DEVELOPMENT OF SECURE COMMUNICATION SCHEMES FOR WIRELESS MESH NETWORKS

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

VANLALHRUAIA

MZU REGISTRATION NO.: 1906308

Ph.D. REGISTRATION NO.: MZU/Ph.D./1694 of 31.07.2019

DEPARTMENT OF COMPUTER ENGINEERING

SCHOOL OF ENGINEERING AND TECHNOLOGY

JUNE, 2025

DEVELOPMENT OF SECURE COMMUNICATION SCHEMES FOR WIRELESS MESH NETWORKS

BY

VANLALHRUAIA

DEPARTMENT OF COMPUTER ENGINEERING

Supervisor

Prof. Ajoy Kumar Khan

Joint Supervisor

Dr. Amit Kumar Roy

Submitted

In partial fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Engineering of Mizoram University, Aizawl

CERTIFICATE

This is to certify that the thesis entitled "*Development of Secure communication schemes for Wireless Mesh Networks*" submitted by Mr. Vanlalhruaia, in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy bonafide record of original research work carried out by him under our supervision and guidance.

This work has not been submitted earlier, either in part or in full, for the award of any degree to any other university or institution.

(Prof. AJOY KUMAR KHAN)

Supervisor & Professor

Department of Computer Engineering Date:

Mizoram University, Aizawl, Mizoram Place:

(Dr. AMIT KUMAR ROY)

Joint Supervisor & Assistant Professor

Department of Computer Science and Engineering- Cyber Security. Date:

Indian Institute of Information Technology, Kottayam, Kerala. Place:

DECLARATION

MIZORAM UNIVERSITY

JUNE 2025

I, **VANLALHRUAIA** hereby declare that the subject matter of this thesis is the record of work done by me, that the contents of this thesis did not form basis of the award of any previous degree by me or to do the best of my knowledge to anybody else, and that the thesis has not been submitted by me for any research degree in any other university/institute.

This is being submitted to the Mizoram University for the **Degree of Doctor of Philosophy in Computer Engineering.**

(VANLALHRUAIA)

(Prof. AJOY KUMAR KHAN)

Supervisor

(Dr. AMIT KUMAR ROY)

(Joint Supervisor)

Dr. V.D AMBETH KUMAR
Head
Department of Computer Engineering

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my Ph.D. supervisor, **Prof. Ajoy Kumar Khan**, for His exceptional guidance, unwavering support, and insightful advice throughout the course of this research. His expertise and encouragement have been instrumental in shaping the quality and direction of this thesis.

I am equally thankful to my joint supervisor, **Dr. Amit Kumar Roy** for His valuable suggestions, technical insights, and constant support. His collaborative mentorship has enriched this research and broadened my perspective on key areas of study.

My heartfelt thanks to the faculty and staff of the Department of Computer Engineering, Mizoram University, for providing a stimulating academic environment and access to essential resources and infrastructure.

I am deeply grateful to my Colleague and fellow researchers for their cooperation, motivation, and the many thought-provoking discussions that helped me navigate this journey.

Above all, I would like to thank my family for their unconditional love, patience, and sacrifices. Their unwavering support has been the bedrock of my perseverance and success.

Lastly, I express my deepest gratitude to the Almighty for granting me the strength, health, and resilience needed to complete this thesis.

(VANLALHRUAIA)

Contents

List Of Tables

List of Figure

Chapter 1

INTRODUCTION

1.1 Wireless Networks

A wireless network is a communication system that allows devices to connect and share data without physical cables, using radio waves, infrared signals, or satellite transmissions. It provides seamless connectivity, enabling users to access the internet, communicate, and exchange information from virtually anywhere. Wireless networks are essential in modern society, supporting applications in homes, businesses, healthcare, education, and smart technologies.

The key advantages of wireless networks include mobility, flexibility, ease of installation, and cost-effectiveness. Unlike wired networks, they eliminate the need for extensive cabling, making them ideal for large-scale and dynamic environments. However, wireless networks also face challenges such as security threats, interference, signal degradation, and bandwidth limitations. Cyber security risks, including unauthorized access and data breaches, remain significant concerns.

With advancements in 5G, artificial intelligence, and encryption technologies**,** wireless networks continue to evolve, offering faster speeds, improved reliability, and enhanced security [1].

1.1.1 Types of Wireless Networks

Wireless networks enable seamless communication without physical cables, using technologies such as radio waves and infrared signals. They are categorized into four primary types depending on their range and usage.

- **Wireless Local Area Network (WLAN)**

A WLAN offers wireless connectivity in confined spaces like residences, workplaces, or college campuses, utilizing Wi-Fi technology (IEEE 802.11).WLANs allow multiple devices to connect to the internet and share data without wired connections, offering flexibility, mobility, and ease of installation. These networks are commonly used in businesses, public places, and educational institutions due to their cost-effectiveness and convenience [1].

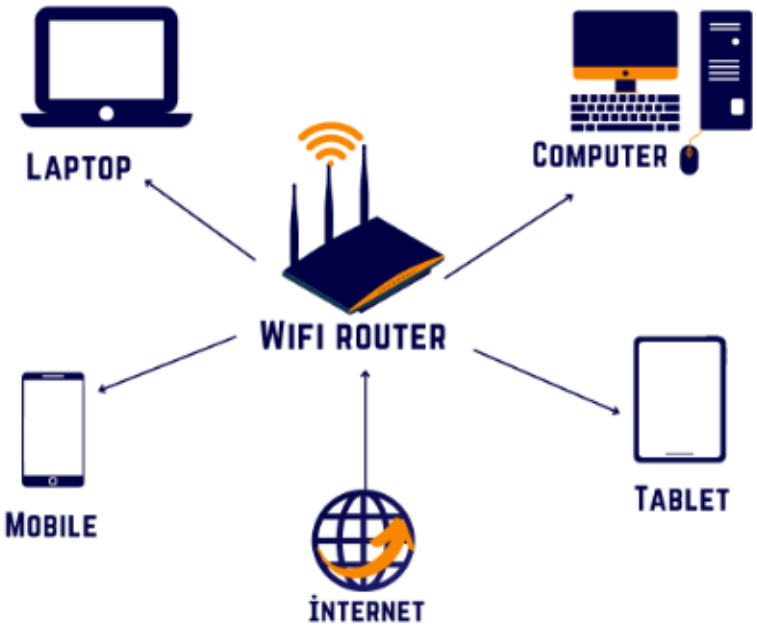

fig 1.1: Wireless LAN [2]

- **Wireless Metropolitan Area Network (WMAN)**

A WMAN extends across a city or metropolitan area, providing broadband wireless access to businesses, government services, and residential users. WiMAX (IEEE 802.16) and 4G LTE are two technologies that allowed for high-speed data transfer and wide-scale connectivity. WMANs play a crucial role in smart city infrastructure, supporting applications like traffic monitoring, public Wi-Fi, and emergency services [3].

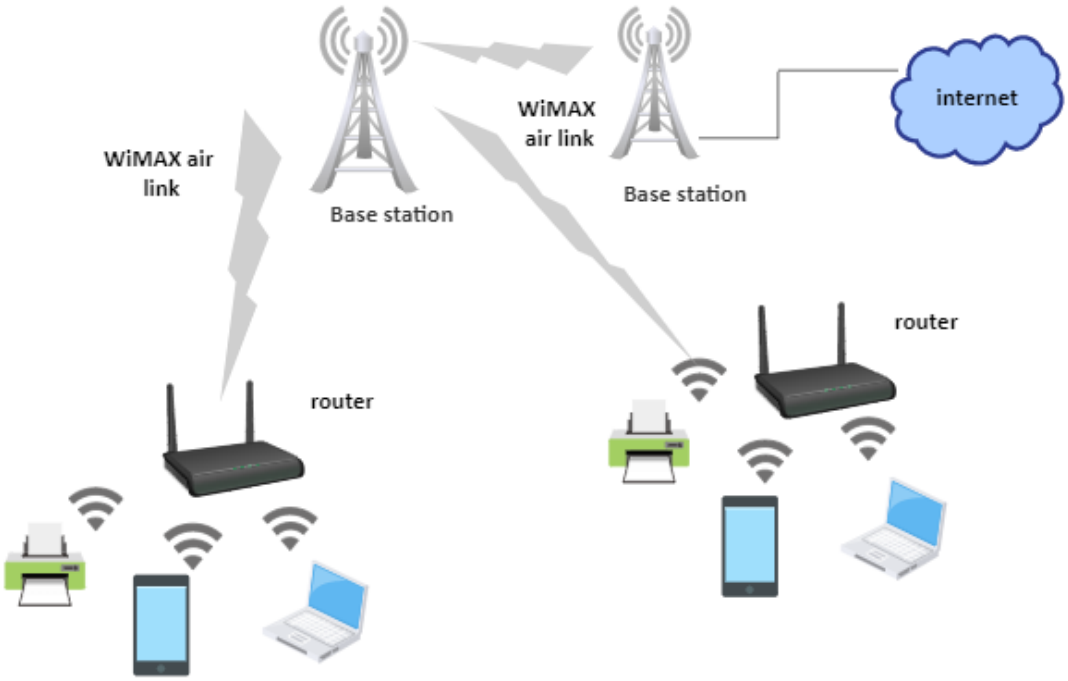

Fig 1.2: Wireless MAN [4]

- **Wireless Wide Area Network (WWAN)**

A WWAN covers large geographic areas, including national and international communication, through cellular networks (3G, 4G, and 5G) and satellite communication. WWANs allow mobile users to access the internet, send messages, and make calls over long distances. These networks support critical applications such as mobile broadband, disaster recovery communication, and global positioning systems (GPS) [5].

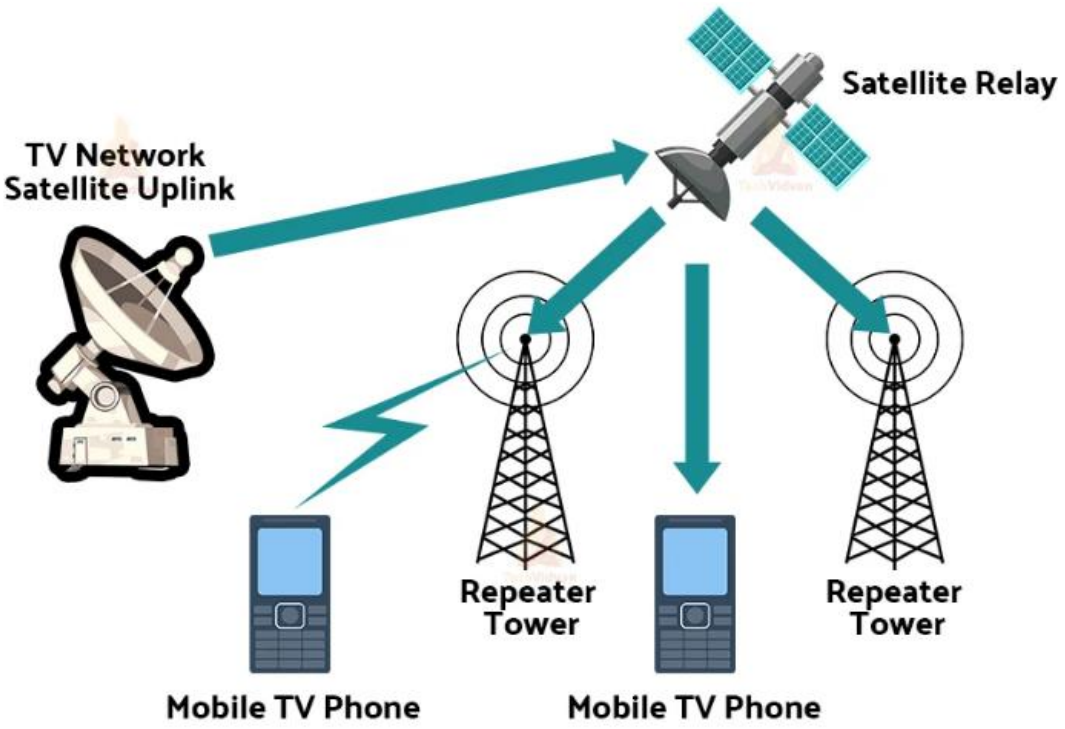

Fig 1.3: Wireless WAN [6]

- **Wireless Personal Area Network (WPAN)**

Short-range connection between individual devices, like smart phones, smart watches, and Internet of Things devices, is made possible via a WPAN.. Technologies like Bluetooth (IEEE 802.15.1), Zigbee, and NFC enable wireless communication over short distances, supporting applications in smart homes, healthcare, and wearable devices [7].

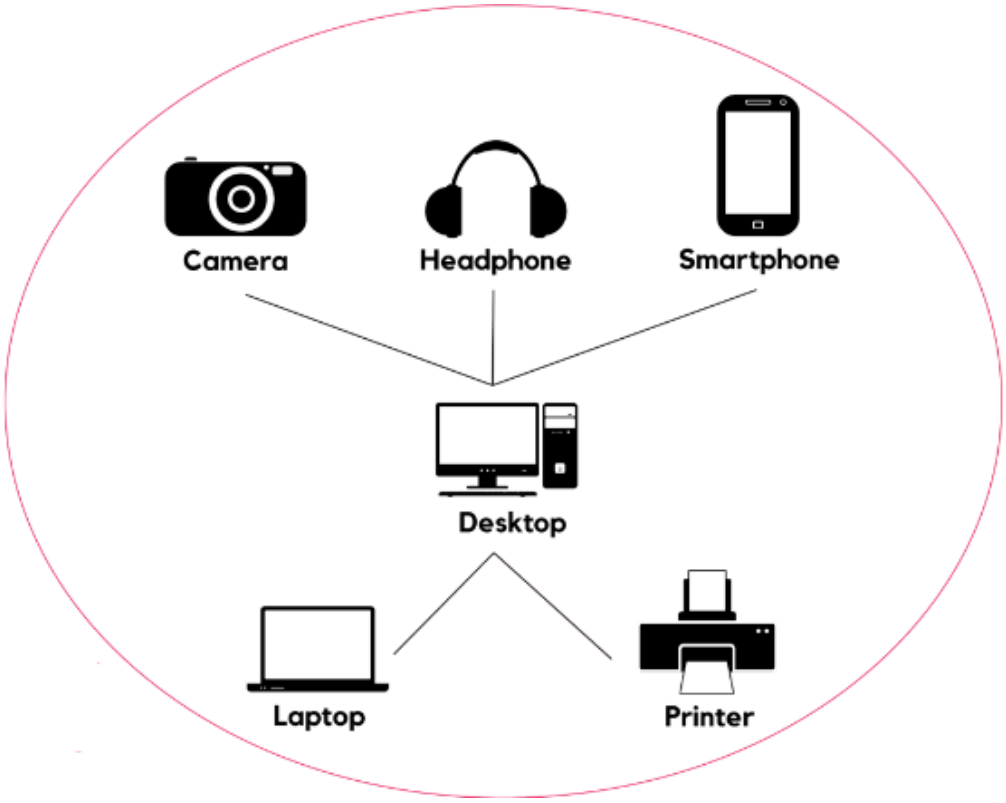

Fig 1.4: wireless PAN [8]

1.2 AdHoc Networks

An ad hoc network is a decentralized wireless network where nodes communicate directly without relying on fixed infrastructure such as routers or base stations. These networks are self-organizing, self-healing, and dynamic, permitting nodes to enter or exit at any moment. Ad hoc networks are commonly used in scenarios where traditional networks are unavailable, such as disaster recovery, military applications, and smart IoT systems [9].

Ad hoc networks offer high flexibility and scalability, making them useful in various real-time applications. However, they also pose challenges such as security risks, limited bandwidth, and energy constraints. AdHoc networks of various kinds have been created to meet certain requirements.

1.2.1 Types of Ad Hoc Networks

- **Mobile Ad Hoc Networks (MANETs)**

A Mobile Ad Hoc Network (MANET) is a network of mobile devices that configure themselves and communicate without wires. Since the nodes are mobile, the network topology frequently changes, requiring adaptive routing protocols like Ad hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) for efficient data transmission [10].

Characteristics of MANETs:

- **Dynamic topology:** Devices frequently move, requiring real-time route updates.
- **Decentralization:** No central authority; nodes function as both hosts and routers.
- **Energy constraints:** Most devices operate on battery power.

Applications of MANETs:

- **Military communication:** Used in battlefield environments where fixed infrastructure is unavailable.
- **Disaster response:** Helps establish emergency communication networks in earthquake or flood-affected areas.
- **IoT and smart cities:** Supports wireless sensor networks in smart environments.

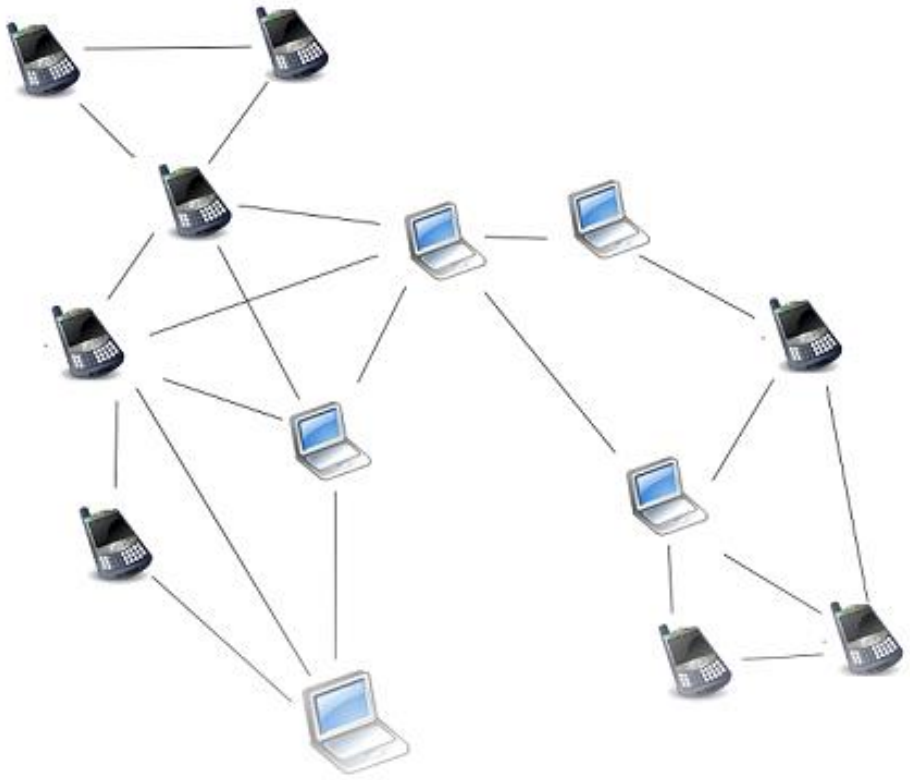

Fig 1.5: Mobile Adhoc Network [11]

- **Vehicular Ad Hoc Networks (VANETs)**

Vehicles may connect with roadside infrastructure and one another over a specialised type of MANET called a Vehicular Ad Hoc Network (VANET). VANETs play a critical role in road safety, traffic management, and autonomous driving[12].

Characteristics of VANETs:

- **High Mobility :**Vehicles in VANET move at high speeds, especially on highways. This causes the network components to shift quickly, making the network extremely dynamic and difficult to have steady connections.
- **Dynamic Topology :**Because of the constant vehicle movements, the network structure changes frequently. Connections between vehicles are

established and broken quickly, which requires efficient and adaptive communication protocols.

- **Predictable Mobility:**Even though vehicles are highly mobile, their movement is generally predictable as they follow roads, traffic signs, and specific routes. This predictability can be used to design better routing and communication strategies in VANET.

Applications of VANETs:

- **Collision prevention:** Vehicles receive early warnings about potential accidents.
- **Traffic optimization:** Reduces congestion by providing dynamic route updates.
- **Autonomous vehicle coordination:** Enables self-driving cars to interact seamlessly.

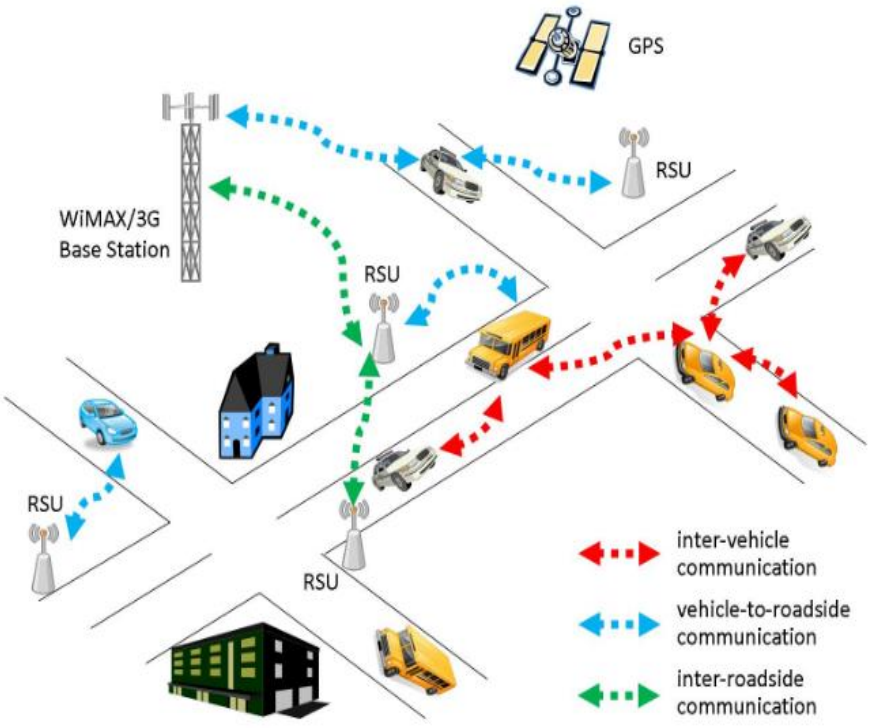

Fig 1.6: VANET [13]

- **Wireless Sensor Networks (WSNs)**

Tiny, low-power sensor nodes make up a Wireless Sensor Network (WSN), which gathers and sends data to a base station. These networks are widely used in environmental monitoring, healthcare, and industrial automation[14].

Characteristics of WSNs:

- **Large-scale deployment:**An area can have multiple numbers of sensor nodes installed.
- **Limited power consumption:** Nodes rely on small batteries or energy-harvesting techniques.
- **Multi-hop communication:**A base station receives data after it has passed via intermediary nodes.

Applications of WSNs:

- **Smart agriculture:** Monitors soil moisture and temperature.
- **Healthcare:** Wearable sensors track heart rate and glucose levels.
- **Disaster management:** Detects earthquakes, wildfires, and air pollution.

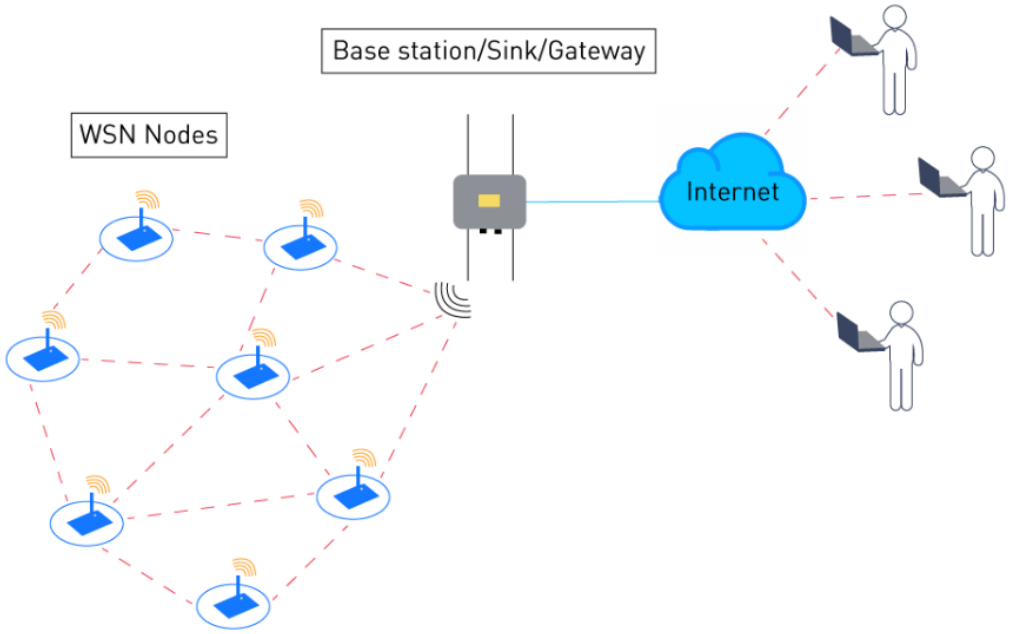

Fig 1.7: Wireless Sensor Network [15]

- **Tactical Ad Hoc Networks (TANETs)**

Tactical Ad Hoc Networks (TANETs) are designed for military and emergency response operations, providing secure and reliable communication in hostile environments. These networks are used where conventional infrastructure is unavailable or compromised.

Characteristics of TANETs:

- **Highly secure:** Uses encryption and authentication protocols to prevent cyber attacks.
- **Resilient to failures:** Can function in challenging terrains with limited connectivity.
- **Autonomous operation:** Works without external infrastructure like satellites or cellular towers.

Applications of TANETs:

- **Battlefield communication:** Provides real-time data exchange between soldiers and command centers.
- **Emergency response:** Used in disaster relief efforts to establish communication in affected areas.
- **Remote surveillance:** Supports reconnaissance missions in inaccessible regions.

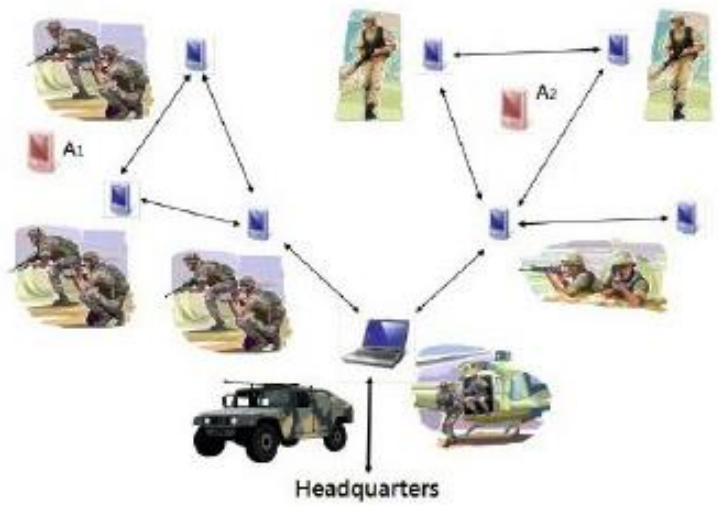

Fig 1.8: Tactical adhoc network[16]

1.3 Wireless Mesh Networks

Wireless mesh networks (WMNs) represent the next generation of wireless networks, characterized by rapid development and a multitude of applications, positioning them as a pivotal technology for the future [17]. They are increasingly recognized as a viable alternative to certain aspects of mobile ad hoc networks (MANETs) [18]. A

WMN comprises radio nodes arranged in a mesh topology, forming a packet-switched network with a static wireless backbone. This backbone's topology is fixed, though it allows for modifications through the addition, removal, or failure of nodes [19].

The promising potential of WMNs has garnered significant attention from both academia and industry, leading to the development of numerous research testbeds and the availability of commercial products [20]. However, several challenges must be addressed before widespread deployment can occur. For example, existing medium access control (MAC) and routing protocols often lack scalability, resulting in significant throughput degradation as the number of nodes or hops increases [17]. Security concerns, such as vulnerabilities to various malicious attacks, are particularly pressing. Adversaries may eavesdrop on wireless communications to obtain confidential information, launch denial-of-service (DoS) attacks through compromised nodes, or alter transmitted data, thereby compromising the network's confidentiality, authenticity, availability, and integrity [19].

Similar to MANETs, WMNs feature a shared medium, absence of a centralized traffic aggregation point, and dynamic topology. These characteristics render traditional wired network security mechanisms unsuitable for direct application in WMNs. Moreover, security solutions designed for MANETs may not be appropriate for WMNs due to differences such as mesh nodes typically being equipped with multiple radios, allowing for simultaneous data transmission and reception across multiple channels [18]. The integration of diverse wireless networks necessitates a heterogeneous-aware design in intrusion detection systems. Additionally, network protocols face new challenges, such as incorporating link information into routing decisions to enhance multi-hop wireless transmission performance [19]. These factors present novel challenges for security mechanisms within WMNs.

Distinct from other wireless networks, WMNs consist of both wireless access and wireless backbone networks. They are dynamically self-organizing, self-configuring, and self-healing, offering easy maintenance, high scalability, and reliable service among network nodes [17]. WMNs are also expected to overcome limitations and

significantly enhance the performance of other wireless networks. As WMNs gain popularity as a replacement technology for last-mile connectivity in home, community, and neighborhood networking, it becomes imperative to design efficient and secure communication protocols [20]. However, current WMN protocols exhibit vulnerabilities that potential attackers can exploit. The lack of a central administrative point further complicates security efforts, making it a paramount concern [17].

Attacks on WMNs can be both external and internal. External attacks are perpetrated by unauthorized intruders who may inject malicious packets to disrupt routing protocols or eavesdrop and replay packets to access network resources [19]. Conversely, internal attacks originate from nodes within the WMN, such as a malicious node dropping packets it is supposed to forward[20]. To mitigate external attacks, robust authentication and access control mechanisms are essential for the practical deployment and use of WMNs. A secure authentication protocol should enable two communicating entities—whether a pair of mesh clients (MCs), mesh routers (MRs), or a combination thereof—to verify each other's authenticity and generate shared session keys for cryptographic enforcement of message confidentiality and integrity [17].

Internal attacks pose a greater challenge, necessitating strong cooperation and coordination among mesh entities to ensure security. Therefore, a robust mechanism based on a trust framework is required to detect malicious nodes within WMNs and mitigate their impact on performance [18]. Furthermore, advanced security measures must be integrated to secure routing across various protocol layers, including the implementation of multi-protocol layer security schemes that adapt to the evolving WMN environment [19].

Table 1.1: Comparison of various issues between Adhoc network and WMN

Issue	**Ad-hoc Networks (MANETs)**	**Wireless Mesh Networks (WMNs)**
Architecture	Infrastructure-less, dynamic topology	Hybrid structure with fixed backbone and dynamic nodes
Topology	Highly dynamic, nodes move frequently	Semi-static with fixed backbone and mobile clients
Scalability	Limited scalability due to dynamic topology	Highly scalable due to dedicated backbone nodes
Reliability	Less reliable due to frequent topology changes	More reliable with multiple redundant paths
Network Stability	Frequent topology updates cause instability	More stable due to backbone nodes
Routing Mechanism	Reactive and proactive protocols (AODV, DSR, OLSR)	Uses mesh-specific routing (HWMP, OLSR) for improved performance
Bandwidth Utilization	Low efficiency due to frequent route breaks	High efficiency with dedicated routing infrastructure

Throughput	Decreases significantly as node count increases	Higher throughput due to multi-radio/multi-channel support
Security	Vulnerable to attacks due to decentralized nature	More robust, but still faces security challenges like DoS and eavesdropping
Deployment Cost	Lower cost, no fixed infrastructure needed	Higher cost due to backbone infrastructure
Maintenance	Requires constant reconfiguration	Self-organizing, self-healing, lower maintenance effort

1.3.1 Architecture of Wireless Mesh Network

WMNs consist of three distinct network components: Internet Gateway Routers (IGWs), Mesh Routers (MRs), and Mesh Clients (MCs). At the highest level, IGWs serve as the connection points to the wired network. Below them, Mesh Routers (also referred to as Access Points) create a multi-hop forwarding structure, directing traffic towards the IGWs and forming the WMN backbone. These routers remain relatively stationary. At the lowest level, Mobile Clients or Nodes function as end-user devices that connect to MRs to access wired network.

- **Internet Gateway Routers** (IGWs) are essential network components that provide access to wired infrastructure, including the Internet or local networks. A wireless mesh network can incorporate multiple gateways to enhance connectivity. Typically, a gateway functions as a computer operating across all five layers of the network model.

- **Mesh Routers** (MRs) are cost-effective, flexible, and easy to deploy. Acting as Access Points (APs), they form the network backbone, covering large areas and connecting both wired and wireless users. These APs are generally stationary, have a low failure rate, and are not constrained by power limitations. This interconnected mesh of APs facilitates communication between mobile devices and network gateways.

- **Mesh Clients** (MCs) encompass various devices such as PDAs, laptops, and mobile phones, each with different mobility levels. These mobile nodes vary significantly in energy efficiency, computational power, and transmission capabilities. They can connect to the wired infrastructure either by directly communicating with a network gateway, depending on their location and transmission range, or by relaying data through intermediate nodes.

A typical WMNs can have three level hierarchical structures of these network elements.

- **Infrastructure or Backbone** WMNs consist of mesh routers that establish a communication framework for client devices. As illustrated in the figure, dashed lines represent wireless links, while solid lines denote wired connections. The backbone of WMNs can be constructed using various radio technologies beyond the commonly employed IEEE 802.11 standards. Mesh routers autonomously form self-configuring and self-healing links, ensuring network resilience. By incorporating gateway functionality, these routers provide Internet access, a concept known as infrastructure meshing. This architecture serves as a backbone for conventional clients and facilitates the integration of WMNs with existing wireless networks through gateway and bridge functionalities. Clients equipped with Ethernet interfaces can connect to mesh routers via wired links, whereas those using the same wireless technology as the mesh routers can establish direct communication. However, if different radio technologies are involved, clients must first connect to base stations that have Ethernet links to mesh routers [21].

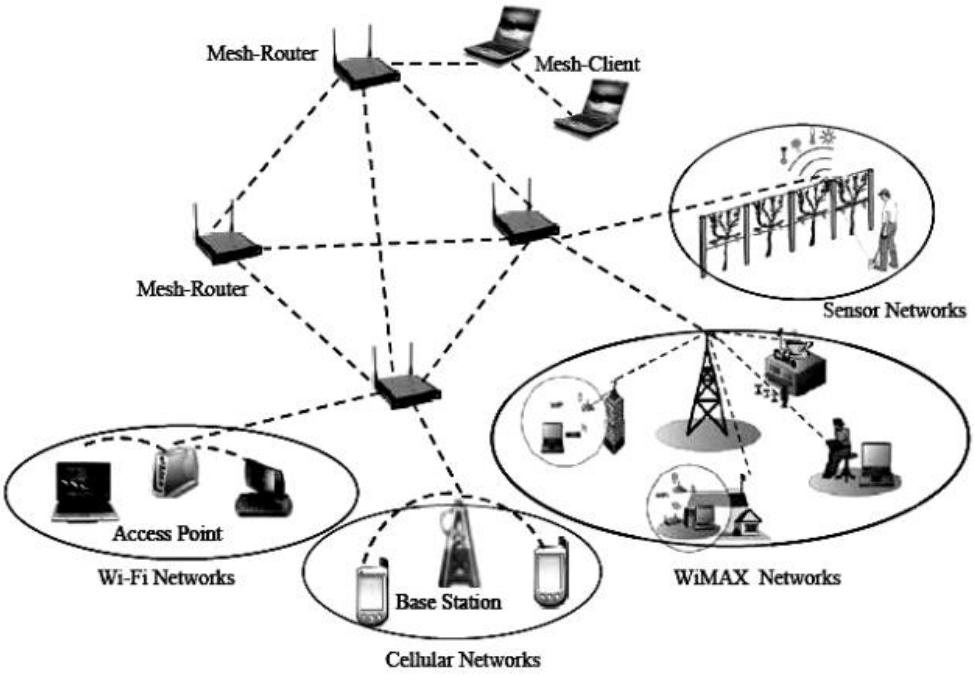

Fig 1.9: Infrastructure WMN [22]

- **Client** WMNs enable peer-to-peer communication among client devices, where the client nodes themselves handle network routing, configuration, and application services. Unlike infrastructure-based WMNs, this architecture does not require mesh routers, as clients directly manage data transmission and connectivity. Client WMNs typically operate using a single type of radio technology, making them functionally similar to conventional ad hoc networks. However, due to the absence of dedicated infrastructure, the responsibility for network management shifts to the end-user devices, requiring them to support additional tasks such as routing and self-configuration [21].

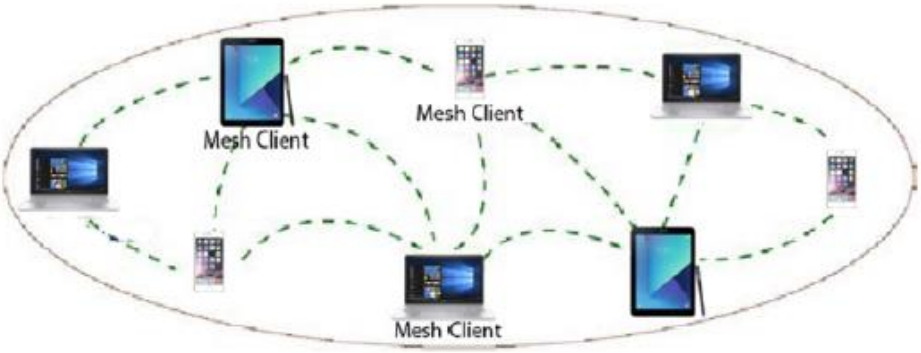

Fig 1.10: Mesh Client WMN [23]

- **Hybrid** WMNs integrate both infrastructure-based and client-based meshing, offering a versatile network architecture. In this model, mesh clients can connect to the network either through mesh routers or by directly communicating with other mesh clients. The infrastructure component facilitates connectivity to external networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks. Meanwhile, the routing capabilities of client nodes enhance network coverage and connectivity within the WMN, improving overall network efficiency and robustness [21].

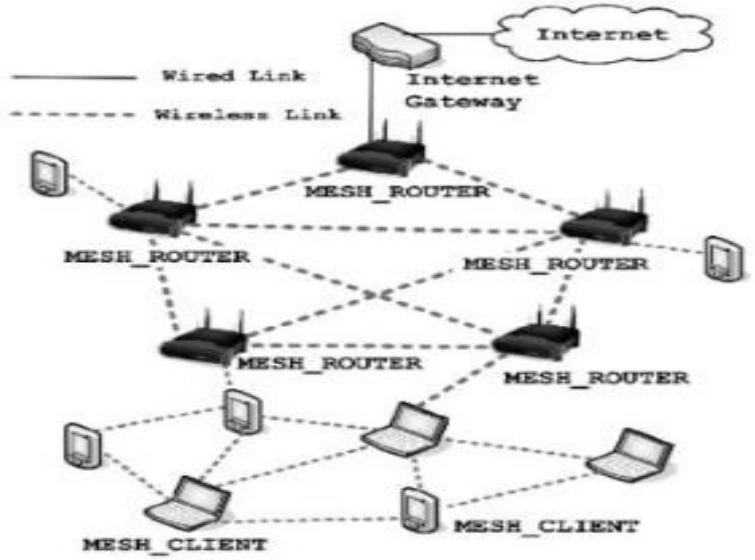

Fig 1.11: Hybrid WMN [24]

1.3.2 Characteristics of Wireless Mesh Networks (WMNs)

Wireless Mesh Networks (WMNs) have emerged as a transformative technology in modern wireless communication systems. Due to their decentralized architecture, self-healing capabilities, and ease of deployment, WMNs are increasingly being adopted in various applications such as smart cities, disaster recovery, industrial automation, and broadband internet access [21]. The following sections outline the characteristics of WMNs.

- **Self-Configuring and Self-Healing Capabilities**

One of the most significant advantages of WMNs is their ability to self-configure and self-heal. Each node in the network can automatically detect new nodes and establish connections without manual intervention. If a node fails or is removed, the network dynamically reconfigures itself to maintain connectivity, thereby improving reliability [25]. This feature is particularly beneficial in dynamic environments such as military operations and emergency response systems, where network stability is crucial.

- **Scalability and Flexibility**

WMNs are highly scalable, allowing seamless expansion as new nodes are added to the network. Unlike traditional networks that require centralized infrastructure, WMNs can grow organically without significant modifications. This scalability makes them suitable for large-scale deployments such as urban Wi-Fi networks and industrial monitoring systems [26]. The flexible architecture of WMNs also supports heterogeneous networks, enabling integration with various wireless technologies such as Wi-Fi, WiMAX, and cellular networks.

- **Multi-Hop Communication**

Unlike single-hop wireless networks, WMNs rely on multi-hop communication, where data is forwarded through multiple intermediate nodes before reaching the destination. This approach extends the network coverage and reduces dependence on

high-power transmission, making WMNs energy-efficient and cost-effective [27]. Multi-hop routing also enhances reliability by providing multiple paths for data transmission, reducing the likelihood of network congestion and failures.

- **High Reliability and Redundancy**

The inherent redundancy in WMNs contributes to their high reliability. Since data packets can traverse multiple routes, the failure of a single node does not disrupt the entire network. Instead, the network dynamically reroutes traffic through alternative paths, ensuring continuous operation. This redundancy is particularly useful in mission-critical applications such as surveillance systems and healthcare monitoring, where uninterrupted connectivity is essential [23].

- **Support for Mobility**

WMNs provide seamless mobility support, allowing users to move across different network areas without experiencing connectivity disruptions. Unlike traditional wireless networks that rely on fixed access points, WMNs can dynamically adjust routing paths to accommodate mobile nodes. This feature is especially beneficial for vehicular networks, mobile healthcare systems, and public safety communications [28].

- **Cost-Effectiveness**

Deploying WMNs is significantly more cost-effective than traditional wired and wireless networks. Since they eliminate the need for extensive cabling and centralized infrastructure, the deployment and maintenance costs are reduced. Additionally, WMNs utilize existing network resources efficiently, enabling service providers to extend network coverage without investing in expensive infrastructure upgrades [26].

- **Energy Efficiency**

WMNs are designed to optimize energy consumption, particularly in battery-powered devices. The multi-hop architecture reduces the need for high-power transmissions, thereby conserving energy and prolonging the lifespan of network nodes. Furthermore, advanced power management techniques, such as adaptive transmission power control and energy-aware routing, enhance the overall energy efficiency of WMNs [25].

- **Integration with Other Networks**

One of the key strengths of WMNs is their ability to integrate with other wireless and wired networks. Through gateway and bridge functionalities, WMNs can interconnect with Wi-Fi hotspots, cellular networks, and sensor networks, enabling seamless communication across different network technologies. This interoperability enhances the overall network efficiency and expands the range of applications for WMNs [28].

1.3.3 Applications of Wireless Mesh Networks (WMNs)

Wireless Mesh Networks (WMNs) have gained widespread adoption across various domains due to their flexible, self-configuring, and cost-effective nature. These networks support numerous applications, ranging from urban connectivity to industrial automation, public safety, and disaster recovery [21]. The following sections outline the key applications of WMNs.

- **Smart Cities and Municipal Wireless Networks**

WMNs play a crucial role in developing smart cities by providing seamless wireless connectivity. Municipalities deploy WMNs to offer city-wide Wi-Fi, intelligent traffic management, surveillance systems, and smart grid communications [26]. These networks enhance public services and improve overall urban efficiency.

- **Disaster Recovery and Emergency Communications**

In disaster-stricken areas where traditional communication infrastructure is damaged, WMNs provide rapid and reliable communication networks. First responders, emergency services, and humanitarian organizations use WMNs for real-time data transmission, coordination, and rescue operations [25].

- **Industrial Automation and IoT**

Industries leverage WMNs to enable real-time monitoring and automation in manufacturing processes. Industrial IoT (IIoT) applications such as predictive maintenance, machine-to-machine communication, and remote monitoring benefit from WMNs' reliability and scalability [23].

- **Healthcare and Telemedicine**

WMNs support healthcare applications by ensuring seamless communication between medical devices, wearable health monitors, and hospital networks. Remote patient monitoring, telemedicine consultations, and emergency medical response systems benefit from WMNs' robust connectivity [28].

- **Public Safety and Surveillance**

Law enforcement agencies and security organizations utilize WMNs for real-time video surveillance, crime prevention, and disaster response. These networks ensure continuous connectivity for body-worn cameras, drones, and sensor-based monitoring systems [27].

- **Rural and Remote Area Connectivity**

WMNs provide broadband access to rural and underserved areas where laying traditional infrastructure is cost-prohibitive. These networks enable internet access, distance education, telemedicine, and e-governance services for remote communities [25].

- **Military and Defense Communication**

Armed forces deploy WMNs for secure battlefield communication, surveillance, and reconnaissance. These networks support mobile units by maintaining reliable and self-healing communication links under dynamic conditions [26].

- **Home and Enterprise Networking**

WMNs simplify network expansion in residential and corporate environments. They eliminate the need for extensive cabling, enabling flexible and cost-effective connectivity for smart homes, office spaces, and IoT-enabled environments [23].

- **Vehicular Networks and Intelligent Transportation Systems (ITS)**

WMNs are used in vehicular communication for traffic management, accident prevention, and vehicle-to-infrastructure communication. Intelligent Transportation Systems (ITS) rely on WMNs for seamless vehicle tracking, toll collection, and navigation services [28].

- **Educational Institutions and Campus Networks**

Universities and schools deploy WMNs to provide campus-wide Wi-Fi coverage, facilitating seamless access to e-learning platforms, digital libraries, and research collaboration tools [27].

1.4 Routing Protocols in wireless mesh networks

Routing protocols in Wireless Mesh Networks (WMNs) play a critical role in ensuring efficient and reliable communication between nodes. These protocols determine the best paths for data packets to travel across the network. WMNs face unique challenges such as dynamic topologies, interference, and multi-hop communication, making routing protocol selection crucial for performance optimization [21].

Routing protocols in WMNs can be broadly classified into three categories:

1.4.1 Proactive: Proactive routing protocols, also known as table-driven protocols, maintain up-to-date routing tables by periodically exchanging information across the network. These protocols ensure that routes to all possible destinations are pre-computed and readily available, reducing latency during data transmission, it provide fast and reliable packet delivery, making them suitable for low-mobility networks communications. However, their main drawback is high control overhead, as frequent routing updates consume bandwidth and processing power. Additionally, maintaining routing tables for all nodes becomes inefficient in large or dynamic networks. Despite these challenges, proactive routing remains a valuable approach for applications requiring stable and consistent connectivity. Optimized Link State Routing (OLSR), Destination-Sequenced Distance-Vector (DSDV), Wireless Routing Protocol (WRP) are falling in this category.

1.4.2 Reactive: Reactive routing protocols, also known as on-demand routing protocols, establish routes only when required, reducing control overhead compared to proactive approaches. Instead of maintaining a constantly updated routing table, these protocols initiate a route discovery process when a source node needs to send data to a destination. This method conserves bandwidth and processing power, making it ideal for dynamic and large-scale networks. While reactive protocols minimize unnecessary routing overhead, they suffer from higher latency due to route discovery delays. Reactive protocols are well-suited for highly mobile networks, such as vehicular ad hoc networks (VANETs), sensor networks, and emergency communication systems, where frequent topology changes make maintaining pre-computed routes inefficient. Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) are falling in this category.

1.4.3 Hybrid : Hybrid routing protocols combine features of both proactive (table-driven) and reactive (on-demand) routing approaches to optimize performance in wireless networks. These protocols aim to achieve a balance between low latency (offered by proactive routing) and reduced overhead (offered by reactive routing). They work by proactively maintaining routes for frequently used destinations while

discovering new routes on demand when needed. Zone Routing Protocol (ZRP) and Temporally Ordered Routing Algorithm (TORA) are falling in this category.

One of our work is base on AODV routing protocol, the detail is explain in the following section.

1.4.4 Ad hoc On-Demand Distance Vector (AODV) routing protocol

The Ad hoc On-Demand Distance Vector (AODV) routing protocol is a reactive routing protocol used in mobile ad hoc networks (MANETs) and wireless mesh networks (WMNs). Unlike proactive protocols, AODV establishes routes only when required, reducing control overhead and improving efficiency. It ensures loop-free and dynamically maintained routes by using sequence numbers and route discovery mechanisms [30].

- **Route Discovery Process**

When a source node needs to communicate with a destination node but lacks an active route, it initiates route discovery using Route Request (RREQ) and Route Reply (RREP) messages[10].

Steps of Route Discovery

1. The source node broadcasts a Route Request (RREQ) message to its neighbors.
2. Intermediate nodes either forward the RREQ or reply if they have a valid route to the destination.
3. The destination node (or an intermediate node with an active route) sends a Route Reply (RREP) message back to the source.
4. The source node receives the RREP and begins data transmission.

- **Route Maintenance Process**

AODV maintains active routes and handles link failures using Route Error (RERR) messages[31].

Steps of Route Maintenance

1. If a link failure occurs, the affected node generates a Route Error (RERR) message and sends it upstream.
2. The source node, upon receiving the RERR, re-initiates the route discovery process if communication is still required.

- **Sequence Numbers and Route Freshness**

1. AODV uses sequence numbers to ensure that nodes always use the latest route information.
2. A node always selects the route with the highest sequence number, preventing loops and outdated routing paths [32].

AODV defines several message types for communication: RREQ, RREP, RERR, and HELLO messages as shown in the following tables[34].

Table 1.2: Route request(RREQ) message format of AODV

Field	Description
Type	Identifies the message as an RREQ
Hop count	Number of hops taken from the source
RREQ ID	Unique identifier for the request
Source IP Address	IP address of the requesting node

Source Sequence Number	Ensures route freshness
Destination IP Address	IP address of the destination node
Destination Sequence Number	Ensures the latest route is selected

Table:1.3. Route Reply (RREP) Message Format of AODV

Field	**Description**
Type	Identifies the message as an RREP
Hop Count	Number of hops from source to destination
Destination IP Address	Address of the destination node
Destination Sequence Number	Latest sequence number of the destination
Source IP Address	Address of the source node
Lifetime	Duration for which the route remains valid

Table: 1.4 Route Error (RERR) Message Format of AODV

Field	Description
Type	Identifies the message as an RERR
Unreachable Destination	Node that is no longer reachable
Unreachable Destination Sequence Number	Latest sequence number for unreachable destination
Source Node Address	Node reporting the error

- **HELLO Messages**
  - HELLO messages are periodically sent to maintain local connectivity between neighboring nodes.
  - They help detect link failures and keep routes active [31].

1.5 Security attacks in wireless Mesh Networks

Wireless Mesh Networks (WMNs) provide flexible and cost-effective communication in various applications. However, their open and decentralized nature makes them vulnerable to various security attacks. These attacks target the confidentiality, integrity, and availability of network communications, affecting the overall performance and reliability of WMNs [21]. These attacks can be classified into internal attacks and external attacks, internal attacks is launch by compromised node within the network where as external attacks is launch my illegitimate node. Also it can be classified into passive attack where an attacker does not alter or disrupt network traffic and Active attack where an attacker actively modifying, injecting, or disrupting network traffic, leading to severe performance degradation. Some of the possible attacks are explain in the following.

- **Eavesdropping** is a passive attack in wireless mesh networks (WMNs) where an unauthorized entity secretly intercepts and monitors data transmissions without altering them. This attack exploits the open nature of wireless communication, making it easy for adversaries within the transmission range to capture sensitive information, such as passwords, financial details, or private messages. Unlike active attacks, eavesdropping does not disrupt the network's functionality but poses a severe threat to data confidentiality and privacy [34]. In multi-hop networks like WMNs, eavesdropping can be both external and internal. External attackers monitor wireless signals within range, while internal attackers store copies of the data they forward without detection. This attack is often the first step before launching more complex security breaches, such as identity theft or traffic analysis. To mitigate eavesdropping, robust encryption protocols, secure key management, and intrusion detection systems should be implemented to ensure secure data transmission and maintain network integrity [21].

- A **traffic analysis attack** is a passive attack in wireless mesh networks (WMNs) where an adversary monitors communication patterns to infer sensitive information about network activities, even without directly accessing the data being transmitted. Since WMNs rely on wireless communication, attackers can easily observe network traffic, identifying frequently used routes, communication frequencies, and key nodes such as gateways or control points [34]. This attack is particularly dangerous in scenarios where network anonymity is critical, such as military or confidential corporate communications. By analyzing packet flow, attackers can determine which nodes are heavily communicating and predict network behavior, leading to further attacks such as denial-of-service (DoS) or targeted node compromise [21].To mitigate traffic analysis attacks, encryption alone is insufficient. Techniques such as traffic padding, anonymous routing protocols, and network obfuscation methods (e.g., onion routing or dummy traffic injection) can help disguise communication patterns and reduce the risk of information leakage.

- A **Denial-of-Service (DoS) attack** in Wireless Mesh Networks (WMNs) is a critical security threat where attackers attempt to disrupt normal network operations by overwhelming network resources, making them unavailable to legitimate users [34]. Since WMNs rely on multi-hop wireless communication, DoS attacks can target different layers of the network, including physical, MAC, and network layers. At the physical layer, attackers can jam communication channels by transmitting continuous noise signals, preventing legitimate nodes from accessing the network. At the MAC layer, attackers can exploit vulnerabilities in protocols like IEEE 802.11 by flooding the network with control packets, leading to collisions and excessive retransmissions. At the network layer, malicious nodes may participate in routing but drop packets selectively or flood the network with excessive route requests, exhausting resources [21].

- A **Wormhole Attack** is a severe security threat in Wireless Mesh Networks (WMNs), where an attacker establishes a low-latency link (tunnel) between two distant network nodes to manipulate routing and communication processes [35]. In this attack, an adversary captures packets from one part of the network and replays them in another location, creating the illusion of a shorter route. This deceptive shortcut can mislead routing protocols, resulting in network traffic being redirected through the wormhole, leading to disruption, selective forwarding, or even complete data interception. Wormhole attacks can occur even without compromising cryptographic security since they exploit routing vulnerabilities rather than encryption weaknesses. These attacks can significantly degrade network performance, cause routing loops, and increase packet loss[34].

- A **Black Hole Attack** is a severe security threat in Wireless Mesh Networks (WMNs), where a malicious node falsely advertises itself as having the shortest path to the destination, thereby attracting all traffic and subsequently dropping it instead of forwarding it [10]. This attack exploits routing protocols, especially in networks using on-demand routing mechanisms like AODV, by responding to route requests with fake route replies. Once the

attacker successfully diverts traffic, it can disrupt communication by discarding packets, leading to network degradation, increased packet loss, and denial of service. Unlike passive attacks like eavesdropping, a black hole attack directly affects network performance by isolating nodes from communication [36].

- A **Grayhole Attack** is a variation of the Black Hole Attack, where a malicious node selectively drops packets instead of discarding all traffic. This selective behavior makes it more challenging to detect than a traditional black hole attack [37]. The attacker first falsely advertises itself as having the best route to the destination. However, instead of dropping all packets like in a black hole attack, it selectively forwards some and discards others, often targeting control packets or specific data types. This attack degrades network performance by causing packet loss, increasing end-to-end delay, and disrupting communication. Because the attacker intermittently behaves normally, traditional detection methods like watchdog and acknowledgment-based mechanisms struggle to identify it [38].

- A **Byzantine Attack** occurs when a set of compromised or malicious nodes within a Wireless Mesh Network (WMN) work together to disrupt network communication by behaving arbitrarily and dishonestly. These nodes may drop, modify, or misroute packets, introduce loops, or delay packet forwarding, making detection complex and challenging [39].Unlike other attacks that originate externally, Byzantine attacks involve trusted network nodes, which makes them difficult to identify. The attacker can degrade network performance by creating routing inefficiencies, misdirecting traffic to congested paths, or falsely advertising optimal routes. This attack can lead to increased packet loss, high latency, and decreased throughput, thereby reducing the reliability of the network [40].

- A **Replay Attack** is a security threat in which an attacker intercepts and retransmits valid data packets to create unauthorized effects within a Wireless Mesh Network (WMN). The attacker does not necessarily modify the

message but replays it later to deceive the network into accepting it as a legitimate request. This attack exploits the absence of proper timestamping or sequence numbering mechanisms, allowing adversaries to gain unauthorized access, impersonate legitimate users, or disrupt communication [41].In WMNs, replay attacks can be particularly dangerous in authentication processes. An attacker may capture an authentication request and resend it to gain access to the network. This can lead to session hijacking, resource exhaustion, or even large-scale service disruptions [42].

- **A Man-in-the-Middle** (MITM) attack occurs when an attacker secretly intercepts and alters communication between two parties without their knowledge. In Wireless Mesh Networks (WMNs), MITM attacks exploit the open nature of wireless communication, allowing adversaries to eavesdrop, modify, or inject malicious data into the network [43].

  How MITM Attacks Work

  Eavesdropping – The attacker listens to ongoing communication between legitimate nodes.

  Packet Injection – Malicious data is inserted into the communication stream.

  Session Hijacking – Attackers impersonate one of the communicating parties to gain unauthorized access.

  Data Modification – Sensitive information such as authentication credentials or routing updates can be altered, leading to network disruption or data theft [44].

- **Rushing attacks,** which specifically target on-demand routing protocols like AODV, were among the first identified threats at the network layer in multi-hop wireless networks. These attacks take advantage of the route discovery process in such protocols. When a node needs a route to a destination, it broadcasts a Route Request (RREQ) message, distinguished by a unique

sequence number. To prevent excessive flooding, nodes forward only the first RREQ they receive and discard subsequent ones with the same sequence number. The protocol enforces a delay before forwarding RREQ messages to prevent collisions. However, in a rushing attack, a malicious node bypasses this delay and rapidly forwards the RREQ message to the destination node before any legitimate intermediate node. As a result, the malicious node becomes part of the route and can then drop data packets, effectively launching a denial-of-service (DoS) attack at the data plane.

- **Impersonation attacks** occur when an adversary attempts to adopt the identity of a legitimate node within a wireless mesh network. By spoofing a valid user node, the attacker can gain unauthorized access to network resources or intercept messages intended for the legitimate node. If the attacker impersonates a mobile node, they can take control of the victim's communications, leading to severe security breaches. In such cases, the adversary gains all privileges of the legitimate node, making detection challenging. Spoofing involves forging a valid MAC or IP address, which is particularly common in multi-hop networks like WMNs. In an IP spoofing attack, an adversary manipulates packet headers by inserting a false source address or replacing it with that of an authorized node. By using a spoofed address, the attacker can hijack active sessions and manipulate network traffic, posing significant security risks.

1.5.1 Layer-Wise Security Issues in Wireless Mesh Networks

Wireless Mesh Networks (WMNs) operate across multiple layers of the network stack, each of which presents unique security vulnerabilities. Addressing these security threats requires a comprehensive approach to ensure the integrity, confidentiality, and availability of network communications [21].

- **Physical Layer Security Issues**

  The physical layer in WMNs is susceptible to jamming attacks, where an adversary intentionally emits radio frequency signals to disrupt communication. Eavesdropping is another concern, as attackers can passively intercept wireless transmissions. Additionally, physical tampering with mesh nodes can compromise the network's security [26].

- **Data Link Layer Security Issues**

  The data link layer is vulnerable to MAC address spoofing, where attackers impersonate legitimate nodes to gain unauthorized access. Traffic injection attacks and replay attacks exploit the lack of proper authentication mechanisms. Furthermore, denial-of-service (DoS) attacks can be launched by flooding the network with bogus frames, leading to congestion and service disruption [45]

- **Network Layer Security Issues**

  Routing-based attacks pose significant threats at the network layer. Black hole and gray hole attacks involve malicious nodes selectively dropping packets, disrupting communication. Wormhole attacks allow attackers to create a fake shortcut in the network, leading to routing misdirection. Additionally, rushing attacks exploit route discovery mechanisms in on-demand routing protocols to manipulate path selection [21].

- **Transport Layer Security Issues**

  The transport layer faces threats such as session hijacking, where an attacker intercepts and takes control of an active communication session. SYN flooding is another attack that exploits the TCP handshake mechanism, leading to resource exhaustion. Man-in-the-middle (MITM) attacks allow adversaries to intercept and alter communication between two nodes [26].

- **Application Layer Security Issues**

  At the application layer, malware attacks, phishing, and distributed denial-of-service (DDoS) attacks are common threats. Attackers can exploit software vulnerabilities to inject malicious code or steal sensitive information. Additionally, inadequate authentication mechanisms can lead to unauthorized access to critical applications and services [45]

1.5.2 Security Services in Wireless Mesh Networks (WMNs)

Wireless Mesh Networks (WMNs) provide flexible, scalable, and self-organizing communication infrastructure. However, their open and decentralized nature makes them vulnerable to various security threats. To mitigate these threats, WMNs require robust security services that ensure confidentiality, integrity, authentication, availability, and non-repudiation [21].

- **Confidentiality**

  Confidentiality ensures that transmitted data is only accessible to authorized users and is protected from eavesdropping attacks. Encryption techniques such as Advanced Encryption Standard (AES) and Public Key Infrastructure (PKI) help maintain data privacy. End-to-end encryption (E2EE) secures communication between nodes, preventing unauthorized interception [26].

- **Integrity**

  Integrity guarantees that data remains unaltered during transmission. Cryptographic hash functions such as SHA-256 and Message Authentication Codes (MACs) help detect unauthorized modifications. Digital signatures ensure message authenticity and prevent man-in-the-middle (MITM) attacks [45]

- **Authentication**

  Authentication verifies the identity of users and devices before granting network access. Extensible Authentication Protocol (EAP), 802.1X authentication, and challenge-response mechanisms are commonly used. Mutual authentication ensures that both the sender and receiver validate each other, preventing impersonation attacks [21].

- **Availability**

  Availability ensures that network resources and services remain accessible despite attacks such as Denial-of-Service (DoS) and Distributed DoS (DDoS). Intrusion Detection Systems (IDS), firewalls, and load balancing mechanisms help mitigate service disruptions. Redundant routing and self-healing capabilities of WMNs enhance network resilience [26].

- **Non-Repudiation**

  Non-repudiation prevents entities from denying their actions. Public Key Infrastructure (PKI) and digital signatures ensure that messages and transactions are traceable to their origin, preventing malicious nodes from repudiating their activities. Log auditing mechanisms further support accountability [45]

1.5.3 Layer-Wise Security Mechanisms for Wireless Mesh Networks (WMNs)

Wireless Mesh Networks (WMNs) require robust security mechanisms at each layer of the network stack to counteract various threats. Implementing a layered security approach enhances the network's resilience against attacks while ensuring secure communication [21].

- **Physical Layer Security Mechanisms**

  To protect against jamming attacks, spread spectrum techniques such as frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) can be employed. Directional antennas and power control mechanisms help reduce signal interception and mitigate eavesdropping risks. Physical security of nodes should also be ensured through tamper-resistant hardware [26].

- **Data Link Layer Security Mechanisms**

  MAC address filtering and access control lists (ACLs) prevent unauthorized access to the network. To counter replay attacks, time-stamped authentication mechanisms and sequence numbers are used. 802.1X-based authentication with Extensible Authentication Protocol (EAP) ensures secure access control. Frame filtering helps mitigate traffic injection attacks, while strong encryption methods like AES (Advanced Encryption Standard) provide data confidentiality [45]

- **Network Layer Security Mechanisms**

  To defend against black hole and gray hole attacks, secure routing protocols such as Secure AODV (SAODV) and Secure Optimized Link State Routing (SOLSR) validate route authenticity. Wormhole attack prevention can be achieved through packet leashes and geographic routing verification. Intrusion Detection Systems (IDS) at the network layer can identify and respond to anomalies in routing behavior. Authentication mechanisms, such as digital signatures and hash chains, help prevent rushing and spoofing attacks [21].

- **Transport Layer Security Mechanisms**

  To mitigate session hijacking and SYN flooding attacks, Transport Layer Security (TLS) and Secure Socket Layer (SSL) encryption are implemented.

Rate-limiting techniques prevent excessive connection requests from overwhelming the network. End-to-end authentication mechanisms, such as IPsec (Internet Protocol Security), ensure secure data transmission [26].

- **Application Layer Security Mechanisms**

  Protecting against malware and phishing attacks requires intrusion detection systems (IDS) and firewalls that analyze network traffic. DDoS mitigation techniques, including rate limiting and traffic filtering, help prevent service disruptions. Strong authentication mechanisms, such as two-factor authentication (2FA) and public key infrastructure (PKI), enhance security at the application level. Regular software updates and patch management help eliminate vulnerabilities that attackers may exploit [45]

1.6 Motivation of thesis

Wireless Mesh Networks (WMNs) are rapidly gaining popularity as an appealing communication technology due to their cost-effectiveness and ease of deployment. As the size and demand for WMNs continue to expand, ensuring robust security becomes a significant challenge in such large-scale network environments. Much like mobile ad hoc networks (MANETs), WMNs currently lack highly efficient and scalable security mechanisms. Their security is particularly vulnerable and can be compromised more easily due to various inherent characteristics, ultimately exposing them to both external threats and internal attacks. Some of the factors that leads to security attack are discussed below:

- Decentralized nature of the network architecture makes it easier for adversaries to carry out attacks.
- The exposure of both channels and nodes within the shared wireless medium disrupts the regular functioning of the routing protocol.
- Dynamic topology restrict the existence of Central trusted authority.

- Attacks targeting various protocol layers can easily disrupt the entire network. An attacker can infiltrate the network, inject harmful packets, and pose as a legitimate node. Once inside, a malicious node can interfere with the regular functioning of the routing protocol, ultimately degrading the network's overall performance.

A commonly adopted defense mechanism involves authentication and authorization processes. In wireless LANs, these functions are handled through Authentication, Authorization, and Accounting (AAA) services, either directly at the access point or via gateways. However, AAA in these networks typically relies on a centralized server. This centralized approach is unsuitable for wireless mesh networks (WMNs). Furthermore, managing security keys in WMNs is significantly more challenging than in wireless LANs, as there is no central authority, trusted third party, or dedicated server to oversee key distribution and management.

Wireless mesh networks are exposed to a wide range of malicious attacks, which makes it essential to design effective mechanisms to ensure secure communication. Existing security solutions introduce various techniques such as authentication methods, secure routing protocols, and packet authentication schemes to mitigate these attacks. However, these approaches often suffer from high communication costs, computational overhead, and node compromise issues. Furthermore, most of the available security solutions were initially developed for wireless LANs and MANET, making them less suitable for the dynamic and decentralized nature of WMNs. Additionally, much of the current research focuses on defending against external threats such as unauthorized access, impersonation, and denial-of-service (DoS) attacks, while limited attention has been given to internal threats like sinkhole, wormhole, and blackhole attacks. Although several studies have been conducted to enhance WMN security, further advancements are still needed to develop reliable, scalable, and cost-effective security solutions tailored specifically for wireless mesh networks.

1.7 Problem Definition

The objective of this research is to develop effective security mechanisms that address user (Client) authentication, secure routing, and Data(packet) Authentication, ensuring reliable and secure communication within Wireless Mesh Networks.

- **Authentication:** The objective is to develop an efficient authentication protocol that establishes authentication protocol between MCs and Mesh Routers (MRs), and among MRs themselves. This will be achieved using a combination of symmetric and asymmetric key cryptography to ensure that unauthorized users are denied access to the network. Additionally, the mechanism will prevent adversaries from infiltrating the network and gaining unauthorized access.

- **Secure Routing:** The objective is to develop an effective detection mechanism to identify compromised nodes within the network that attempt to divert legitimate traffic towards malicious paths/Nodes. This detection process will rely on monitoring the behavior of neighboring nodes using techniques such as hop-count analysis and trust-based evaluation. By applying these techniques, the proposed mechanism aims to prevent internal attacks and ensure secure and reliable routing for data transmission within Wireless Mesh Networks (WMNs).

- **Data Authentication:** Safeguarding communication traffic requires ensuring both confidentiality through encryption and maintaining the integrity and authenticity of transmitted messages. Protecting integrity not only covers the accuracy of individual messages but also ensures the correct order and delivery sequence, preventing replay, reordering, or deletion attacks. To achieve this, a robust data packet authentication protocol is introduced, utilizing efficient cryptographic techniques to enhance message security within the network.

1.8 Thesis Contribution

In this research work, effective methods are proposed to ensure secure communication in Wireless Mesh Networks (WMNs). These methods incorporate three primary mechanisms:

- **Authentication:** For ensuring secure authentication among various mesh entities in WMNs, we propose two distinct protocols. The first protocol introduces Fast authentication and secure handover mechanism based on a pre-own ticket, which facilitates secure authentication between users (Mesh Clients - MCs) and the Access point (Mesh Router - MR). The second protocol focuses on enhancing the handoff process by proposing an efficient handoff authentication scheme between clients and Mesh Access Points (MAPs). During handover, different types of tickets are employed to establish mutual authentication between mesh entities, ensuring a seamless and secure transition as clients move across the network.

- **Secure Routing:** To create a secure and reliable logical communication path within WMNs, we propose trust base detection of malicious node that attract network traffic towards itself, the proposed mechanism identify malicious nodes attempting to collectdata traffic and drop it instead of forwarding to next node, ultimately leading to internal attacks. The proposed protocol presents a trust-based framework that maintain a list of trusted node from previous experience, a malicious node attempting to behave as a legitimate node is identified by cross checking.

- **Data Authentication:** To ensure data packet authentication among mesh entities within WMNs, we propose an efficient common key scheme that verifies each packet as it traverses through multiple hops. This multi-hop packet authentication ensures that data remains secure at each relay point, preventing tampering or forgery. Additionally, the protocol is further extended by incorporating a pre-shared pairwise key mechanism, where unique keys are established between communicating nodes in advance. This

approach not only enhances packet integrity but also effectively mitigates the risk of malicious packet injection and impersonation attacks, ensuring that only verified nodes participate in the communication process. Together, these mechanisms strengthen overall packet security and improve the trustworthiness of data exchange within the wireless mesh network.

1.9 Thesis Organization

This thesis is organized into multiple chapters, each addressing key components of Wireless Mesh Network (WMN) security, including authentication, secure routing and data authentication. The organization is as follows:

Chapter 1 – Introduction: This chapter provides a detailed overview of wireless networks, including types of wireless and ad hoc networks, with a special focus on Wireless Mesh Networks (WMNs). It discusses their architecture, characteristics, applications, routing protocols, and security challenges. The chapter also outlines the motivation for this research, defines the problem, states the research objectives, summarizes the main contributions, and presents the overall organization of the thesis.

Chapter 2 – Literature Review: A critical review of existing research is presented, covering various authentication protocols, handoff authentication, routing security schemes and data authentication mechanisms approaches in WMNs. The limitations and research gaps identified in the literature serve as the foundation for the proposed solutions.

Chapter 3 – Mutual Authentication and Secure Handover Protocol for Wireless Mesh Network: This chapter proposes authentication protocols aimed at securing communication between Mesh Clients (MCs) and Mesh Routers (MRs), as well as among MRs. It introduces ticket-based methods combining symmetric and asymmetric cryptography to ensure efficient and secure user authentication.

Chapter 4 – Pre-distributed Ticket Base Client Handoff Authentication Protocol For Wireless Mesh Network: This chapter focuses on the fast handoff

authentication problem in WMNs, where mobile clients move between different mesh routers. The proposed protocol reduces handoff latency and authentication delay through pre-issued tickets and optimized message exchanges, ensuring seamless and secure transitions without involving a central authority.

Chapter 5 – Enhancement of AODV Routing Protocol To Counter Black hole Attack: A trust-based routing mechanism is introduced to detect and mitigate internal threats especially black hole attacks for AODV routing protocol. The system evaluates node behavior based on trust metrics and hop-count consistency, ensuring that routing paths are both secure and reliable.

Chapter 6 – Common Group Key Generation Protocol for Hop by Hop Packet Authentication for Wireless Mesh Network: This chapter presents a lightweight multi-hop packet authentication scheme using common and pairwise pre-shared keys. It ensures message integrity, prevents tampering, and defends against replay and impersonation attacks while maintaining low communication overhead.

Chapter 7 – Conclusion and Future Work: The final chapter summarizes the key findings of the research, highlighting the contributions made toward improving WMN security. It also outlines potential future directions, including the integration of AI-driven security models and support for heterogeneous mesh environments.

1.10 summary

Chapter 1 provides an overview of wireless networks with a special focus on Wireless Mesh Networks (WMNs). It introduces different types of wireless and ad hoc networks, highlighting the advantages and challenges of WMNs in comparison to Mobile Ad Hoc Networks (MANETs). The chapter discusses WMN architecture, characteristics, applications, and common routing protocols, with emphasis on the AODV protocol. It also outlines major security threats, including internal and external attacks, and proposes the need for efficient authentication, secure routing, and data authentication mechanisms. Finally, it presents the research motivation, objectives, contributions, and organization of the thesis.

Chapter 2

LITERATURE REVIEW

Wireless Mesh Networks (WMNs) have emerged as a practical solution for providing scalable, flexible, and cost-effective wireless connectivity. However, their decentralized structure and open communication environment expose them to numerous security threats, including unauthorized access, routing manipulation, and packet tampering. Robust authentication is a fundamental requirement to ensure only legitimate users and devices can access the network. Various methods, such as pre-shared keys, certificate-based authentication, and identity-based cryptography, have been proposed, but many struggle to achieve efficiency, scalability, and resilience to internal attacks. In addition, mobile users require fast and secure handoff authentication to maintain seamless connectivity across different mesh routers. While ticket-based schemes and cryptographic techniques have been developed to reduce handoff delays, issues such as increased communication overhead and vulnerability to impersonation attacks persist. Similarly, secure routing is crucial to prevent attacks like black hole, gray hole, and wormhole attacks, but existing trust-based or cryptographic routing approaches often face limitations in detection accuracy and scalability. Finally, packet authentication plays a key role in safeguarding data integrity across multi-hop networks. Despite the use of cryptographic keys and hashing mechanisms, packet-level security solutions often introduce computational overhead and fail to address sophisticated attacks. This chapter reviews these research challenges and gaps in detail.

2.1 Authentication

Authentication is a critical concern in Wireless Mesh Networks (WMNs). Preventing unauthorized users from accessing the network without permission is essential to maintain security and ensure that adversaries cannot infiltrate the network to disrupt its normal operations. However, due to the open nature of wireless communication, providing robust authentication in WMNs is challenging. Adversaries can easily

eavesdrop on messages exchanged within the network and inject fabricated or replayed messages into the communication channels.

To prevent unauthorized access and ensure secure communication. Two prevalent authentication methods in WMNs are Pre-Shared Key (PSK) authentication and certificate-based authentication.

Pre-Shared Key (PSK) Authentication: In this approach, a secret key shared in advance among nodes is used to verify identities. There are two types of shared keys:

- **Pair-wise Key**: A unique key shared between two nodes, such as between a user node (UN) and an authentication server (AS), or between neighboring mesh nodes (MNs).
- **Group Key**: A common key shared among all nodes within a specific group.Regularly updating PSKs is essential to defend against potential statistical attacks by adversaries.

Certificate-Based Authentication: This method requires nodes to present a digital certificate containing their public key, which is verified and signed by a trusted Certificate Authority (CA). Typically, each legitimate user obtains a certificate from the CA within their domain. However, challenges arise when users roam across different domains, necessitating solutions for cross-domain authentication. Additionally, the IEEE 802.11s standard introduces the Simultaneous Authentication of Equals (SAE) protocol, a password-based authentication and key establishment method designed for peer-to-peer scenarios in WMNs. SAE is based on the Diffie-Hellman key exchange and is utilized in both IEEE 802.11s mesh networking and WPA3 for secure initial key exchanges. These authentication mechanisms are vital for securing WMNs against unauthorized access and potential attacks, ensuring the integrity and reliability of the network.

One of the significant advantages of Wireless Mesh Networks (WMNs) is their support for user node (UN) mobility. To maintain network security, it's essential to authenticate roaming UNs effectively. As a mobile node moves, it must continuously

discover neighboring nodes within its communication range. Upon identifying a new neighbor, mutual authentication between the two nodes is necessary. Additionally, if a node re-enters the range of a previous neighbor, re-authentication is crucial to prevent adversaries from exploiting the interval between the last and current associations, thereby mitigating potential impersonation attacks. To address these challenges, various authentication protocols have been proposed to support fast and secure handovers in WMNs. For instance, some protocols focus on reducing authentication latency during handovers by utilizing pre-established keys or tickets, ensuring that mobile nodes can quickly and securely reconnect to the network as they move. Implementing robust authentication mechanisms is vital for maintaining the security and efficiency of WMNs, especially in scenarios involving frequent node mobility.

While many authentication schemes in Wireless Mesh Networks (WMNs) focus on verifying user nodes (UNs), the authentication of mesh nodes (MNs) is often overlooked. This oversight can expose the network to various attacks, such as impersonation, sinkhole, and wormhole attacks. To mitigate these threats, it's essential to establish mechanisms that allow UNs to authenticate MNs and enable mutual authentication between MNs. However, implementing these authentication protocols must be balanced against the potential overhead they introduce, considering that wireless users and MNs often have constraints related to battery life, processing power, and memory capacity.

In 2006, Wei et al. Proposed seamless handoff support in wireless mesh networks, aiming to minimize packet loss during the handoff process. It proposes two data caching mechanisms: En-route and Promiscuous, which cache data at nodes on the flow route and nodes overhearing packet transmission, respectively. The proposed caching mechanisms incur no extra network overhead and improve data availability, reducing packet loss and delay, and significantly improving VoIP quality. The proposed caching mechanisms, while effective for improving handoff performance and minimizing packet loss, may introduce some security concerns such as Data exposure to unauthorized node due to overhearing, Cached data manipulation in case

if the node is compromised which can farther launch replay attack, the caching mechanisms do not incorporate strong authentication and encryption methods, there could be a lack of confidence in the data being cached. This can hinder the trustworthiness of the data packets being forwarded, especially if the packets are cached by nodes that do not have verified identities[46].

In 2008, Xu et al. perform analysis on fast EAP re-authentication protocol and compared with EAP-TSL performance. The EAP re-authentication protocol provides a consistent, method-independent, and low latency re-authentication mechanism for intra-domain handoff authentication, the authentication delay of the EAP re-authentication protocol is significantly less than that of the EAP-TLS protocol. The EAP re-authentication Protocol (ERP) derives an Extended Master Session Key (EMSK) in initial EAP exchange to generate a re-authentication Root Key (rRK) for subsequent handovers. The local server derives a re-authentication MSK (rMSK) from the rRK and distributes it via an EAP-Re-auth message, enabling local re-authentication without communicating with the home server. The handover begins with EAP-Initiate/Re-auth-Start and EAP-Initiate/Re-auth messages between the mobile terminal and the new authenticator. Even though ERP out perform EAP-TSL in Authentication Delay, Message Exchange Requirement, Efficiency in Key Management and Security Computation Cost, It have certain drawback such as absent of Client certificate that can lower security risk, Dependent on local authentication server that may be compromised and Limited Use of Extended Master Session Key(EMSK)[47].

In 2012, Zhang et al. proposed Identity base handoff authentication scheme, The proposed scheme comprise of two steps Handoff preparation and Handoff initialization. In the first phase The mobile node (MN) contacts the identity-based private key generator (PKG) and provides its identity information (e.g., MAC address). The PKG generates and sends back a private key to the MN and similarly does the same for the new AP that it intends to connect to. This ensures that both entities have their private keys ready for subsequent interactions. In second step the

MN communicates with the new AP to initiate the handoff process. The steps carries out in this process is as follows:

Key Derivation: When the MN enters the coverage area of AP2, it begins the authentication process. The MN first derives a cryptographic key (Kc) and additional parameters needed for this procedure. This step includes generating a random number (kc) for the key derivation process, which enhances security by introducing randomness.

Generating Message: The MN computes a message (mc) based on the derived key (Kc). This message acts as authentication information that proves the MN's identity to AP2. The MN effectively creates a message that encapsulates identity verification data.

Sending Encrypted Message to AP2:The MN encrypts the previously derived message using the key (Kc) and sends it to AP2. This encrypted message typically contains the MN's identity and session-related data that AP2 will need to authenticate the MN.

AP2 Computes its Response: Upon receiving the encrypted authentication request from the MN, AP2 uses its own private key (derived from the PKG) to compute its response. This includes generating its own cryptographic key for communication with the MN and ensuring that all exchanges remain confidential.

AP2's Response to MN: AP2 sends a response back to the MN, which includes a verification/challenge information intended to confirm its identity. This response helps ensure that the MN has not only connected to an AP that can be trusted, but it also validates that AP2 is indeed the correct AP that the MN wishes to associate with.

MN Validates AP2:The MN computes its version of the response from AP2 by using the information obtained from AP2's public key and its own secret key. If the computed value matches the information received from AP2, the MN can be confident it is communicating with a legitimate AP.

Final Verification and Key Agreement: Finally, the MN sends its verification information back to AP2, completing the mutual authentication process. Both parties, having successfully validated each other, proceed to agree on a session key (PTK) that will be used for the duration of their communication. This key agreement is crucial for maintaining the confidentiality of their subsequent data exchanges[48].

The proposed scheme is resistance to passive eavesdropping, impersonation attacks, replay attacks, and man-in-the-middle attacks, also achieve forward/backward secrecy. But the reliability of PKG is a big issue in terms of security.

In 2013, Li et al. proposed ticket base authentication protocol, It consist of two parts Login authentication and Handover authentication. Both the protocols. Both depends on three types of keys- a pairwise master key (PMK), a pairwise transient key (PTK)and a group transient key (GTK) for authentication between mesh entities. As mesh clientswere restricted with power constraint the exchanged of these keys should be minimized. Securitythreat lied in both Login and Handover Authentication Protocols. Firstly, during LAP the N_{M2}, $N_{C2}$and Θ_C were transmittedin a plaintext format as C→ MAP_1: N_{M2}in step 5 and MAP1 →C: N_{C2}, $\Theta_C$in step 6.

Therefore, attacker could easily obtained the nonce and transfer ticket Θ_C and misused it. Secondly, during HAP the Θ_C are transmitted in the plaintext format as C →MAP_x: Θ_C,N_{C2}, V_{KMAC} (N_C). Therefore, intruder could easily tampered the integrity of the transfer ticket Θ_C which involved I_C, where I_C was rarely changed.

In their scheme, authentication was done within one hop between the client and requesting MAP which is good achievement However, Sharing Nonce in login authentication and transfer ticket in plaintext form and redistributing the similar ticket among other MAPs could violate the security[49].

In 2014, Xu et al. proposed ticket base handoff authentication , The proposed protocol presents a novel scheme aimed at enhancing the efficiency of handoff processes in wireless mesh networks (WMNs). It introduces a localized handoff mechanism that allows mobile clients (MCs) to communicate seamlessly with target

mesh routers (MRs) while minimizing handoff latency without altering the original authentication protocol. The proposed scheme is lightweight, making it suitable for mobile users in power-constrained environments, as it relies on user-carrying tickets and symmetric key operations, which do not require third-party involvement for re-authentication. However, the paper acknowledges certain limitations, such as the additional storage overhead of 1344 bits for tickets of candidate MRs, which may be a concern for MCs with limited storage capacity. Despite this, the authors argue that this overhead is negligible compared to the overall storage capabilities of mobile terminals. The scheme also demonstrates resilience against various attacks, including eavesdropping and replay attacks, enhancing its security profile. The paper presents a trusted handoff protocol designed for Wireless Mesh Networks (WMNs), emphasizing the need for mobile nodes to complete access authentication with minimal delay while ensuring security for both the nodes and the handoff network[50].

In 2014, Xiao et al. proposed a trusted handoff protocol designed for Wireless Mesh Networks (WMNs), emphasizing the need for mobile nodes to complete access authentication with minimal delay while ensuring security for both the nodes and the handoff network. The proposed protocol incorporates several technologies, including a hierarchical network model, Elliptic Curve Cryptography (ECC), trust evaluation, and grey relevance analysis. It mandates that the mobile platform's configuration be measured prior to accessing the handoff network, allowing only those that meet security requirements to connect. The authors claim that their protocol outperforms the Efficient Mesh Security Association (EMSA) authentication scheme in terms of success rate and average delay, as verified through formal analysis and simulation[51].

However, the paper acknowledges limitations, particularly in addressing the handoff process within WMNs, as EMSA does not adequately meet performance and identity protection requirements during handoff . Additionally, the selection of appropriate FHR members and the establishment of secure connections with them are not sufficiently explored .

In 2016 Lai et al. presents a review of Li et al.'s fast handover authentication mechanism for wireless mesh networks, highlighting its limitations and proposing an improved protocol. The authors identify that Li et al.'s approach suffers from security vulnerabilities, such as the transmission of sensitive information in plaintext and reliance on high-quality tamper-proof devices (TPDs), which restricts its applicability in real-world scenarios. The proposed new mechanism addresses these issues by enhancing security and scalability while preserving client privacy, making it suitable for devices with limited computational power[52].

The authors emphasize that their improved handover authentication protocol not only meets essential security requirements but also outperforms existing protocols in terms of authentication delay. However, they acknowledge that while the new handover authentication protocol is more secure, the paper contributes to the field by proposing a more efficient and reliable solution for handover authentication in wireless networks. Overall there is room for enhancing the performance in terms of efficiency by reducing computational complexity without compromising security.

In 2016 Yang et al. presents a novel design for handoff authentication in wireless mesh networks (WMN), aimed at reducing delays associated with handoff processes. The authors introduce an attribute-based encryption (ABE) method for key pre-distribution messages, which ensures constant computation and communication costs, independent of the number of neighboring mesh routers. This design allows for immediate handoff authentication upon completion of login authentication, enhancing the efficiency of the process. Additionally, the security of the proposed protocol is bolstered by incorporating the home mesh router's digital signature in the handoff ticket and key pre-distribution messages, effectively mitigating forgery attacks[53].

However, the paper acknowledges limitations related to the distribution of pairwise master keys (PMKs). As the number of mobile users increases, the PMK distribution can become burdensome and consume significant network bandwidth, which may hinder scalability . Overall, while the proposed scheme offers a secure and efficient

solution for WMN, the challenges associated with PMK distribution remain a critical concern.

In 2016, Geetanjali and Hemraj presents a Fast Handoff Technique (FHT) aimed at reducing handoff latency in Wireless Mesh Networks (WMN). It highlights the challenges faced during the handoff authentication process, particularly the delays that occur when a roaming client connects to a Foreign Mesh Router (FMR) and needs to authenticate itself to access network services. The proposed technique addresses these issues by generating tickets for handoff authentication, which minimizes both computation and communication overhead, thus enhancing efficiency. However, the paper also acknowledges existing limitations in previously proposed techniques, such as security threats, computational overhead, and communication overhead, which still persist despite improvements. The authors emphasize the need for a resilient technique that overcomes these drawbacks while maintaining low latency. The evaluation of FHT against other methods, such as Ticket Handoff Authentication (THA) and secure Context Transfer Protocol (CTAR), demonstrates its effectiveness in reducing handoff latency and computational overhead[54].

In 2016, Yang et al. present a new handover authentication protocol designed for wireless networks, addressing the increasing access requirements and the challenges of ensuring security and efficiency in such environments. The proposed protocol aims to provide user anonymity and untraceability while achieving high efficiency, which are critical features for protecting user privacy in mobile internet services[55].

However, the paper acknowledges limitations in existing protocols, such as inefficiencies and failure to provide user untraceability, which the proposed protocol aims to overcome .

Despite its advantages, the paper does not detail specific performance metrics or comparisons with other protocols, which could provide a clearer understanding of its effectiveness in practical scenarios. This lack of empirical data may limit the assessment of its real-world applicability.

In 2017, Sharma et al. presents a security architecture for Wireless Mesh Networks (WMN) aimed at enhancing authentication and attack detection, particularly against cloned Access Point (AP) attacks and internal threats. It highlights the need for effective security mechanisms in WMNs, which are often vulnerable to various attacks due to their architecture that connects mobile users wirelessly while maintaining wired connections at higher levels to mitigate energy constraints and node failures . The proposed architecture utilizes trusted routers for authentication and employs gateways to detect cloned APs by cross-referencing new AP information with an existing database[56].

One of the key advantages of the proposed solution is its ability to provide better detection accuracy while reducing computational and communication overheads, thus improving overall network performance . However, the paper acknowledges that the cost of achieving privacy and security in WMNs is high, which may limit the implementation of such security measures. Additionally, the paper notes that existing security mechanisms are limited, indicating a gap in the current research landscape that needs to be addressed .

In 2017Zhou et al. presents a lightweight identity authentication protocol (LIAP) designed for vehicular ad-hoc networks (VANETs), focusing on enhancing security during vehicle handover between road-side units. LIAP utilizes a dynamic session secret process, which offers advantages such as resistance to major existing attacks and improved efficiency with low resource consumption . However, the authors identify significant limitations, including the lack of user location privacy protection and vulnerability to parallel session attacks . To address these issues, the paper proposes enhancements that concatenate the terminal's pseudo-identity with a random number, encrypting this information to mitigate user location tracking risks . Despite these improvements, the protocol still faces challenges related to computational overhead due to the required operations, which may affect performance[57].

In 2018,Nanda et al. presents a comprehensive overview of security schemes related to authentication in dynamic wireless mesh networks, highlighting their limitations

and challenges . It introduces the Geo Location Oriented Routing (GLOR) protocol and discusses its existing authentication scheme, proposing enhancements through a lightweight hybrid authentication model .The proposed scheme is designed to address the limitations of the previous protocols, which often hinder the full potential of mesh networks due to their reliance on static protocols and rigid security frameworks[58].

The authors emphasize the importance of authentication in ensuring network security, particularly as dynamic mesh networks evolve and are adopted in various fields. They propose three scenarios for their hybrid authentication scheme: full authentication, quick authentication, and new node authentication, which aim to improve resource utilization and defend against security threats. However, a significant limitation noted is that mobile devices may not always have access to the authentication server, potentially restricting network expansion and coverage.

In 2018, Geetanjali and Hemraj presents a novel approach to authentication in Wireless Mesh Networks (WMNs) using Elliptic Curve Diffie-Hellman (ECDH) cryptography, aimed at reducing authentication latency and communication overhead. The proposed mechanism is designed to enhance the efficiency of the authentication verification process while ensuring security. The authors compare their method with existing schemes, particularly focusing on the performance metrics such as authentication delay and computational overhead, demonstrating that their approach significantly reduces these issues compared to traditional methods like polynomial-based key generation[59].

However, the paper acknowledges certain limitations. While the ECDH method improves authentication speed, it may still be vulnerable to specific attacks, such as Denial of Service (DoS) attacks, which can affect the overall security of the network. Additionally, the complexity of implementing such cryptographic techniques in real-world scenarios may pose challenges. The authors emphasize the need for further research to address these vulnerabilities and enhance the robustness of the proposed authentication mechanism.

In 2018, Wang et al. presents an anonymous batch handover authentication protocol designed for wireless mesh networks (WMNs), addressing the challenges posed by frequent handover events due to client mobility. The proposed protocol utilizes group signature techniques to pre-distribute handover keys, enhancing both efficiency and security in the handover authentication process. Unlike existing protocols, it avoids group signature correlation operations during the authentication phase, which contributes to improved performance. However, the paper does not explicitly discuss limitations of the proposed protocol, which could include potential vulnerabilities in the group signature technique or scalability issues in larger networks. Additionally, while the performance analysis indicates better efficiency compared to related protocols, it lacks a comprehensive comparison with all existing methods [7][9]. Overall, the paper contributes valuable insights into secure handover authentication in WMNs but could benefit from a more thorough exploration of its limitations[60].

In 2019, Geetanjali and Hemraj proposes a secure handoff procedure for mesh clients, focusing on generating tickets that facilitate authentication as clients move between different zones of mesh routers. The authentication server plays a crucial role by generating and updating tickets based on the clients' zonal router ranges, thereby reducing storage overhead and enhancing security by centralizing ticket management. The proposed technique aims to mitigate issues related to authentication delay and various probabilistic scenarios, demonstrating its legitimacy through empirical analysis[61].

However, the paper identifies several limitations. The communication between mesh routers (MRs) during the handoff process may expose the system to security threats such as Denial of Service (DoS) attacks and message forging, which can lead to significant delays and communication overhead. Additionally, the pre-distribution of keys can incur extra traffic overhead, and the storage of keys and tickets at mesh clients may lead to resource constraints, including memory and energy consumption issues.

In 2019, Geetanjali et al. presents a secure handoff procedure designed for wireless mesh networks (WMNs), focusing on the generation and assessment of tickets for

mesh clients (MCs) distributed among various zones of mesh routers (MRs) based on their transmission range. A trusted third-party authentication server is proposed to manage the ticketing process, which enhances the security and efficiency of handoffs when MCs move outside the range of their current MR. The mechanism aims to reduce storage overhead and security threats by ensuring that tickets are stored distributively across MRs, thus validating the authenticity of handoff clients effectively[62].

However, the paper identifies limitations in the ticket-based handoff approach, particularly concerning security vulnerabilities such as message forging and denial-of-service (DoS) attacks, which can lead to communication overhead and delays during the handoff process. Additionally, the basic approach requires MRs to communicate with the home MR for every client, resulting in repeated authentication processes that can slow down the handoff.

In 2019, Amit Kumar Roy and Ajoy Kumar Khan presents a comprehensive study on Wireless Mesh Networks (WMNs), emphasizing the critical need for efficient key management and authentication mechanisms to address security vulnerabilities inherent in these networks. It proposes a group key agreement protocol based on the Diffie-Hellman protocol and digital signatures, facilitating secure authentication between a trusted authority (TA) and mesh clients, which enhances communication efficiency and reduces packet loss due to attacks . The authors highlight the importance of clustering WMNs into groups to implement effective security measures[63].

However, the proposed scheme has limitations, such as the burden of pre-loaded keys on network members, making it suitable only for small, fixed networks . Additionally, while the protocol improves communication and computational costs.

In 2019, Xiang et al. presents a novel blockchain-based authentication protocol designed to enhance security in WLAN mesh networks. It emphasizes the necessity of secure authentication for both users and access points (APs) to mitigate vulnerabilities associated with traditional methods, which often rely on centralized

servers and public key infrastructures (PKI). The proposed method treats user authentication requests as transactions, utilizing a public ledger to monitor and manage malicious attacks effectively. One of the key advantages of this approach is its ability to reduce deployment costs and eliminate the need for key delivery systems, thereby streamlining the authentication process. Additionally, the results indicate that the blockchain-based authentication can significantly decrease authentication delays in multi-hop environments, which is crucial for maintaining performance in wireless networks[64].

However, the paper acknowledges limitations, such as the need for additional configurations of trusted third-party agencies for effective deployment and the potential for increased complexity in managing the blockchain infrastructure.

In 2020, Amit Kumar Roy and Ajoy Kumar Khan presents a novel authentication protocol designed to enhance the efficiency of handover processes in mobile devices accessing the Internet through mesh networks. It emphasizes the necessity for a reliable and efficient authentication scheme to mitigate issues such as temporary disconnection, authentication delays, and unauthorized access, particularly during the transition between mesh access points (MAPs). The proposed protocol aims to ensure mutual authentication between the client and MAP while preserving the privacy of the transfer ticket[65].

However, the paper identifies several limitations in existing protocols, including the transmission of sensitive information in plaintext, which exposes users to security threats. Additionally, the reliance on multiple key types for authentication can lead to increased complexity and power consumption, which is a significant concern for resource-constrained mesh users. The research highlights the need for scalable and secure solutions, particularly in large wireless mesh networks, where existing methods may falter due to fixed dependencies on domain-based structures.

In 2020, Sharma et al. presents an ID-based signcryption authentication algorithm designed to enhance secure communication during the handoff process in wireless mesh networks (WMN). It addresses the challenge of user mobility, which is

increasingly significant due to the widespread deployment of wireless technologies. The proposed solution incorporates a proxy-based hierarchical network and employs a caching-list-based pre-fetching technique to minimize handoff latency. The algorithm ensures high security while reducing the percentage of compromised nodes, authentication delay, and communication costs, leading to an increased packet delivery ratio[66].

the paper highlights the advantages of reduced authentication costs and lower packet drop rates compared to existing methods like IPGS and TBHA.

In 2021, Kumar et al. presents a pairing-free identity-based two-party authenticated key agreement protocol utilizing hexadecimal extended ASCII Elliptic Curve Cryptography (ECC). It aims to enhance secure communication and the exchange of confidential information in wireless sensor networks (WSN), addressing the challenges posed by existing identity-based protocols, which suffer from inadequate security, high computation costs, and latency due to pairing and mapping functionalities . The proposed scheme is designed to improve security strength while reducing costs, outperforming traditional methods such as the Bin and Balls Authentication scheme and Loss-Tolerant Authentication scheme[67].

However, the paper acknowledges limitations associated with the existing bilinear pairing methods, which are not only complex but also vulnerable to various attacks, including man-in-the-middle and reflection attacks . Additionally, the reliance on public key infrastructure (PKI) introduces overheads in key generation and management, which complicates its application in WSN .

Table 2.1: Comparative analysis of Authentication Protocols

Year	Approach	Strengths	Weaknesses
2006[46]	Proposes network-layer data caching using En-route and Promiscuous caching methods to reduce packet loss during handoff.	Simple to implement; reduces packet loss and delay; supports VoIP.	No security mechanism; does not protect against malicious access.
2008[47]	Uses EAP Re-authentication Protocol (ERP) to avoid full EAP-TLS during intra-domain handoff by using derived keys.	Very low delay; minimizes AAA server load; suitable for real-time apps.	Limited to intra-domain; needs initial EAP-TLS setup.
2012[48]	Employs Identity-Based Cryptography (IBC) with online/offline encryption to reduce mobile node computation.	Low overhead; perfect forward/backward secrecy; no certificates needed.	Requires IBC infrastructure; not compatible with legacy PKI systems.

2013[49]	Uses pre-issued tickets from a central server for local re-authentication at neighboring access points.	No server contact needed during handoff; low latency; scalable.	Requires secure ticket lifecycle management; replay risks if exposed.
2014[50]	Implements symmetric-key ticket pre-distribution to support fast handoff without 802.1x changes.	Low overhead; standards compatible; eliminates third-party bottlenecks.	No privacy support; risk of replay attacks if tickets not managed.
2014[51]	Uses ECC, TPM, and trust evaluation to permit handoff only if the mobile node is trustworthy.	High trust assurance; secure against impersonation and tampering.	High computational cost; not mobile-device friendly.
2016[52]	Enhances ticket security by encrypting sensitive data and eliminating the need for TPDs.	Efficient and privacy-preserving; prevents impersonation.	Initial setup complexity; ticket protection must be strong.
2016[53]	Uses Attribute-Based Encryption	Constant computational cost; early	Complex setup; requires ABE-compatible devices.

	(ABE) and pre-signed tickets for scalable and secure pre-authentication.	authentication; scalable.	
2016[54]	Uses signal strength (SNR) to pre-authenticate clients for fast handoff with minimal cryptography.	Very low delay; effective in simulated environments.	Lacks strong security guarantees; no privacy protections.
2016[55]	Provides mutual authentication using pseudonyms for anonymity and untraceability.	Strong privacy; protects identity and location; mutual trust.	Complex protocol; higher overhead.
2017[56]	Introduced SAAADsecurity architecture using trusted routers to detect cloned AP and internal attacks; VoIP-focused.	Improved detection accuracy, reduced overhead, real-time suitability	Limited scalability, relies on centralized databases for AP validation
2017[57]	Enhanced LIAP using quadratic residues to resist location	High efficiency, user anonymity, reduced handover delay	May increase computation on roadside units, complex ticket management

	tracking & parallel session attacks.		
2018[58]	Applied three-level hybrid authentication (full, quick, new node) with GLOR protocol.	Resource efficient, adaptable to various scenarios	Relies on geolocation, lacks robust evaluation for large-scale attacks
2018[59]	Used Diffie-Hellman ECC for reduced authentication delay.	Low latency, reduced overhead, theoretical and simulation validation	No real deployment, only evaluated on ns2, lacks detailed threat analysis
2018[60]	Group signature-based batch handover without involving signature verification at each step.	High efficiency, anonymity, privacy preservation	Initial setup is complex, assumes secure initial distribution
2019[61]	Zone-based ticket generation by AS; stored centrally, validated during roaming.	Reduced storage overhead on clients, fast roaming	Depends on central server, delay in large mesh due to lookup latency
2019[62]	Used probabilistic	Low delay, scalable, NS2	Ticket storage still decentralized, risk in node

	model to assess tickets at zonal routers; optimized for large/small networks.	tested on multiple scenarios	compromise
2019[63]	Cluster-based authentication using Diffie-Hellman & digital signatures.	Efficient key management, cluster-wise isolation of threats	High setup cost, assumes pre-established trust authority
2019[64]	Used blockchain as decentralized ledger for authentication transactions.	No central server needed, tamper-proof records	High computation, potential delay due to consensus protocol
2020[65]	Ticket-based fast handover with privacy-preserving ticket sharing.	Preserves privacy, efficient handover, minimized latency	Ticket pre-distribution can burden mobile nodes, limited by power/bandwidth
2020[66]	ID-based signcryption authentication algorithm (ISAA) using proxy-based hierarchical network	fast handoff through pre-fetching, High security using signcryption (combined encryption + signature),Effective	Relies on pairing operations, which are computationally expensive. Not Applicable for low-power devices.

	architecture and caching list-based pre-fetching for intra/inter-domain handoffs in Wireless Mesh Networks (WMNs).	against replay, spoofing, and man-in-the-middle attacks, significant reduction in authentication delay and packet drop.	
2021[67]	Pairing free identity based two party authenticated key agreement protocol (ID-2PAKA) using hexadecimal extended ASCII with ECC to enhance security while minimizing computation for Wireless Sensor Networks (WSNs).	Low computational cost, Enhanced identity security via ASCII encoding, Optimized for resource constrained environments like WSNs, Efficient key generation and verification, Lower energy consumption and total computation time.	Focuses on two party communication only, not suitable for multi party/group scenarios, Does not explicitly address handoff scenarios.

2.2 Secure Routing

To ensure availability, routing protocols must be resilient to both dynamic changes in network topology and potential malicious attacks. Numerous routing protocols have been proposed for Wireless Mesh Networks (WMNs) [68]. Most of these protocols rely on the assumption of trustworthy cooperation among participating devices, which are expected to follow a certain "code of conduct." However, various security threats still exist some due to inherent flaws in the protocols themselves, and others stemming from the absence of traditional identification and authentication mechanisms [69].

These threats can be broadly categorized into two sources. The first originates from external attackers who may inject false routing information, replay outdated messages, or manipulate legitimate routing data. Such actions can lead to network partitioning or increased traffic load due to unnecessary retransmissions and inefficient routing paths. The second, and often more severe, type of threat arises from compromised nodes within the network. These nodes can disseminate incorrect routing information while appearing legitimate, making detection difficult. Simply requiring routing information to be signed by each node is insufficient, as compromised nodes still possess valid private keys and can therefore generate seemingly authentic signatures.

To defend against external threats, routing information can be protected using cryptographic techniques similar to those used for securing data traffic. However, such methods are largely ineffective against threats from compromised nodes. Detecting malicious behavior based solely on routing information is also challenging in WMNs due to their dynamic and constantly evolving topologies.

Nonetheless, certain properties of WMNs can be leveraged to achieve secure routing. For instance, because WMN routing protocols must inherently accommodate outdated information due to frequent topology changes, false routing data from compromised nodes can be treated as valid. As long as a sufficient number of nodes remain trustworthy, the protocol can identify alternate paths that circumvent

compromised nodes. This capability often depends on the inherent redundancy of WMNs. Many protocols such as ZRP, DSR, TORA, and AODV are designed to discover multiple routes, allowing nodes to switch to an alternative path when the primary route is suspected of failure.

Multipath routing extends this concept further by efficiently utilizing multiple routes without relying on message retransmission [70]. The main idea involves transmitting redundant information across additional paths for the purpose of error detection and correction. For instance, if there are n disjoint routes between two nodes, n−r of them can be used to transmit data, while the remaining r routes are used to carry redundant information. This redundancy ensures that even if some paths are compromised, the receiver may still be able to verify the integrity of the received data.

Despite these mechanisms, most routing protocols for WMNs remain fundamentally cooperative, operating under an implicit "trust your neighbor" assumption [71]. This leaves them vulnerable to malicious nodes, which can disrupt network functionality by injecting false routing updates, replaying or altering legitimate updates, or advertising misleading routing information. Several specific attacks have been identified that target routing functionality in WMNs[72]:

- **Eavesdropping**: An attacker may passively listen to network traffic to extract sensitive information. Even without decrypting payloads, routing data alone can reveal relationships between nodes, their approximate locations, and the overall network topology.
- **Sinkhole and Wormhole Attacks**: In these attacks, a malicious node manipulates the routing protocol to advertise itself as having the shortest or most optimal path to certain destinations. This enables the attacker to intercept traffic intended for other nodes. Once positioned on the route, the node may launch a denial-of-service (DoS) attack by dropping all packets (black hole), selectively forwarding them (gray hole), or initiating a man-in-the-middle attack.

- **Routing Table Overflow**: Here, the attacker attempts to flood a node's routing table by creating numerous bogus routes to non-existent nodes. The objective is to exhaust the memory allocated for routing entries, preventing legitimate routes from being established or maintained, thereby destabilizing the routing protocol.

- **Rushing Attack**: This attack targets on-demand routing protocols. To limit overhead from flooding Route Request (RREQ) messages, many protocols allow only the first RREQ received to be forwarded. An attacker exploiting this behavior can quickly forward RREQs, increasing the chance that routes including the attacker will be selected, thus bypassing legitimate alternatives.

- **Sleep Deprivation Attack**: As introduced in [73], this attack is particularly effective in networks where nodes are battery-powered. The attacker attempts to drain the victim's battery by initiating frequent route requests or sending unnecessary packets. Since even devices not offering services must participate in routing, they are forced to expend energy, potentially leading to early battery depletion.

- **Location Disclosure Attack**: In this type of attack, adversaries extract information about node positions or the overall structure of the network. This can occur through analysis of routing metadata or by exploiting protocol behavior.

Given these threats, Lundberg proposed several criteria that a secure ad hoc mesh routing protocol should satisfy[72]:

- **Certain Discovery**: If a valid route exists between two nodes, the protocol must reliably discover it. Moreover, the source node must be assured that the route leads to the intended destination.

- **Isolation**: The protocol should be capable of identifying and isolating misbehaving nodes, preventing them from interfering with routing. Alternatively, it should be inherently resilient to malicious node activity.

- **Lightweight Computation**: Since many devices in WMNs are resource-constrained, the protocol must minimize computational overhead to preserve battery life and performance.
- **Location Privacy**: Routing protocols must safeguard location information, even in message headers. Passive observers or attackers should not be able to infer node locations or network layout simply by monitoring unencrypted metadata. Furthermore, protocols should be designed such that an attacker must remain actively engaged in malicious behavior to disrupt the network—making transient or minimal effort attacks ineffective.

Out of several routing protocols, our research focus on AODV routing protocol which is most popular in literature and discuss in the following section.

2.2.1 Security in AODV routing protocol

AODV is a reactive routing protocol designed for ad hocand wireless mesh networks, meaning it finds routes only when needed (on-demand), rather than maintaining a full routing table at all times. The protocol does not deals with security mechanism of the routing it is susceptible to various attack as in the table below:

Table 2.2: Vulnerability of AODV Routing Protocol

Vulnerability	**Attack Type**	**Impact**
Black Hole	DoS	Packet Loss
Gray Hole	Selective DoS	Intermittent Packet Loss
Worm Hole	Topology Manipulation	Interception or Redirection
Rushing	Route manipulation	Insecure routes favored
Location Disclosure	Privacy leak	Reveals node positions or

		movements
Sleep Deprivation	Resource attack	Rapid battery drain
Lack of Authentication	Protocol flaw	Enables spoofing and replay attacks
Routing Table Overflow	Resource exhaustion	Blocks valid routing entries

Out of several attack, black hole attack attract attention of large number of researcher and several number of mitigation technique have been proposed.

In 2020 SashiGurung and Sidartha Chauhan classified the mitigation technique in different categories[74]:

- **Cryptography based scheme**: It encompasses all solutions that utilize cryptographic techniques such as symmetric key encryption, digital signatures, or hashing for encryption, authentication, and ensuring data integrity, in order to protect the network against potential attacks.
- **Overhearing-Based Scheme:** This approach includes all solutions where each node monitors the transmissions of its neighboring nodes to assess their behavior. If a neighboring node exhibits abnormal or suspicious activity, it is identified as malicious, and this information is propagated throughout the network.
- **Sequence Number Threshold-Based Scheme:** In this method, the source node establishes a threshold based on the sequence number field in the reply packets. Any reply packet with a sequence number exceeding this threshold is considered suspicious and is subsequently discarded.
- **Acknowledgment-Based Scheme:** This scheme involves sending acknowledgment packets to confirm the successful reception of transmitted

data. A lack of acknowledgment may indicate malicious activity or packet loss.

- **Clustering-Based Scheme:** Here, the network is organized into clusters. A designated cluster head is responsible for detecting black hole attacks within its cluster and disseminating alerts throughout the network.
- **Cross-Layer Collaboration-Based Scheme:** This category includes solutions where two or more layers of the network protocol stack cooperate to identify and detect malicious behavior within the network.
- **Cross-Checking-Based Scheme:** In this method, the source node verifies the legitimacy of an intermediate node by cross-checking with either its next hop or previous hop. This helps determine whether the intermediate node is behaving maliciously or not.
- **Trust-Based Scheme:** These solutions evaluate the trustworthiness of nodes based on their interactions with neighboring nodes. If a node's trust value, calculated from observed transmission behavior, falls below a pre-defined threshold, it is classified as malicious.
- **IDS-Based Scheme**

  This approach relies on specialized nodes known as Intrusion Detection System (IDS) nodes, which monitor nearby transmissions to identify malicious behavior. Upon detecting any anomaly, the IDS node broadcasts an alert throughout the network to initiate the isolation of the malicious node.

In 2007, HesiriWeerasinghe presents an enhanced AODV-based routing protocol designed to detect and mitigate cooperative black hole attacks in MANETs. In such attacks, multiple malicious nodes collude to mislead the routing mechanism, falsely advertising optimal paths to intercept and drop packets. The authors propose a defense mechanism using a Data Routing Information (DRI) table and a cross-checking system involving Further Request (FREQ) and Further Reply (FREP) messages. This approach allows the source node to verify the reliability of intermediate nodes based on past interactions and the credibility of their neighbors[75].

The protocol is evaluated through simulations against standard AODV and an existing solution the results show that the proposed method significantly improves throughput and reduces packet loss, even under varying conditions like node mobility and terrain size. However, the improved security comes at the cost of increased control packet overhead (5–8%) and slightly higher end-to-end delay due to additional verification steps. The approach also assumes the trustworthiness of certain nodes, which may not hold in all scenarios. Moreover, energy efficiency and scalability for large or resource-constrained networks remain unaddressed, limiting its practicality in some real-world deployments.

In 2007,Yu et al. present A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks.This paper addresses the issue of black hole attacks in MANETs by proposing a distributed and cooperative detection mechanism. The main idea is to allow nodes to locally monitor their one-hop neighbors and collaborate with others when suspicious behavior is identified. Specifically, when a node identifies a neighbor that might be dropping packets (a hallmark of a black hole), it triggers a cooperative verification phase, where multiple nodes analyze the suspicious node's behavior by exchanging routing and data forwarding information. If the majority confirms malicious intent, the black hole node is isolated from the network. The approach aligns with the decentralized nature of MANETs and aims to preserve performance even in high traffic conditions. Simulation results highlight improved packet delivery ratios, high black hole detection accuracy, and reduced overhead compared to earlier schemes. However The scheme assumes honest behavior from the majority of nodes, which can be compromised in cases of colluding malicious nodes, It may be computationally and communicatively intensive, especially in large or highly mobile networks, The scheme lacks a recovery mechanism if false positives occur[76].

In 2009, Medadian et al. present a Combat mechanism for black hole attack, the work aim to enhance the security of the AODV (Ad-hoc On-demand Distance Vector) routing protocol by defending it against black hole attacks through neighbor-based negotiation. Rather than immediately accepting the first Route Reply (RREP)

received, the source node delays route establishment and queries multiple neighboring nodes that claim to have a valid path to the destination. By comparing the responses and verifying consistency among the nodes, the protocol attempts to identify malicious nodes that respond deceptively with false high-sequence numbers and short paths (typical of black holes). If a node's reply is inconsistent with others or known topology information, it is flagged as malicious. However The protocol still suffers from delays due to the waiting and validation period before establishing routes. If multiple neighboring nodes are compromised and collude, they can bypass detection by giving consistent false replies. It assumes sufficient node density so multiple replies are available to perform validation sparse networks may limit effectiveness[77].

In 2012, Baadache&Belmehdi presents a cryptographic acknowledgment based method using Merkle trees to detect packet dropping behavior in MANETs. The proposed approach introduces a three-node monitoring structure: when a source node A sends a packet to destination C via intermediate node B, the destination node C returns a cryptographic value (hash) derived from the packet. Node B appends its own value and forwards both to A. Using these, node A can reconstruct the Merkle root and verify that B has correctly forwarded the packet. If the hash does not match, node B is suspected of dropping or modifying packets. This method helps detect selfish (energy-preserving) and malicious (DoS) nodes, and works under both reactive (AODV) and proactive (OLSR) routing protocols. It also outperforms watchdog and 2-hop ACK methods . However the protocol Relies on cryptographic operations, which may not be suitable for resource-constrained devices due to processing and energy overhead also In highly dynamic topologies, node reordering or mobility might disrupt the verification sequence[78].

In 2013, Tan & Kim proposes a security enhancement for AODV called Secure Route Discovery (SRD-AODV) aimed at mitigating black hole attacks. In AODV, nodes can reply to Route Request (RREQ) messages by claiming to have a valid path, which is exploited by black hole nodes. SRD-AODV counters this by introducing threshold-based verification of destination sequence numbers in both

RREQ and RREP messages. The source node checks whether the RREP's sequence number is unusually high (a typical black hole behavior) compared to its own threshold values before trusting the route. Similarly, the destination node also checks the sequence number of incoming RREQs. This dual-side verification helps reduce the chances of route hijacking. However assumption of pre-defined static threshold sequence number may not be effective in highly dynamic network and collaborative black hole attacks can be launched effectively[79].

In 2014, Dhiman and Sood present the enhanced 2ACK (two-hop acknowledgment) mechanism to detect and isolate selfish or black hole nodes while reducing the routing overhead caused by the original 2ACK protocol. In 2ACK, if node A sends data through node B to node C, node C sends an acknowledgment packet (2ACK) back to A. This confirms successful forwarding by B. The authors propose optimizing the authentication process of these 2ACK packets to reduce redundant or unnecessary 2ACK transmissions. A fraction of packets (determined by an acknowledgment ratio) are chosen for acknowledgment, balancing detection accuracy and network load. They introduce MAC-layer support to further streamline detection and reduce end-to-end delays. But the protocol still introduces some control overhead, especially in high-density networks where acknowledgment ratios need tuning. Nodes must synchronize timers for tracking unacknowledged packets, which can be problematic in high-mobility scenarios,performance heavily depends on the selection of threshold values, which may vary across scenarios, also It does not distinguish between malicious and overloaded nodes, potentially leading to false detection[80].

In 2015, Dorri and Nikdel introduces an AODV-based detection scheme specifically designed to address cooperative black hole attacks, where multiple malicious nodes work together to deceive the network. The main innovation lies in the use of a modified Data Routing Information (DRI) table, which tracks whether a node has received data from or sent data through a neighboring node. When a Route Reply (RREP) is received, the source node verifies both the next-hop (NHN) and previous-hop (PHN) nodes associated with the RREP generator using their DRI entries. A

recursive verification mechanism is used to validate trustworthiness before using the route. If any inconsistencies are found such as an NHN claiming not to have received from the RREP sender the node is marked as malicious. The method detects and isolates all black hole collaborators in the path, even if the malicious node is not the one sending the RREP. However the protocol Introduces computational overhead due to the recursive path verification and DRI updates, Additional data exchanges for checking NHN/PHN can delay route establishment in real-time systems[81].

In 2016, Kumar et al. proposed a protocol that enhances the AODV routing protocol to improve its security against black hole attacks, focusing on detecting abnormal routing behavior during route discovery. The proposed solution modifies the packet processing mechanism of AODV by analyzing sequence numbers and timestamps of RREP messages. The idea is based on the observation that malicious nodes typically respond faster and with higher than normal sequence numbers. The solution uses a threshold based filtering mechanism to identify suspicious nodes. To reduce additional overhead, the scheme reuses HELLO messagesnormally used for neighbor discovery to propagate warning alerts when a black hole is detected. The simulation result demonstrates that the proposed system significantly improves packet delivery ratio, reduces delay, and minimizes routing overhead under attack conditions. But The use of static threshold values for sequence number comparisons can lead to false positives or negatives, especially in fast-changing topologies.The system relies on the first RREP assumption being malicious, which may not always be true HELLO message payload increase packet size. It is less effective against multiple or collaborative black hole attacks[82].

In 2017, Gurung and Chauhan introduces MBDP-AODV (Mitigating Black Hole effects through Detection and Prevention), an improved AODV routing protocol designed to dynamically detect black hole attacks. Unlike previous static-threshold methods, this approach calculates a dynamic threshold for destination sequence numbers using multiple RREP packets during route discovery. By analyzing sequence number deviations statistically, it avoids over-reliance on the first RREP received and detects anomalies more accurately. The protocol classifies nodes based

on behavior (normal, suspected, or malicious), improving its resilience to black hole and gray hole attacks. It also identifies sequence number based gray hole attacks, where attackers selectively drop packets after advertising a valid path. However multiple RREP may always not available in congested network and also introduce high computational complexity[83].

In 2019, El-Semary and Diab proposed chaotic map base black hole node detection, In this study, the authors present BP-AODV, a secure extension of the traditional AODV protocol tailored to resist both single and cooperative black hole attacks in mobile ad hoc networks (MANETs). The key innovation lies in the incorporation of a chaotic map-based challenge-response-confirm mechanism during the route discovery process. When a source node initiates a route request, it generates a challenge value, which is sent to the destination. The destination, in turn, calculates a unique response using a chaotic map function that is difficult for attackers to replicate. This response is sent back to the source along with the route reply, and later the destination broadcasts the confirmation parameters to all intermediate nodes, allowing them to validate the response and confirm that the route is secure. Additionally, the protocol implements a trust mechanism during data forwarding, where nodes are assigned trust scores based on how reliably they forward packets. Routes through nodes with poor trust records are avoided. While the protocol is effective at preventing both routing and forwarding stage attacks, it requires more computational power and memory to handle the chaotic functions and additional message types. Furthermore, requirement of multiple route cause significant delay in large network[84].

In 2020, Terai et al. addresses an advanced variant of black hole attacks known as smart black hole attacks, where the malicious node attempts to mimic legitimate routing behavior by intelligently predicting sequence numbers. Traditional black hole defense mechanisms rely on fixed or dynamically computed thresholds for sequence numbers to detect abnormal replies, but these smart attackers can bypass such defenses by crafting seemingly legitimate responses. To counter this, the authors propose a prevention method that uses predictive modeling supported by local

cooperation among nodes. The source node collects historical sequence number and timestamp data from its neighbors and uses linear regression(least square method) to estimate the expected sequence number growth over time. When a route reply is received, the source compares the sequence number to the predicted value, allowing a small margin of error defined by a tunable parameter. If the reply significantly deviates, it is flagged as suspicious. This method does not depend on cryptographic tools but rather statistical analysis, making it lightweight yet effective. However, it depends heavily on accurate time data and the reliability of neighbor information. If node clocks are desynchronized or if too few neighbors participate, prediction accuracy drops. The system is also sensitive to the threshold margin, requiring careful tuning to balance detection and false positives[85].

In 2020, Saputra et al. proposed a detection scheme called the Enhanced Check Agent (ECA) to counter blackhole attacks in Wireless Sensor Networks (WSNs). The proposed method was implemented on a ZigBee-based mesh network, leveraging the ECA mechanism to improve data transmission integrity. The approach builds upon two existing concepts: the traditional “Check Agent” method and a hybrid detection strategy. Unlike the random checking in the earlier proposed approach, ECA uses sequential agent transmission to inspect each node systematically. When a node fails to respond to a check agent, it is marked as suspicious and blacklisted. This blacklist is distributed throughout the network to avoid malicious nodes in future routing decisions. The performance evaluation showed that the method significantly improves throughput, even restoring it to nearly 100% under blackhole attack scenarios, making it highly effective for increasing QoS in WSNs[86].

However, the method has notable limitations. The inclusion of a checking mechanism in every routing decision adds processing time, which leads to increased packet delay, particularly with larger packets. This tradeoff could affect latency sensitive applications. Moreover, the approach assumes only one malicious node in the network and doesn’t explore scenarios with multiple or colluding attackers, raising concerns about scalability and robustness. Finally, because the method is tied

closely to ZigBee (IEEE 802.15.4) technology, its generalizability to other network types, especially mobile ad hoc networks (MANETs), remains unverified.

In 2020, Vatambeti et al. introduced a novel technique for detecting black hole and gray hole attacks in Mobile Ad Hoc Networks (MANETs) using a technique based on Gray Wolf Optimization (GWO). Their method integrates trust based data aggregation with the bio-inspired GWO algorithm, which mimics the leadership hierarchy and hunting behavior of gray wolves in nature. The key idea is to evaluate the behavior of nodes over time by analyzing packet forwarding rates and trust metrics, and then use the optimization algorithm to dynamically identify malicious nodes. The proposed scheme aims to not only detect attacks with high accuracy but also ensure that the selected routing paths are stable and trustworthy. The authors claim that their technique achieves an impressive 98.5% detection accuracy and improves the packet delivery ratio (PDR) to 98.2% in simulated environments[87].

Despite these promising results, the method has certain limitations. One of the primary concerns is its computational complexity. GWO, being a metaheuristic algorithm, requires multiple iterations and fine-tuning of parameters, which can lead to higher processing overhead—a significant drawback in MANETs where nodes are resource-constrained and often operate on limited battery power. Additionally, the model's detection relies on consistent node behavior, making it less effective against gray hole attacks that are intermittent or probabilistic in nature. Finally, the paper does not address how the system would scale in high-mobility or large-network scenarios, where frequent topology changes could impact the timeliness and accuracy of detection.

In 2021, Sathyaraj et al. proposed a host-based black hole detection and prevention technique in MANETs using an enhanced version of the Chicken Swarm Optimization (CSO) algorithm, referred to as Improved Crossover Chicken Swarm Optimization (ICCSO). The method is built upon the AODV routing protocol and enhances it with intelligent routing based on swarm behavior and crossover operations from genetic algorithms. In this model, each node’s behavior is analyzed using performance metrics like Packet Delivery Ratio (PDR) and Received Signal

Strength Indicator (RSSI). If a node is identified as malicious (e.g., low PDR or weak RSSI indicating packet drops), it is excluded from the routing path. The ICCSO also uses an enhanced partially mapped crossover to fine-tune the optimization process and select optimal, secure routing paths[88].

This approach demonstrates improved detection of malicious behavior and increases the overall packet delivery while maintaining lower end-to-end delays compared to existing methods. The model also dynamically adapts to varying network conditions, making it suitable for flexible MANET environments.

However, the technique has some drawbacks. First, the computational intensity of ICCSO, particularly due to the incorporation of both swarm intelligence and crossover operations, makes it unsuitable for low-power or energy-constrained nodes typically found in MANETs. Additionally, while PDR and RSSI are helpful metrics, they are also affected by normal fluctuations in wireless communication, which can lead to false positives—classifying non-malicious nodes as attackers.

In 2022, Kheeramani and Thakur proposed a technique for detecting and removing multiple black hole attacks in MANETs by extending the AODV protocol using a mechanism based on sending forged packets and sequence number variation (SNV). Their approach addresses one of the core weaknesses in standard AODV routing—its vulnerability to manipulated Route Reply (RREP) messages, which attackers exploit by advertising fake short paths with high destination sequence numbers. To counter this, the proposed method modifies AODV's RREQ and RREP structures by including a secure "protected field" and tracking the variation in sequence numbers. When a forged RREP with abnormally high sequence numbers is detected, the corresponding node is flagged as malicious and excluded from routing decisions[89].

This method is particularly effective in identifying multiple black hole attackers rather than just isolated ones, which is a common limitation in many other detection models.

However, the model has certain limitations. Its success hinges heavily on the assumption that malicious nodes will always advertise exaggerated sequence numbers, which may not hold true if attackers adopt more sophisticated or stealthy behaviors. Furthermore, while it enhances security, the approach does not incorporate encryption or trust models, making it susceptible to forgery by insider threats or cooperative attackers who mimic normal behavior.

In 2022, Virendra Dani introduced a model titled iBADS (Improved Black-hole Attack Detection System), which employs a trust-based weighted method for the identification and isolation of black hole nodes in MANETs. The core idea is to compute a dynamic trust value for every node based on its past behavior in forwarding data packets. This trust value is calculated using a threshold-based weighting mechanism, where parameters like the number of successfully forwarded packets and node responsiveness are used to determine how reliable a node is within the network. Nodes with trust scores below a certain threshold are considered malicious and excluded from routing tables. The proposed model aims to improve routing security without relying on encryption or heavy computational techniques. Its strength lies in its ability to make adaptive decisions based on network behavior, which helps maintain high packet delivery ratios and low latency, especially in static or moderately dynamic environments[90].

Despite its benefits, the system has a few critical limitations. One of the primary concerns is that trust computation is centralized, which contradicts the decentralized nature of MANETs and introduces a single point of failure. Also, the model assumes that all nodes will have consistent behavior over time, which is not always true in highly mobile or dynamic scenarios.

In 2023, IdrissMoumen et al. proposed an innovative AODV-based defense framework that not only addresses blackhole attacks in MANETs but also integrates energy efficiency and environmental sustainability as core objectives. This work recognizes that while security is essential in MANETs, energy constraints are equally pressing, especially in scenarios like disaster recovery or remote deployments where battery life is limited. The proposed mechanism incorporates a multifaceted strategy:

it evaluates routes based on energy-aware metrics, supports collaborative energy sharing, implements energy-efficient intrusion detection, and even considers solar-powered routing and energy harvesting. By optimizing both the security and energy consumption, this framework aims to extend the overall network lifespan while maintaining secure communication pathways[91].

The blackhole mitigation strategy is embedded in the route selection logic, which avoids nodes that show irregular or inconsistent forwarding behavior. Intrusion detection is performed with minimal monitoring overhead by selectively sampling network traffic and adapting the detection rate based on network activity. Simulation results demonstrate improved packet delivery ratio, network lifetime, and reduced carbon footprint, making the approach both secure and eco-conscious.

However, this model comes with inherent trade-offs. The integration of energy-awareness into the routing decision process may lead to sub-optimal path selection when energy-efficient paths overlap with less secure or unreliable ones. The model assumes the availability of energy-harvesting capabilities and collaboration among nodes, which might not always be feasible in practical MANET scenarios.

In 2024, ElamparithiPandian et al. proposed a fuzzy inference-based system for detecting and preventing black hole attacks in Mobile Ad Hoc Networks (MANETs). The method focuses on integrating multiple node-related factors such as trust value, node authentication, energy level, message integrity, and the involvement of a Certificate Authority (CA) to assess whether a node is trustworthy or malicious. Before route discovery in the network begins, each node undergoes a verification process where its behavior and status are evaluated using a fuzzy logic system. The CA is responsible for issuing certificates only to nodes that pass the authentication process. Nodes without valid certification or with suspicious behavior are excluded from participating in routing. Its fuzzy logic engine allows it to make nuanced decisions based on multiple factors, which can be particularly effective in ambiguous or uncertain environments[92].

Despite its effectiveness, the approach has notable drawbacks. The reliance on a centralized Certificate Authority presents a scalability issue and introduces a single point of failure—contradictory to the decentralized nature of MANETs. In highly mobile scenarios, maintaining up-to-date certificates and trust values can be cumbersome, and delays in certification renewal may inadvertently isolate legitimate nodes.

In 2024, Rahul Chakravorty et al. proposed a hybrid security solution for MANETs that combines artificial neural networks (ANNs) with DNA cryptography to effectively detect and prevent black hole attacks. The approach is applied within the On-Demand Multicast Routing Protocol (ODMRP) framework. The core idea is to train a neural network using key node behaviors—such as packet drop rate, sequence number anomalies, and route update patterns—to classify nodes as normal or malicious. In parallel, DNA cryptographic techniques are used to secure routing messages, ensuring confidentiality and integrity during route discovery and data transmission. The model benefits from the ANN's ability to learn from dynamic patterns in node behavior, making it suitable for detecting both known and unknown (zero-day) attack signatures. Meanwhile, DNA cryptography adds a lightweight yet highly secure layer of protection to routing messages by encoding them in a biologically inspired DNA format, which is complex for attackers to decipher. However, The combined use of neural networks and cryptography results in high computational and memory overhead, making it impractical for resource-constrained MANET nodes. Training neural networks also requires a substantial dataset and initial offline learning, which may not be feasible in dynamic, real-time environments[93].

Table 2.3: Comparative analysis Black hole attack mitigation Techniques

Year	Approach	Strength	Weakness
2007[75]	Extends AODV by adding a Data Routing Information (DRI) table and a cross-checking mechanism using Further Request (FRq) and Further Reply (FRp). It ensures that a node has both sent and received data to/from its neighbors before trusting it.	- Effectively detects cooperative black hole attacks. - Improves throughput and reduces packet loss. - Incorporates simulation and performance comparisons against baseline AODV and other solutions.	- 5–8% increased overhead due to extra route requests. - Slight increase in packet loss during secure discovery. - Delay route setup due to added verifications.
2007[76]	Fully distributed, cooperative detection system where nodes collect local info and use 1-hop neighbor trust evaluation. Suspicious nodes are	- High detection rate even with multiple attackers. - Lower control overhead under increasing traffic. - Robust against false RREP by verifying claims	- Ineffective in high-mobility scenarios. - Detection relies on consistent neighbor behavior, which might not hold in volatile networks. - Lacks extensive scalability evaluation.

	verified through peer cooperation.	collaboratively.	
2009[77]	Proposes a neighbor negotiation strategy: when a node receives multiple RREPs, it waits and cross-verifies responses from all neighbors before selecting the route.	- Improves security without significant delay. - Detects attackers without modifying AODV core logic. - Demonstrates better packet delivery ratio in simulation.	- Waiting for replies may cause higher initial route discovery delay. - Vulnerable if all neighbor nodes collude. - Limited detection capability in fast-moving topologies.
2012[78]	Introduces a Merkle-tree based authentication mechanism to verify packet forwarding. Each node uses cryptographic hashes to validate that intermediate nodes forwarded data correctly.	- Detects selfish and malicious (black/gray hole) nodes. - Works in both proactive and reactive protocols. - Superior to watchdog and 2-hop ACK in detection reliability.	- Adds cryptographic overhead. - Needs synchronization and extra computations at nodes. - Ineffective if nodes do not respond timely or hashes are manipulated.

2013[79]	Proposes SRD-AODV, which requires both source and destination to verify sequence numbers in RREQ/RREP using pre-defined thresholds before route setup.	- Works well in different simulated environments. - Improves packet delivery ratio compared to basic AODV. - Adds lightweight validation to standard protocol.	- Relies on pre-defined sequence number thresholds, which may not adapt to all scenarios. - Does not handle collaborative (cooperative) black holes. - Sensitive to sequence number spoofing.
2014[80]	Modified 2ACK scheme with RSA-based dynamic key generation to authenticate packets	- Improves detection of selfish nodes - Reduces energy consumption - Increases packet delivery	- Adds routing overhead - Fluctuating throughput - Less resistance to collusion attacks
2015[81]	Enhances AODV with DRI table and a dual-hop verification. Uses Next-Hop Node (NHN) and Previous-Hop Node (PHN) data	- Detects all black hole nodes in a path in one run. - No false positives due to dual verification. - Reduced packet overhead and processing	- Complexity increases due to bidirectional trust checks. - Malicious nodes must be known or inferred from DRI values. - Depends heavily on accurate DRI maintenance.

	from RREP to trace and eliminate all malicious nodes in a path using an iterative checking algorithm.	time.	
2016[82]	Enhanced AODV using modified RREP processing and HELLO messages for blackhole detection	- High Packet Delivery Ratio (~93%) - Minimal routing overhead - Improved E2E delay	- Slight increase in overhead - Does not consider cooperative or multiple blackhole attackers
2017[83]	Introduces MBDP-AODV, which uses dynamic thresholding based on observed destination sequence numbers to detect anomalies (e.g., sudden high sequence numbers indicating black	- Adaptable to changing network conditions. - Requires no extra tables or packet formats. - Effective under DoS/black hole scenarios.	- May generate false positives during route instability. - Sequence number deviations may occur due to legitimate mobility. - Detection depends on proper tuning of dynamic thresholds.

	holes).		
2019[84]	Builds on AODV and SAODV, adding chaotic map-based secret sharing for RREQ/RREP authentication. Also verifies both route discovery and forwarding behavior, preventing cooperative attacks.	- Defends against cooperative black hole and forwarding phase attacks. - Outperforms SAODV and PCBHA in simulation. - Uses chaotic maps to avoid static key management.	- Increases computational complexity due to chaotic systems. - Requires synchronization of secrets between source and destination.
2020[85]	Local info sharing among neighboring nodes in AODV	- Detects smart blackhole attacks - Reduces attack success rate - Maintains network performance	- Assumes honest node cooperation - Vulnerable to colluding nodes - Adds communication overhead
2020[86]	Sequential check agent with blacklist mechanism in ZigBee WSN	- Increases throughput up to 100% - Reduces checking time with single	- Delay increases with packet size - Limited scalability - Dependent on accurate agent routing

		packet - More reliable than random agent approach	
2020[87]	GWO with trust setup data aggregation	- High detection rate (98.5%) - Improves packet delivery (98.2%) - Trust model increases robustness	- Requires optimal parameter tuning - Computationally intensive - High energy usage in dense networks
2021[88]	ICCSO algorithm with RSSI & PDR analysis	- Enhanced detection over basic CSO - Discards infected nodes early - Reduces delay and improves PDR	- Needs precise fitness evaluation - Overhead from crossover process - Less effective under high node mobility
2022[89]	Sequence number variation technique in AODV	- Detects fake route replies - Effective against blackhole and grayhole - Verified using NS2 simulation	- Depends on sequence number integrity - Simulation-based validation only - May fail with complex attackers
2022[90]	Node trust score based on	- Lightweight and flexible	- Misclassification risk with poor thresholds

	thresholding	- Adapts to network changes - Works with on-demand protocols	- May not scale well - No comprehensive test in large networks
2023[91]	Energy-aware AODV routing with green enhancements	- Combines energy efficiency and security - Extends network lifetime - Supports collaborative energy sharing	- Adds complexity to routing - Requires accurate energy metrics - Trade-off between energy and security
2024[92]	Fuzzy inference using trust, CA, and authentication	- Multi-criteria detection improves accuracy - Prevents blackhole via certificate validation - Improves PDR and reduces delay	- Certificate Authority is a potential bottleneck - Complex fuzzy rule handling - Overhead from authentication process
2024[93]	ANN-based classification with DNA encryption	- Strong protection against blackhole attacks - Enhances	- High resource consumption - Needs large training dataset - Complex to implement on constrained devices

		confidentiality and packet delivery - Uses both ANN and cryptography for robustness	

2.3 Packet Authentication

Packet authentication is a crucial security mechanism in computer networks that ensures data integrity and verifies the identity of the sender for every transmitted packet. Its primary goal is to protect the network from attacks such as spoofing, tampering, and replay attacks, especially in environments like wireless Mesh networks, mobile ad hoc networks (MANETs), Vehicular Ad-Hoc Network, and the Internet. When a data packet is sent across a network, packet authentication mechanisms verify that the packet has not been altered during transmission and that it truly originates from the claimed sender. This is commonly achieved using cryptographic techniques like Message Authentication Codes (MACs) or digital signatures.

In symmetric-key authentication, both sender and receiver share a secret key. The sender computes a MAC using this key and attaches it to the packet. The receiver recomputes the MAC using the same key and compares it to the received one. If they match, the packet is authenticated.

In asymmetric-key systems, the sender signs the packet using their private key. The receiver then uses the sender's public key to verify the signature. This provides stronger security and supports non-repudiation but is computationally more expensive.

Packet authentication is especially important in dynamic and decentralized networks, where nodes frequently join and leave, and traditional centralized security controls may be unavailable. Packet authentication protects against unauthorized access, data tampering, and identity spoofing by verifying each packet's origin and integrity.

In 2003, Zhu et al. proposed LHAP (Lightweight Hop-by-Hop Authentication Protocol) to ensure network access control in mobile ad hoc networks (MANETs) by providing lightweight and efficient hop-by-hop authentication of packets. LHAP operates independently of the underlying routing protocol, serving as a general-purpose authentication layer. The protocol uses two major cryptographic mechanisms: one-way key chains for packet authentication and the TESLA protocol for establishing trust among neighboring nodes. Each node maintains a TRAFFIC key chain, which it discloses sequentially to authenticate each transmitted packet. Authentication is performed immediately upon reception, avoiding the delay typically introduced by TESLA's periodic key disclosure. Additionally, LHAP supports very long key chains using multilevel hash chains, extending the protocol's applicability in long-term deployments.
LHAP provides strong hop-by-hop authentication with minimal computational and communication overhead, making it practical for resource-constrained environments. Its routing-protocol independence makes it a versatile solution for multiple MANET implementations. The protocol achieves near-instantaneous packet verification and supports flexible deployment through integration with existing routing messages for reduced bandwidth overhead. However it still suffers from key disclosure delay in certain conditions, which can affect real-time packet forwarding. The protocol also assumes loosely synchronized clocks and secure bootstrapping of public keys. Moreover, while it thwarts unauthorized access effectively, it lacks mechanisms to detect or respond to insider threats from compromised nodes[94].

In 2008, Akbani et al. proposed Hop-by-Hop Efficient Authentication Protocolto be a robust, efficient authentication mechanism for MANETs, focusing on the authentication of messages at each hop to prevent propagation of malicious data. HEAP uses a modified version of the HMAC construction involving two keys: an

inner key (ikey) shared among all one-hop neighbors for broadcast authentication, and an outer key (okey) that is a pairwise key between sender and receiver. This dual-key architecture provides a fine-grained control over security and enables both unicast and broadcast authentication. The protocol is optimized to provide high-speed processing with minimal memory footprint and energy consumption, characteristics critical for mobile and sensor networks.HEAP significantly improves performance compared to existing schemes such as TESLA and LHAP. Its security is formally proven under strong adversarial models for both outsiders and insiders with partial key knowledge. The protocol is versatile, working seamlessly with multicast, unicast, and broadcast messages. It is particularly effective at countering packet injection from unauthorized entities while consuming minimal network resources.Despite its robust performance, HEAP is primarily secure against outsider attacks and offers limited protection against compromised insider nodes who know shared keys. It also depends on a secure initialization phase to distribute ikey and okey, which may be challenging in a completely decentralized or dynamic network without a central authority[95].

In 2010, Li and Liu proposed ID-based Multiple Secrets Key Managementprotocol that offers a fully distributed identity-based key management system tailored for cluster-based mobile ad hoc networks. It overcomes the limitations of centralized PKI systems by leveraging distributed Private Key Generators (D-PKGs), each hosted on cluster heads, to generate and share a master private key collaboratively. The protocol includes mechanisms for network initialization, key revocation, periodic multiple-secret key updates, and authenticated group key generation. It also incorporates an efficient one-round identity-based group key agreement (ID-AGKA) scheme. The underlying cryptographic framework is based on bilinear pairings and elliptic curve operations, which ensure strong security with lower key sizes and reduced communication bandwidth.IMKM achieves a high degree of resiliency, scalability, and efficiency. It supports dynamic group membership and can securely revoke compromised nodes without reinitializing the entire network. It distributes trust and avoids single points of failure. Its one-round group key agreement protocol offers implicit key authentication and ensures both forward and backward

secrecy.IMKM still requires some initial setup involving a central trusted authority to pre-configure system parameters and public/private keys. If an adversary compromises a threshold number of D-PKGs, the system security is at risk[96].

In 2012, Li et al. developed Source Anonymous Message Authenticationfor wireless sensor networks (WSNs) to enable hop-by-hop message authentication while preserving source anonymity. Based on a modified ElGamal signature scheme over elliptic curves, SAMA ensures that an attacker cannot deduce the identity of the message originator even with access to the complete anonymity set (AS). Each node constructs a signature using the public keys of all group members and a randomly chosen subset of intermediate values. The signature is verified by any receiver using the public keys of the anonymity set. The design is tailored to be resilient against adaptive chosen-message attacks, while enabling intermediate nodes to verify and drop malicious messages immediately.SAMA achieves three key goals: unconditional sender anonymity, efficient hop-by-hop message verification, and resilience to node compromise without relying on threshold cryptography. Despite its strengths, SAMA requires that all public keys be pre-distributed and assumes a trusted security server (SS) that cannot be compromised[97].

In 2013, Tan et al. performs a comprehensive vulnerability analysis of the Hybrid Wireless Mesh Protocol (HWMP), the default routing protocol used in IEEE 802.11s wireless mesh networks. It identifies attacks that exploit mutable and non-mutable field modification, route spoofing, replay, and insider manipulation of path metrics. Based on this analysis, the authors propose a set of security requirements for HWMP and assess existing solutions such as BIP, CCMP, SHWMP, IBC-HWMP, ECDSA-HWMP, and Watchdog-HWMP. They present a quantitative comparison based on complexity and performance, and propose a sample secure HWMP design.The study offers a foundational framework for developing future secure HWMP protocols by identifying security gaps and setting precise requirements.Although the analysis is thorough, the paper does not provide a fully implemented or tested security protocol. Many of the evaluated solutions fail to meet all the proposed security requirements,

especially in the face of internal attacks. The framework is conceptual and requires further development to be practical in real-world applications[98].

In 2014, Parmar and Jinwala proposed an Aggregate MAC-based authentication scheme for WSNs focuses on enhancing the security and efficiency of data aggregation in wireless sensor networks (WSNs) using Aggregate Message Authentication Codes (AMACs). WSNs are highly constrained in terms of energy, memory, and bandwidth, and in-network processing (e.g., data aggregation) is often employed to minimize communication costs. However, combining aggregation with security, especially authentication and integrity, is challenging due to conflicting needs: aggregation typically alters data, while authentication relies on verifying the integrity of unaltered messages. To address this, the authors propose a cluster-based scheme where AMACs can be effectively utilized. AMACs allow multiple message authentication codes, generated by different nodes, to be aggregated into a fixed-size code, thus reducing transmission overhead. The protocol uses symmetric-key cryptography to maintain authentication efficiency and resource constraints, and suggests that clusters can locally aggregate MACs to reduce communication costs without compromising integrity verification at the base station. This paper introduces a hybrid approach that balances secure message authentication with the bandwidth-saving benefits, it reduces message size and communication overhead.The approach is only suitable for specific scenarios where original data (sensor readings) are available for verification at the base station, as AMACs still require access to original messages[99].

In 2016, Gao et al. proposed an anonymous authentication scheme for wireless mesh networks (WMNs) based on identity-based proxy group signatures (IPGS). The core idea is to enable mutual authentication between mesh clients and network infrastructure without exposing the identities of the users, thereby preserving privacy while maintaining security. Their hierarchical architecture includes a root trusted authority, domain managers, and group gateways, which manage proxy credentials and group keys. When a user joins the network, authentication occurs through delegation, and only the group manager can later reveal the real identity in case of

disputes. The scheme employs bilinear pairings and elliptic curve cryptography to sign and verify messages efficiently. The use of proxy group signatures ensures that any member of a group can sign messages on behalf of the group without revealing their individual identity. It simplifies key management by removing the need for conventional public key infrastructures and supports fast handover authentication, critical for mobile mesh clients.The scheme assumes a complex hierarchical trust infrastructure and requires trusted setup and secure key distribution. If the root authority or domain managers are compromised, user privacy and system integrity may be at risk[100].

In 2017, KaraoğlanAltop et al. proposed a distributed key establishment protocol that addresses the absence of a trusted third party (TTP) in WMNs by enabling collaborative key generation among mesh nodes. Using elliptic curve identity-based cryptography (EC-IBC), DKEM distributes the network's master private key across multiple mesh routers through threshold and additive secret sharing mechanisms. The protocol ensures that a coalition of mesh routers (above a threshold) is required to reconstruct private keys, making the system more resilient to node compromise. The DKEM design is optimized for resource constraints, with mesh routers handling computationally intensive tasks and mesh clients focusing on minimal processing. Additionally, the protocol incorporates a repeat-request mechanism to improve success rates during key generation under dynamic conditions.DKEM offers a robust, fully distributed, certificate-less key establishment mechanism that removes the dependency on centralized infrastructure, enhancing resiliency in hostile or ad hoc environments. However DKEM assumes secure initial authentication channels and physically tamper-resistant mesh routers[101].

In 2017, Regan and Manickam introduce Adaptive Learning-Based Routing Protocol (ALRP) for WMNsto counter malicious behaviors especially wormhole attacks in wireless mesh networks by combining adaptive learning techniques with a layered security model. The system works on two levels: (1) using two-hop neighbor information to detect abnormalities in routing behavior, and (2) applying a learning mechanism at the mesh router using Bloom filters to track IP and MAC address

patterns. Cluster heads play a critical role in managing security, analyzing traffic, and isolating malicious nodes based on traffic deviations. The protocol aims to adapt to changes in network topology and attack patterns in real time, using minimal overhead. ALRP integrates machine learning principles into network routing to enable dynamic detection and prevention of attacks. By continuously updating trust metrics and using low-cost data structures like Bloom filters, it effectively balances computational complexity with real-time responsiveness, making it suitable for hybrid WMNs.However Bloom filters may yield false positives, and the scheme's success heavily depends on the proper tuning of learning parameters and cluster head configurations[102].

In 2017, Mohamed Abd-El-Azim Hossa et al. proposed an intelligent, automated intrusion detection system (IDS) tailored for detecting black-hole and gray-hole attacks in Mobile Ad Hoc Networks (MANETs). The proposed solution integrates Adaptive Neuro-Fuzzy Inference Systems (ANFIS) with Genetic Algorithms (GA) to enhance the efficiency and accuracy of a fuzzy logic-based IDS. This model automates the generation and optimization process. It begins by extracting key behavior parameters Forward Packet Ratio (FPR) and Average Destination Sequence Number (ADSN) as inputs. These metrics are used to determine the trustworthiness (Fidelity Level) of a node. The system operates in stages: data collection and preparation, ANFIS initialization (using Gaussian membership functions), and GA optimization, which tunes the parameters to minimize classification errors. Nodes are labeled as legitimate or malicious based on whether the output fidelity level exceeds a threshold. Once detected, malicious nodes are blacklisted, excluded from routing tables, and information about them is propagated across the network. It achieves high detection accuracy while adapting well to different types of malicious behaviors. The results showed significant improvements in Packet Delivery Ratio (PDR) in both low and high mobility scenarios, recovering up to 37.8% of delivery loss caused by black-hole and gray-hole attacks. But the effectiveness is highly decline as the mobility increase[103].

In 2017, S. V. N. Santhosh Kumar and YogeshPalanichamy proposed S-SELDRIP which is a lightweight protocol developed to strengthen data dissemination security in distributed wireless sensor network environments, especially those involving multiple owners and users. It is designed to minimize communication overhead during data dissemination while maintaining robust security measures. Functioning within a multi-owner, multi-user framework, S-SELDRIP allows network owners to delegate dissemination rights to selected users. This delegation enables users to distribute data on behalf of the owners, facilitating scalable and efficient data management across large networks. The protocol is organized into five key phases:

System Initialization and Setup: This phase involves generating partial group public and private keys.

Registration of Network Owners and Users: Both owners and users are authenticated and registered. Network owners register with the AS and network users register with network owner.

Optimal Routing Path Construction: The protocol determines the most efficient paths for data transmission using Energy efficient rule base routing(EERBR).

Data Packet Transmission: Data is securely transmitted across the network using group digital signature.

Packet Reception and Verification: Received packets are verified to ensure their integrity and authenticity, using timestamp and group key.

S-SELDRIP intelligently identifies which sensor nodes require the disseminated data and employs multi-hop communication to deliver it. This selective dissemination approach reduces unnecessary flooding and improves routing efficiency. Compared to traditional protocols, S-SELDRIP has demonstrated better energy efficiency by leveraging selective dissemination and minimizing control packet overhead. However, one limitation is its sensitivity to high node density[104].

In 2018, Xu et al. developed ESMAV scheme to ensure secure communication within vehicular networks, supporting both Vehicle-to-Vehicle (V2V) and Vehicle-

to-Infrastructure (V2I) interactions over LTE-V wireless technologies. It provides a reliable and secure radio interface crucial for seamless vehicular communications. The scheme is structured into four primary phases: system initialization, anonymous identity generation and message signing, message verification, and identity tracking. Each of these stages is vital for maintaining both the security and the efficiency of the overall communication process. In the system initialization phase, essential cryptographic parameters and keys are generated, forming the foundation for secure operations in later phases. The anonymous identity generation phase enables vehicles to create pseudonymous identities, thereby protecting real user identities and enhancing privacy during communication sessions. During the message signing phase, vehicles use cryptographic methods to sign messages, ensuring their authenticity and protecting their integrity during transmission. The message verification phase involves validating the received messages to confirm that they have not been altered or tampered while in transit. The final identity tracking phase allows for authorized monitoring of vehicle identities, enabling authorities to trace communications when necessary, without compromising everyday user privacy. ESMAV offers a comprehensive security framework that supports privacy preservation, defends against multiple types of cyber attacks, ensures accountability through non-frameability, and provides non-repudiation capabilities. But the absence of an efficient revocation system. If a vehicle's credentials are compromised the system lacks a practical way to revoke that identity or key[105].

Table 2.4: Comparative analysis of Packet authentication techniques

Year	Approach	Strength	Weakness
2003[94]	Hop-by-hop authentication using TESLA and key chains	- Efficient - Supports multicast - Not routing protocol-dependent	- Requires long key chains - Vulnerable to key compromise over time
2008[95]	Comparison of authentication schemes using simulations	- HEAP is low-latency - Memory-efficient - DoS-resistant	- TESLA has high latency - Requires synchronization - LHAP vulnerable to insider attacks
2010[96]	ID-based threshold cryptography	- Resilient to Sybil and certificate spoofing - Avoids single point of failure	- Complex certificate handling - Requires secure regional grouping
2012[97]	ECC-based anonymous authentication	- Low overhead - Supports hop-by-hop authentication - Resists replay	- Assumes secure ECC environment - Implementation complexity may vary
2013[98]	Comparative analysis of HWMP secure variants	- Detailed vulnerabilities analysis - Presents new security requirements	- No existing protocol meets all security goals - High complexity in mutable field protection
2014[99]	Cluster-based use of Aggregate MACs (AMAC)	- Reduces transmission overhead - Maintains	- Limited to certain scenarios - Conflicts between AMAC and

		authentication	aggregation reduce flexibility
2016[100]	Proxy + identity-based signatures for authentication	- Provides anonymity - Efficient mutual authentication - Reduces PKI reliance	- May introduce proxy trust issues - Identity leakage risk under strong attacks
2017[101]	Identity-based cryptography + threshold secret sharing	- High resilience - Avoids TTP - Efficient under certain thresholds	- Trade-off between security and performance - Low thresholds needed for fast setup
2017[102]	Machine learning for malicious node detection in routing	- Improves packet delivery and delay - Detects wormhole attacks	- May increase computation - Detection efficacy depends on training and thresholds
2017[103]	Adaptive Neuro-Fuzzy Inference System (ANFIS) optimized with Genetic Algorithm (GA)	- Automates fuzzy system creation - Effectively detects black-hole and gray-hole attacks - Uses ANFIS and GA for optimization	- Requires careful parameter tuning - May have overhead due to optimization stages
2017[104]	Distributed protocol with hop-by-hop authentication for data dissemination in WSN	- Overcomes single-point failure - Provides hop-by-hop authentication - Energy efficient - Scalable for	- Still requires trusted third party (AS) - Limited to urban settings - Does not fully protect against all security

		distributed systems	threats
2018[105]	Identity-based message authentication scheme with batch verification for LTE-V networks	- Efficient and scalable - Supports mutual authentication - Provides privacy preservation and non-frameability - Reduces signaling overhead	- May require strong trusted entities - Batch verification adds complexity - Does not fully eliminate impersonation risks

2.4 Summary

Chapter 2 presents an extensive review of existing security features in Wireless Mesh Networks (WMNs), highlighting their strengths and shortcomings. It critically examines various authentication mechanisms, including Pre-Shared Keys (PSK), certificate-based, identity-based, and ticket-based protocols, noting that many solutions either compromise performance or lack resistance to internal threats. The chapter also explores handoff authentication protocols designed to maintain secure connectivity for mobile users; however, most existing schemes suffer from security vulnerabilities or impose excessive storage and computational burdens on resource-constrained devices.

Further, the chapter analyzes secure routing mechanisms aimed at detecting and mitigating malicious activities like black hole, gray hole, and wormhole attacks. Despite several trust-based and cryptography-driven routing approaches, many fail to achieve a balance between scalability and accurate threat detection. Additionally, data packet authentication methods leveraging cryptographic keys, hashing, or digital signatures have been studied, yet they often introduce processing delays and are inadequate in countering advanced attacks like packet tampering or injection.

Overall, this chapter identifies the need for efficient, lightweight, and scalable security mechanisms specifically designed for WMNs. The limitations of current approaches in addressing fast authentication, secure handover, trustworthy routing, and reliable data integrity form the basis for the novel solutions proposed in the subsequent chapters.

Chapter 3

MUTUAL AUTHENTICATION AND SECURE HANDOVER PROTOCOL FOR WIRELESS MESH NETWORK

3.1 Overview

Wireless Mesh Networks (WMNs) have become the preferred choice for service providers due to their cost-effectiveness and ability to provide extensive network coverage. However, ensuring secure and seamless handoffs in such networks poses a significant challenge due to client mobility and the inherently open nature of the medium. Additionally, the resource constraints of client devices necessitate lightweight computation and communication during both handoff authentication and login authentication phases, which are the focal points of this work. To address these challenges, this work proposes a authentication scheme tailored for WMNs. The scheme revolves around the use of dynamically generated tickets and encrypted session data to facilitate secure communication within the network. These tickets ensure that only authorized nodes can initiate connections, the proposed scheme is the integration of cryptographic techniques, including symmetric and asymmetric encryption. These techniques bolster the security of the authentication process, providing resilience against various security threats . By leveraging these cryptographic mechanisms, the scheme ensures the authenticity of network entities. The proposed authentication scheme addresses the challenges of secure handoffs and lightweight authentication in WMNs. Through the use of dynamically generated tickets and cryptographic techniques, it provides a secure and efficient solution for authentication. Our proposal is effective in terms of the overhead associated with authentication, according to the performance and security analyses.

3.2Proposed System

The proposed system is an authentication methodology based on tickets issued by Ticketing Agents (TA), who would be a trusted third party, in order to strike a healthy balance between security and efficiency.

3.2.1 Trust Model : In the trust model, the TA is a central authority who issue the ticket for MRs and MCs, but the transfer ticket is issue by the Home Mesh Router(HMR). The trust relationship is as shown in Figure: 3.1.

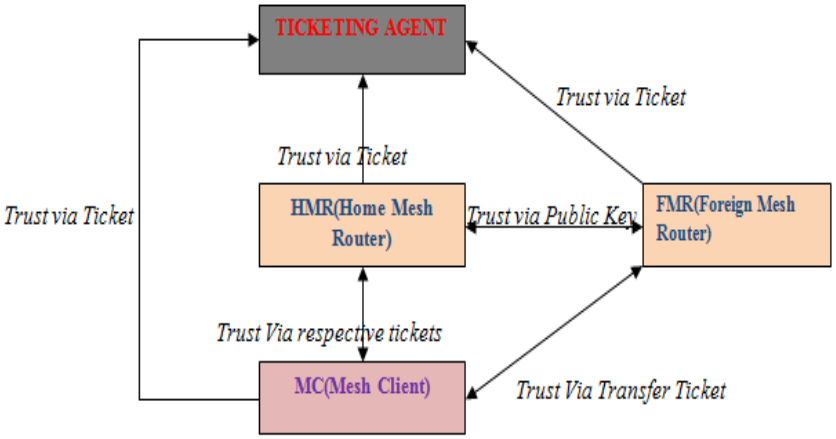

Fig 3.1: Trust relationship among entities

- TA-HMR: Trust between TA and HMR is via Ticket issued by TA, the ticket is signed by the TA which is verified by HMR.
- TA-MC: Trust between TA and MC is via Client ticket issue by TA that can be verified by the Client.
- HMR-MC: Mutual trust between MC and HMR is via their respective ticket issued by TA
- HMR-FMR(Foreign Mesh Router): The two neighbouring MRs trust each other by public key Crypto system.
- MC-FMR: MC and FRM trust each other by transfer ticket issued by HMR.

3.2.2 Different Types of Tickets: There are three types of tickets employ in the proposed protocol

Client Ticket*(Tc)*:The MC ticket is issued by *TA* and the MC submit this ticket to HMR to prove it is a legitimate user of the network

$T_c = \{ I_c, I_A, P_c, \varsigma_{exp}, Sig_A \}$

Where

I_C : Identity of MC who is having the Ticket issued by TA

I_A: Identity of the TA who issued the Ticket.

P_c: Public Key of the Client who is having the Ticket.

ς_{exp}: Expiry time of the ticket.

Sig_A: Signature of the TA who is issuing the ticket.

Mesh Router Ticket*(T_M):* MR ticket issue by TA upon request by any MR

$T_M = \{ I_M, I_A, P_M, \varsigma_{exp}, Sig_A \}$

Where

I_M : Identity of MR who is having the Ticket issued by TA

I_A: Identity of the TA who issued the Ticket.

P_M: Public Key of MR who is having the Ticket.

ς_{exp}: Expiry time of the ticket.

Sig_A: Signature of the TA who is issuing the ticket.

Transfer Ticket *(Θ_c)* : A transfer ticket issue by MR

$\Theta_c = \{ I_{CR}, I_M, I_A, \varsigma_{exp}, V_{KMAC}(I_{CR}, I_M, I_A, \varsigma_{exp}) \}$

Where

I_{CR} : Anonymous Identity of MC who is having the Ticket issued by HMR.

I_M : Identity of MR who is Issue ticket to MC.

I_A: Identity of the TA.

ς_{exp}: Expiry time of the ticket.

3.2.3 Login Authentication Protocol: Assuming that the MR had a ticket from TA and the MC also received its ticket from the TA. Each MR periodically broadcast its ID in its coverage area to declare that it is ready to accept an incoming connection.

1. A Mesh Client C moves into the coverage area of HMR received the ID, It submit Its ticket T_C along with a nonce N_C. HMR check the expiry, If not expired it verify the signature Sig_Apresent in the ticket.

2. Upon successful verification, MR generate a nonce N_M and calculate $K_{MAC}=N_C||N_M$, Encrypt Its own ticket T_M along with nonce N_M and $V_{KMAC}(N_C)$ with the public Key of the client present in the ticket received from the client ticket.

3.Upon receiving the encrypted message C decrypt with its private Key. The expiry time and Sig_A is verified. If the verification is successful, C calculate $K_{MAC}=N_C||N_M$ and verify $V_{KMAC}(N_C)$. If the verification is successful, It send back $V_{KMAC}(N_M)$ to proved that it successfully calculate K_{MAC}.

4. When the HMR received $V_{KMAC}(N_M)$, it calculate $V_{KMAC}(N_M)$ from the K_{MAC}that is already generated , it compare $V_{KMAC}(N_M)$ it calculate and the one it received, If they are match it authenticate the MC. From this point K_{MAC} is used as a session key and the session is encrypted with session key. The HMR generate transfer ticket Θ_c and send it to a client. The identity of MC in transfer ticket is as $I_{CR}= H(I_C||N_M)$ to protect client identity while roaming to FMR. Also $\{\Theta_c,K_{MAC}\}$ is send to each one hop neighbor by HMR encrypted with their own public key.

3.2.4 Handover Authentication Protocol: Proposed Handover Authentication Protocol(HAP) is an enhancement of Lai et.al.[52], It works base on the Elliptic curve Deffiehellman Key Exchange protocol(ECDKE) with pre-computation of some information without necessity of the prior knowledge of the next FMR to visit, the pre-computation facilitate fast handover authentication with little storage overhead.

In order to employ ECDKE for fast handover, It is assumed that the elliptic curve domain parameters is known to MC and FMR. The domain parameters (a,b,p,G,n) are

a,b : coefficient of the elliptic curve

p : size of the finite field(prime)

G: base point of the elliptic curve

n: order of the elliptic curve

When a MC received handover ticket from HMR it perform the following action:

(1) It generate private Key N_{CH} such that $1< N_{CH}<$ n

(2)Calculate $N_{CH}G$

(3) Calculate H($\Theta_c || N_{CH}G||I_{CR}$)

keep it ready for fast handover, Similarly each MRs in the neighborhood of HMR perform the following :

(1) It generate private Key N_{FH}such that $1<N_{FH}<$ n

(2)Calculate $N_{FH}G$

(3) Calculate H($\Theta_c || N_{FH}G||ID_F$) ($ID_F$ is identity of FMR)

keep it ready for fast handover.

When a MC enter the area of FMR where it find better signal strength with the ID_F broadcast by FMR. Then the handover authentication protocol is carried out as follows:

1. The roaming Mesh client submit {H(Θ_c|| $N_{CH}G$||I_{CR}), $N_{CH}G$, I_{CR}}(note that H(Θ_c|| $N_{CH}G$||I_{CR}) is pre-calculated) to FMR, Upon receiving {H(Θ_c|| $N_{CH}G$||I_{CR}), $N_{CH}G$, I_{CR}} from Client, FMR identify corresponding ticket from its database using I_{CR} and if not expired, It verify the validity of the received message from Θ_c received from HMR and $N_{CH}G$, I_{CR} received from MC. If valid, It calculate new K_{MAC} value as $K_{MAC}=N_{FH}N_{CH}G$, then it send back {H(Θ_c|| $N_{FH}G$||ID_F), $N_{FH}G$, $V_{KMAC}(N_{CH}G$)} to MC.

2.When the MC received {H(Θ_c||$N_{FH}G$||ID_F), $N_{FH}G$, $V_{KMAC}(N_{CH}G$)}(note that H(Θ_c||$N_{FH}G$||ID_F) is pre-calculated), It verify H(Θ_c||$N_{FH}G$||ID_F), if valid it calculate $K_{MAC}=N_{FH}N_{CH}G$ and verify $V_{KMAC}(N_{CH}G)$, if the verification is successful the MC authenticate FMR and send back $V_{KMAC}(N_{FH}G)$.

3. When the FMR received $V_{KMAC}(N_{FH}G)$ and verified, It authenticate the MC.

3.3 Security Analysis: This section provides a detailed evaluation of the proposed authentication protocol, analyzing its effectiveness against common security threats and how it achieve security and privacy.

3.3.1Mutual authentication: Mutual authentication means both the communicating parties verifies each other for legality to access the network. In the proposed protocol both parties exchange their ticket, the signature of TA present in the ticket provide legality information of both parties. Mesh Access point Encrypt Its ticket with public Key of the client, Only the client can decrypt and extract a nonce N_M. Even though N_C is transfer in the plain text, an attacker do not have the knowledge of N_M it cannot calculate K_{MAC}, if K_{MAC} cannot be calculated the correct value of $V_{KMAC}(N_M)$ cannot be calculated. Also $K_{MAC}$is send to FMR in encrypted form ,only Client and FMR can generate valid V_{KMAC}so that mutual authentication can be achieved in handoff authentication. Message exchanges and computation in communicating parties in login and handover authentication protocol is shown in figure 3.2.

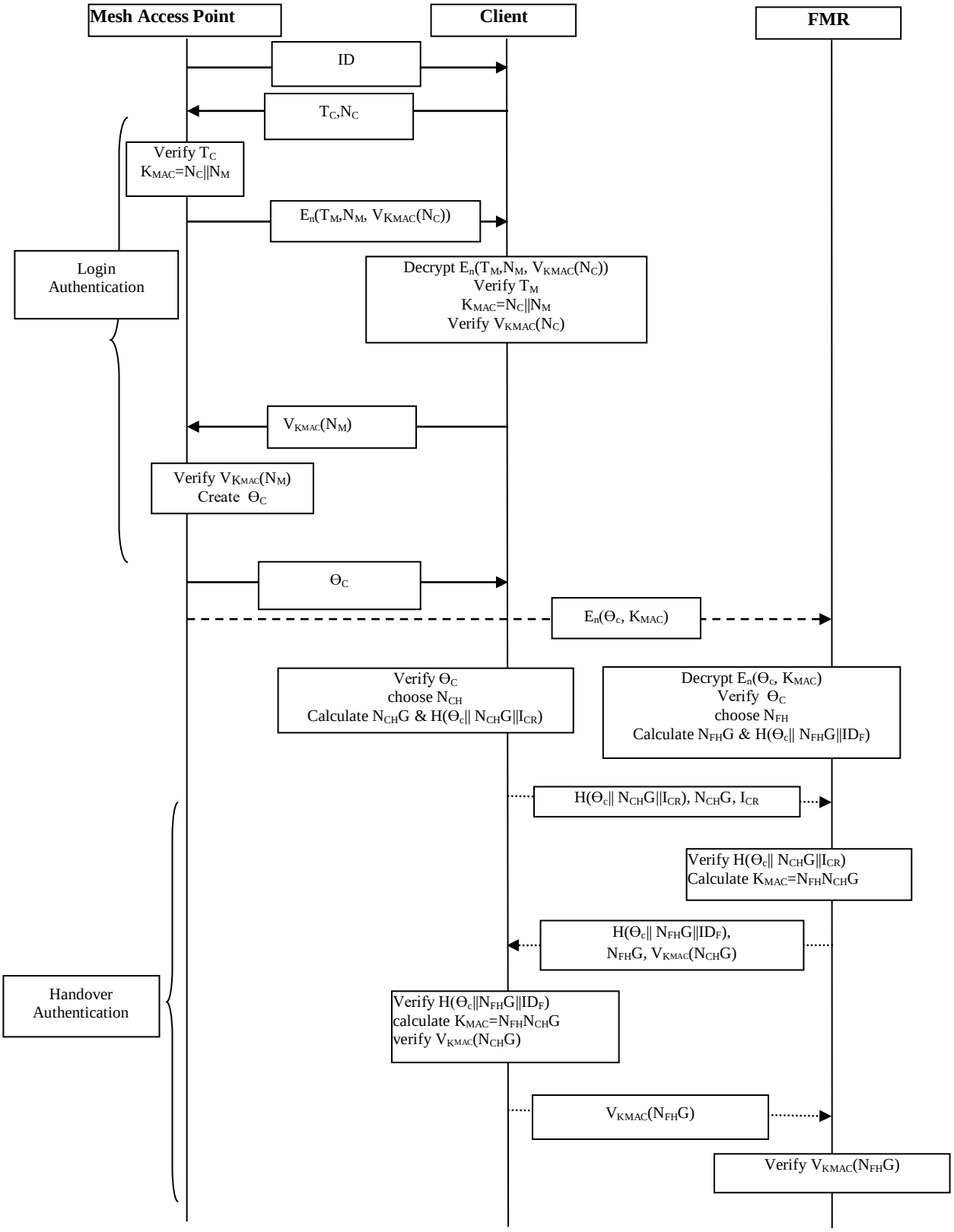

Fig 3.2: Login and Handover Authentication

3.3.2 Replay Attack: An attacker listening communication channel may replay these messages later to gain access the network or to make the client to believed him/her a valid Mesh Access point. An encryption of random nonce N_M protect replay attack. Without the knowledge of N_M valid K_{MAC} cannot be generated during login authentication.In handoff authentication K_{MAC} and transfer ticket is encrypted to FMR, It is impossible for adversary to generate valid digest of the ticket.

3.3.3 Forgery Attack: In login Authentication the ticket and signature of TA ensure that the tickets are not modified. In handover authentication any modification will be easily detected by either parties because they have exactly same transfer ticket and K_{MAC}.

3.3.4 Privacy: Privacy of the client is protected while roaming. The real identity is used only in the initial login authentication subsequent Mess Access Points do not have the knowledge of the real identity of the client.

3.3.5 Forward backward security: The proposed protocol achieved forward backward security by creating new session key each time handover take place, the Mesh Client and FMR generate new Nonce, these new Nonces are combine with the base point in an elliptic curve before exchanging between them. It is protected by elliptic curve discrete logarithm problem.

3.4 Performance analysis: The performance is analyzed based on

the number of cryptographic operation involved and message exchange during login and handover authentication, for this we refer the comparison table from [52] and [65] even though they applied different algorithms for some operation like Signature verification(RSA-1024 and ECDSA respectively), Hash(SHA-1 and SHA-2 respectively) etc. Both of them have same amount of computational time for same algorithm(RSA encryption and decryption)Table 3.1. shows the comparison of proposed protocol with the similar existing protocol, the proposed protocol perform better in login authentication latency this is because the number of message exchange and cryptographic operation is reduced without lowering security threat. In handover authentication, proposed protocol it is slightly better than [52] due to the pre-

computation of point multiplication on Elliptic curve, [65] protocol have low latency during handover but it suffer from security threat like forgery attack on transfer ticket, absence of forward backward security.

Table 3.1: Performance Comparison of Proposed protocol with Existing protocols

		Ours		Lai et al[52].		Roy et al[65].	
operation	Time(ms)	Login	Handover	Login	Handover	Login	Handover
T_E(RSA-1024)	1.420	1	0	2	0	2	0
T_D(RSA-1024)	33.30	1	0	2	0	2	0
T_{Sig}(RSA-1024)	33.30	0	0	0	0	0	0
T_{Ver}(RSA-1024)	1.420	2	0	2	0	2	0
T_{MAC}(HMAC)	0.015	5	4	0	5	6	4
T_H(SHA-1)	0.009	1	2	6	3	0	0
T_{PMUL}(ECC-128)	~0.376	0	2	0	2	0	0
Number of Transmission		4	3	6	3	6	2
Authentication latency		37.644+4d	0.83+3d	72.334+6d	0.854+3d	72.37+6d	0.06+2d

3.5 Conclusion: The rapid login authentication algorithm for wireless mesh networks we offered in this study reduces the computational and communication overhead, making it more practical for a device with constrained resources. The proposed protocol conforms with the required authentication security criteria. The proposed handover authentication mechanism has somewhat lower computational latency than[57] and has higher security than[65], Analysis and performance comparison show that the proposed protocol perform better compare to the similar existing protocol. Further Research could focus on developing advanced ticket management protocols that minimize latency and overhead while ensuring robust security. These protocols could incorporate techniques such as efficient ticket distribution, dynamic ticket lifetimes, and optimized ticket revocation mechanisms. The integration of ticket-based authentication with emerging technologies such as blockchain and distributed ledger technology (DLT) could offer tamper-resistant ticket issuance and validation mechanisms, enhancing the overall security and transparency of the authentication process. By exploring these future research directions, scholars and practitioners can advance the state-of-the-art in ticket-based authentication for wireless mesh networks, paving the way for more secure, efficient, and resilient network infrastructures in the future.

Chapter 4

PRE-DISTRIBUTED TICKET BASE CLIENT HANDOFF AUTHENTICATION PROTOCOL FOR WIRELESS MESH NETWORK

4.1 Overview

A major issue in WMNs is handoff delay, which occurs when a mobile client moves out of the range of its current mesh router (Home Mesh Router, HMR) and needs to connect to a new one (Foreign Mesh Router, FMR). This handoff process is crucial for maintaining communication quality but often leads to problems such as increased communication delay and security vulnerabilities.

As mesh clients move, the signal-to-noise ratio (SNR) drops, prompting the need for a new router with better signal strength. However, this dynamic behavior complicates secure and efficient authentication. Existing security methods struggle due to high overhead and poor key management. This work identifies a persistent gap in ensuring fast, lightweight, and secure handoff authentication and proposes a new approach to address this. The proposed method focuses on speed and security. This work presents a pre-distributed ticket based authentication scheme for handling the client handoff in WMNs. The proposed work is one way authentication that is the Mesh Client is authenticated by Mesh Router and the initial login Authentication is not cover in this work.

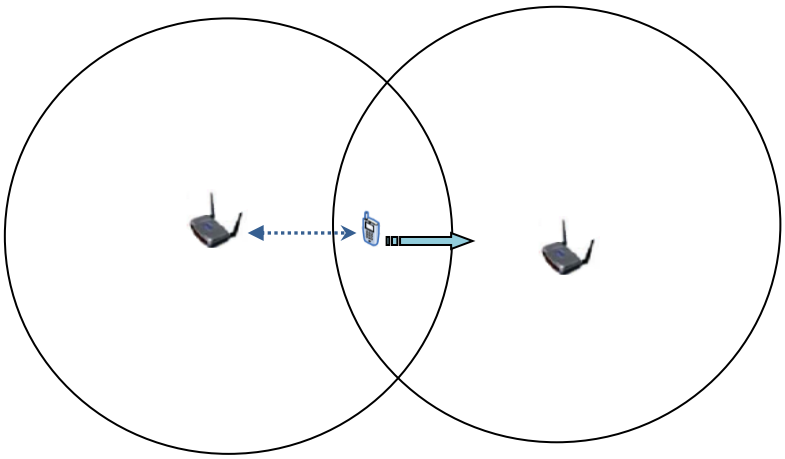

Fig 4.1: Handoff scenario for Wireless Mesh Network

4.2 Proposed system

In the proposed system, it is assumed that there exists a trusted Central Ticketing Agent (CA) who is responsible for generating tickets and distributing the ticket to the Mesh Routers. It is also assumed that all mesh entities are synchronized with the same timer clock which is monotonically increasing. In the proposed protocol it is not required to have a pair-wise master key or group key so the key management overhead is reduced. The CA is also responsible for key generation and distribution to the other nodes.

Table 4.1: Notation

NotationUsed	**Description**
g	Generator
modp	Moduloprime
HMR	HomemeshRouter
FMR	ForeignmeshRouter
CA	CentralTicketingAgent
PU	Publickey
PV	PrivateKey
SK	Sharedsecretkey
T_i	TransferTicketofClienti

4.2.1 Initialregistrationphase

In the initial deployment of the network, each Mesh Router and Mesh Client must register to the CA. In the registration process, the CA provide g and p to the mesh

entities, the CA give its public key for signature verification and assign private Key PV to each entity and a public key PU is calculated as

$$PU = g^{pv} \bmod p$$

If the newly register node is $Client_i$, the CA generates transfer ticket T_i, and the ticket is distributed to all the Mesh Routers.

$$T_i = \{ID_i, t, Sig_{CA}\}$$

ID_i:IdentityofClient$_i$

t: life duration of ticket after issued by Mesh Router

Sig_{CA}:SignatureofCA

4.2.2 Handoff Authentication phase

After successful authentication of Mesh Client by HMR, it moves to the area of FMR where it finds better signal strength, then the handoff process is taken place as the following steps.

Roaming $Client_i$ send a handoff request message to HMR along with the ID of which FMR, it wishes to connect. Each Mesh Router knows the identity and public key of one-hop neighbours for routing functionality[62]

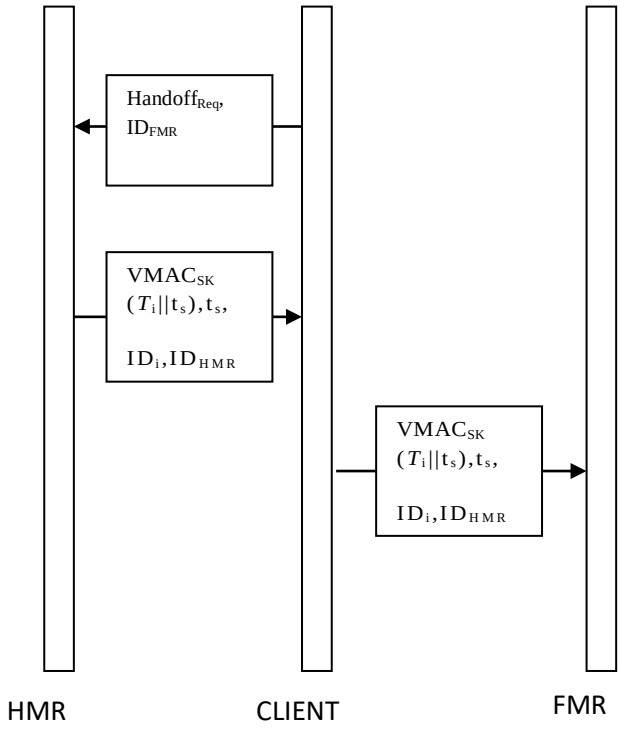

Fig 4.2: Handoff Message exchange

Upon receiving the request, the HMR calculate SK and it share with targeted FMR as follows

$$SK=PU_{FMR}{}^{PV} \text{mod} p$$

*(*This can be calculated in advanced in order to reduce computational time*)*

Sends a message M to Mesh Client.

$$M = \{ VMAC_{SK} (T_i||t_s), t_s, ID_i, ID_{HMR} \}$$

$VMAC_{SK}(T_i||t_s)$:Key Hash value of ticket afterconcatenating withthe timestamp.

t_s:thetimestampofsendingticketto$Client_i$

ID_i:Identity of $Client_i$

ID_{HMR}:IdentityofHomeMeshrouter

Client$_i$ forward the message M to targeted FMR, upon receiving M, FMR marks the time of received (t_r) and perform the following

- Extract ID_{HMR} and calculate SK (*This can be pre-calculated*)
- ID_i is extracted and the corresponding ticket T_i is identified.
- Calculate $VMAC_{SK}(T_i||t_s)$

The Client is authenticated if the following conditions are satisfied:

1) Calculated $VMAC_{SK}(T_i||t_s)$= Received $VMAC_{SK}(T_i||t_s)$
2) $t_s < t_r$
3) $t_r - t_s \leq t$

4.3 Security Analysis

(1)The handoff ticket is generated at the time of registration and distributed, this handoff ticket cannot be forge by any mesh router due to the signature on the ticket itself, any attempt to forge can be easily detected by verifying the signature.

(2)In the handoff process the ticket is transfer in MAC form which can be produced by the home mesh Router and foreign mesh router only because no other mesh router can generate same MAC key.

(3) If an adversary capture message exchange in a handoff process and try to produce this message later on to the foreign mesh router, this can be easily detected by $VMAC_{SK}$ ($T_i||t_s$), since t_s is the timestamp which cannot be valid later on.

4.4 Performance Analysis

(1) The handoff ticket generation is one time and it is in initial registration and it does not effect performance in handoff process.

(2) $VMAC_{SK}$ is calculated two times, one each in home mesh router and foreign mesh router. Two message transfer, one from Home Mesh router to Client and another from Client to Foreign Mesh Router.

(3) Mesh Client is free from any computation.

4.5 CONCLUSION

The proposed protocol minimized the computational overhead and number of message exchanges during handoff process to authenticate the client. It is only one side authentication process. The handoff latency reduction is at the expense of storage overhead on the Mesh Router, but the client is free from computation and storage overhead.

Chapter 5

ENHENCEMENT OF AODV ROUTING PROTOCOL TO COUNTER BLACKHOLE ATTACK

5.1 Overview

Wireless Mesh Networks (WMNs) offer flexible and scalable communication solutions but are vulnerable to various security threats, including black hole attacks. These attacks take use of routing systems' reactive nature like the Ad hoc On-Demand Distance Vector (AODV), which is commonly employed in WMNs. Black hole attacks disrupt network operations by falsely advertising optimal paths, leading to data packet losses. To tackle this, we propose a detection mechanism that identifies malicious nodes in AODV-based WMNs. Our approach utilizes destination sequence number comparison and hop count verification to identify inconsistencies caused by black hole nodes.

AODV is the most commonly used on-demand routing protocol among all available options. However, since security was not a primary focus during its development, malicious nodes can exploit vulnerabilities in the protocol to carry out various attacks. During the route discovery phase of AODV, when a source node broadcasts a Route Request (RREQ) to find a route to the destination, the malicious node responds with a Route Reply (RREP) that claims it has a fresh route to the destination. The malicious node sets a high sequence number in the RREP, indicating that its route is fresher than any other routes that might be discovered. The source node, trusting this information, updates its routing table to direct traffic to the malicious node, believing it to be the quickest and most reliable path. Once the malicious node successfully inserts itself into the routing path, it intercepts all data packets intended for the destination. Instead of forwarding these packets, the malicious node discards them, effectively creating a "black hole" where data enters but does not emerge from the other side. When a single

malicious node attacks the network, it is called single black hole attack but when multiple black hole node work together it become cooperating black hole attack. This kind of attack greatly reduce network performance.

5.2 Proposed Protocol

One of the advantages of AODV routing protocol is the ability of an intermediate node send route reply if it has a valid route, this greatly reduce route discovery time if the network size is large. But this open opportunity for an attacker to send fake route reply to disguise the source node in order to attract data traffic. This paper aim to reduce route discovery time and detect black hole node. In order to achieve these the following assumptions are made:

- The source node and the destination node are not black hole node.
- Even if the cooperating black hole nodes exist, the black hole node who receive route request always send route reply instead of forwarding to another black hole node.
- Black hole node does not have intelligence to calculate destination sequence number or hop count.
- Black hole node does not changes behavior.
- Other types of attack are not considered in the proposed protocol.

In the proposed protocol each node maintains a list of trusted nodes, If a particular node send data packet to the destination successfully this indicate that there is no black hole node, so every nodes along the path including source and destination add one another in their trusted list. This can be achieved by adding ID by each node along the path in first data packet, then the destination node can send back along with acknowledgement and each node on the path can copy this list of trusted nodes. The proposed protocol consists of three steps:

(i)Route request

(ii) Route reply and route verification

(iii) Route confirmation.

When the source node wants to send data, it broadcast RREQ, an intermediate node who does not have valid route rebroadcast RREQ ultimately when RREQ reach the destination then the destination sends back RREP, then the route is valid and data packet can be sent. An intermediate node who have valid route(or claim to have valid route in case black hole node) perform the following:

(i)Check whether the source node is trusted node.

*(a)*if so send RREP, upon receiving RREP the source node checks its own trusted list and found that the intermediate node is trusted node then data packet can be sent.

*(b)*If the source node is not trusted node, send RREP to source and send route verification message towards the destination. The route verification message has the following fields {*source ID, destination ID, destination sequence number, intermediate node ID, Hop count* for each node along the destination}

<table>
<tr><td colspan="5">Source ID</td></tr>
<tr><td colspan="5">Destination ID</td></tr>
<tr><td colspan="5">Destination sequence number</td></tr>
<tr><td>Intermediate node ID</td><td>Next node ID</td><td>…</td><td>….</td><td>…</td></tr>
<tr><td>hop count</td><td>hop count=previous hopcount -1</td><td>….</td><td>….</td><td>….</td></tr>
</table>

Fig 5.1: Route verification message format

Upon receiving route verification message, a node performs the following:

(ii)Check whether it have route to destination, whether the destination sequence number are same, if its hop counts equal to previous hop count-1. If any check is failed, declare all the nodes(*forth field*) in route verification message as black hole nodes.

If all check is pass, check whether the source is trusted node, if so send route confirmation message otherwise insert its own ID and hop count and forward to the next node.The route verification message keeps forwarding until trusted node or destination node is found.

5.3 Security Analysis

The security of the proposed protocol is validated by analyzing its ability to detect Black Hole attacks in the network. In the conducted NS-3 simulation with 30 mesh routers with 10 black hole nodes and the simulation parameter are as shown in Table 5.1, the Black Hole detection rate of each router is evaluated. Black Hole nodes in the network launch attacks by falsely advertising optimal routes, causing packet drops and disrupting network reliability. The proposed protocol incorporates a detection mechanism to mitigate this threat.

The detection performance is summarized in Table 5.2 under the "Black Hole Detection Rate (%)" column. The average detection rate achieved by the proposed protocol is **82.76%**, significantly enhancing the network's resilience compared to conventional AODV, which lacks Black Hole mitigation measures. Figure 5.2 visually represents the Black Hole detection rate for individual routers, demonstrating the proposed protocol's capability to effectively identify malicious nodes and prevent data loss caused by Black Hole attacks.

Table 5.1: Simulation parameter

Parameter	**Value**
Area	500m × 500m
Data rate	5 pks/s
Packet Size	64 bytes
Traffic	CBR
Transmission Range	250m

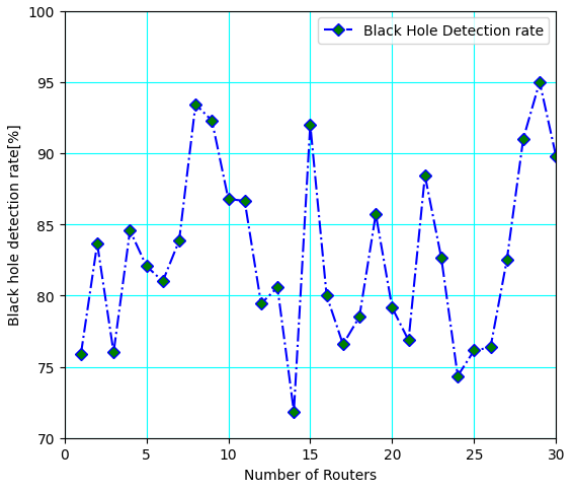

Fig 5.2 : Black Hole detection rate

5.4 Performance Analysis

To evaluate the performance of the proposed protocol, comparative simulations were conducted using NS-3 with three scenarios: AODV without Black Hole**,** AODV with Black Hole nodes**,** and theProposed Protocol**.**

Table 5.2: Throughput, Packet Delivery Ratio, End to End Delay Comparison and black hole detection rate

Routers	Throughput(Mbps)			Packet Delivery Ratio(%)			End to End Delay(ms)			Black Hole Detection rate(%)
	AODV with black hole	AODV without Black Hole	Proposed	AODV with black hole	AODV without Black Hole	Proposed	AODV with black hole	AODV without Black Hole	Proposed	Proposed
1	9.88	15.03	15.62	76.81	87.85	86.97	290.25	245.73	23.85	75.86
2	12.08	14.74	15.8	82.27	83.71	88.62	448.03	184.86	147.64	83.64
3	13.18	14.1	21.97	77.14	80.64	92.75	415.81	274.19	119.78	76
4	10.04	14.04	21.97	83.09	85.73	94.59	298.03	102.65	34.43	84.57
5	7.13	16.41	22.93	83.34	86.79	96.51	373.81	281.11	174.54	82.07
6	7.08	13.41	25.18	77.39	86.12	84.86	445.36	133.42	174.57	81
7	12.07	12.31	22.85	82.6	81.98	92.94	110.25	297.27	38.45	83.86
8	14.18	18.44	22.47	75.08	85.64	88.26	149.14	132.65	148.88	93.43
9	15.04	14.97	24.82	81.27	83.71	84.5	140.25	139.5	148.52	92.29

								7		
10	14.05	11.62	20.86	75.66	86.98	93.67	104.69	258.8	128.77	86.79
11	5.91	14.22	20.72	79.29	84.48	86.33	158.03	258.8	198.84	86.64
12	6.13	13.52	17.8	81.85	83.81	91.65	358.03	100.34	89.88	79.43
13	11.19	17.74	21.61	74.99	82.46	85.69	398.58	223.42	137.98	80.57
14	9.13	15.32	19.08	81.44	82.37	94.4	199.25	287.27	173.86	71.86
15	15.1	13.64	23.65	76.48	87.94	88.72	162.14	64.19	36.88	92
16	9.08	17.45	19.04	78.05	82.56	90.46	269.95	153.42	76.97	80
17	12.02	13.12	21.58	79.62	79.77	87.25	249.81	279.57	179.86	76.57
18	15.14	19.59	23.72	80.53	79.48	95.96	232.47	159.57	49.88	78.5
19	10.07	15.37	24.39	79.46	78.91	93.3	363.58	64.96	155.73	85.71
20	13.13	10.63	15.8	77.14	81.21	89.36	183.58	100.34	161.34	79.14
21	13.93	17.05	23.72	80.37	79.77	90.37	382.69	138.8	136.88	76.86
22	9.14	10.98	16.48	83.26	84.87	91.56	148.14	50.34	86.85	88.43
23	14.87	19.02	24.86	79.13	80.73	92.75	205.81	58.04	151.84	82.64
24	6.83	14.62	24.22	78.55	84.1	88.17	385.81	287.27	129.73	74.36
25	13.13	12.48	24.14	83.09	85.35	97.16	106.92	201.11	99.87	76.14
26	6.14	13.35	20.29	79.04	83.33	90.28	133.81	291.88	127.64	76.36
27	12.01	18.38	19.33	84.83	83.33	90.64	309.45	100.34	99.61	82.5
28	13.03	15.84	24.22	79.46	78.42	95.69	355.03	227.2	176.04	91

								7		
29	11.06	16.18	23.32	75.24	84.48	88.99	310.85	168.8	150.64	95
30	15.93	20	21.93	84.99	81.21	96.51	409.14	278.04	33.8	89.79
Avg	**11.26**	**15.11**	**21.48**	**79.72**	**83.26**	**90.96**	**269.96**	**184.80**	**119.78**	**82.76**

The following key performance metrics were analyzed:

- **Throughput**

Throughput reflects the total number of data packets successfully delivered per unit time. The proposed protocol achieved an average throughput of 21.48 Mbps, outperforming both AODV without Black Hole **(**15.11 Mbps**)** and AODV with Black Hole **(**11.26 Mbps**).** Figure 5.3(a)-(c) illustrates the throughput comparison across different protocols, demonstrating the superior data transmission capability of the proposed method.

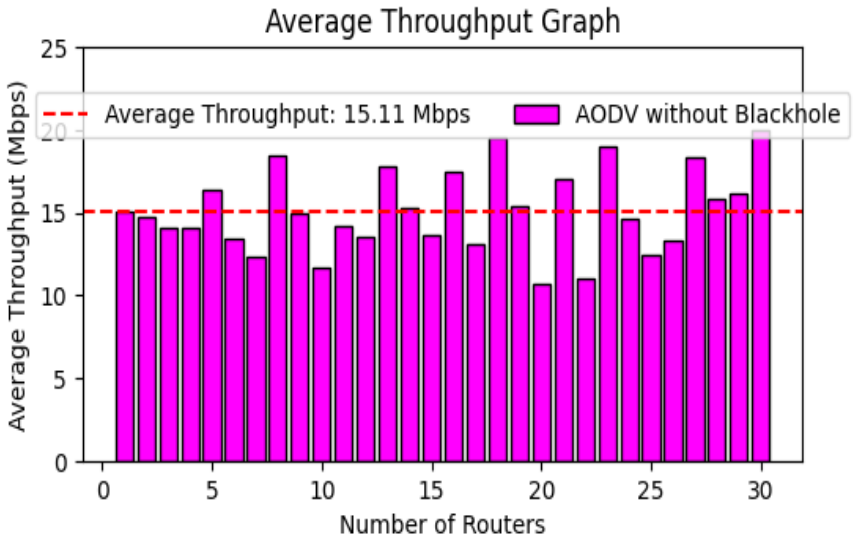

Fig 5.3 (a) Throughput for AODV without Black Hole.

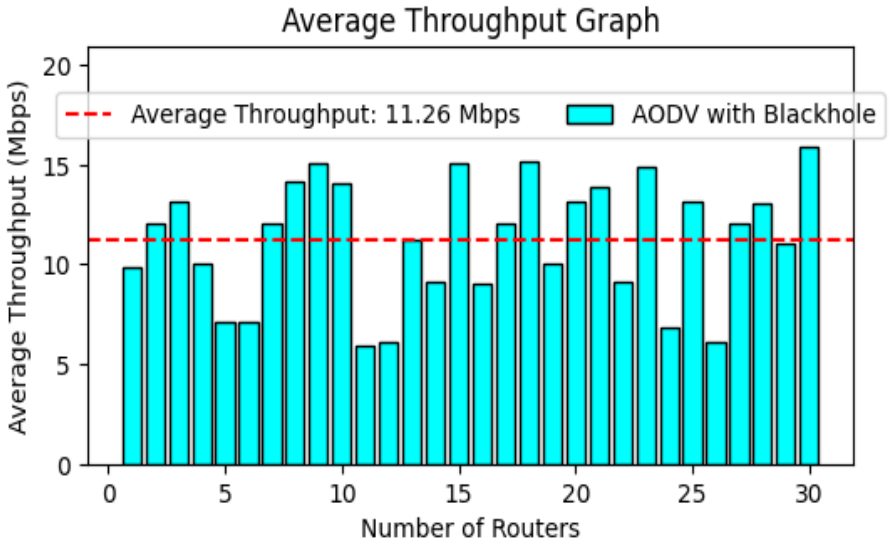

Fig 5.3 (b)Throughput for AODV with Black Hole.

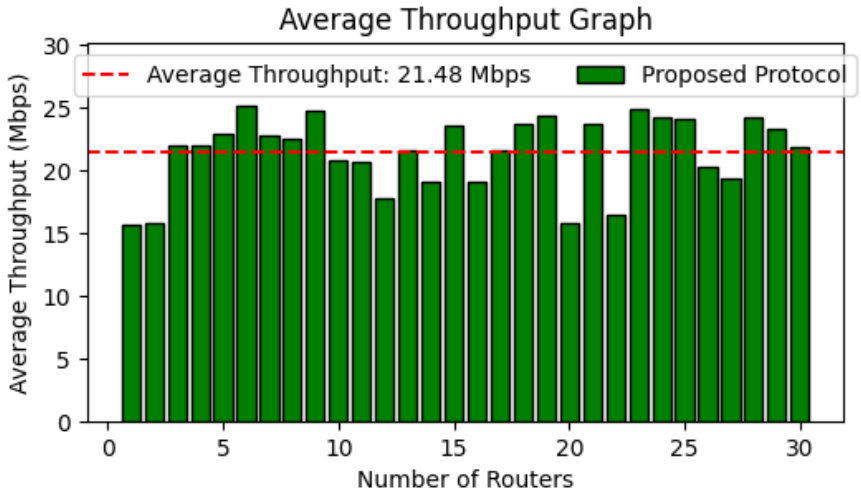

Fig 5.3 (c) Throughput for Proposed Protocol.

- **Packet Delivery Ratio (PDR)**

PDR is defined as the ratio of successfully received packets to the total packets sent. As shown in Figure 5.4(a)-(c), the proposed protocol achieved a PDR of **90.96%**, higher than AODV without Black Hole (**83.26%**) and AODV with Black Hole (**79.72%**), indicating improved reliability in packet delivery even in the presence of malicious nodes.

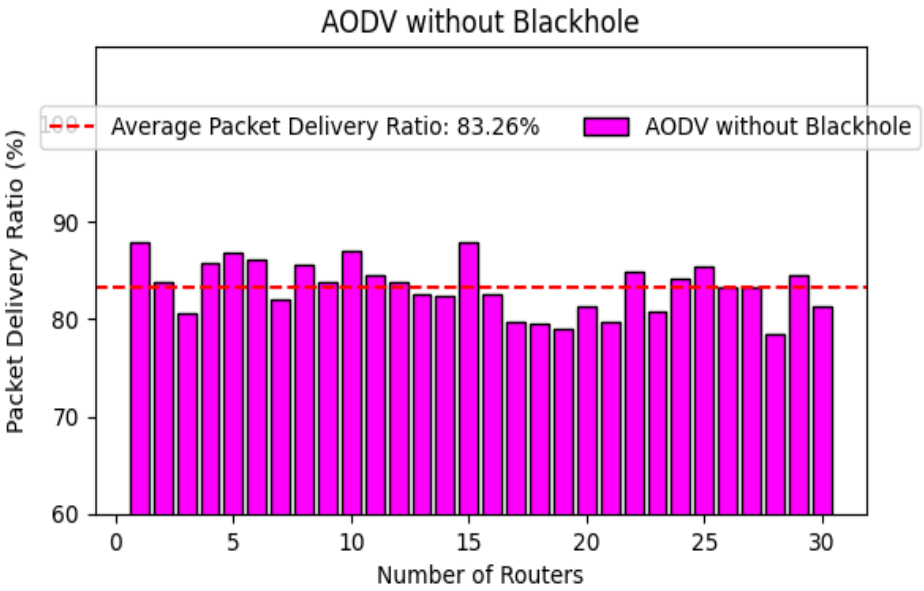

Fig 5.4 (a) Packet delivery ratio for AODV without Black Hole.

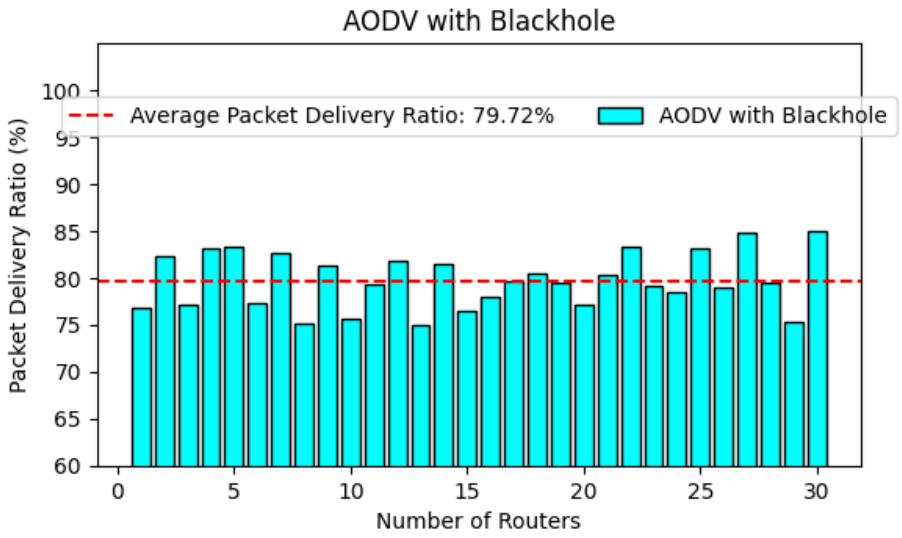

Fig 5.4 (b) Packet delivery ratio for AODV with Black Hole

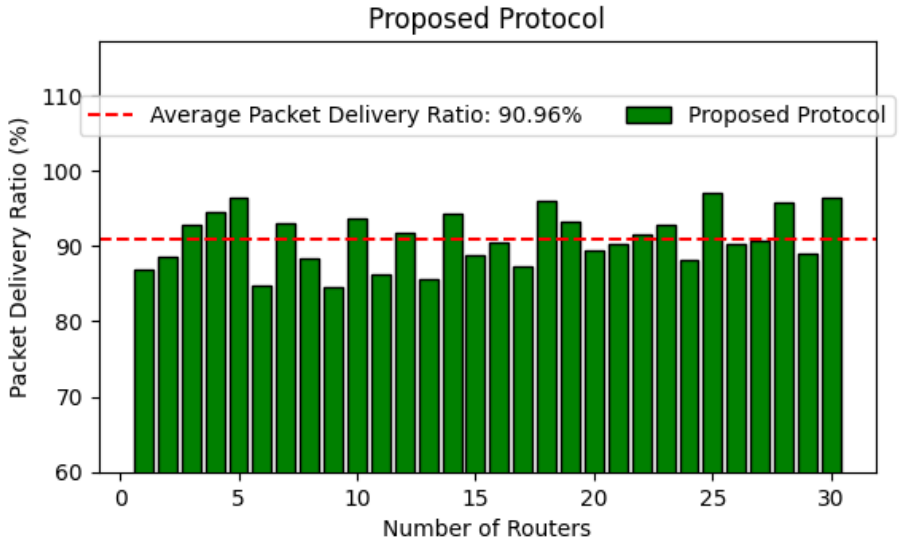

Fig 5.4 (c): Packet delivery ratio for Proposed Protocol

- **End-to-End Delay**

The average time it takes for a packet to go from its source to its destination is measured by this statistic. Lower delay indicates better performance. The proposed protocol demonstrated an average end-to-end delay of **119.78 ms**, significantly lower than AODV with Black Hole (**269.96 ms**) and without Black Hole (**184.80 ms**), as depicted in figure 5.5(a) to (c).

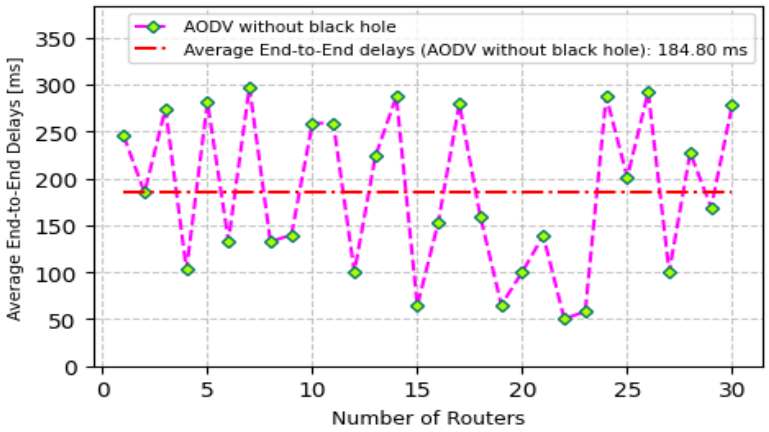

Fig 5.5(a) End to End delay for AODV without black Hole

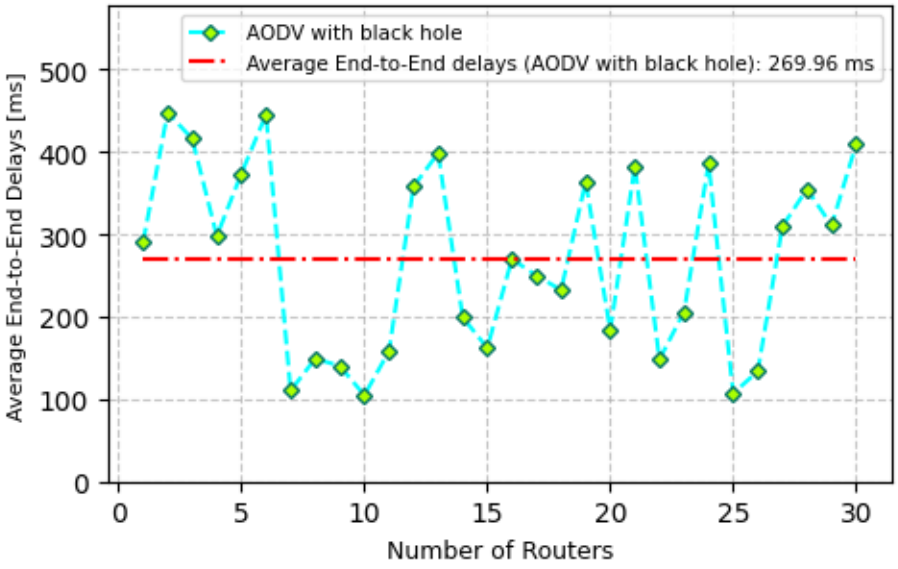

Fig 5.5(b) End to End delay for AODV with black Hole

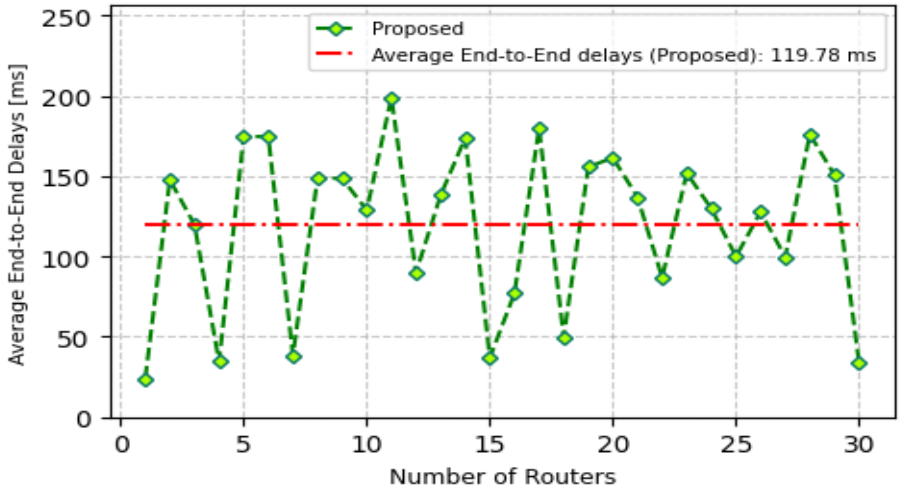

Fig 5.5 (c) End to End delay for Proposed Protocol

5.5 Conclusion

The proposed protocol detects black hole node with the help of trusted node, instead of detecting black hole node by source all the trusted node cooperating in detection of black Hole node, the proposed protocol reduces data traffic for detection of black hole node as it does not send route verification message to the source node. This also reduce bandwidth consumption. The nodes with higher number of trusted nodes perform faster in detection/route confirmation, the node highly involve in data transfer have higher number of trusted nodes. The performance of the proposed protocol in throughput, end to end delay and packet delivery ratio is better in comparison with AODV and AODV with black hole node.

Chapter 6

COMMON GROUP KEY GENERATION PROTOCOL FOR HOP BY HOP PACKET AUTHENTICATION FOR WIRELESS MESH NETWORK

6.1 Overview

The architecture offers multi-hop transmission between mesh entities to offer continuous internet access [106]. The distributed nature of WMNs allows the clients to get access to the internet within the mesh networks [107]. However, the distributed and scalable nature of WMNs prohibits the presence of centralised authority in WMNs. Due to the absence of centralised authority, WMNs has certain security limitations. Attacks could be easily launched in the absence of centralised authority in WMNs. Attacks occur during multi hop communication among mesh entities when an attacker injects harmful packets into the network, disrupting its normal functioning and leading to performance decline [108][17]. Consequently, security is a crucial concern in Wireless Mesh Networks (WMNs). In WMNs, since end-user packets are relayed in a multi-hop manner, authenticating these packets through this multi-hop process is essential [109][110]. To address such attacks, we proposed an efficient multi-hop packet authentication protocol called 'efficient packet authentication through the Diffie-Hellman approach (EPADH)'. This protocol effectively defends against well-known threats, including replay and impersonation attacks.

6.2 Proposed Protocol

The proposed EPADH creates a common group key (CGK) that is then distributed among all the mesh entities in Wireless Mesh Networks (WMNs). Subsequently, the CGK is utilized for authenticating packets in a multi-hop manner. The mesh entities utilize the CGK to encrypt and decrypt packets for authentication purposes. If a packet is sent without encryption or encrypted with keys other than the CGK, it is deemed malicious and discarded. Additionally, EPADH provides end-to-end encryption and ensures the confidentiality of packets exchanged between mesh

entities. In our proposed protocol, the CGK is produced by a Group Controller (GC) using the Diffie-Hellman Key Exchange protocol. The Mesh Routers (MRs) in WMNs do not have limitations on power, we presume that this MR can function as the GC and generate a CGK for all Member Nodes (MNs) within its group.

6.2.1 Proposed Protocol for CGK generation between GC and MNs

Step 1 GC generates its public key

$$CG_i = g^{ni} \bmod p \quad (1)$$

where n_i is GC's private key.

Step 2 MNs generates its public key

$$MN_i = g^{mi} \bmod p \quad (2)$$

where m_i is the MN's private key.

GC and MN exchange their public key

Step 3 GC generates its secret key SK_i

$$SK_i = MN^{ni}{}_i \bmod p \quad (3)$$

Step 4 MNs generates its secret key SK_i

$$SK_i = CG^{mi}{}_i \bmod p \quad (4)$$

At steps 3 and 4 GC and MN compute the same shared secret Key

Step 5 Ultimately, GC creates the CGK by combining all the public keys obtained from MNs.

$$CGK_l = \left(\prod_{MN_i} \right) \bmod p \quad (5)$$

Step 6 After generating the CGK, GC distribute CGK to all the MNs in an encrypted form as

$$ES_{Ki}(CGK_l) \quad (6)$$

Step 7 Upon receiving$ES_{Ki}(CGK_l)$, each MNs decrypt it as

$$DS_{Ki}(CGK_l) \quad (7)$$

Later, the CGK is used for encrypting and decrypting the transmitted packets over the insecure channel throughout the network.

6.3 Security Analysis

In this section, we examined our suggested protocol EPADH in two segments: first, the authentication of packets to defend against replay attacks, and second, measures to prevent impersonation attacks.

6.3.1 Packet authentication to resist replay attack

Assuming that MNs A, B, C, D and a GC shown in Figure 6.1. GC generated the CGK and distributed the CGK to MNs A, B, C, and D. The subsequent actions occurred to verify the packet between the source node A and the destination node D in a multi-hop manner along the path .

Step 1 Node A encrypts the packet that include message m_1, nonce N_1 and its identity ID_A using the CGK as E_{CGKl} $(m_1||N_1||ID_A)$ and forward to its neighbour node B.

Step 2 When node B receives the encrypted packet it decrypt using CGK shared among the nodes as $D_{CGKl}(m_1||N_1||ID_A)$. Node B attached its identity ID_B to the existing packet and forwards it to its next-hop node C in an encrypted form as E_{CGKl} $(m_1||N_1||ID_A||ID_B)$.

Step 3 When node C receives the encrypted packet it decrypt using using the CGK shared among the nodes as D_{CGKl} $(m_1||N_1||ID_A||ID_B)$. Node C attached its identity ID_C to the existing packet and forwards to its next-hop node D in an encrypted form as E_{CGKl} $(m_1||N_1||ID_A||ID_B||ID_C)$.

Step 4 Upon receiving the encrypted packet, node D decrypts using the common key CGK shared among the nodes as D_{CGKI} ($m_1||N_1||ID_A||ID_B||ID_C$). Since node D is the intended recipient, it will not transmit the packet to its neighbouring nodes.

Step 5 The same procedure is carried out from steps 1 to 4 for each new packet, with the nonce value increasing to ensure the freshness of every new packet and to guard against replay attacks. Successful encryption and decryption of the packet lead to authentication among the nodes A, B, C, and D, as external intruders will not be able to encrypt or decrypt the packets without access to the CGK.

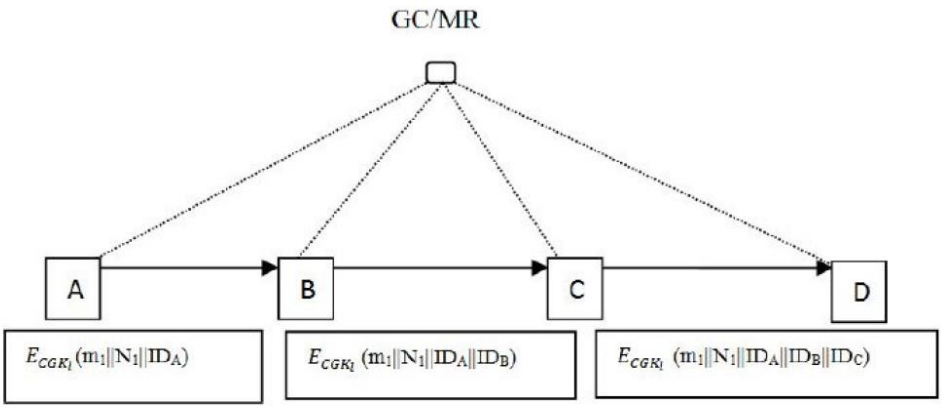

Fig6.1: Packet authentication to resist replay attack between MNs A,B,C and D

6.3.2 Packet authentication to resist impersonation attack

It is assumed that the MNs have already shared a pair–wise keys, which were distributed by the GC as illustrated in Figure 6.2, to provide protection against impersonation attacks during the subsequent steps.

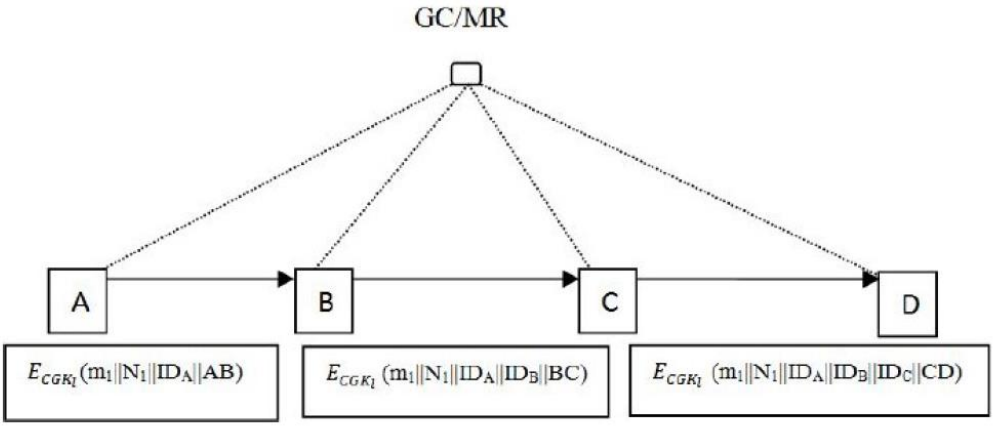

Fig 6.2: Packet authentication to resist impersonation attack between MNs A,B,C and D

Step 1 Node A has pre-shared pair-wise keys AB, AC, and AD with nodes B, C, and D respectively. Node A encrypt the packet containing message m_1, nonce N_1, its identity ID_A and pair-wise key AB using the CGK as E_{CGKl} $(m_1||N_1||ID_A||AB)$ and forward to its neighbour node B.

Step 2 Similar to node A, Node B also has pre-shared pair-wise keys BA, BC, and BD with nodes A, C, and D respectively. upon receiving encrypted packet, node B decrypts the the packet using CGK that is shared among the nodes as E_{CGKl} $(m_1||N_1||ID_A||AB)$. Node B attached its identity ID_B and pair-wise key BC to the existing packet and forwards it to its next hop node C in an encrypted form as E_{CGKl} $(m_1||N_1||ID_A||ID_B||BC)$

Step 3 Node C pre-shared a pair-wise keys CA, CB, and CD with nodes A, B, and D. On the receipt of the encrypted packet, node C decrypts the packet using the CGK shared among the nodes as E_{CGKl} $(m_1||N_1||ID_A||ID_B||BC)$. Node C attached its identity ID_C and pair-wise key CD to the existing packet and forwards to its next hop node D in an encrypted form as E_{CGKl} $(m_1||N_1||ID_A||ID_B||ID_C||CD)$.

Step 4 Upon receiving the encrypted packet, node D decrypts the packet using the CGK shared among the nodes as E_{CGKl} ($m_1||N_1||ID_A||ID_B||ID_C||CD$). Since node D is the intended recipient, it will not pass the packet on to its neighboring nodes..

In the previous steps, if we consider that node B aims to impersonate node A and send the packet to node C, it would be impossible for node B to do so because it lacks knowledge of the pre-shared keys that exist between node A and node C, specifically the pair-wise key AC or CA.. In this scenario we consider one way communication from A to D, but in case of omni directional communication a message from B to C can be detected and decrypted by node A, this needs to improved in future research.

6.4 Performance Analysis

The performance of the proposed protocol has been evaluated through simulation using the Network Simulator (NS3). The simulation parameters utilised for assessing the proposed protocol are presented in Table 6.1. The experimental results of the proposed 'EPADH' protocol are compared with existing protocols based on key performance metrics, including latency, throughput, packet delivery ratio, and memory utilisation.

Table 6.1 : Experimental setup

Parameter	*Values*
Simulator	NS3
Traffic types	CBR/UDP
Simulation area	1,000 × 1,000 m
MAC layer protocol	IEEE 802.11
Number of MAP's	2
Number of clients	100, 300
Transmission range of MAP's	250 meters
Transmission range of mesh clients	100 meters
Routing protocol	AODV
Packet size	512 bytes
Simulation time	100 sec
Node placement	Randomly

- **Latency** We follow the same setup as considered in HEAP protocol [95]. Packets were sent from one source node to five nodes that were 1, 2, 3, 4 and 5 hops away from the source node, respectively. A source node sent 10,000 packets and computes the mean end-to-end latency of each packets. The results of mean latency between source node and five nodes with different hops are shown in Table 6.2 and plotted in Figure 6.3 for all the protocols. In LHAP's case [94] if a node newly joined or rejoined the network between source and destination, then it may require to wait one TESLA interval to authenticate packets. In HEAP's case, if a node newly joined or rejoined the network between source and destination, In this case, every node must regenerate the n + 1 new keys, leading to delays in packet authentication and placing unnecessary strain on each resource-limited node. In our proposed EPADH framework, key generation is carried out by the GC, which has unlimited resources. If a node joins or rejoins the network between the source and destination, the GC recalculates the keys and distributes them to the nodes for the purpose of packet authentication after a brief delay. Our protocol does not incorporate TESLA, which causes delayed key disclosure as seen in LHAP. EPADH is tested under two scenarios – first, for effective packet authentication to prevent replay attacks, and second, for effective

packet authentication to prevent impersonation attacks. In both scenarios, EPADH produces consistent results post-simulation. However, because of key pre-sharing, the second scenario leads to greater resource usage compared to the first scenario. The experimental findings in Table 6.2 and Figure 6.3 indicate that EPADH results in lower latency than existing protocols.l. Further, we simulate the latency under different scenario with 300 nodes and extend the number of hops to 8 between the source and destination to compute the efficiency of our protocol as shown in Table 6.3 and plotted in Figure 6.4.

Table 6.2: Mean Latency Vs Number of Hops with 100 Nodes

Protocol	*Hop 1*	*Hop 2*	*Hop 3*	*Hop 4*	*Hop 5*
Li and Liu (2010)	10 ms	18 ms	22 ms	29 ms	30 ms
Tan et al. (2013)	11 ms	14 ms	18 ms	25 ms	29 ms
Parmar and Jinwala (2014)	30 ms	32 ms	35 ms	39 ms	42 ms
Gao et al. (2016)	32 ms	34 ms	38 ms	39 ms	46 ms
Altop et al. (2017)	10 ms	16 ms	25 ms	33 ms	35 ms
Regan and Manickam (2017)	15 ms	18 ms	22 ms	27 ms	31 ms
Abdel-Azim et al. (2018)	19 ms	22 ms	28 ms	32 ms	35 ms
Akbani et al. (2008)	4 ms	10 ms	13 s	14 ms	16 ms
Zhu et al. (2003)	80 ms	82 ms	94 ms	100 ms	100 ms
EPADH	2 ms	5 ms	10 ms	12 ms	14 ms

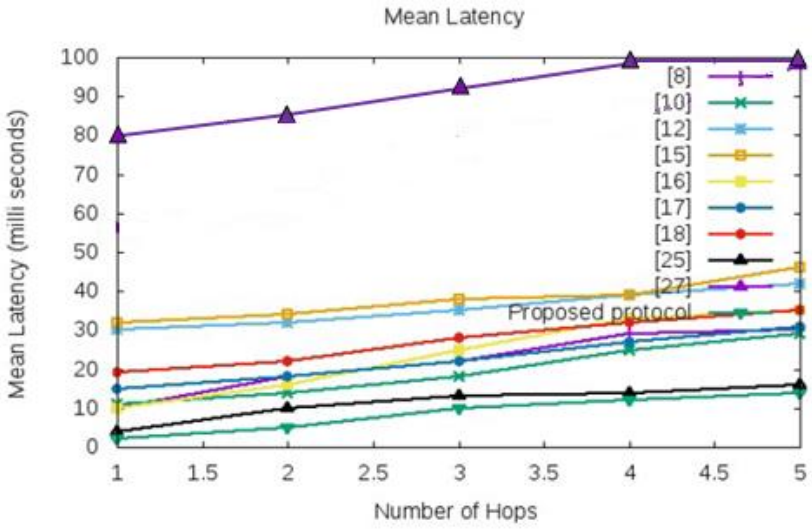

Fig 6.3: Mean latency Vs Number of Hops with 100 Nodes

Table 6.3: Mean Latency Vs Number of Hops with 300 Nodes

Protocol	*Hop 1*	*Hop 2*	*Hop 3*	*Hop 4*	*Hop 5*	*Hop 6*	*Hop 7*	*Hop 8*
Li and Liu (2010)	18 ms	22 ms	25 ms	28 ms	33 ms	36 ms	39 ms	42 ms
Tan et al. (2013)	22 ms	24 ms	28 ms	33 ms	36 ms	40 ms	42 ms	45 ms
Parmar and Jinwala (2014)	30 ms	33 ms	35 ms	39 ms	42 ms	46 ms	49 ms	53 ms
Gao et al. (2016)	34 ms	38 ms	42 ms	46 ms	49 ms	52 ms	54 ms	56 ms
Altop et al. (2017)	18 ms	23 ms	24 ms	26 ms	28 ms	33 ms	37 ms	40 ms
Regan and Manickam (2017)	20 ms	22 ms	24 ms	28 ms	30 ms	36 ms	40 ms	43 ms
Abdel-Azim et al. (2018)	21 ms	23 ms	26 ms	30 ms	32 ms	35 ms	38 ms	41 ms
Akbani et al. (2008)	10 ms	16 ms	22 s	25 ms	29 ms	30 ms	32 ms	34 ms
Zhu et al. (2003)	51 ms	54 ms	56 ms	58 ms	62 ms	65 ms	68 ms	70 ms
EPADH	6 ms	12 ms	15 ms	18 ms	25 ms	28 ms	30 ms	33 ms

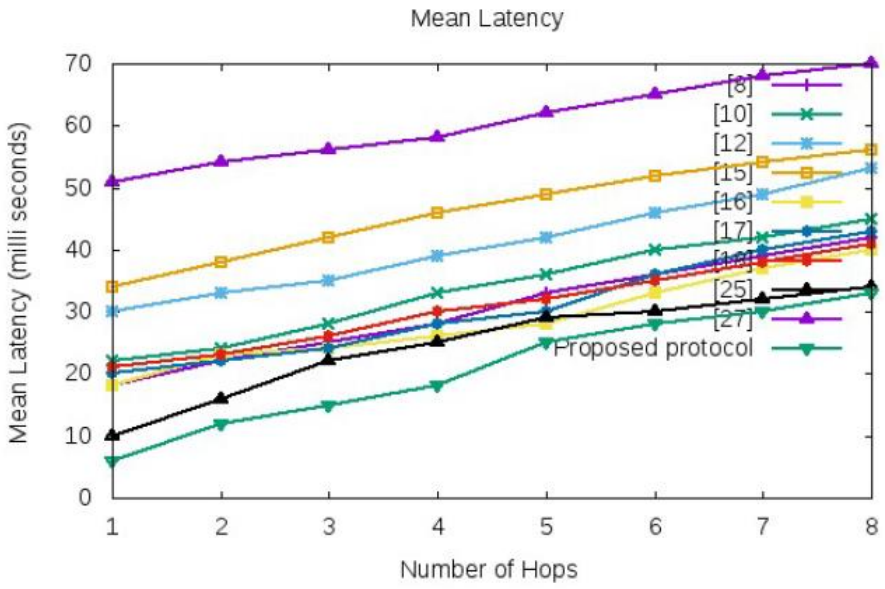

Fig 6.4:Mean Latency Vs Number of Hops with 300 Nodes

- **Throughput and packet delivery ratio**: We consider identical configuration as examined in the HEAP protocol. Packets were sent from one sender node to nine different receiver nodes. Out of which the distance between sender node and three receiver nodes were one hop away, the distance between sender node and three receiver nodes were two hops away

and the distance between sender node and three receiver nodes were three hops away. Sender sent the packets at different transmission rate that starts form 1 packet/second to 100 packets/second. Total 10,000 packets were transmitted from the sender side and each packet consists a data of 512 bytes. Mean throughput of all the nine nodes was computed and the results are shown in Table 6.4 and plotted in Figure 6.5. We also calculate the total number of packets successfully received by each node out of 10,000, resulting in the packet delivery ratio for each node, as illustrated in Table 6.6 and depicted in Figure 6.7. Table 6.4 indicates that HEAP and LHAP experience a decline in throughput once the packet rate exceeds 20 packets per second, rendering them inefficient and unreliable for the network, while EPADH demonstrates an improvement in throughput with an increased packet rate (packets/sec) when compared to other existing protocols. Table 6.6 reveals that HEAP and LHAP's packet delivery ratio decreases after surpassing 20 packets per second, whereas EPADH shows an enhancement in the packet delivery ratio with an increase in packet rate (packets/sec) relative to existing protocols.

Table 6.4 :Mean throughput (bytes/sec) vs. packet rate (pkts/sec) with 100 nodes

Protocol	*10 pkts/sec*	*20 pkts/sec*	*40 pkts/sec*	*60 pkts/sec*	*80 pkts/sec*	*100 pkts/sec*
Li and Liu (2010)	1,300	2,520	5,010	7,350	9,690	10,920
Tan et al. (2013)	1,500	2,535	5,025	7,580	9,699	10,950
Parmar and Jinwala (2014)	2,000	2,605	5,040	7,610	9,710	10,970
Gao et al. (2016)	2,010	2,603	5,080	7,645	9,740	10,978
Altop et al. (2017)	2,030	2,670	5,100	7,600	8,000	9,050
Regan and Manickam (2017)	2,000	2,630	4,500	5,800	6,200	6,800
Abdel-Azim et al. (2018)	1,400	2,000	3,050	4,080	5,030	6,000
Akbani et al. (2008)	300	8,200	6,600	6,100	6,500	6,400
Zhu et al. (2003)	310	8,200	6,300	6,300	6,800	6,600
EPADH	2,600	2,810	5,500	7,900	9,800	10,990

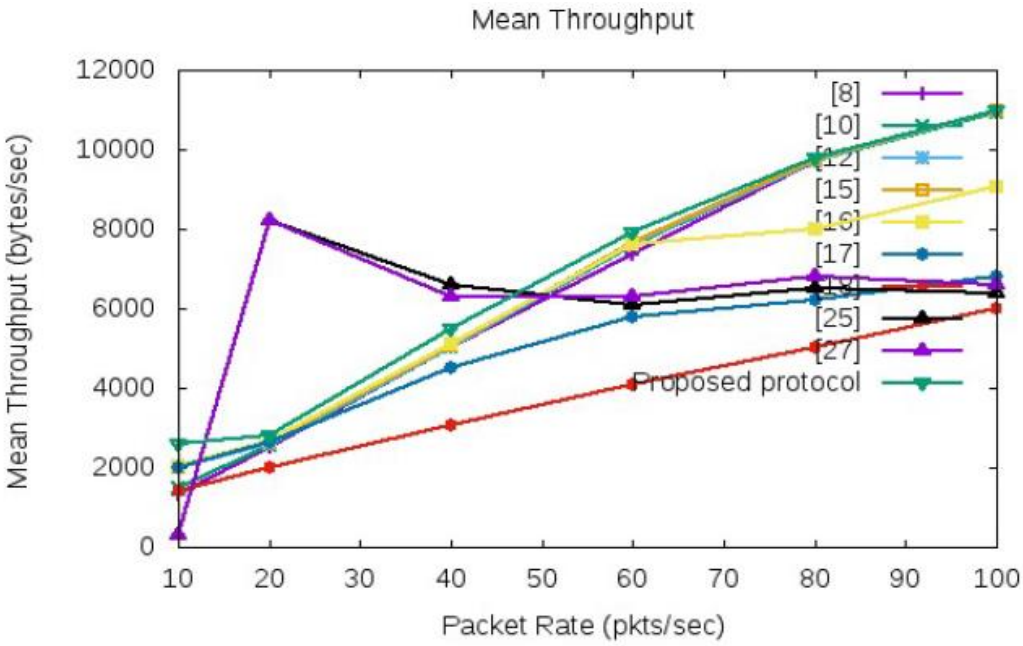

Fig: 6.5: Mean throughput (bytes/sec) vs. packet rate (pkts/sec) with 100 nodes

Table 6.5:Mean throughput (bytes/sec) vs. packet rate (pkts/sec) with 300 nodes

Protocol	*50 pkts/sec*	*100 pkts/sec*	*150 pkts/sec*	*200 pkts/sec*	*250 pkts/sec*	*300 pkts/sec*
Li and Liu (2010)	2,300	420	7,010	9,350	1,050	2,000
Tan et al. (2013)	2,500	4,535	7,025	9,580	1,099	2,095
Parmar and Jinwala (2014)	4,000	4,605	7,040	9,610	1,070	2,070
Gao et al. (2016)	4,010	4,603	7,080	9,645	1,040	2,078
Altop et al. (2017)	4,030	4,670	7,100	9,600	1,050	1,050
Regan and Manickam (2017)	4,000	4,630	6,500	7,800	8,200	8,500
Abdel-Azim et al. (2018)	2,400	4,000	5,050	6,080	4,030	8,000
Akbani et al. (2008)	600	16,200	8,600	8,100	8,800	8,500
Zhu et al. (2003)	610	16,200	8,300	8,300	7,010	8,600
EPADH	4,600	4,810	7,500	9,900	1,080	2,090

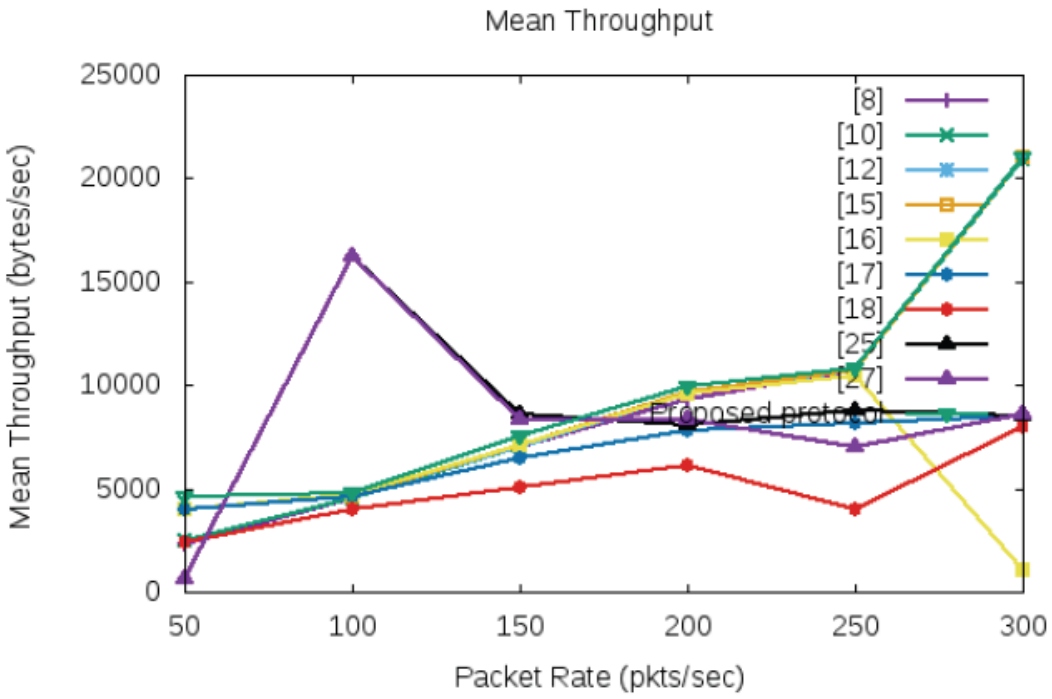

Fig 6.6: Mean Throughput Vs Packet rate with 300 nodes

Table 6.6: Mean packet delivery ratio (%) vs. packet rate (pkt/sec) with 100 nodes

Protocol	*10 pkts/sec*	*20 pkts/sec*	*40 pkts/sec*	*60 pkts/sec*	*80 pkts/sec*	*100 pkts/sec*
Li and Liu (2010)	32%	29%	43%	48%	72%	85%
Tan et al. (2013)	35%	33%	47%	50%	73%	86%
Parmar and Jinwala (2014)	36%	35%	50%	66%	78%	88%
Gao et al. (2016)	39%	41%	56%	68%	80%	89%
Altop et al. (2017)	40%	52%	55%	65%	69%	73%
Regan and Manickam (2017)	36%	41%	42%	44%	58%	62%
Abdel-Azim et al. (2018)	30%	31%	33%	39%	49%	53%
Akbani et al. (2008)	35%	87%	70%	65%	68%	66%
Zhu et al. (2003)	38%	83%	66%	66%	70%	68%
EPADH	50%	57%	60%	71%	85%	93%

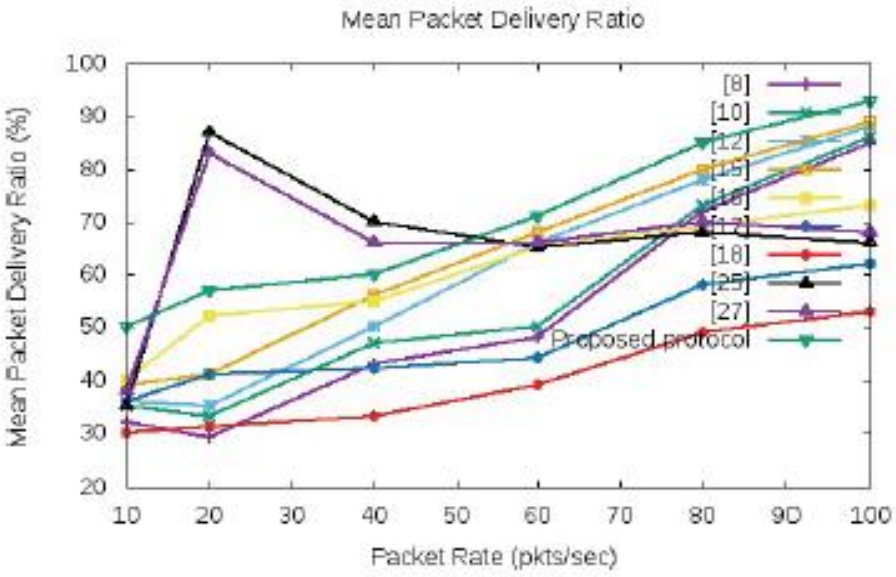

Fig 6.7: Mean packet delivery ratio (%) vs. packet rate (pkt/sec) with 100 nodes

Table 6.7: Mean packet delivery ratio (%) vs. packet rate (pkt/sec) with 300 nodes

Protocol	*50 pkts/sec*	*100 pkts/sec*	*150 pkts/sec*	*200 pkts/sec*	*250 pkts/sec*	*300 pkts/sec*
Li and Liu (2010)	45%	43%	47%	49%	52%	55%
Tan et al. (2013)	47%	44%	48%	51%	54%	57%
Parmar and Jinwala (2014)	48%	47%	50%	53%	56%	59%
Gao et al. (2016)	51%	53%	56%	59%	61%	63%
Altop et al. (2017)	53%	55%	57%	60%	63%	65%
Regan and Manickam (2017)	48%	50%	53%	55%	58%	60%
Abdel-Azim et al. (2018)	43%	45%	48%	53%	56%	58%
Akbani et al. (2008)	50%	52%	57%	63%	66%	69%
Zhu et al. (2003)	47%	50%	52%	58%	59%	62%
EPADH	55%	57%	61%	64%	68%	72%

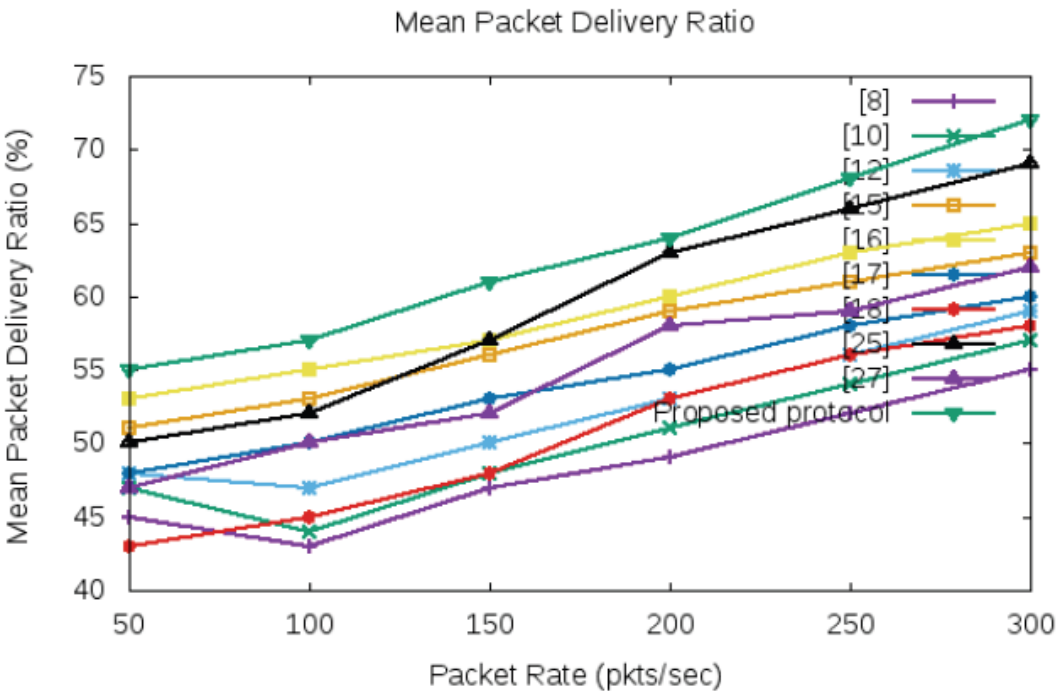

Fig 6.8 : Mean packet delivery ratio (%) vs. packet rate (pkt/sec) with 300 nodes

- **Memory requirements** : Before the transmission starts, LHAP protocol [119] generates the hash key chains which was pre-computed and stored offline. However, when there is a shortage of keys, each node must stop the transmissions and generate new key chains for further transmissions. Therefore, a long key chain is required to be generated and store to avoid the frequent halting of transmission. Furthermore, the LHAP protocol employs TESLA for the bootstrapping process, leading to a delay in packet authentication. Consequently, each receiving node must retain the received packets in a cache until the key is revealed. This necessitates a significant amount of cache memory to hold incoming packets at the receiving nodes. The HEAP protocol, on the other hand, requires the generation and storage of (n + 1) new keys for every node, meaning that each neighbour needs one pair-wise key and one neighborhood key, resulting in substantial memory demands that are neither effective nor dependable for any network. Similar to HEAP, we consider five neighbors per node for EPADH. Based on the cache size requirements and the duration of a key chain, we calculate the memory

needs for each protocol, which are presented in Table 6.8 and Figure 6.9. We consider enough cache size for storing all the packets during the key updates. An interval of 1 second for key update with at most 100 packets/second were considered throughout the simulation. Our suggested protocol 'EPADH' excludes key chains and TESLA. Additionally, in EPADH, key generation is managed by the GC, enabling MNs to conserve their limited resources. The simulation results shows the memory usage per node in both the existing protocols and EPADH. EPADH utilizes just 118 bytes per node.

Table 6.8: Memory requirement (bytes) vs. duration of key chain (mins)

Protocol	*10 mins*	*20 mins*	*40 mins*	*50 mins*	*60 mins*
Li and Liu (2010)	200	400	420	470	500
Tan et al. (2013)	210	300	460	510	550
Parmar and Jinwala (2014)	295	310	430	550	580
Gao et al. (2016)	250	250	250	250	250
Altop et al. (2017)	230	280	390	397	397
Regan and Manickam (2017)	230	250	260	266	289
Abdel-Azim et al. (2018)	235	240	300	300	310
Akbani et al. (2008)	190	190	190	190	190
Zhu et al. (2003)	400	630	800	810	960
EPADH	118	118	118	118	118

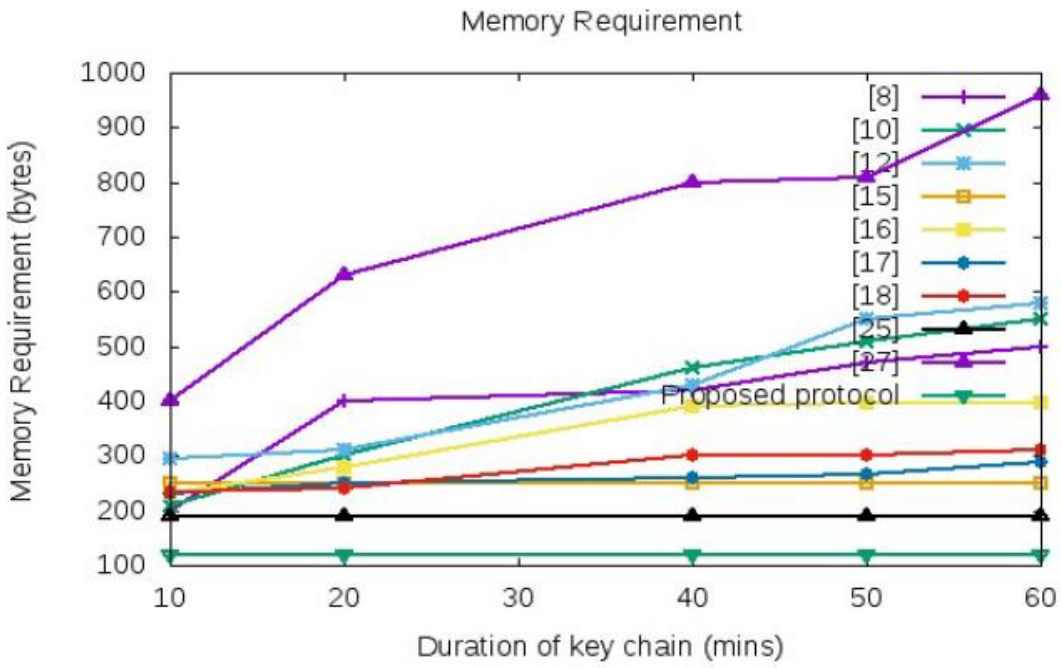

Fig 6.9: Memory requirement (bytes) vs. duration of key chain (mins)

6.5 Conclusion

We introduced a highly efficient end-to-end packet authentication protocol designed for multi-hop Wireless Mesh Networks (WMNs). Our suggested protocol EPADH provides both packet authentication and end-to-end encryption to ensure confidentiality. EPADH enables Mobile Nodes (MNs) to conserve their limited resources by not generating the keys, unlike existing protocols that require each node to create keys, leading to significant memory usage. In EPADH, the keys are produced by the Gateway Controller (GC), which is not subject to power limitations, thus allowing MNs to authenticate packets effectively. EPADH was evaluated against existing protocols, and simulation results indicate that it outperforms them in terms of latency, throughput, packet delivery ratio, and memory use.However, EPADH is limited to the centralised approach, where the GC generates the CGK for all the nodes within the group. Moreover, EPADH is based on Deffie-Hellman key exchange approach with a key size of 2,048 bits. In the future, the protocol can be extended towards the decentralised approach while considering more efficient protocols such as ECC with smaller key size of 224 bits.

Chapter 7

CONCLUSION AND FUTURE SCOPE

Wireless Mesh Networks (WMNs) are emerging as a promising solution for providing scalable, cost-effective, and self-configuring wireless communication. However, their open and decentralized nature introduces significant security challenges, particularly in the areas of user authentication, secure routing, fast handoff, and data integrity. This thesis addresses these challenges by proposing a comprehensive security framework that enhances the reliability and trustworthiness of WMNs.

The thesis presents three major contributions. First, it introduces efficient authentication protocols that ensure secure access control between Mesh Clients (MCs) and Mesh Routers (MRs), as well as among MRs themselves. These protocols leverage a combination of symmetric and asymmetric cryptography and ticket-based approaches to reduce computational overhead while maintaining robust security.

Second, the work proposes a fast handoff authentication scheme that minimizes latency during client transitions between mesh routers. By pre-distributing authentication tickets and reducing dependency on centralized servers, the handoff process becomes seamless and more efficient, which is crucial for mobile applications and real-time communication.

Third, a secure routing mechanism is developed based on a trust evaluation model. This model detects and isolates malicious nodes that attempt to disrupt routing by misleading the protocol, specifically black hole attacks for AODV routing Protocol. The framework is further strengthened with a lightweight, multi-hop data authentication scheme, which verifies each data packet using shared keys to ensure end-to-end integrity and prevent forgery, replay, or injection attacks.

Simulation results validate the effectiveness of the proposed solutions, demonstrating improvements in authentication delay, packet delivery ratio, and detection accuracy compared to existing methods.

Future Scope

While the proposed framework significantly improves the security posture of WMNs, several areas remain open for future exploration. First, integrating machine learning techniques for real-time anomaly detection and adaptive trust computation can further enhance routing security and intrusion detection. These intelligent models can adapt to network dynamics and detect previously unseen attack patterns.

Second, expanding the proposed protocols to support heterogeneous WMNs involving IoT devices, drones, and vehicular networks (VANETs) can address more complex scenarios. Ensuring interoperability and lightweight security in such environments is a critical challenge.

Lastly, the implementation of the proposed framework in real-world testbeds and its evaluation under practical constraints, such as power consumption and hardware limitations, will provide deeper insights and validate its deployability. Future work can also explore blockchain-based decentralized trust management to eliminate single points of failure and enhance transparency in node behavior verification.

REFERENCES

[1] Stallings, W. (2013). *Wireless Communications & Networks: Pearson New International Edition*. Pearson Higher Ed.

[2] https://www.zenarmor.com/docs/network-basics/what-is-wlan, April,2025

[3] Perkins, C.(2017). *Mobile Networking and Wireless Networks*. Addison-Wesley.

[4] https://www.edrawmax.com/templates/1020790, April, 2025

[5]Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C. (2014). What will 5G be?. *IEEE Journal on selected areas in communications*, *32*(6), 1065-1082.

[6]https://techvidvan.com/tutorials/iot-protocols, April, 2025

[7] Tanenbaum, A.S. and Wetherall, D.J.(2021). *Computer Networks*. 6th ed. Pearson.

[8]https://www.techslang.com/definition/what-is-a-personal-area-network, April, 2025

[9] Tanenbaum, A.S. and Wetherall, D.J., (2020). *Computer Networks*. 5th ed. Pearson.

[10]Royer, E. M., & Perkins, C. E. (1999, August). Multicast operation of the ad-hoc on-demand distance vector routing protocol. In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking* (pp. 207-218).

[11]https://study.com/academy/lesson/mobile-ad-hoc-networks-applications-advantages-disadvantages.html, April, 2025

[12]Hartenstein, H., &Laberteaux, K. (Eds.). (2009). *VANET: vehicular applications and inter-networking technologies*. John Wiley & Sons.

[13]https://thecustomizewindows.com/2023/01/what-is-vehicular-ad-hoc-network, April, 2025

[14]Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E., (2002). Wireless sensor networks: a survey. *Computer Networks*, 38(4), pp.393-422.

[15]https://www.monolithicpower.com/en/learning/mpscholar/sensors/advanced-topics-in-sensing/wireless-sensing-networks, April, 2025

[16] Albanese, M., De Benedictis, A., Jajodia, S., &Shakarian, P. (2012). A probabilistic framework for localization of attackers in manets. In *Computer Security–ESORICS 2012: 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings 17* (pp. 145-162). Springer Berlin Heidelberg.

[17]Sen, J. (2013). Security and privacy issues in wireless mesh networks: A survey. In *Wireless networks and security: issues, challenges and research trends* (pp. 189-272). Berlin, Heidelberg: Springer Berlin Heidelberg.

[18]Sen, J., &Funabiki, N. (2011). Secure routing in wireless mesh networks. *Wireless Mesh Networks*, 237-280.

[19]Lopez, M. A., Baddeley, M., Lunardi, W. T., Pandey, A., &Giacalone, J. P. (2021, July). Towards secure wireless mesh networks for UAV swarm connectivity: Current threats, research, and opportunities. In *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 319-326). IEEE.

[20]Sen, J. (2012, March). Secure and privacy-preserving authentication protocols for wireless mesh networks. In *Applied Cryptography and Network Security* (pp. 3-34). IntechOpen.

[21]Akyildiza, I. F., Wangb, X., &Wangb, W. (2005). Wireless mesh networks: a survey. Computer Networks. *Computer Network, Elsevier*.

[22]Sauram, S., Uthansakul, P., &Uthansakul, M. (2011). Design of Node Locations for Indoor Wireless Mesh Network. *ECTI Transactions on Electrical Engineering, Electronics, and Communications*, *9*(2), 276-283.

[23]Akyildiz, I. F., & Wang, X. (2005). A survey on wireless mesh networks. *IEEE Communications magazine*, *43*(9), S23-S30.

[24] Pirzada, A. A., Portmann, M., &Indulska, J. (2009). Aodv-hm: A hybrid mesh ad-hoc on-demand distance vector routing protocol. *Journal of Research and Practice in Information Technology*, *41*(1), 65-84.

[25]Zhang, W., Wang, Z., Das, S. K., & Hassan, M. (2008). Security issues in wireless mesh networks. *Wireless Mesh Networks: Architectures and Protocols*, 309-330.

[26]Lai, X., Ji, X., Zhou, X., & Chen, L. (2017). Energy efficient link-delay aware routing in wireless sensor networks. *IEEE sensors journal*, *18*(2), 837-848.

[27]Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (No. rfc3561).

[28]Dong, J. (2009). *Secure and robust communication in wireless mesh networks* (Doctoral dissertation, Purdue University).

[29]Lai, X., Ji, X., Zhou, X., & Chen, L. (2017). Energy efficient link-delay aware routing in wireless sensor networks. *IEEE sensors journal*, *18*(2), 837-848.

[30]Royer, E. M., & Perkins, C. E. (1999, August). Multicast operation of the ad-hoc on-demand distance vector routing protocol. In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking* (pp. 207-218).

[31]Abolhasan, M., Wysocki, T., &Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. *Ad hoc networks*, *2*(1), 1-22.

[32]Royer, E. M., &Toh, C. K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. *IEEE personal communications*, *6*(2), 46-55.

[33]Pathan, A. S. K. (Ed.). (2016). *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press.

[34]Shivlal, M., & Kumar, S. U. (2012). Performance analysis of secure wireless mesh networks. *Research Journal of Recent Sciences*,1(3), 80-85

[35]Hu, Y. C., Perrig, A., & Johnson, D. B. (2003, March). Packet leashes: a defense against wormhole attacks in wireless networks. In *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)* (Vol. 3, pp. 1976-1986). IEEE.

[36]Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., &Nemoto, Y. (2007). Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. *Int. J. Netw. Secur.*, *5*(3), 338-346.

[37]Kanu.G, Piyush.K. S &Anjana.J.D (2014). A Survey on Grey Hole Attack in Wireless mesh Networks. *International Journal of Computer Applications*, 95(23), pp.23–29.

[38]Dharmendra.M, Deepak.S&Sunil.P (2015). A Review on Gray Hole Attack in Wireless Sensor Network. *International Journal of Computer Applications*. 122(2) ,pp. 33-36

[39]Vijayanand, R., Devaraj, D., &Kannapiran, B. (2018). Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Computers & Security*, *77*, 304-314.

[40]Liu, X., Lim, T. J., & Huang, J. (2020). Optimal byzantine attacker identification based on game theory in network coding enabled wireless ad hoc networks. *IEEE Transactions on Information Forensics and Security*, *15*, 2570-2583.

[41]Singh, V., & Pandey, S. K. (2018, December). Revisiting cloud security threats: Replay attack. In *2018 4th International Conference on Computing Communication and Automation (ICCCA)* (pp. 1-6). IEEE.

[42]Singh, M., &Pati, D. (2020). Countermeasures to replay attacks: A review. *IETE Technical Review*, *37*(6), 599-614.

[43]Javeed, D., MohammedBadamasi, U., Ndubuisi, C. O., Soomro, F., & Asif, M. (2020). Man in the middle attacks: Analysis, motivation and prevention. *International Journal of Computer Networks and Communications Security*, *8*(7), 52-58.

[44]Ylli, E., &Fejzaj, J. (2021, May). Man in the Middle: Attack and Protection. In *RTA-CSIT* (pp. 198-204).

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

[46]Wei, H. Y., Kim, S., Ganguly, S., &Izmailov, R. (2006, September). Seamless handoff support in wireless mesh networks. In *2006 1st workshop on operator-assisted (wireless mesh) community networks* (pp. 1-8). IEEE.

[47]Xu, Q., Wan, C., & Hu, A. (2008, December). The performance analysis of fast EAP re-authentication protocol. In *2008 international symposium on computer science and computational technology* (Vol. 1, pp. 99-103). IEEE.

[48]Zhang, Y. H., Chen, X. F., Li, H., & Cao, J. (2012). Identity-based construction for secure and efficient handoff authentication schemes in wireless networks. *Security and Communication Networks*, *5*(10), 1121-1130.

[49]Li, C., Nguyen, U. T., Nguyen, H. L., & Huda, N. (2013). Efficient authentication for fast handover in wireless mesh networks. *computers & security*, *37*, 124-142.

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

[51]Xiao, P., He, J., & Fu, Y. (2014). An access authentication protocol for trusted handoff in wireless mesh networks. *Computer Standards & Interfaces*, *36*(3), 480-488.

[52]Lai, Y. M., Cheng, P. J., Lee, C. C., & Ku, C. Y. (2016). A new ticket-based authentication mechanism for fast handover in mesh network. *PloS one*, *11*(5), e0155064.

[53]Yang, X., Huang, X., Han, J., & Su, C. (2016). Improved handover authentication and key pre-distribution for wireless mesh networks. *Concurrency and Computation: Practice and Experience*, *28*(10), 2978-2990.

[54]Rathee, G., & Saini, H. (2016). A fast handoff technique in wireless mesh network (FHT for WMN). *Procedia Computer Science*, *79*, 722-728.

[55]Yang, X., Zhang, Y., Liu, J. K., & Zeng, Y. (2016, August). A trust and privacy preserving handover authentication protocol for wireless networks. In *2016 IEEE Trustcom/BigDataSE/ISPA* (pp. 138-143). IEEE.

[56]Sharma, P. K., Mahajan, R., & Surender. (2017). A security architecture for attacks detection and authentication in wireless mesh networks. *Cluster Computing*, *20*, 2323-2332.

[57]Zhou, Z., Zhang, H., & Sun, Z. (2017). An improved privacy-aware handoff authentication protocol for VANETs. *Wireless personal communications*, *97*, 3601-3618.

[58]Nanda, A., Nanda, P., He, X., Puthal, D., &Jamdagni, A. (2018, January). A novel hybrid authentication model for geo location oriented routing in dynamic wireless mesh networks. In *International conference on system sciences*.

[59]Rathee, G., & Saini, H. (2018). Authentication Through Elliptic Curve Cryptography (ECC) Technique in WMN. *International Journal of Information Security and Privacy (IJISP)*, *12*(1), 42-52.

[60]Wang, D., Xu, L., Wang, F., & Xu, Q. (2018). An anonymous batch handover authentication protocol for big flow wireless mesh networks. *EURASIP Journal on Wireless Communications and Networking*, *2018*, 1-8.

[61] Rathee, G., & Saini, H. (2019). Secure handoff technique with reduced authentication delay in wireless mesh network. *International Journal of Advanced Intelligence Paradigms, 13*(1–2), 130–154.

[62] Rathee, G., Jaglan, N., Saini, H., Gupta, S. D., & Kanaujia, B. K. (2019). Probabilistic verification scenarios with reduced authentication delay for handoff clients in mesh networks. *Wireless Personal Communications, 104*, 1553–1571.

[63] Roy, A. K., & Khan, A. K. (2019). Efficient authentication and key management scheme for wireless mesh networks. *International Journal of Internet Technology and Secured Transactions, 9*(1–2), 184–200.

[64] Jiang, X., Liu, M., Yang, C., Liu, Y., & Wang, R. (2019). A blockchain-based authentication protocol for WLAN mesh security access. *Computers, Materials & Continua, 58*(1).

[65] Roy, A. K., & Khan, A. K. (2020). Authentication protocol with privacy preservation for handover in wireless mesh networks. In *First International Conference on Sustainable Technologies for Computational Intelligence: Proceedings of ICTSCI 2019* (pp. 383-395). Springer Singapore.

[66] Sharma, P. K., Mahajan, R., & Surender. (2020). ID-based signcryption authentication algorithm for intra- and inter-domain handoff in wireless mesh networks. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 44*(2), 659–667.

[67] Kumar, V., Ray, S., Dasgupta, M., & Khan, M. K. (2021). A pairing-free identity-based two-party authenticated key agreement protocol using hexadecimal extended ASCII elliptic curve cryptography. *Wireless Personal Communications, 118*, 3045–3061.

[68] Waharte, S., Boutaba, R., Iraqi, Y., & Ishibashi, B. (2006). Routing protocols in wireless mesh networks: Challenges and design considerations. *Multimedia Tools and Applications, 29*(3), 285–303.

[69] Murphy, S. (2002). Routing protocol threat analysis. *Internet Draft, draft-murphy-threat-00. txt*.

[70] Garcia-Luna-Aceves, J. J. (2005). Multipath routing in wireless mesh networks.

[71] Yi, S., Naldurg, P., &Kravets, R. (2001, October). Security-aware ad hoc routing for wireless networks. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing* (pp. 299-302).

[72] Lundberg, J. (2000). Routing security in ad hoc networks. *Helsinki University of Technology, http://citeseer. nj. nec. com/400961. html*.

[73] Stojano, F., & Anderson, R. (1999). The resurrecting duckling: Security issues for wireless ad hoc networks. In *Seventh International Workshop Proceedings, Lecture Notes in Computer Science*.

[74] Gurung, S., & Chauhan, S. (2020). A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability. *Wireless Networks, 26*, 1981–2011.

[75] Weerasinghe, H., & Fu, H. (2007). Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. In *Proceedings of the 2007 International Conference on Future Generation Communication and Networking (FGCN 2007)* (Vol. 2, pp. 362–367). IEEE.

[76] Yu, C. W., Wu, T. K., Cheng, R. H., & Chang, S. C. (2007). A distributed and cooperative black hole node detection and elimination mechanism for ad hoc networks. In *Emerging Technologies in Knowledge Discovery and Data Mining: PAKDD 2007 International Workshops Nanjing, China, May 22-25, 2007 Revised Selected Papers 11* (pp. 538-549). Springer Berlin Heidelberg.

[77] Medadian, M., Yektaie, M. H., & Rahmani, A. M. (2009). Combat with black hole attack in AODV routing protocol in MANET. In *Proceedings of the 2009 First Asian Himalayas International Conference on Internet* (pp. 1–5). IEEE.

[78] Baadache, A., & Belmehdi, A. (2012). Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks. *Journal of Network and Computer Applications, 35*(3), 1130–1139.

[79] Tan, S., & Kim, K. (2013). Secure route discovery for preventing black hole attacks on AODV-based MANETs. In *Proceedings of the 2013 IEEE 10th International Conference on High Performance Computing and Communications & Embedded and Ubiquitous Computing* (pp. 1159–1164). IEEE.

[80] Dhiman, D., & Sood, N. (2014). Enhanced 2ACK scheme for reducing routing overhead in MANETs. In *Proceedings of the 2014 International Conference on Parallel, Distributed and Grid Computing* (pp. 120–125). IEEE.

[81] Dorri, A., & Nikdel, H. (2015). A new approach for detecting and eliminating cooperative black hole nodes in MANET. In *Proceedings of the 2015 7th Conference on Information and Knowledge Technology (IKT)* (pp. 1–6). IEEE.

[82] Kumar, J., Kulkarni, M., Gupta, D., & Indu, S. (2015). Secure route discovery in AODV in presence of black-hole attack. *CSI Transactions on ICT, 3*, 91–98.

[83] Gurung, S., & Chauhan, S. (2018). A dynamic threshold-based approach for mitigating black-hole attack in MANET. *Wireless Networks, 24*(8), 2957–2971.

[84] El-Semary, A. M., & Diab, H. (2019). BP-AODV: Blackhole-protected AODV routing protocol for MANETs based on chaotic map. *IEEE Access, 7*, 95197–95211.

[85] Terai, T., Yoshida, M., Ramonet, A. G., & Noguchi, T. (2020). Blackhole attack cooperative prevention method in MANETs. In *Proceedings of the 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW)* (pp. 60–66). IEEE.

[86] Saputra, R., Andika, J., & Alaydrus, M. (2020). Detection of blackhole attack in wireless sensor network using enhanced check agent. In *Proceedings of the 2020 Fifth International Conference on Informatics and Computing (ICIC)* (pp. 1–4). IEEE.

[87] Vatambeti, R., Supriya, K. S., & Sanshi, S. (2020). Identifying and detecting black hole and gray hole attack in MANET using gray wolf optimization. *International Journal of Communication Systems, 33*(18), e4610.

[88] Sathyaraj, P., & Kannan, K. (2021). Host based Detection and Prevention of Black Hole attacks by AODV-ICCSO Algorithm for security in MANETs.

[89] Delkesh, T., &JabraeilJamali, M. A. (2019). EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs. *Journal of Ambient Intelligence and Humanized Computing*, *10*, 1897-1914.

[90] Dani, V. (2022). iBADS: An improved Black-hole Attack Detection System using Trust based Weighted Method. *Journal of Information Assurance & Security, 17*(3).

[91] Moumen, I., Rafalia, N., Abouchabaka, J., &Chatoui, Y. (2023). AODV-based Defense Mechanism for Mitigating Blackhole Attacks in MANET. In *E3S Web of Conferences* (Vol. 412, p. 01094). EDP Sciences.

[92] Pandian, E., Soundar, K. R., Gunasekaran, S., & Anantharajan, S. (2024). Fuzzy heuristics for detecting and preventing black-hole attack. *International Arab Journal of Information Technology, 21*(1), 85–93.

[93] Chakravorty, R., Prakash, J., & Srivastava, A. (2024). An efficacious neural network and DNA cryptography-based algorithm for preventing black hole attacks in MANET. *Soft Computing, 28*(5), 4667–4679.

[94] Zhu, S., Xu, S., Setia, S., & Jajodia, S. (2003). LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks. In *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops* (pp. 749–755). IEEE.

[95] Akbani, R., Korkmaz, T., & Raju, G. V. S. (2008). HEAP: A packet authentication scheme for mobile ad hoc networks. *Ad Hoc Networks, 6*(7), 1134–1150.

[96] Li, L. C., & Liu, R. S. (2010). Securing cluster-based ad-hoc networks with distributed authorities. *IEEE Transactions on Wireless Communications, 9*(10), 3072–3081.

[97] Li, Y., Li, J., Ren, J., & Wu, J. (2012). Providing hop-by-hop authentication and source privacy in wireless sensor networks. In *Proceedings of IEEE INFOCOM 2012* (pp. 3071–3075). IEEE.

[98] Tan, W. K., Lee, S. G., Lam, J. H., & Yoo, S. M. (2013). A security analysis of the 802.11s wireless mesh network routing protocol and its secure routing protocols. *Sensors, 13*(9), 11553–11585.

[99] Parmar, K., &Jinwala, D. C. (2014). Aggregate MAC based authentication for secure data aggregation in wireless sensor networks. In *Intelligent Computing Methodologies: 10th International Conference, ICIC 2014, Taiyuan, China, August 3-6, 2014. Proceedings 10* (pp. 475-483). Springer International Publishing.

[100] Gao, T., Peng, F., & Guo, N. (2016). Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network. *EURASIP journal on wireless communications and networking*, *2016*, 1-10.

[101] Altop, D. K., Bingöl, M. A., Levi, A., & Savaş, E. (2017). DKEM: Secure and efficient distributed key establishment protocol for wireless mesh networks. *Ad Hoc Networks, 54*, 53–68.

[102] Regan, R., & Manickam, J. M. L. (2017). Detecting and denying malicious behavior using adaptive learning-based routing protocols in wireless mesh network. *Applied Mathematics, 11*(4), 1155–1162.

[103] Abdel-Azim, M., Salah, H. E. D., & Eissa, M. E. (2018). IDS against black-hole attack for MANET. *International Journal of Network Security, 20*(3), 585–592.

[104] Santhosh Kumar, S. V. N., & Palanichamy, Y. (2018). Energy-efficient and secured distributed data dissemination using hop-by-hop authentication in WSN. *Wireless Networks, 24*, 1343–1360.

[105] Xu, C., Huang, X., Ma, M., & Bao, H. (2018). A secure and efficient message authentication scheme for vehicular networks based on LTE-V. *KSII Transactions on Internet and Information Systems*.

[106] Subhash, P., & Ramachandram, S. (2015). Secure neighbour discovery in wireless mesh networks using connectivity information. In *Proceedings of the 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 2061–2066). IEEE.

[107] Franklin, D., McDonald, A., & Roshan, P. (2007). Wireless mesh networks: A survey. In *Proceedings of the 2007 International Conference on Wireless Networks, Communications and Mobile Computing* (pp. 1–7). IEEE.

[108] Qazi, S., Mu, Y., & Susilo, W. (2008, December). Securing wireless mesh networks with ticket-based authentication. In *2008 2nd International Conference on Signal Processing and Communication Systems* (pp. 1-10). IEEE.

[109] Santhanam, V., Vaidehi, V., & Radha, S. (2008). An efficient authentication scheme for wireless mesh networks. In *Proceedings of the International Conference on Signal Processing, Communications and Networking (ICSCN 2008)* (pp. 437–442). IEEE.

[110] Altman, E., & Keren, G. (2016). Security issues in wireless mesh networks. In *Handbook of Wireless Sensor and Mobile Ad Hoc Networks: Architectures and Protocols* (pp. 301–320). Springer.

[111] Li, L. C., & Liu, R. S. (2010). Securing cluster-based ad-hoc networks with distributed authorities. *IEEE Transactions on Wireless Communications, 9*(10), 3072–3081.

[112] Tan, W. K., Lee, S. G., Lam, J. H., & Yoo, S. M. (2013). A security analysis of the 802.11s wireless mesh network routing protocol and its secure routing protocols. *Sensors, 13*(9), 11553–11585.

[113] Parmar, K., & Jinwala, D. C. (2014). Aggregate MAC-based authentication for secure data aggregation in wireless sensor networks. In *Intelligent Computing Methodologies: 10th International Conference (ICIC 2014)* (pp. 475–483). Springer.

[114] Gao, T., Peng, F., & Guo, N. (2016). Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network. *EURASIP journal on wireless communications and networking, 2016*, 1-10.

[115] Altop, D. K., Bingöl, M. A., Levi, A., & Savaş, E. (2017). DKEM: Secure and efficient distributed key establishment protocol for wireless mesh networks. *Ad Hoc Networks, 54*, 53–68.

[116] Regan, R., & Manickam, J. M. L. (2017). Detecting and denying malicious behavior using adaptive learning-based routing protocols in wireless mesh network. *Applied Mathematics and Information Sciences, 11*, 1155–1162.

[117] Abdel-Azim, M., Salah, H. E. D., & Eissa, M. E. (2018). IDS against black-hole attack for MANET. *International Journal of Network Security, 20*(3), 585–592.

[118] Akbani, R., Korkmaz, T., & Raju, G. V. S. (2008). HEAP: A packet authentication scheme for mobile ad hoc networks. *Ad Hoc Networks, 6*(7), 1134–1150.

[119] Zhu, S., Xu, S., Setia, S., & Jajodia, S. (2003). LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks. In *Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops* (pp. 749–755). IEEE.

LIST OF PAPERS BASED ON THESIS

Journals:

1. **Vanlalhruaia**, Khan, A.K, & Roy, A.K.(2024). Fast Authentication and Secure Handover for Wireless Mesh Network. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(3), 1057–1065.

2.**Vanlalhruaia**, Khan, A.K, & Roy, A.K. (2025)Securing AODV Against Black Hole Attack For Wireless Mesh Network**,** *Journal of Information Systems Engineering and Managemen*t, 10(37),1192-1202

3.**Chhakchhuak, V**., Khan, A. K., & Roy, A. K. (2025). Common key multi-hop packet authentication protocol for wireless mesh networks. *International Journal of Information and Computer Security*, *26*(3), 236-254.

Conference:

1.**Vanlalhruaia**, & Khan, A. K. (2023). Security Challenges During Handoff Authentication Operation for Wireless Mesh Network. In *Advances in Signal Processing, Embedded Systems and IoT: Proceedings of Seventh ICMEET-2022* (pp. 397-405). Singapore: Springer Nature Singapore.

2. **Vanlalhruaia**, &Khan, A. K. (2022, December). Fast handoff authentication of client in wireless mesh network. In *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)* (pp. 1954-1957). IEEE.

BIODATA OF THE CANDIDATE

Name : Vanlalhruaia

Date of Birth :24/11/1981

Email : hruai_a56@yahoo.com/mzut160@mzu.edu.in

Address : Dr. C.Silvera Building, Tuikhuahtlang, Aizawl, Mizoram

Marital status : Married

Educational Details:

B.E(C.Sc&Engg.) : Jorhat Engineering college, Dibrugarh University

M.Tech(I.T) : Tezpur University

Ph.D. course work : Mizoram University

PARTICULARS OF THE CANDIDATE

NAME OF CANDIDATE : Vanlalhruaia

DEGREE : Ph.D.

DEPARTMENT : COMPUTER ENGINEERING

TITLE OF THE THESIS : DEVELOPMENT OF SECURE COMMUNICATION SCHEMES FOR WIRELESS MESH NETWORKS

DATE OF ADMISSION :31.7.2019

APPROVAL OF RESEARCH PROPOSAL:

1.DRC : 28-October,2020

2.BOS : 29-October,2020

3.SCHOOL BOARD : 5-November,2020

MZU REGISTRATION No. :1906308

Ph.D REGISTRATION No. :MZU/Ph.D/1694 of 31.7.2019

EXTENSION : NA

(Dr.VD AMBETH KUMAR)

Head

Department Of Computer Engineering

ABSTRACT

DEVELOPMENT OF SECURE COMMUNICATION SCHEMES FOR WIRELESS MESH NETWORKS

AN ABSTRACT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

VANLALHRUAIA

MZU REGISTRATION NO.: 1906308

Ph.D. REGISTRATION NO.: MZU/Ph.D./1694 of 31.07.2019

DEPARTMENT OF COMPUTER ENGINEERING
SCHOOL OF ENGINEERING AND TECHNOLOGY

JUNE, 2025

ABSTRACT

DEVELOPMENT OF SECURE COMMUNICATION SCHEMES FOR WIRELESS MESH NETWORKS

BY

VANLALHRUAIA

DEPARTMENT OF COMPUTER ENGINEERING

Supervisor: Prof. Ajoy Kumar Khan

Joint Supervisor: Dr. Amit Kumar Roy

DEPARTMENT OF COMPUTER ENGINEERING, SCHOOL OF ENGINEERING AND TECHNOLOGY, MIZORAM UNIVERSITY

JUNE, 2025

ABSTRACT

Chapter 1: Introduction

This chapter lays the foundation for the study by detailing the evolution, architecture, characteristics, and applications of Wireless Mesh Networks (WMNs). It identifies critical security threats affecting WMNs due to their open, decentralized nature. The chapter defines the research problem, outlines the motivation, and summarizes the contributions of the thesis, which focuses on designing lightweight, secure, and efficient communication protocols for WMNs.

Chapter 2: Literature Review

A comprehensive review of existing security protocols in WMNs is conducted, focusing on three key areas: authentication, secure routing, and packet authentication. The chapter highlights limitations in current schemes, such as high overhead, lack of scalability, and inadequate resistance to internal as well as external attacks. Gaps identified in efficiency and security, key management, and routing security form the rationale for proposing new solutions in the subsequent chapters.

Chapter 3: Mutual Authentication and Secure Handover Protocol

This chapter presents a mutual authentication and secure handover protocol using a ticket-based mechanism. It ensures fast, seamless mobility for mesh clients while maintaining strong authentication. Security analysis confirms protection against replay, forgery, and privacy breaches. Performance evaluation demonstrates reduced authentication delay and improved handover efficiency compared to existing methods.

Chapter 4: Pre-Distributed Ticket-Based Handoff Authentication

A Client one way handoff authentication protocol using pre-distributed tickets is proposed to further minimize delay and overhead during client transitions. The design avoids repeated authentication exchanges with centralized servers. Analytical and simulation results confirm strong resistance to impersonation and replay attacks, while achieving faster handoff and low computational cost at the expenses of memory

Chapter 5: AODV Enhancement Against Blackhole Attacks

This chapter introduces a modified AODV routing protocol that detects and isolates blackhole nodes using route verification and route confirmation mechanisms. The enhanced protocol improves throughput, packet delivery ratio and end to end delay in comparison to normal AODV and AODV in presence of Black Hole node.

Chapter 6: Common Group Key Generation for Hop-by-Hop Packet Authentication

A group key generation protocol is proposed to authenticate data packets in a hop-by-hop manner. The protocol ensures low latency, scalability, and protection against replay and impersonation attacks. Simulation results validate reduced key computation time, improved delivery ratio, and minimal memory overhead for large-scale mesh deployments.

Chapter 7: Conclusion and Future Scope

The thesis concludes with a summary of the key contributions: lightweight authentication, secure routing, and packet-level integrity in WMNs. The proposed protocols outperform existing solutions in security and performance metrics. Future research directions include adaptive security mechanisms using machine learning and

extending the protocols for integration with next-generation networks like 5G and IoT-based mesh systems.

Keywords

Wireless Mesh Networks (WMNs), Secure Routing, Mutual Authentication, Handoff Authentication, Group Key Agreement, AODV, Blackhole Attack, Packet Authentication, Trust Management, Replay Attack, Network Security, Cryptography, Deffie Hellman Key Exchange.