooperative transmission: a cure for the curse of boundary nodes in selfish packet-forwarding wireless networks. *Communications, IEEE Transactions*, 57(1):203–213.

[Hao.Y and James.S, 2006] Hao.Y and James.S (2006). Scan:self-organized network-layer security in mobile ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, vol.24:261–273.

[Haq.A and Naveed.A, 2007] Haq.A and Naveed.A (2007). Securing channel assignment in multi-radio multi-channel wireless mesh networks. In *Wireless Communications and Networking Conference, IEEE.*

[Hayajneh et al., 2009] Hayajneh, T., Krishnamurthy, P., and Tipper, D. (2009). Deworm: a simple protocol to detect wormhole attacks in wireless ad hoc networks. In *Network and System Security, 2009. NSS'09. Third International Conference on*, pages 73–80.

[He and Mitchell, 2004] He, C. and Mitchell, J. C. (2004). Analysis of the 802.11 i 4-way handshake. In *Proceedings of the 3rd ACM workshop on Wireless security*, pages 43–50.

[Hoang.L and Uyen.T, 2003] Hoang.L and Uyen.T (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2):32–46.

[Hu et al., 2003] Hu, Y.-C., Perrig, A., and Johnson, D. (2003). Packet leashes: a defense against wormhole attacks in wireless networks. In *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, volume 3, pages 1976–1986.

[Hu et al., 2005] Hu, Y.-C., Perrig, A., and Johnson, D. B. (2005). Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wirel. Netw, Kluwer Academic Publishers*, 11:21–38.

[Huang and Lee, 2003] Huang, Y.-a. and Lee, W. (2003). A cooperative intrusion detection system for ad hoc networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, SASN '03, pages 135–147, New York, NY, USA. ACM.

[Islam et al., 2009] Islam, M. S., Hamid, M. A., and Hong, C. S. (2009). Shwmp: a secure hybrid wireless mesh protocol for ieee 802.11s wireless mesh networks. In *Transactions on Computational Science VI, Springer*, pages 95–114.

[Johnson et al., 2001a] Johnson, D., Menezes, A., and Vanstone, S. (2001a). The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, 1(1):36–63.

[Johnson et al., 2001b] Johnson, D. B., Maltz, D. A., Broch, J., et al. (2001b). Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. *Ad hoc networking*, 5:139–172.

[Khabbazian et al., 2009] Khabbazian, M., Mercier, H., and Bhargava, V. (2009). Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks. *Wireless Communications, IEEE Transactions on*, 8(2):736–745.

[Khalil et al., 2007] Khalil, I., Bagchi, S., and B., N. (2007). Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks. *Computer Networks*, 51(13):3750–3772.

[Khalil et al., 2010] Khalil, I., Bagchi, S., Rotaru, C. N., and Shroff, N. B. (2010). Unmask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. *Ad Hoc Networks*, 8(2):148–164.

[khan, 2011] khan, A.-S. (2011). *security of self-organizing networks,MANET,WSN,WMN,VANET*. Arobinda Gupta.

[Kumaran and Semapondo, 2010] Kumaran, S. and Semapondo, C. (2010). Hybrid wireless mesh network for universal access: Opportunities and challenges. In *Telecommunications (AICT), 2010 Sixth Advanced International Conference, IEEE*, pages 390–397.

[Lazos.L and Krunz.M, 2011] Lazos.L and Krunz.M (2011). Selective jamming/ dropping insider attack in wireless mesh networks. *IEEE Communications Society*, 25:30–33.

[Li and Yang, 2012] Li, J.-y. and Yang, Y. (2012). Research on dos attacks and resist method based on 4-way handshake in 802.11 i. In *Electrical, Information Engineering and Mechatronics 2011, Springer*, pages 631–637.

[Malkani et al., 2011] Malkani, Y., Chalmers, D., and Wakeman, I. (2011). Secure device association: Trends and issues. In *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*.

[Marina and Das, 2001] Marina, M. K. and Das, S. R. (2001). On-demand multipath distance vector routing in ad hoc networks. In *Network Protocols, 2001. Ninth International Conferenc, IEEE*, pages 14–23.

[Marina and Das, 2006] Marina, M. K. and Das, S. R. (2006). Ad hoc on-demand multipath distance vector routing. *Wireless Communications and Mobile Computing*, 6(7):969–988.

[Marshall, 2002] Marshall, J. (2002). An analysis of srp for mobile ad hoc networks. *IEEE Internet Computing)*, 12:30–36.

[Marti et al., 2000] Marti, S., Giuli, T. J., Lai, K., Baker, M., et al. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *International Conference on Mobile Computing and Networking: Proceedings of the 6 th annual international conference on Mobile computing and networking*, volume 6, pages 255–265.

[Martignon et al., 2008] Martignon, F., Paris, S., and Capone, A. (2008). Mobisec: a novel security architecture for wireless mesh networks. In *Proceedings of the 4th*

ACM symposium on QoS and security for wireless and mobile networks, pages 35–42.

[Martignon et al., 2011] Martignon, F., Paris, S., and Capone, A. (2011). Dsa-mesh: a distributed security architecture for wireless mesh networks. *Security and Communication Networks, Wiley Online Library*, 4(3):242–256.

[Marti.S et al., 2000] Marti.S, Giuli.T, and Kevin.L (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *International Conference on Mobile Computing and Networking*.

[Mendonca et al., 2012] Mendonca, M., Obraczka, K., and Turletti, T. (2012). The case for software-defined networking in heterogeneous networked environments. In *Proceedings of the 2012 ACM conference on CoNEXT student workshop*, pages 59–60.

[Meng et al., 2013] Meng, B., Huang, W., and Li, Z. (2013). Automated proof of resistance of denial of service attacks using event with theorem prover. *Journal of Computers*, 8(7).

[Muhammad Sharif, 2012] Muhammad Sharif, A. A. (2012). A novel wormhole detection technique for wireless ad hoc networks. *Int. J. Advanced Networking and Applications*, 03(05):516–521.

[Muhammad.S and Choong.S, 2009] Muhammad.S and Choong.S (2009). Security issues in wireless mesh networks. In *IEEE/IPSJ International Symposium on Applications and the Internet*, pages 717–722.

[Naveed et al., 2007] Naveed, A., Kanhere, S. S., and Jha, S. K. (2007). Topology control and channel assignment in multi-radio multi-channel wireless mesh networks. In *Mobile Adhoc and Sensor Systems, 2007. MASS 2007. IEEE Internatonal Conference on*, pages 1–9.

[P802.11w/D0.0, 2006] P802.11w/D0.0, I. (2006). Amendment 11: Protected management frames, ieee. In *Draft Standard, March 2006, work in progress*.

[Papadimitratos.P and Haas.J, 2003] Papadimitratos.P and Haas.J (2003). Secure link state routing for mobile ad hoc networks. In *Symposium on Applications and the Internet Workshops (SAINT'03 Workshops)*, pages 175–192.

[Papadimitratos.P and Haas.Z.J, 2002] Papadimitratos.P and Haas.Z.J (2002). Secure routing for mobile ad hoc networks. In *Proceedings of the SCS Communication Networks and Distributed Systems Modelling Simulation Conference (CNDS'02)*.

[Parag and Kalman.G, 2010] Parag and Kalman.G (2010). A security framework for wireless mesh networks. *Wireless Communication & Mobile Computing*, 11:371–391.

[Paris et al., 2011] Paris, S., Nita-Rotaru, C., Martignon, F., and Capone, A. (2011). Efw: A cross-layer metric for reliable routing in wireless mesh networks with selfish participants. In *INFOCOM, 2011 Proceedings IEEE*, pages 576–580.

[Parker et al., 2006] Parker, Patwardhan.A, and Joshi.A (2006). Cross-layer analysis for detecting wireless misbehavior. In *Consumer Communications and Networking Conference*.

[Pelechrinis et al., 2008] Pelechrinis, K., Iliofotou, M., and Krishnamurthy, S. V. (2008). Denial of service attacks in wireless networks: The case of jammers. *Communications Surveys & Tutorials, IEEE*, 13(2):245–257.

[Perkins and Bhagwat, 1994] Perkins, C. E. and Bhagwat, P. (1994). Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. *ACM SIGCOMM Computer Communication Review*, 24(4):234–244.

[Peters and Heath, 2009] Peters, S. W. and Heath, R. W. (2009). The future of wimax: multihop relaying with ieee 802.16 j. *Communications Magazine, IEEE*, 47(1):104–111.

[Ping.Y and Yue.W, 2010] Ping.Y and Yue.W (2010). A survey on security in wireless mesh networs. *IETE TECHINICAL REVIEW*, 27(1):6–14.

[Poovendran and Lazos, 2007] Poovendran, R. and Lazos, L. (2007). A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. *Wireless Networks*, 13(1):27–59.

[Pourbabai, 1988] Pourbabai, B. (1988). Tandem behavior of an m/m¡/1/n -> g/m/1 queuing system. *Computers & Mathematics with Applications*, 16(3):215–220.

[Redwan and Kim, 2008] Redwan, H. and Kim, K.-H. (2008). Survey of security requirements, attacks and network integration in wireless mesh networks. In *New Technologies, Mobility and Security, NTMS'08, IEEE*, pages 1–5.

[Refaei et al., 2005] Refaei, M., Srivastava, V., DaSilva, L., and Eltoweissy, M. (2005). A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In *Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005. The Second Annual International Conference on*, pages 3–11.

[Ricardo.C and Luiz.C, 2010] Ricardo.C and Luiz.C (2010). Ieee 802.11s multihop mac:a tutorial. *Communications Surveys & Tutorials, IEEE*, 13:52–67.

[Sahil.S and Anil.G, 2006] Sahil.S and Anil.G (2006). Current state of art research issues and challenges in wireless mesh networks. In *IEEE Second International conference on computer Engineering and Applications*, pages 1–17.

[Samad et al., 2012] Samad, F., Abu Ahmed, Q., Shaikh, A., and Aziz, A. (2012). Jam:mitigating jellyfish attacks in wireless ad hoc networks. In *Emerging Trends and Applications in Information Communication Technologies*, volume 281 of *Communications in Computer and Information Science*, pages 432–444.

[Seth et al., 2010] Seth, S., Gankotiya, A., and Jindal, A. (2010). Current state of art research issues and challenges in wireless mesh networks. In *Computer Engineering and Applications (ICCEA), 2010 Second International Conference, IEEE*, volume 1, pages 199–203.

[Shariful.Md and Hamid, 2009] Shariful.Md and Hamid, A. (2009). Shwmp:a secure hybrid wireless mesh protocol for ieee802.11s wireless mesh networks. *Springer-Verlag Berlin Heidelberg*, 1:95–114.

[Singh and Sharma, 2013] Singh, R. and Sharma, T. P. (2013). A secure wlan authentication scheme. *IEEK Transactions on Smart Processing & Computing*, 2(3):176–187.

[Srinivasan et al., 2005] Srinivasan, K., Ndoh, M., and Kaluri, K. (2005). Advanced wireless networks for underground mine communications. pages 1–4.

[Sudip.M et al., 2011] Sudip.M, Ranjit, Mohan, and Rohith.S (2011). Improving reliability of jamming attack detection in ad hoc networks. *International Journal of Communication Networks and Information Security (IJCNIS)*, 3:57–66.

[Tamer.M and Vivek.S, 2005] Tamer.M and Vivek.S (2005). A reputation-based mechanism for isolating selfish nodes in ad-hoc networks. In *Mobile and Ubiquitous Systems: Networking and Services:IEEE*, pages 3–11.

[Tamilselvan.L and Sankaranarayanan.V, 2007] Tamilselvan.L and Sankaranarayanan.V (2007). Prevention of blackhole attack in manet. In *Wireless Broadband and Ultra Wideband Communications, International Conference on*, volume 0, page 21.

[Thamilarasu.G et al., 2005] Thamilarasu.G, Balasubramanian.A, Mishra.S, and Sridhar.R (2005). A cross-layer based intrusion detection approach for wireless ad hoc networks. In *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, page 861.

[Thomas et al., 2001] Thomas, R. W., Raines, R. A., Baldwin, R. O., and Temple, M. A. (2001). Simulation, modeling, and evaluation of satellite-based multicasting protocols. In *Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th*, volume 1, pages 305–309.

[Trong.H and Dai.T, 2006] Trong.H and Dai.T (2006). Adaptive algorithms to enhance routing and security for wireless pan mesh networks. In *OTM workshops*, pages 585–594.

[Ud.S, 2009] Ud.S (2009). *contribution to securing wireless mesh network.* thesis, University of wollongong.

[Van Phuong et al., 2007] Van Phuong, T., Canh, N. T., Lee, Y.-K., Lee, S., and Lee, H. (2007). Transmission time-based mechanism to detect wormhole attacks. In *Asia-Pacific Service Computing Conference, The 2nd IEEE*, pages 172–178.

[Wang, 2006] Wang, X. (2006). Intrusion detection in wireless ad-hoc networks. In *30th Annual IEEE Inter-national Computer Software and Applications Conference (COMPSAC) doctorial symposium*.

[Wang and Wong, 2007] Wang, X. and Wong, J. (2007). An end-to-end detection of wormhole attack in wireless ad-hoc networks. In *Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International*, volume 1, pages 39–48.

[Wang et al., 2009] Wang, X., Wong, J., and Stanley, F.and Basu, S. (2009). Cross-layer based anomaly detection in wireless mesh networks. In *Applications and the Internet, 2009. SAINT '09. Ninth Annual International Symposium on*, pages 9–15.

[Wang.X and Wong.J, 2007] Wang.X and Wong.J (2007). Cross-layer based anomaly detection in wireless mesh networks. In *IEEE International Conference on Multimedia and Ubiquitous Engineering (MUE'07)*, pages 9–15.

[Wen et al., 2010] Wen, M., Yin, Z., Long, Y., and Wang, Y. (2010). An adaptive key management framework for the wireless mesh and sensor networks. *Wireless Sensor Network*, 2(9).

[Xie and Wang, 2008] Xie, J. and Wang, X. (2008). A survey of mobility management in hybrid wireless mesh networks. *Network, IEEE*, 22(6):34–40.

[Xiu-feng et al., 2010] Xiu-feng, Q., Jian-wei, L., and Sangi, A. (2010). Mtsr: wormhole attack resistant secure routing for ad hoc network. In *Information Computing and Telecommunications (YC-ICT), 2010 IEEE Youth Conference*, pages 419–422.

[Xu et al., 2010] Xu, X., Tang, S., Mao, X., and Li, M. (2010). Distributed gateway placement for cost minimization in wireless mesh networks. In *Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on*, pages 507–515.

[Xu.W et al., 2003] Xu.W, Trappe.W, Yanyong.Z, and Wood.T (2003). The feasibility of launching and detecting jamming attacks in wireless networks. pages 286–297.

[Yi et al., 2009] Yi, P., Tong, T., Liu, N., Wu, Y., and Ma, J. (2009). Security in wireless mesh networks: challenges and solutions. In *Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference, IEEE*, pages 423–428.

[Yih-Chun.H and Johnson.D.B, 2003] Yih-Chun.H and Johnson.D.B (2003). Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks. *Elsevier*, 1:175–192.

[Zhang and Fang, 2006] Zhang, Y. and Fang, Y. (2006). Arsa: an attack-resilient security architecture for multihop wireless mesh networks. *Selected Areas in Communications, IEEE Journal on*, 24(10):1916–1928.

[Zhang et al., 2008] Zhang, Z., Nait-Abdesselam, F., Ho, P.-H., and Lin, X. (2008). Radar: a reputation-based scheme for detecting anomalous nodes in wireless mesh networks. In *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, pages 2621–2626.

[Zhang.Y, 2008] Zhang.Y (2008). *Security in Wireless Mesh Networks*. CRC.

[Zhen and Srinivas, 2003] Zhen, J. and Srinivas, S. (2003). Preventing replay attacks for secure routing in ad hoc networks. volume 2865 of *Lecture Notes in Computer Science*, pages 140–150.

[Zhong and Xu, 2010] Zhong, L. and Xu, C. (2010). Byzantine attack with anypath routing in wireless mesh networks. pages 711–715.

[Zhou et al., 2012] Zhou, J., Cao, J., Zhang, J., Zhang, C., and Yu, Y. (2012). Analysis and countermeasure for wormhole attacks in wireless mesh networks on a real testbed. In *Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference*, pages 59–66.

[Zonghua.Z et al., 2008] Zonghua.Z, Nait.A.F, and Djahel (2008). Arsos: An adaptive, robust, and sub-optimal strategy for automated deployment of anomaly detection system in manets. In *International Journal of Network Security & Its Applications*, pages 606–613.

List of Publications based on the Research Work

Refereed Journals

K. Ganesh Reddy, P. Santhi Thilagam, (2014), ”Reputation based Cross-layer Intrusion Detection System for Wormhole Related Attacks in Wireless Mesh Networks” Security and Communication Networks -Journal- Wiley, doi: 10.1002/sec.955.
URL:http://www.onlinelibrary.wiley.com/doi/10.1002/sec.955/full

K. Ganesh Reddy, P. Santhi Thilagam (2013),. ”Hierarchical Wireless Mesh Networks Scalable Secure Framework.” International Journal of Information and Network Security (IJINS) Volume no: 2, Page no:167-176.
URL:http://iaesjournal.com/online/index.php/IJINS/article/view/1494/667

K. Ganesh Reddy, P. Santhi Thilagam, (2012). ”Securing Wireless Mesh Networks: State of the Art and Challenges ” Computer Science Review- Journal - Elsevier (Paper submitted on 26th October 2012 and waiting for review).

K. Ganesh Reddy, P. Santhi Thilagam (2014),. Multi-level key management mechanism for hybrid wireless mesh networks.” International Journal of Information Security (Springer publications). (Submitted on 17/09/2014 and waiting for review).

Conference Proceedings

K. Ganesh Reddy, P. Santhi Thilagam, and Nageswara Rao (2012). ”Cross-layer IDS for Rushing attack in Wireless Mesh Networks”. In Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology (CCSEIT ’12). ACM, New York, Page no:396-400.
URL:http://dl.acm.org/citation.cfm?id=2393283

K. Ganesh Reddy, P. Santhi Thilagam (2012). ”Taxonomy of Network Layer Attacks in Wireless Mesh Network.” Advances in Computer Science, Engineering & Applications. Springer, Advances in Intelligent Systems and Computing Volume no:167, Page no:927-935.

URL:http://link.springer.com/chapter/10.1007%2F978-3-642-30111-7_90

K. Ganesh Reddy, and P. Santhi Thilagam (2012). ”Intrusion detection technique for wormhole and following jellyfish and byzantine attacks in wireless mesh network.” Advanced Computing, Networking and Security. Springer, Lecture Notes in Computer Science Volume no:7135, Page no:631-637.
URL:http://link.springer.com/chapter/10.1007%2F978-3-642-29280-4_73