



Werabe University
Institute of Technology
Department of Information Technology

Developing Innovative and Effective Security Mechanisms and Protocols to
Enhance MANET and WSN

By: Abdulhafiz Nasir

A Thesis submitted to Department of Information Technology, Institute of Technology
Requirement for the Degree of Master's in Computer Networking and Security

Jun 2026
Werabe, Ethiopia

Werabe University
Institute of Technology
Department of Information Technology

Developing Innovative and Effective Security Mechanisms and
Protocols to Enhance MANET and WSN

By: Abdulhafiz Nasir
Name of Major Advisor: Dr. Chandra Srinivas.
Co Advisor Negash Kor

A Thesis submitted to Department of Information Technology, Institute of Technology

Requirement for the Degree of Master's in Computer Networking and Security

Jun 2026
Werabe, Ethiopia

APPROVAL PAGE

I, the advisor of the thesis entitled Developing Innovative and Effective Security Mechanisms and Protocols to Enhance MANET and WSN developed by Abdulhafiz Nasir here by certify that the recommendation and suggestions made by the board of examiners are appropriately incorporated into the final version of the thesis.

Dr. Chandra Srinivas.

Major Advisor

Signature

Date

Negash Kor

Co-advisor

Signature

Date

We, the undersigned, members of the Board of Examiners of the thesis by Abdulhafiz Nasir have read and evaluated the thesis entitled Developing Innovative and Effective Security Mechanisms and Protocols to Enhance MANET and WSN and examined the candidate during open defense. This is, therefore, to certify that the thesis is accepted for partial fulfillment of the requirement of the degree of Master of Science in Computer Networking and security.

Chairperson

Signature

Date

Internal Examiner

Signature

Date

External Examiner

Signature

Date

Final approval and acceptance of the thesis is contingent upon submission of its final copy to the office of Postgraduate Studies (OPGS) through the Department Graduate Council (DGC) and School of Graduate Committee (SGC).

Department Head

Signature

Date

School Dean

Signature

Date

Office of Postgraduate Studies

Signature

Date

Dean

DECLARATION

I hereby declare that this Master Thesis entitled Developing Innovative and Effective Security Mechanisms and Protocols to Enhance MANET and WSN is my original work. That is, it has not been submitted for the award of any academic degree, diploma or certificate in any other university. All sources of materials that are used for this thesis have been duly acknowledged through citation.

Abdulhafiz NAsir

Name of Student

Signature

Date

RECOMMENDATION

I, the advisor(s) of this thesis, hereby certify that I have read the revised version of the thesis entitled Developing Innovative and Effective Security Mechanisms and Protocols to Enhance MANET and WSN prepared under my guidance by Abdulhafiz Nasir submitted in partial fulfillment of the requirements for the degree of Masters of computer Networking and security. Therefore, I recommend the submission of revised version of the thesis to the department following the applicable procedures.

Dr. Chandra Srinivas



Major Advisor

Signature

Date

Negash Kor

Co-advisor

Signature

Date

ACKNOWLEDGMENT

First and most essentially, I thank God, the Almighty, for giving me numerous blessings, knowledge, and opportunities to finally finish this thesis. Words cannot express my gratitude to my friend Nuri Redela, who suggested the idea of pursuing a second degree, funded the whole process, and gave me his invaluable support and feedback. This would not have been possible without him. Many thanks to my advisor, Dr. Chandra S., who read my numerous revisions, and offered guidance and support to make some sense of the confusion and also I would thanks my Co-advisor Negash Kor he support to make guidance with many comments in each chapters. I would be remiss in not mentioning my family, especially my brother Mukemil Nasir. Their belief in me has kept my spirits and motivation high during this process. Lastly, I am also grateful to my classmates and my office mates, for their editing help, late-night feedback sessions, and moral support. Thanks, should also go to the research assistants, and study participants from the university, who impacted and inspired me

ABBREVIATION

AI .	Artificial Intelligent
ELK.	Elastic search, Log stash, Kibana
IDPS.	Intrusion Detection and Prevention System
IDS.	Intrusion Detection System
IPS.	Intrusion prevention System
IoT.	Internet of Things
LCA.	Lightweight Cryptographic Algorithms
MANET.	Mobile Ad Hoc Network
MISP.	Malware Information Sharing Platform & Threat Sharing
RP.	Routing Protocol
TBS.	Trust-Based Security
WSN.	Wireless Sensor Network
PDR.	Packet delivery ratio
TBS.	Trust-Based Security
LCA.	Lightweight Cryptographic Algorithms
BSP.	Binary Space Partitioning

List of Tables

Table 1: Summary of Related Works and Their Associated Gaps	23
Table 2: Security Mechanisms in MANETs and WSNs	24
Table 3: Security Enhancements in MANETs and WSNs	29
Table 4: Evaluation Methodology for IDPS in MANETs and WSNs.....	32
Table 5: Utilization of Detection Techniques in Network Security	39

List of Figures

Figure 1: The architecture of the proposed intrusion detection system.....	37
Figure 2: Sensor Nodes	40
Figure 3: Sample code For Intrusion Detection Algorism:	41
Figure 4: Intrusion Prevention System [1]	42
Figure 5: Centralized Management Console	43
Figure 6: NS-3 Simulation Software configuration	49

ABSTRACT

Mobile Ad Hoc Networks are decentralized, self-configuring networks that lack a fixed infrastructure and are characterized by dynamic topologies. These characteristics make MANETs particularly vulnerable to various security threats, including routing attacks, unauthorized access, and resource exhaustion. The advancements in MANET security, emphasizing secure, intrusion detection systems (IDS), and lightweight cryptographic techniques. Enhance authentication and integrity, effectively mitigating attacks. Intrusion detection systems, employing both anomaly-based and signature-based approaches, detect and respond to malicious activities. Lightweight cryptographic solutions, address the network's resource constraints while maintaining robust security. Future directions in MANET security research include leveraging machine learning for improved threat detection. Wireless Sensor Networks consist of numerous sensor nodes that collaboratively monitor and report on environmental conditions. The inherent limitations of these deployments in potentially hostile environments create significant security challenges. The current strategies for enhancing WSN security, with a focus on secure data aggregation, authentication protocols, and energy-efficient security mechanisms. Lightweight mutual authentication protocols provide essential security features without imposing significant resource overhead. This study focuses on developing innovative and effective security mechanisms and protocols to enhance the security, reliability, and performance of MANET and WSN environments. The proposed approach integrates lightweight cryptographic techniques, trust-based routing mechanisms, intelligent intrusion detection systems, and adaptive security strategies to provide comprehensive protection against attacks such as black hole, wormhole, Sybil, and denial-of-service attacks. The framework is designed to improve secure communication while minimizing energy consumption, routing overhead, and processing complexity. The proposed model also incorporates real-time monitoring and adaptive response mechanisms to detect and isolate malicious nodes efficiently. Furthermore, the study emphasizes maintaining Quality of Service (QoS) metrics such as packet delivery ratio, throughput, latency, and network lifetime. Simulation and performance evaluation are expected to demonstrate that the proposed framework provides improved attack detection accuracy, enhanced routing reliability, better energy efficiency, and stronger overall network security compared to existing approaches. The research contributes to the development of scalable, lightweight, and intelligent security solutions suitable for dynamic and resource-constrained MANET and WSN environments. Research in Mobile Ad Hoc Networks and Wireless Sensor Networks has focused heavily on improving network security, reliability, and energy efficiency. Several researchers proposed secure routing protocols to defend against attacks such as black hole, wormhole, Sybil, and denial-of-service attacks. Trust-based and cryptographic security mechanisms have been widely adopted to improve authentication, confidentiality, and data integrity in decentralized network environments. The methodology to be followed must focus on designing lightweight, adaptive, and secure mechanisms. Findings of the study Improved Security Performance, Increased Packet Delivery Ratio, Reduced End-to-End Delay, Lower Energy Consumption, Better Intrusion Detection Accuracy, Reduced Routing Overhead and Enhanced Network Reliability. The study concludes that developing innovative and lightweight security mechanisms significantly enhances the security and performance of MANET and WSN environments. The proposed security framework effectively addresses major vulnerabilities. The study interprets Security Enhancement, Improved Packet Delivery Ratio, Reduced Energy Consumption, Lower Delay and Overhead And Scalability and Adaptability.

Table of Content

CHAPTER ONE	1
INTRODUCTION.....	1
1.1 Background of the Study.....	1
1.2 Problem of the Statement	5
1.3 Research Question.....	6
1.4 Research Objectives	7
1.4.1 General objective.....	7
1.4.2 Specific Objective	7
1.5 Significance of the Study	7
1.6 Scope and Limitation of the Study	9
1.7 Organization of the Thesis	11
CHAPTER TWO	12
LITERATURE REVIEW and RELATED WORKS	12
2.1 Introduction	12
2.1.1 Security Threats in MANET and WSN.....	14
2.1.3 Challenges and Future Directions	15
2.2 Related Works and Research Gaps	16
2.2.1 Summary of related works and their associated gaps.....	20
CHAPTER THREE.....	26
RESEARCH METHODOLOGY	26
3.1 Overview	26
3.2 Research Design.....	26
3.3 Data Collection Technique.....	26
3.4 Framework Development.....	27
3.5 Evaluation Methodology	30
3.6 System Development Tools	31
3.7 Ethical considerations	34
CHAPTER FOUR.....	35
PROPOSED FRAMEWORK	35
4.1 Introduction	35
4.2 Overview	37
4.3. Components of the Proposed IDPS Framework.....	39
4.3.1. Sensor Nodes.....	39
4.3.2. Base Stations	40

4.3.3. Intrusion Detection Algorithms.....	40
4.3.4. Intrusion Prevention Mechanisms	41
4.3.5. Centralized Management Console.....	42
4.4. Framework Implementation	43
CHAPTER FIVE.....	46
RESULTS AND DISCUSSION	46
5.1 INTRUSION DETECTION INTRUSION PREVENTION SYSTEM.....	46
5.2 Evaluation Framework for Detecting Threats and Attacks	47
5. 3 Experimental Results and analysis.....	48
5.2.1 Test to determine Intrusion Detection and Prevision System	49
CHAPTER SIX	52
CONCLUSION AND RECOMMENDATION	52
6.1 Conclusion.....	52
6.2 Findings.....	53
6.3 Recommendations	53
7. REFERENCES.....	56

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Mobile Ad Hoc Networks (MANET) and Wireless Sensor Networks (WSN) have emerged as versatile and vital communication paradigms, enabling a wide range of applications across various domains. To develop innovative and effective security mechanisms and protocols to enhance network security in Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs). Systematically, including challenges, potential approaches, and innovative ideas. I'll make it thorough but structured.

Mobile Ad Hoc Networks (MANET): MANET is a self-configuring network of mobile devices connected by wireless links. These networks are highly adaptable and can be set up quickly without the need for pre-established infrastructure. MANETs find applications in both military and civilian domains, such as battlefield communication, emergency response, vehicular networks, and even smartphone-based communication. They are characterized by the following key features:

- **Dynamic Topology:** MANETs exhibit dynamic topologies, as nodes can join, leave, or move within the network. This adaptability makes them suitable for scenarios where infrastructure-based networks are infeasible.
- **Decentralized:** MANETs often lack a central control or infrastructure. Nodes communicate directly with each other, making routing and security a complex task.
- **Resource Constraints:** MANET nodes are typically resource-constrained in terms of processing power, memory, and energy. This makes traditional security mechanisms less practical and necessitates lightweight solutions.
- **Vulnerabilities:** The absence of a centralized authority and the dynamic nature of the network make MANETs vulnerable to various security threats, including eavesdropping, data modification, and denial of service attacks.

Wireless Sensor Networks (WSN): WSNs consist of numerous small, resource-constrained sensors that collaborate to monitor physical or environmental conditions. These networks play a crucial role in applications such as environmental monitoring, smart agriculture, healthcare, and industrial automation. Key attributes of WSNs include:

- **Distributed Sensing:** WSN nodes are distributed throughout an area of interest, collecting data from their surroundings. This data is then transmitted to a central location for analysis.
- **Resource Limitations:** Sensor nodes are typically tiny and battery-powered, which imposes stringent resource constraints. Extending the lifetime of these nodes is a significant concern.
- **Data-centric:** WSNs are data-centric, with a primary focus on collecting and transmitting data. Data collected is often highly valuable and sensitive, as it may pertain to critical applications like patient health monitoring or environmental disaster detection.
- **Deployment in Harsh Environments:** Many WSN deployments occur in challenging or remote environments, such as forests, industrial facilities, or disaster-stricken areas, where traditional infrastructure is absent.
- **Communication Challenges:** WSNs face communication challenges, including intermittent connectivity, varying data rates, and the need for efficient data routing. Security mechanisms should not unduly burden communication or compromise the network's ability to meet its objectives.
- 🏠 **Security Challenges in MANET and WSN:** Both MANET and WSN share common security challenges stemming from their dynamic, resource-constrained, and decentralized nature. These challenges include but are not limited to:
 - ✓ **Dynamic Topology Management:** Securing the network when nodes continuously join, leave, or move within the network is complex.
 - ✓ **Resource-Efficient Cryptography:** Designing security mechanisms that don't deplete the limited resources of these devices is essential.
 - ✓ **Data Privacy and Integrity:** Ensuring that data remains confidential, is not tampered with, and is only accessible to authorized entities is crucial.
 - ✓ **Authentication and Access Control:** Verifying the authenticity of nodes and restricting access to authorized entities is challenging in decentralized networks.
 - ✓ **Intrusion Detection and Prevention:** Identifying and mitigating malicious activity without relying on a central authority is a daunting task.

⚙️ Principles for Effective Security Mechanisms

1. Lightweight: Minimize computation, energy, and memory usage.
2. Robust: Resist both insider and outsider attacks.
3. Scalable: Adapt to network growth.
4. Self-organizing & autonomous: Function without centralized control.
5. QoS-aware: Security should not drastically degrade performance.

⚙️ Innovative Security Mechanisms and Protocol Approaches

➡️ Key Management & Authentication

Challenge: Traditional PKI is heavy; symmetric keys are vulnerable to compromise.

Innovative Approaches: Identity-based cryptography (IBC): Uses node identity to generate keys dynamically. Lightweight Blockchain: Distributed ledger for authentication in MANETs/WSNs. Context-aware authentication: Node behavior, location, and mobility patterns are used to authenticate.

➡️ Intrusion Detection & Prevention

Challenge: Attack patterns in dynamic networks are hard to detect.

Approaches: Behavioral anomaly detection using machine learning. Collaborative intrusion detection: Nodes cooperate to identify malicious nodes. Reputation-based systems: Nodes maintain trust scores for neighbors; malicious nodes are isolated.

➡️ Secure Routing Protocols

MANET Routing Attacks: Blackhole, wormhole, grayhole.

Innovations: Trust-aware routing: Routes chosen based on neighbor trust scores. Multipath routing with redundancy: Transmit data over multiple paths to prevent interception. Lightweight cryptographic routing: Use hash chains or symmetric key encryption for route integrity.

➡️ Data Confidentiality & Integrity

For WSNs: Data aggregation at cluster heads can be vulnerable.

Innovations: Homomorphic encryption: Allows computations on encrypted data for aggregation without decryption. Dynamic key rotation: Periodically updates keys to reduce exposure. Secure data aggregation protocols: Combine multi-sensor data securely while detecting malicious nodes.

➡️ Privacy-Preserving Mechanisms

Challenge: Sensor readings or node locations may reveal sensitive information.

Innovations: Anonymity and pseudonym schemes: Mask node identities. Differential privacy: Add controlled noise to sensor data before transmission. Secure location-based routing: Avoid revealing node positions while routing.

➡ Adaptive Security Protocols

Idea: Network security adapts based on context. Energy-aware encryption: Stronger security for critical data, lighter for routine data. Mobility-aware intrusion detection: Adjust thresholds based on node speed and topology changes.

➡ Cross-layer Security

Integrate security across multiple network layers (MAC, network, application): Detect jamming attacks at MAC layer and coordinate with routing protocols. Prevent replay attacks by combining timestamp validation (network layer) and key refresh (application layer).

🧩 Suggested Research Directions / Innovations

AI-powered adaptive trust management in MANETs to detect evolving threats.

Blockchain-based lightweight authentication for decentralized WSNs.

Homomorphic encryption for secure in-network data aggregation.

Hybrid cryptography protocols optimized for low-power, resource-constrained nodes.

Cross-layer cooperative security to enhance detection and response without overloading nodes.

🧩 Evaluation Metrics

- Energy consumption
- Network throughput and latency
- Packet delivery ratio
- Detection accuracy of malicious nodes
- Resistance against specific attacks

1.2 Problem of the Statement

Despite the existence of numerous security mechanisms and protocols for MANETs and WSNs, current solutions still face limitations related to high computational overhead, excessive energy consumption, weak attack detection accuracy, poor scalability, insecure routing, and lack of adaptability to dynamic network conditions. Therefore, there is a need to develop innovative, lightweight, intelligent, and energy-efficient security mechanisms and protocols capable of providing reliable, scalable, and comprehensive protection against evolving security threats in MANET and WSN environments.

Mobile Ad Hoc Networks (MANET) and Wireless Sensor Networks (WSN) have revolutionized the way we connect and gather data in a multitude of applications. However, their inherent vulnerabilities have grown more pronounced as they've become integral to our daily lives. As MANET and WSN applications continue to expand into sensitive and mission-critical areas, there is a growing need for innovative, lightweight, adaptive, and efficient security mechanisms capable of providing strong protection while maintaining acceptable Quality of Service (QoS), energy efficiency, and scalability. The problem at hand is the urgent need to bolster the network security of MANET and WSN due to the following critical challenges:

- ❖ **Dynamic Topology Vulnerabilities:** The dynamic nature of MANETs, where nodes frequently join or leave the network or change their positions, creates an ever-shifting landscape that is ripe for exploitation. Attackers can easily manipulate network routes, inject malicious nodes, or eavesdrop on communications in this fluid environment, jeopardizing the integrity of data and communication.
- ❖ **Resource Constraints:** MANET and WSN nodes operate under stringent resource limitations, with limited processing power, memory, and energy reserves. Traditional security mechanisms, which often demand significant computational resources, are impractical in these environments. As a result, protecting these networks without impairing their functionality is an intricate balancing act.
- ❖ **Authentication and Access Control:** In the absence of a centralized authority, authenticating nodes and ensuring access control become formidable challenges. MANET and WSN should only allow legitimate nodes to participate while preventing unauthorized entities from compromising the network. Achieving this while maintaining efficiency is a complex task.

- ❖ **Data Confidentiality and Integrity:** In WSNs, data collected from sensors is often highly sensitive and valuable, encompassing critical information in healthcare, environmental monitoring, and industrial processes. Ensuring that this data remains confidential, unhampered, and accessible only to authorized parties is vital. Breaches could lead to catastrophic consequences.
- ❖ **Intrusion Detection and Prevention:** Identifying and mitigating malicious activity in MANET and WSN is intricate due to the lack of a centralized perimeter and the presence of potentially compromised nodes. Intrusion detection and prevention mechanisms need to be tailored to the network's dynamic, self-organizing nature.
- ❖ **Communication Overhead:** Conventional security mechanisms can introduce significant communication overhead, leading to reduced network efficiency and increased energy consumption. The challenge is to design security solutions that minimize this overhead while still effectively safeguarding network assets.
- ❖ **Heterogeneity:** MANETs and WSNs often comprise a variety of devices with different capabilities and communication interfaces. This diversity makes it challenging to implement uniform security mechanisms that cater to the needs of all network components

1.3 Research Question

1. How can security threats and vulnerabilities in MANETs and WSNs be effectively identified and analyzed?
2. How can secure and efficient routing be achieved in MANETs and WSNs?
3. How can authentication and key management be improved in resource-constrained networks?
4. How can malicious activities and intrusions be detected accurately in real time?
5. How can trust among network nodes be enhanced to reduce insider attacks?

1.4 Research Objectives

1.4.1 General objective

Developing innovative and effective security mechanisms and protocols to enhance the network security of Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs) by improving authentication, secure routing, intrusion detection, data confidentiality, integrity, and trust management while maintaining energy efficiency and network performance.

1.4.2 Specific Objective

1. To identify and analyze major security threats, vulnerabilities, and attacks affecting MANETs and WSNs.
2. To develop secure and lightweight routing protocols that improve data transmission reliability and attack resistance.
3. To design efficient authentication and key management mechanisms suitable for MANET and WSN environments.
4. To develop intelligent intrusion detection and prevention mechanisms for accurate and real-time attack detection.
5. To implement trust-based mechanisms for detecting and isolating malicious nodes.
6. To evaluate and compare the performance of the proposed mechanisms using standard simulation metrics and tools.

1.5 Significance of the Study

The significance of Developing Innovative and Effective Security Mechanisms and Protocols to Enhance MANET and WSN” is profound and multifaceted, as these networks play pivotal roles in various critical domains. This study holds considerable importance due to the following reasons:

Data Protection and Privacy: MANET and WSN often handle sensitive data, such as military communications, healthcare information, and environmental data. Enhancing security ensures data confidentiality and integrity, protecting individuals and organizations from data breaches and privacy violations.

Reliable Communication: In emergency response scenarios, battlefield communication, and remote environmental monitoring, network reliability is paramount. Improved security

mechanisms help maintain communication even in the face of adversarial attacks, ensuring critical information is delivered when needed.

Resource Efficiency: MANET and WSN are typically resource-constrained. Enhanced security solutions tailored to these constraints ensure efficient resource utilization, prolonging the lifespan of network nodes and minimizing energy consumption.

Adaptability to Dynamic Environments: Many applications of MANET and WSN involve dynamic and harsh environments where infrastructure-based networks are impractical. Enhanced security mechanisms enable these networks to adapt to changing conditions, making them more resilient.

Diverse Applications: MANET and WSN are used in a wide range of applications, from healthcare to agriculture, from military operations to smart cities. Improved security is vital to guarantee the safety and functionality of these applications, directly impacting people's lives and the efficiency of organizations.

Reduced Vulnerabilities: MANET and WSN are susceptible to various security threats, including eavesdropping, data tampering, and denial of service attacks. By addressing these vulnerabilities, the study contributes to a safer and more reliable digital ecosystem.

Strategic Importance: In military operations and critical infrastructure protection, the security of MANET and WSN is of strategic importance. Enhancing network security ensures the confidentiality of sensitive information and the reliability of communication, which are vital in defense and national security contexts.

Research and Technological Advancements: The study may lead to the development of novel security mechanisms and protocols that can be applied beyond MANET and WSN, contributing to the broader field of cyber security and fostering technological advancements.

Economic Impact: MANET and WSN contribute to economic growth through efficiency improvements and cost savings in various industries. A secure network infrastructure protects these investments, fostering economic stability and growth.

Resilience in Disaster Scenarios: In disaster management and response, MANET and WSN play crucial roles in collecting and transmitting critical data. Improved security mechanisms ensure the resilience of these networks, enabling more effective disaster response.

1.6 Scope and Limitation of the Study

The scope of a study aimed at enhancing Mobile Ad Hoc Networks (MANET) and Wireless Sensor Networks (WSN) can be quite broad and may encompass various aspects of these wireless communication technologies. Here are some potential scopes and areas of study for enhancing MANET and WSN:

❖ **Performance Improvement**

Analyze and improve the performance metrics such as throughput, latency, and packet delivery ratio in MANET and WSN.

Investigate the use of advanced routing protocols to enhance network performance.

❖ **Security**

Investigate security threats and vulnerabilities in MANET and WSN and propose solutions to enhance network security.

Authentication mechanisms for securing communication in these networks.

❖ **Routing Protocols(RP)**

Investigate the routing protocols for both MANET and WSN to handle dynamic network topologies.

Consider hybrid routing protocols that can adapt to changing network conditions..

❖ **Simulation and Modeling**

Develop simulation models and tools to evaluate and test the proposed enhancements in a controlled environment before deployment.

Limitations of the study for Developing Innovative and Effective Security Mechanisms and Protocols to Enhance MANET and WSN” should be acknowledged to provide a clear understanding of the scope and potential constraints of the research. These limitations may include:

- ✓ **Diversity of Network Scenarios:** MANET and WSN are used in a wide range of applications, each with its unique requirements and challenges. **Resource Variability:** While resource constraints are a common characteristic of these networks, the extent of limitations can vary significantly between deployments. The study may not address all possible resource constraints, and the proposed security mechanisms may not suit every resource scenario.

- ✓ **Simulation Environments:** Many studies rely on simulations to evaluate security mechanisms. While simulations provide controlled environments, they may not fully capture the complexity and unpredictability of MANET and WSN deployments.
- ✓ **Heterogeneity Challenges:** Addressing the heterogeneity of devices and communication interfaces within MANET and WSN networks is a complex issue. The study may focus on specific types of devices or interfaces, potentially limiting the applicability of the proposed security solutions.
- ✓ **Scalability Concerns:** Scalability is a critical factor in MANET and WSN, especially in large-scale deployments. The study may not fully address the challenges related to the scalability of security mechanisms and may focus on smaller network sizes.
- ✓ **Assumptions and Simplifications:** To make the research manageable, some assumptions and simplifications may be necessary. These assumptions may not fully represent the complexity of real-world scenarios.
- ✓ **Interoperability Issues:** Interoperability among different devices and protocols can be challenging, and the study may not comprehensively address these challenges in the context of MANET and WSN.
- ✓ **Evolution of Threats:** The security landscape is constantly evolving, with new threats and attack techniques emerging. The study may not address all possible threats or anticipate future security challenges.
- ✓ **Ethical and Legal Considerations:** The study may not comprehensively address the ethical and legal considerations related to network security, such as data privacy and compliance with regulations, which can vary by jurisdiction.
- ✓ **Cost and Deployment Constraints:** Deploying and maintaining enhanced security mechanisms can be costly. The study may not fully consider the financial and logistical constraints that organizations or individuals may face in implementing these measures.

1.7 Organization of the Thesis

This Thesis is organized with six chapters. Chapter one presents introduction of the thesis including background, about statement of problem, objectives, significance, scope and limitation of the study. The next part of the thesis discusses about literatures related to the existing enhancing Mobile Ad Hoc Networks (MANET) and Wireless Sensor Networks (WSN) and their limitations. Chapter three presents about the methodology of the study. In chapter four, proposed framework and its implementation is discussed. The results and discussion of thesis is presented in chapter five and finally the research is concluded and future works are presented in chapter six.

CHAPTER TWO

LITERATURE REVIEW and RELATED WORKS

2.1 Introduction

Mobile Ad Hoc Networks (MANET) and Wireless Sensor Networks (WSN) are two prominent wireless communication paradigms with numerous applications in fields such as military, healthcare, environmental monitoring, and disaster management. However, due to their inherent characteristics, including open wireless communication channels and resource constraints, these networks are highly vulnerable to security threats. This literature review explores the current state of research on enhancing the security of MANET and WSN, emphasizing key developments, challenges, and trends in the field. Mobile Ad Hoc Networks (MANET) and Wireless Sensor Networks (WSN) are decentralized wireless communication systems that operate without fixed infrastructure. These networks are widely applied in military communication, disaster recovery, environmental monitoring, healthcare systems, industrial automation, smart cities, and Internet of Things (IoT) environments. Due to their distributed architecture, dynamic topology, open wireless medium, and limited resources, MANET and WSN systems are highly vulnerable to numerous security threats and cyber-attacks.

Researchers in Mobile Ad Hoc Networks and Wireless Sensor Networks have proposed several mechanisms to address security challenges such as unauthorized access, packet dropping, routing manipulation, denial-of-service attacks, node impersonation, and malicious traffic injection. Existing studies mainly focus on secure routing, cryptographic protection, trust management, intrusion detection systems, energy-efficient communication, and intelligent attack detection.

Secure routing protocols such as Secure AODV (SAODV), ARAN, SEAD, and Ariadne were introduced to protect routing information and improve secure communication in MANET environments. These protocols use authentication and cryptographic techniques to prevent routing attacks and malicious modifications of routing packets. Similarly, in WSNs, secure cluster-based routing mechanisms and lightweight encryption protocols were developed to reduce energy consumption while ensuring confidentiality and integrity of transmitted data.

Trust management systems became another important research area in MANET and WSN security. Trust-based mechanisms evaluate node behavior using packet forwarding reliability, cooperation level, and communication consistency to identify malicious nodes and improve secure routing decisions. Researchers proposed dynamic trust evaluation algorithms capable of isolating untrusted nodes and improving network reliability.

Intrusion Detection Systems (IDS) also gained significant attention in wireless network security research. Signature-based IDS, anomaly-based IDS, specification-based IDS, and hybrid IDS models were introduced to detect malicious activities such as black hole attacks, wormhole attacks, Sybil attacks, selective forwarding, flooding attacks, and denial-of-service attacks. More recently, machine learning and artificial intelligence approaches have been integrated into IDS systems to improve attack detection accuracy and adaptive response mechanisms.

Energy efficiency remains a major concern in WSN security research because sensor nodes have limited battery power and computational capability. Researchers proposed lightweight security algorithms, low-overhead authentication techniques, and energy-aware secure routing protocols to minimize power consumption while maintaining acceptable security performance. Cross-layer security approaches and QoS-aware security mechanisms were also explored to improve network performance and communication reliability.

Furthermore, block-chain-based security frameworks, cloud-assisted security systems, and software-defined networking (SDN)-based architectures have recently emerged as modern approaches for improving decentralized trust management, authentication, and secure communication in wireless networks. These technologies aim to provide scalability, transparency, and real-time security monitoring.

Despite these advancements, existing MANET and WSN security mechanisms still face several limitations including high computational complexity, excessive energy consumption, scalability challenges, limited adaptability to dynamic topology changes, and poor real-time attack detection performance. These unresolved issues create the need for more intelligent, lightweight, adaptive, and integrated security frameworks.

2.1.1 Security Threats in MANET and WSN

Security threats in MANET and WSN can be categorized into several types, including eavesdropping, data tampering, denial of service attacks, and node compromise. Various studies have identified and analyzed these threats. For instance, in "Security in Wireless Sensor Networks: A Survey" by [1], the authors provide an early overview of security threats in WSN.

2.1.2 Key Security Mechanisms

Several security mechanisms have been proposed to safeguard MANET and WSN. Cryptographic techniques, authentication protocols, and intrusion detection systems are some of the widely studied methods. "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks" by [2] provides an in-depth analysis of security mechanisms and their applicability in MANET and WSN.

- Trust-Based Security (TBS):

Trust-based security models have gained prominence in recent years. These models establish trust levels among network nodes and adapt security measures accordingly. Research, such as "A Survey of Trust Management and Resource Discovery in Self-Organizing Networks" by Misheard and Molva delves into the concept of trust in MANET and its implications for security. However, recent literature focusing specifically on trust management and its effectiveness in addressing evolving security threats in MANET and WSN is scarce, indicating a research gap in this area.

- Energy-Efficient Security:

Energy efficiency is a critical concern in both MANET and WSN due to their resource-constrained nature. Researchers have explored techniques to implement security mechanisms while minimizing energy consumption. "Energy-Efficient Security for Wireless Sensor Networks" by [3] is an influential work in this domain, proposing energy-efficient cryptographic algorithms and protocols. However, further research is needed to evaluate the practical implementation and performance of these techniques in real-world scenarios.

- Intrusion Detection Systems (IDS):

Intrusion detection systems (IDS) are essential for identifying malicious activities in MANET and WSN. Research, such as "Intrusion Detection in Wireless Ad-Hoc Networks" by Tseng et al. [4], focuses on the development of efficient IDS tailored to the unique characteristics of these networks. Recent studies have explored machine learning-based approaches for anomaly

detection in MANET and WSN, indicating a shift towards more sophisticated intrusion detection techniques. However, the effectiveness of these approaches in dynamic and resource-constrained environments remains an open research question.

- Secure Routing Protocols:

Secure routing protocols are critical for maintaining data confidentiality and integrity during transmission. Studies like "A Survey on Secure Routing Protocols for MANETs" by [5] provide comprehensive insights into secure routing strategies. Recent research has proposed novel secure routing protocols that integrate cryptographic techniques with dynamic trust management mechanisms to adapt to changing network conditions and mitigate routing attacks. However, further empirical evaluation is required to assess the scalability and resilience of these protocols in large-scale MANET and WSN deployments.

2.1.3 Challenges and Future Directions

Energy Efficiency:

One of the primary challenges in securing MANET and WSN is to develop security mechanisms that do not excessively drain the limited energy resources of the network nodes. Energy-efficient security solutions are crucial to ensure the longevity and sustainability of these networks [6].

Scalability:

As the number of nodes in MANET and WSN grows, scalability becomes a significant concern. Security mechanisms and protocols must be designed to handle large-scale networks efficiently while maintaining a high level of security [7].

Adaptation to Network Dynamics:

MANETs are highly dynamic, with nodes joining and leaving the network frequently. Security mechanisms must adapt to these changes to ensure that the network remains secure. This adaptability is critical for maintaining connectivity and data integrity [8].

Resilience to Zero-Day Attacks:

Zero-day attacks, which exploit previously unknown vulnerabilities, pose a significant threat to MANET and WSN. Developing intrusion detection and prevention systems that can detect and respond to these attacks is a critical research direction [9].

Lightweight Cryptographic Algorithms (LCA):

The resource-constrained nature of WSN and the mobility of MANET nodes necessitate the development of lightweight cryptographic algorithms. These algorithms should provide strong security without consuming excessive computational resources [10].

Machine Learning and AI Integration:

The integration of machine learning and artificial intelligence (AI) into MANET and WSN security is a promising avenue for future research. Machine learning can be used to detect anomalous behavior and identify security threats more accurately [11].

Cross-Layer Security:

Cross-layer security approaches that combine information from multiple protocol layers can improve the effectiveness of security mechanisms. Research in this area can lead to more robust and adaptive security solutions [12].

Secure Data Aggregation:

In WSN, secure data aggregation is essential to protect data as it travels through the network to the sink. Developing efficient and secure data aggregation techniques is a vital aspect of WSN security research [13].

Trust Management:

Trust-based security models, which establish trust levels among network nodes, should be further explored and enhanced to create more robust and adaptable security solutions [14].

Standardization and Interoperability:

Standardization of security protocols and mechanisms is critical for ensuring interoperability between different MANET and WSN deployments. This will facilitate the widespread adoption of secure practices [15].

Despite significant progress in enhancing MANET and WSN security, numerous challenges persist. These include the development of lightweight cryptographic algorithms, resilience to zero-day attacks, and energy-efficient security solutions. Future research should also consider the integration of machine learning and artificial intelligence for improved threat detection.

2.2 Related Works and Research Gaps

Several previous studies have contributed significantly to the development of secure communication mechanisms for MANET and WSN systems.

Researchers working on Secure AODV (SAODV) enhanced the traditional AODV routing protocol by introducing digital signatures and hash chains to secure routing messages and

prevent route manipulation attacks. Although SAODV improved routing security, the protocol increased computational overhead and routing delay due to cryptographic operations.

The ARAN protocol introduced certificate-based authentication mechanisms to protect MANET routing processes from malicious nodes. ARAN improved authentication and routing integrity but suffered from scalability limitations and high certificate management complexity.

Trust-based routing models proposed by several researchers evaluated node behavior dynamically to improve secure route selection. These models enhanced detection of selfish and malicious nodes but required continuous monitoring and trust calculation processes that consumed additional network resources.

Researchers also introduced lightweight encryption schemes for WSN environments to reduce energy consumption while ensuring confidentiality and authentication. These techniques improved resource efficiency but often provided weaker protection against sophisticated multi-stage attacks.

Intrusion Detection Systems based on anomaly detection and machine learning algorithms demonstrated improved attack classification and real-time monitoring capabilities. Artificial intelligence techniques such as neural networks, support vector machines, and fuzzy logic were applied to identify malicious traffic patterns and abnormal node behavior. However, these intelligent approaches often required high processing capability and large training datasets.

Cluster-based security mechanisms improved energy efficiency and communication organization in WSNs by grouping nodes into clusters managed by cluster heads. Although these methods reduced communication overhead, cluster head failure introduced additional reliability and security concerns.

Block-chain-based security approaches were also explored to provide decentralized trust management and tamper-resistant communication. While blockchain enhanced data integrity and transparency, its implementation introduced high computational and energy overhead unsuitable for lightweight sensor networks.

Hybrid security frameworks combining cryptography, trust management, and intrusion detection systems achieved stronger multi-layer protection against attacks. However, most hybrid approaches became increasingly complex and difficult to deploy in highly dynamic and resource-constrained environments. Recent research (2023–2025) on MANET, WSN, and IoT security has focused on lightweight cryptography, AI-based intrusion detection systems, blockchain-enabled

trust management, secure routing, cross-layer security, and hybrid security frameworks. Researchers aim to improve attack detection accuracy, routing reliability, scalability, and energy efficiency in resource-constrained and highly dynamic wireless environments

Overall, previous related works provided valuable contributions to MANET and WSN security research but still left several important challenges unresolved.

Research gaps represent areas where current knowledge and solutions are insufficient or incomplete. Here are some research gaps in MANET and WSN security:

Energy-Efficient Security Mechanisms: Current security mechanisms for MANET and WSN often consume significant energy resources, which can be a critical issue for battery-constrained devices. There is a need for the development of more energy-efficient security solutions to extend the network's lifetime without compromising security.

Cross-Layer Security Integration: While security measures are typically implemented within individual protocol layers, there is a lack of comprehensive cross-layer security integration. Research is needed to explore how information from different protocol layers can be effectively combined to provide more robust and adaptive security solutions.

Machine Learning for Anomaly Detection: Machine learning techniques have shown promise in anomaly detection in traditional networks, but their application in MANET and WSN is relatively unexplored. There is a gap in understanding how machine learning can be effectively employed to detect and respond to security threats in these networks.

Quantitative Risk Assessment: There is a need for more extensive research on quantitative risk assessment methodologies tailored to MANET and WSN. This includes assessing the impact of potential threats, vulnerabilities, and security measures on network performance.

User-Centric Security: While researchers have focused on enhancing network-level security, there is a research gap in understanding and addressing the security awareness, perceptions, and practices of end users and administrators in MANET and WSN. Research in this area can help tailor security solutions to user needs and behaviors.

Secure Data Aggregation in WSN: Securing data aggregation is a critical aspect of WSN security. Research is needed to develop efficient and secure data aggregation techniques that protect data as it traverses the network while minimizing resource consumption.

Standardization and Interoperability: The lack of standardization in security protocols and mechanisms hinders interoperability between different MANET and WSN deployments. Research should focus on defining common security standards and practices to enable seamless communication and collaboration.

Zero-Day Attack Resilience: MANET and WSN are vulnerable to zero-day attacks, which exploit previously unknown vulnerabilities. There is a research gap in developing effective intrusion detection and prevention mechanisms to detect and respond to such attacks proactively.

Threats in the Era of IoT: With the proliferation of the Internet of Things (IoT), MANET and WSN are increasingly interconnected with diverse devices. Research should explore the emerging security threats and challenges that arise in this IoT context and develop solutions accordingly.

Usability and Human Factors: The usability of security mechanisms and their impact on network performance are often overlooked. Research is needed to assess how security solutions can be designed to be user-friendly and minimize disruptions to network operation.

Security mechanisms commonly employed in Mobile Ad hoc Networks (MANETs) and Wireless Sensor Networks (WSNs):

Lack of Lightweight Security Mechanisms Many existing protocols rely on computationally intensive cryptographic operations that consume excessive battery power and processing resources. Resource-constrained WSN nodes cannot efficiently support complex security algorithms for long periods.

High Energy Consumption

Current intrusion detection systems, trust evaluation models, and encryption mechanisms increase communication overhead and energy usage, reducing network lifetime.

Limited Multi-Attack Protection

Several existing approaches focus on individual attacks such as black hole or wormhole attacks rather than providing comprehensive protection against multiple simultaneous threats.

Poor Scalability

Many security frameworks perform effectively only in small or medium-sized networks but fail under large-scale or highly mobile network conditions.

Inadequate Real-Time Attack Detection

Traditional IDS approaches often fail to detect attacks quickly and accurately in rapidly changing MANET environments.

High False Positive and False Negative Rates

Many anomaly-based intrusion detection systems incorrectly classify legitimate nodes as malicious or fail to detect actual attackers.

Weak Adaptability to Dynamic Topology Changes

MANET environments experience frequent topology changes caused by node mobility, yet many existing protocols cannot adapt effectively.

Increased Routing and Communication Overhead

Secure routing mechanisms frequently increase packet overhead, routing delay, and bandwidth consumption.

Limited Integration of Intelligent Technologies

Although machine learning and artificial intelligence techniques show promising results, their integration into lightweight and adaptive wireless security systems remains limited.

Poor QoS and Security Balance

Several security approaches improve protection but significantly reduce network throughput, increase latency, and lower packet delivery performance.

2.2.1 Summary of related works and their associated gaps

Research on securing Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs) has grown significantly due to the increasing use of decentralized and infrastructure-less communication systems in military operations, environmental monitoring, healthcare, transportation, and disaster recovery applications. Numerous security mechanisms and protocols have been proposed to address vulnerabilities such as routing attacks, data tampering, node compromise, denial of service attacks, and energy depletion attacks. Despite these contributions, several limitations and research gaps remain unresolved.

Early studies focused mainly on cryptographic approaches such as symmetric and asymmetric encryption techniques to provide confidentiality, authentication, and integrity in MANETs and WSNs. Protocols including secure variants of AODV, DSR, and LEACH attempted to protect routing information from malicious nodes. While these methods improved communication

security, they introduced significant computational and energy overheads, particularly in WSNs where sensor nodes possess limited battery power, processing capability, and memory resources. Most traditional cryptographic mechanisms were therefore unsuitable for highly dynamic and resource-constrained environments.

Several researchers proposed trust-based and reputation-based security mechanisms to identify malicious nodes through behavioral monitoring and trust evaluation. These approaches improved detection of insider attacks such as black hole, gray hole, and selective forwarding attacks. However, many trust models suffered from slow convergence, inaccurate trust estimation, high communication overhead, and vulnerability to collusion attacks where multiple malicious nodes cooperate to manipulate trust values. In addition, trust calculations were often centralized or semi-centralized, reducing scalability and adaptability in highly mobile MANET environments.

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have also been extensively investigated for MANET and WSN security. Signature-based IDS approaches demonstrated high detection accuracy for known attacks, whereas anomaly-based IDS techniques were capable of identifying unknown attacks. Machine learning and artificial intelligence methods such as Support Vector Machines (SVM), Artificial Neural Networks (ANN), Decision Trees, and Deep Learning algorithms further enhanced attack detection performance. Nevertheless, many IDS/IPS solutions generated high false positive rates, consumed considerable computational resources, and lacked real-time responsiveness. Furthermore, most proposed IDS models were tested only under limited simulation conditions and failed to consider realistic large-scale heterogeneous network environments.

Cluster-based and hierarchical security protocols were introduced to improve scalability and energy efficiency in WSNs. Secure clustering schemes enhanced data aggregation and minimized communication overhead while protecting cluster heads from compromise attacks. Although these methods improved network lifetime and routing efficiency, many protocols assumed static network topologies and trusted cluster heads, which is impractical in hostile environments where nodes may be captured or compromised. Additionally, frequent re-clustering processes increased energy consumption and network instability.

Researchers also explored lightweight authentication and key management protocols specifically designed for resource-constrained sensor networks. Techniques based on hash functions, elliptic curve cryptography, and lightweight encryption algorithms reduced computational complexity

and improved energy efficiency. However, several lightweight protocols remained vulnerable to replay attacks, node replication attacks, impersonation attacks, and key compromise attacks. Many studies also overlooked secure key distribution and dynamic rekeying mechanisms in rapidly changing MANET topologies.

Recent advancements integrated blockchain, software-defined networking (SDN), fog computing, and Internet of Things (IoT) technologies into MANET and WSN security architectures. Blockchain-based solutions enhanced decentralization, transparency, and trust management, while SDN-enabled frameworks improved centralized monitoring and attack mitigation. Similarly, fog and edge computing reduced latency and improved distributed processing. Despite these advancements, such technologies often introduced excessive communication overhead, storage requirements, and computational complexity that exceeded the capabilities of lightweight sensor nodes. Scalability, interoperability, and energy optimization therefore remain major concerns.

Another significant research area involved energy-aware secure routing protocols. Researchers developed optimization algorithms and metaheuristic approaches such as Genetic Algorithms, Ant Colony Optimization, Particle Swarm Optimization, and Fuzzy Logic systems to achieve balanced security and energy consumption. Although these methods improved routing efficiency and network lifetime, many solutions prioritized either security or energy conservation independently rather than jointly optimizing both objectives. Consequently, maintaining strong security while preserving Quality of Service (QoS), low latency, and minimal energy consumption continues to be a challenge.

Additionally, most existing studies relied heavily on simulation tools such as NS-2, NS-3, MATLAB, OMNeT++, and QualNet for performance evaluation. While simulation-based experiments demonstrated improvements in metrics such as packet delivery ratio, throughput, detection rate, delay, routing overhead, and energy consumption, many proposed mechanisms lacked real-world experimental validation and deployment in practical environments. The absence of standardized datasets, benchmark attack scenarios, and realistic mobility models further limits fair comparison among different security protocols.

Overall, the literature demonstrates substantial progress in developing security mechanisms and protocols for MANETs and WSNs. However, important gaps still exist, including the need for lightweight and adaptive security frameworks, efficient trust management systems resistant to

collusion attacks, low-overhead real-time IDS/IPS solutions, scalable secure routing mechanisms, robust key management protocols, and integrated approaches that jointly optimize security, energy efficiency, QoS, and network lifetime. Future research should therefore focus on intelligent, hybrid, and context-aware security solutions capable of operating effectively in dynamic, heterogeneous, and resource-constrained MANET and WSN environments.

Table 1: Summary of Related Works and Their Associated Gaps

Author/Year	Used Protocol/Technique	Contribution	Associated Gaps
Hussain & Fathima (2024)	Federated Learning with Deep Learning IDS	Improved intrusion detection accuracy in MANET environments.	High computational overhead and training complexity.
Sharma et al. (2024)	Machine Learning-based IDS for WSN	Enhanced cyber-attack detection and anomaly identification.	Limited real-time adaptability and energy efficiency.
Keerthana & Babu (2025)	Trust Management and Secure Communication Framework	Improved secure routing and node trust evaluation in WSNs.	Scalability challenges in large dynamic networks.
Azzaoui et al. (2024)	Lightweight Cooperative IDS with RPL Protocol	Reduced memory and power consumption in IoT/WSN security.	Difficulty detecting sophisticated and hybrid attacks.
Krishna et al. (2025)	Hybrid Deep Learning Flooding Attack Detection	Increased MANET attack detection accuracy and routing security.	Deep learning models consume high processing resources.
Kumari et al. (2024)	Fuzzy Q-Learning Sinkhole Prevention Mechanism	Improved sinkhole attack prevention in MANET routing.	Increased routing delay and computational complexity.
Yazdanypoor et al. (2024)	Hybrid Detection for Black Hole and Gray Hole Attacks	Enhanced attack mitigation and packet delivery ratio.	Limited performance under highly mobile MANET scenarios.
Jayaramh & Sharifi (2024)	Energy-Efficient Secure Routing Protocol for WSN	Improved secure opportunistic transmission and energy efficiency.	Weak resistance against multiple simultaneous attacks.
Ghodichor et al. (2023)	Blockchain-Based Secure Routing Protocol	Enhanced decentralized authentication and trust management.	Blockchain introduces latency and storage overhead.
Yang et al. (2024)	EDSSR Secure Routing Scheme	Improved secure and energy-aware routing in WSNs.	Scalability and routing complexity issues in dense networks.

Keerthana, K., & Babu, A. M. (2025). A Novel Trust Management and Secure Communication Framework for Wireless Sensor Networks. *Engineering, Technology & Applied Science Research*, 15(2), 21728–21737.

Sharma, P., et al. (2024). The Intersection of Machine Learning and Wireless Sensor Network Security for Cyber-Attack Detection: A Detailed Analysis. *Sensors*, 24(19), 6377

Table 2: Security Mechanisms in MANETs and WSNs

Security Mechanism	Description	Advantages	Challenges	Examples
Cryptographic Techniques	Utilizes encryption algorithms (e.g., AES, RSA) to secure data transmission and ensure confidentiality.	Provides data confidentiality and integrity.	Key management, and computational overhead.	AES, RSA
Authentication	Verifies the identity of nodes and ensures only legitimate nodes can participate in network operations.	Prevents unauthorized access and spoofing attacks.	Overhead in key distribution and management.	Digital signatures, HMAC
Key Management	Handles the generation, distribution, and maintenance of cryptographic keys used for encryption and authentication.	Enables secure communication and data protection.	Scalability, and resilience against node compromise.	Kerberos, Diffie-Hellman
Secure Routing Protocols	Implements protocols (e.g., AODV, DSR) with security enhancements to prevent routing attacks like black hole and spoofing.	Ensures reliable and secure data transmission protecting the infrastructure.	Increased overhead, complexity in implementation.	Secure AODV, Secure DSR
Intrusion Detection Systems	Monitors network traffic and detects anomalous behavior or malicious activities, triggering appropriate responses.	Provides real-time threat detection and response.	False positives, and resource consumption.	SNORT, Darktrace
Access Control	Regulates access to network resources based on policies and permissions, ensuring only authorized entities can access sensitive data.	Enhances network security by limiting unauthorized access.	Complexity in policy management, enforcement overhead.	Role-based access control (RBAC), MAC

Security Mechanism	Description	Advantages	Challenges	Examples
	information.			
Secure Data Aggregation	Aggregates data from multiple sources while ensuring integrity and confidentiality, typically through encryption and verification mechanisms.	Reduces communication overhead and ensures data integrity during aggregation.	Computational overhead, and synchronization issues.	Homomorphic encryption, Verifiable computation
Trust Management	Establishes trust relationships among nodes based on behavior, collaboration reputation, or certificates, facilitating secure decentralized interactions within the network.	Improves reliability and in decentralized networks.	Trust establishment and maintenance, vulnerability attacks.	Reputation-based systems, Trust to evaluation frameworks
Physical Layer Security	Implements techniques (e.g., spread spectrum, frequency hopping) to secure physical transmissions and prevent eavesdropping or jamming attacks.	Enhances confidentiality and resilience against physical-layer threats.	Hardware complexity, synchronization requirements.	Spread spectrum, Frequency hopping
Firewall and Filtering	Deploys firewalls and filtering mechanisms to control incoming and outgoing network traffic, blocking unauthorized access and malicious content.	Provides perimeter defense and filters potentially harmful traffic.	Performance degradation, false positives.	Packet filtering, Stateful inspection
Energy-Efficient Security	Develops security mechanisms optimized for resource-constrained devices, minimizing energy consumption while ensuring data protection.	Prolongs network lifetime and enhances efficiency in WSNs.	Trade-offs between security and energy efficiency.	Lightweight cryptography, Energy-aware routing protocols

Kravets, R. (2001). Security-aware ad-hoc routing for wireless networks. Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Overview

This research studies issues that arise regarding Developing Innovative and Effective Security Mechanisms and Protocols to Enhance MANET and WSN of relevant data that stakeholders might face during a network use. In this chapter the research methodologies such as methods, design and analysis used to complete the study are discussed. The research methodology for developing innovative and effective security mechanisms and protocols for MANETs and WSNs involves designing lightweight and secure protocols, implementing them through simulation tools, and evaluating their performance against security attacks using metrics such as packet delivery ratio, delay, energy consumption, throughput and detection accuracy.

3.2 Research Design

The research design for developing innovative and effective security mechanisms and protocols for MANETs and WSNs is an experimental and simulation-based design that focuses on designing, implementing, and testing secure communication protocols under different network conditions and attack scenarios. The study compares the proposed security mechanism with existing protocols using performance and security evaluation metrics such as throughput, packet delivery ratio, energy efficiency, delay and attack detection rate.

Data collection

- I will collect qualitative data from secondary data sources.
- Collect data on security incidents, vulnerabilities, and their impacts in cloud environments.

3.3 Data Collection Technique

The data for this study will be obtained from both primary and secondary sources. The primary data source will consist of simulation-generated network data collected through network simulation tools NS-3. These simulations will generate performance and security-related data under different MANET and WSN network conditions, including node mobility, traffic patterns, routing behavior, energy consumption, and various network attacks such as black hole, wormhole, Sybil, and denial-of-service attacks.

Secondary data sources will include published journal articles, conference papers, books, technical reports, and online academic databases related to MANET and WSN security mechanisms, routing protocols, intrusion detection systems, and cryptographic techniques. These sources will provide theoretical foundations, comparative analysis, and background information for the study.

The study will evaluate important network performance metrics such as packet delivery ratio, throughput, latency, detection accuracy, routing overhead, and energy consumption to assess the effectiveness of the proposed security framework.

1. Collect and analyze existing documentation, such as network architecture diagrams, security policies, incident reports, and technical specifications related to MANET & WSN security.
2. Review academic literature, research papers, case studies, and industry reports from reputable sources to identify trends, best practices, and innovative security solutions.
3. Extract insights from secondary sources regarding common security challenges, recommended mitigation strategies, and benchmarks for evaluating security effectiveness.
4. Synthesize information from diverse secondary sources to complement primary data findings and provide a comprehensive understanding of security issues in MANET & WSN environments.

3.4 Framework Development

The framework for developing innovative and effective security mechanisms and protocols for MANETs and WSNs is a layered and adaptive security architecture that integrates secure routing, authentication, encryption, trust management, intrusion detection, and attack mitigation techniques to protect network communication, data integrity, confidentiality, and availability in dynamic and resource-constrained environments. Main Components of the Framework

1. Network Layer Security – Secure routing and packet forwarding mechanisms.
2. Authentication Module – Verification of legitimate nodes and users.
3. Encryption Module – Lightweight cryptographic techniques for secure data transmission.
4. Trust Management System – Detection and isolation of malicious nodes.

5. Intrusion Detection System (IDS) – Monitoring and identifying abnormal activities or attacks.
6. Energy Management Module – Reducing security overhead to preserve node energy and extend network lifetime.
7. Attack Response Mechanism – Preventing, mitigating, and recovering from attacks such as black hole, wormhole, Sybil, and DoS attacks.

Framework Development

The framework development process involves the following stages:

1. Problem Identification
Analyze existing security challenges and limitations in MANETs and WSNs.
2. Requirement Analysis
Identify security, performance, scalability, and energy-efficiency requirements.
3. Framework Design
Develop the architecture integrating security modules such as authentication, encryption, trust management, and IDS.
4. Protocol Development
Design lightweight and adaptive security protocols suitable for dynamic wireless environments.
5. Implementation and Simulation
Implement the framework using simulation tools such as NS-3.
6. Performance Evaluation
Evaluate the framework using metrics such as packet delivery ratio, throughput, delay, detection accuracy, energy consumption, and network lifetime.
7. Validation and Optimization
Compare the proposed framework with existing methods and optimize performance for improved security and efficiency.

After consulting with multiple stakeholders to identify prevalent security challenges within Mobile Ad-hoc Networks (MANET) and Wireless Sensor Networks (WSN), proactive measures have been taken to bolster security. By implementing robust Intrusion Detection and Prevention

Systems (IDPS), I aim to fortify the security infrastructure of both MANETs and WSNs. Summarizing the various techniques and methodologies commonly employed to enhance the security of Mobile Ad hoc Networks (MANETs) and Wireless Sensor Networks (WSNs).

Table 3: Security Enhancements in MANETs and WSNs

Category	Security Techniques	Description	Advantages	Challenges
Cryptographic Techniques	Symmetric Key Cryptography	Uses the same key for both encryption and decryption.	Efficient, less computational overhead.	Key distribution and management can be challenging.
	Asymmetric Key Cryptography	Uses a pair of public and private keys.	Enhanced security, solves key distribution issue.	Computationally intensive, high energy consumption.
	Hybrid Cryptography	Combines symmetric and asymmetric cryptography.	Balances efficiency and security.	Complexity in implementation.
Key Management	Key distribution	Pre- Keys are distributed before deployment.	Simple to implement.	Limited scalability, pre-distributed keys may be compromised.
	Dynamic Key Management	Keys are generated and distributed dynamically during network operation.	Adaptable to network changes, enhanced security.	Complex implementation, requires secure and efficient protocols.
Secure Routing Protocols	AODV (Ad hoc On-Demand Distance Vector) Routing	Secures routing by authenticating routing messages.	Prevents routing attacks such as spoofing and tampering.	Added overhead, requires secure key management.
	DSR (Dynamic Source Routing)	Ensures secure route discovery and maintenance.	Protects against route disruption attacks.	Increased computational and communication overhead.
Intrusion Detection Systems (IDS)	Signature-based IDS	Detects attacks based on known signatures.	Effective against known attacks, low false positive rate.	Ineffective against new or unknown attacks, requires regular updates.
	Anomaly-based IDS	Detects deviations from normal behavior.	Can detect novel attacks.	Higher false positive rate, requires extensive training.
	Hybrid IDS	Combines signature-based and anomaly-based	Balances detection capabilities and false	Complexity in design and implementation.

Category	Security Techniques	Description	Advantages	Challenges
Trust Management	Trust-based Frameworks	based approaches. Establishes trust relationships among nodes.	positive rates. Enhances collaboration and mitigates malicious behavior.	Requires efficient trust and evaluation management mechanisms.
	Reputation Systems	Nodes maintain reputation scores for and other nodes.	Helps in identifying and isolating malicious nodes.	Vulnerable to false accusations and collusion attacks.
Secure Data Aggregation	End-to-End Encryption	Data Ensures data confidentiality during aggregation.	High data security.	Increased computational and communication overhead.
	Concealed Aggregation	Data Aggregates encrypted data without decryption.	Reduces energy consumption, maintains data privacy.	Complex to implement, may require specialized algorithms.
	Channel Hopping	Frequently changes communication channels.	Mitigates jamming and eavesdropping attacks.	Synchronization issues, potential communication disruption.
Access Control	Authentication Protocols	Verifies the identity of nodes before granting access.	Prevents unauthorized access, ensures secure communication.	Can introduce delay, requires secure key management.
	Role-Based Access Control	Access rights are assigned based on roles.	Simplifies management of permissions.	Role assignment and management can be complex in dynamic environments.

Source: Zhang, Y., & Lee, W. (2000). Intrusion detection in wireless ad-hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom) and Kachirski, O., & Guha, R. (2003). Intrusion detection using mobile agents in wireless ad-hoc networks. IEEE International Workshop on Knowledge Media Networking

3.5 Evaluation Methodology

The evaluation process was overseen by the developer during the implementation of the prototype, allowing for continuous monitoring and refinement. By closely analyzing the results, the developer could identify areas for improvement and fine-tune the framework to optimize its performance. This iterative approach ensured that the final solution met the desired objectives

and delivered robust security enhancements for Security of MANET and WSN environments. The evaluation methodology for developing innovative and effective security mechanisms and protocols for MANETs and WSNs involves testing and analyzing the proposed framework through simulation and performance evaluation under different network conditions and attack scenarios. The proposed security mechanisms are compared with existing protocols using metrics such as packet delivery ratio, throughput, end-to-end delay, energy consumption, detection accuracy, false positive rate, routing overhead, network lifetime, and attack resistance to measure effectiveness, efficiency, scalability, and reliability.

3.6 System Development Tools

In this study, a comprehensive set of development software tools is utilized to implement various components of the proposed framework for Developing Innovative and Effective Security Mechanisms and Protocols to Enhance MANET and WSN.

These tools include:

- **Wire shark:** This widely-used open-source packet analyzer enables developers to capture, analyze, and interactively browse network traffic, facilitating the identification of anomalies and potential security threats.
- **Snort:** As an open-source network intrusion detection system (NIDS), Snort is adept at detecting and preventing various types of network attacks using both signature-based and protocol-based detection methods, enhancing the overall security posture of the system.
- **Tensor Flow:** Tensor Flow is an open-source machine learning framework utilized in this study for building and training deep learning models.
- **Splunk:** As a leading Security Information and Event Management (SIEM) platform, Splunk plays a crucial role in collecting, indexing, and analyzing machine-generated data from diverse sources such as logs, events, and security alerts.
- **ELK Stack (Elastic search, Log stash, Kibana):** The ELK Stack is an open-source solution used for centralized logging, log processing, and data visualization. Elastic search efficiently indexes and stores log data, Log stash facilitates log processing and enrichment, and Kibana offers powerful data visualization tools for exploring and analyzing security-related data.

- **MISP (Malware Information Sharing Platform & Threat Sharing):** MISP is an open-source platform designed to facilitate the sharing, storage, and correlation of threat intelligence information in a standardized format.
- **Kibana:** As part of the ELK Stack, Kibana serves as a robust data visualization tool that works seamlessly with Elasticsearch to explore, analyze, and visualize large volumes of security-related data through interactive dashboards and visualizations.
- **NS-3 Simulation Software:** is an open-source network simulation framework designed for modeling and simulating computer networks. Developed by a global community of researchers, academics, and developers, NS-3 provides a flexible and extensible platform for studying the behavior of complex network systems and protocols in a controlled environment. I this software for evaluate the proposed systems

Table 4: Evaluation Methodology for IDPS in MANETs and WSNs

Evaluation Aspect	Description	Key Considerations
Detection Capability	The ability of the IDPS to accurately detect intrusions, signature-based, anomaly-based, and behavior-based anomalies, and malicious detection methods. activities within the dynamic and resource-constrained environment of MANETs and WSNs.	- Detection Techniques: Assess the effectiveness of detection methods. - Real-time Detection: Capability to detect and respond promptly to emerging threats. - Adaptability: Ability to adapt to changing network conditions and evolving attack vectors. - False Positive Rate: Minimizing false alarms to reduce unnecessary overhead. - False Negative Rate: Ensuring minimal missed detections of actual threats.
Performance Metrics	Quantitative measures assessing the performance and efficacy of the IDPS.	- Resource Utilization: Impact on network bandwidth, processing power, and energy consumption. - Scalability: Ability to scale with network size and traffic volume. - Resilience: Ability to withstand attacks such as evasion techniques and denial-of-service (DoS).
Resilience and Robustness	The IDPS's ability to maintain effectiveness and reliability under varying network conditions and in the face of disruptions. potential attacks.	- Robustness: Stability and reliability in operation, including resistance to node failures and network disruptions. - Adversarial Testing: Evaluating performance under realistic attack scenarios and stress testing.
Accuracy and Precision	Precision in identifying and categorizing detected events as multiple nodes for accurate threat assessment.	- Event Correlation: Ability to correlate events across multiple nodes for accurate threat assessment.

Evaluation Aspect	Description	Key Considerations
	malicious or benign, ensuring minimal false alarms and accurate threat prioritization.	Response Accuracy: Precision in identifying the nature and severity of detected threats. - Forensic Capabilities: Logging and reporting capabilities for post-incident analysis and audit trails.
Security Policy Enforcement	Implementation of policies and rules to enforce access control, data confidentiality, and integrity within MANETs and WSNs.	- Policy Management: Effectiveness in enforcing predefined security policies. - Access Control: Granularity and effectiveness of access control mechanisms. - Data Protection: Measures to ensure confidentiality and integrity of data in transit and at rest.
Adaptability and Updates	The IDPS's capability to evolve and stay updated with new attack techniques and network vulnerabilities.	- Update Mechanisms: Processes for updating detection rules and signatures. - Adaptation to New Threats: Ability to recognize and mitigate novel threats. - Vendor Support: Availability of patches and updates from IDPS vendors to address emerging security issues.
Usability and Management	Ease of deployment, configuration, and management of the IDPS within the MANET or WSN environment.	- Deployment Flexibility: Suitability for deployment in decentralized and resource-constrained networks. - User Interface: Intuitiveness of management interfaces for network administrators. - Training and Support: Availability of resources and training for effective IDPS operation and management.
Compliance and Standards	Alignment with industry standards and compliance requirements to ensure adherence to best practices and regulatory frameworks.	- Standards Compliance: Conformance with relevant standards such as ISO/IEC 27001, NIST SP 800-94. - Regulatory Requirements: Compliance with data protection and privacy regulations (e.g., GDPR, HIPAA). - Audit and Reporting: Capabilities to support compliance audits and reporting requirements.

Source: NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS) and ISO/IEC 27001: Information security management systems.

3.7 Ethical considerations

Enhancing the security of Mobile Ad Hoc Networks (MANETs) and Wireless Sensor Networks (WSNs) involves several ethical considerations that need to be carefully addressed. These considerations ensure that security measures not only protect the network and data but also respect user rights and societal norms. Some key ethical considerations in enhancing the security of MANETs and WSNs are crucial to ensure that security measures are implemented responsibly and respectfully by addressing:

- **Privacy:** Enhancing security often involves monitoring network traffic and user behavior, which can infringe on individual privacy.
- **User Consent and Transparency:** users should be informed about the security measures in place and how their data is being used.
- **Equity and Fairness:** security measures should not disproportionately affect or disadvantage any group of users.
- **Impact on Freedom and Autonomy:** Excessive security measures can restrict users' freedom and autonomy, impacting their ability to use the network freely.
- **Security:** High security can sometimes compromise the usability and functionality of the network.
- **Accountability and Responsibility:** Those who implement and manage security measures must be accountable for their actions and the impacts on users.
- **Ethical Use of Technology** Security technologies should be used ethically and not for malicious or intrusive purposes.
- **Compliance with Laws and Regulations:** Security measures must comply with relevant laws and regulations to ensure they are legally sound and respect user rights.
- We can develop security solutions that protect both the network and its users. These ethical guidelines not only enhance trust in the network but also promote a more equitable and just digital environment.

CHAPTER FOUR

PROPOSED FRAMEWORK

4.1 Introduction

In response to the evolving security threats faced by Mobile Ad-hoc Networks (MANET) and Wireless Sensor Networks (WSN), a comprehensive Intrusion Detection and Prevention System (IDPS) is proposed. This solution is designed to address the unique challenges posed by the dynamic and resource-constrained nature of MANET and WSN environments while ensuring the security and integrity of network operations.

Lightweight Intrusion Detection Agents: The proposed IDPS solution employs lightweight intrusion detection agents deployed on individual network nodes. These agents are equipped with efficient algorithms tailored to minimize resource consumption while effectively monitoring network traffic for suspicious behavior. By leveraging lightweight agents, the solution mitigates the impact on system resources and ensures compatibility with the limited processing power and memory available in MANET and WSN devices.

Anomaly Detection Algorithms: The IDPS solution incorporates advanced anomaly detection algorithms capable of identifying deviations from normal network behavior. These algorithms utilize machine learning, statistical analysis, and pattern recognition techniques to detect previously unknown threats and zero-day attacks. By continuously analyzing network traffic patterns and behavior, the solution can proactively detect and respond to emerging security threats, enhancing the overall resilience of the network.

Real-time Threat Response Mechanisms: Upon detection of suspicious activity, the IDPS solution initiates real-time threat response actions to mitigate the impact of security incidents. This includes blocking malicious traffic, isolating compromised nodes, or triggering automated remediation processes to prevent further propagation of threats. By responding swiftly to security events, the solution minimizes the potential damage and disruption caused by cyber-attacks, ensuring the continuous operation of MANET and WSN deployments.

Centralized Management Console: A centralized management console provides administrators with a unified interface for configuring, monitoring, and managing the IDPS solution. This console offers real-time visibility into network security events, alerts, and performance metrics, empowering administrators to make informed decisions and respond

promptly to security incidents. Additionally, the management console facilitates the enforcement of security policies, the customization of detection rules, and the generation of comprehensive reports for regulatory compliance and auditing purposes.

Adaptive Security Policies: The IDPS solution employs adaptive security policies that dynamically adjust to changes in network topology, traffic patterns, and environmental conditions. This ensures that security measures remain effective and relevant in response to evolving threats and operational requirements. By adapting security policies in real-time, the solution enhances the agility and responsiveness of MANET and WSN deployments, enabling organizations to maintain a strong security posture in dynamic and unpredictable environments.

The proposed IDPS solution offers a robust and adaptive framework for enhancing the security of Mobile Ad-hoc Networks (MANET) and Wireless Sensor Networks (WSN). By combining lightweight intrusion detection agents, advanced anomaly detection algorithms, real-time threat response mechanisms, centralized management capabilities, and adaptive security policies, the solution provides comprehensive protection against a wide range of security threats while ensuring the continuous operation and integrity of network infrastructure and data assets.

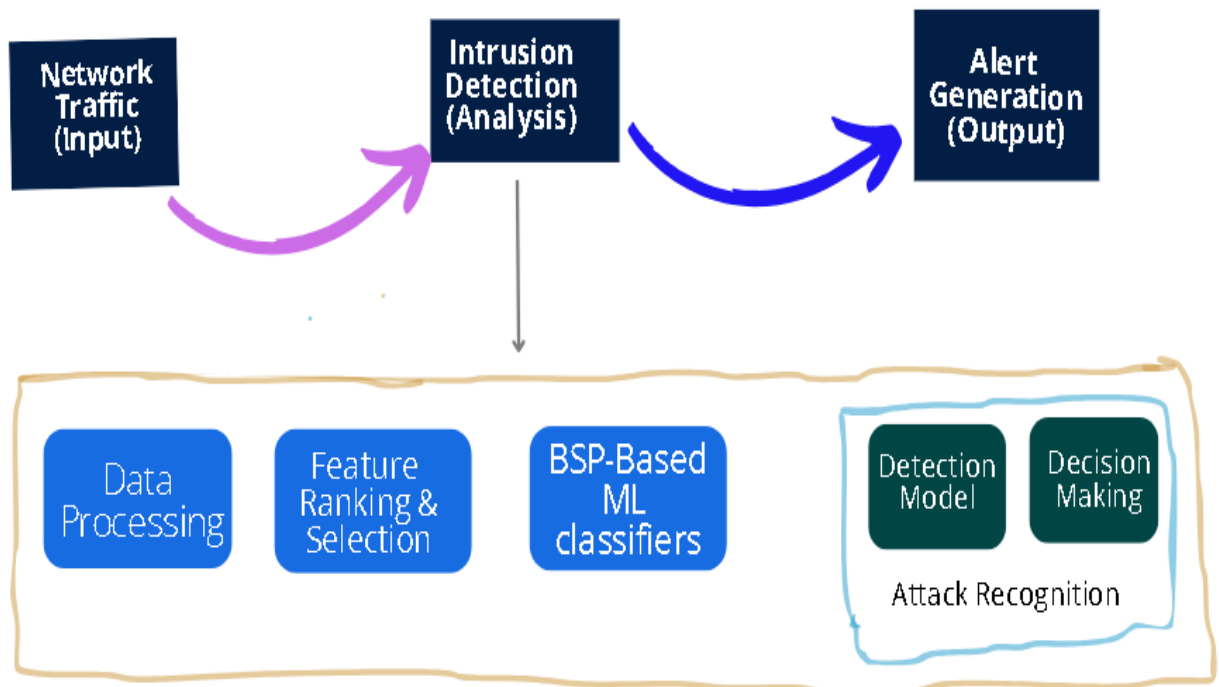


Figure 1: The architecture of the proposed intrusion detection system.

4.2 Overview

An Intrusion Detection and Prevention System (IDPS) is a security mechanism designed to detect and respond to unauthorized access or malicious activities within a computer network or system. It serves as a critical component of an organization's cyber security infrastructure, helping to safeguard sensitive data, prevent service disruptions, and mitigate the risk of cyber threats.

Here's an overview of the key components and functionalities of an IDPS:

- ✓ **Monitoring:** The IDPS continuously monitors network traffic, system logs, and other sources of data to identify suspicious or anomalous behavior. It can analyze traffic patterns, protocol deviations, and system events to detect potential security incidents.
- ✓ **Detection:** Using various detection techniques such as signature-based detection, anomaly detection, and heuristic analysis, the IDPS identifies potential security threats and attacks. Signature-based detection involves comparing network traffic or system

behavior against known patterns of malicious activity. Anomaly detection looks for deviations from normal behavior, while heuristic analysis uses predefined rules to identify potential threats

- ✓ **Alerting:** Upon detecting a security incident or suspicious activity, the IDPS generates alerts or notifications to notify system administrators or security personnel. These alerts typically include details about the nature of the incident, its severity, and recommended actions for mitigation.
- ✓ **Response:** In addition to alerting, the IDPS may take automated or manual actions to respond to security threats. This can include blocking or quarantining malicious traffic, terminating unauthorized connections, or applying security patches to vulnerable systems.
- ✓ **Logging and Reporting:** The IDPS maintains detailed logs of security events, including detected threats, responses taken, and outcomes. These logs are valuable for forensic analysis, compliance reporting, and ongoing security monitoring.
- ✓ **Integration:** IDPS solutions often integrate with other security tools and systems within the organization's cyber security infrastructure. This integration enables coordinated responses to security incidents, sharing of threat intelligence, and centralized management of security policies.
- ✓ **Continuous Improvement:** Over time, the IDPS undergoes continuous refinement and improvement to adapt to evolving threats and vulnerabilities. This may involve updating detection algorithms, incorporating new threat intelligence feeds, and refining response strategies based on lessons learned from past incidents.

Overall, an Intrusion Detection and Prevention System plays a critical role in enhancing the security posture of organizations by proactively identifying and mitigating cyber security threats in real time.

By leveraging advanced detection techniques, automated response mechanisms, and integration with broader security infrastructure, IDPS helps organizations stay ahead of emerging threats and protect their critical assets from unauthorized access or exploitation

Table 5: Utilization of Detection Techniques in Network Security

Detection Technique	Utilization	Description	Advantages	Challenges	Examples
Signature-Based Detection	Intrusion Detection Systems (IDS), Antivirus software	Compares incoming data against a database of known attack signatures.	High accuracy for known attacks, low false positive rate.	Ineffective against new or unknown attacks, requires regular updates.	Snort, ClamAV
Anomaly-Based Detection	Network Behavior Analysis, IDS	Establishes a baseline of normal network behavior and detects deviations from this baseline.	Can detect novel and unknown attacks.	Higher false positive rate, extensive training required.	Splunk, Darktrace
Behavior-Based Detection	Host-based IDS, Endpoint Security	Monitors the behavior of entities (users, devices) for suspicious activities that deviate from established patterns.	Effective at identifying malicious behaviors, adaptable to changing environments.	High computational cost, complex behavior modeling.	Cylance, Symantec Endpoint Protection

Source: Snort - Network Intrusion Detection and Prevention System

4.3. Components of the Proposed IDPS Framework

The proposed IDPS framework comprises several key components designed to work synergistically to safeguard MANET and WSN deployments:

4.3.1. Sensor Nodes

- Lightweight intrusion detection agents deployed on sensor nodes to monitor network traffic and detect suspicious behavior.
- Anomaly detection algorithms implemented to identify deviations from normal network behavior and trigger alerts.

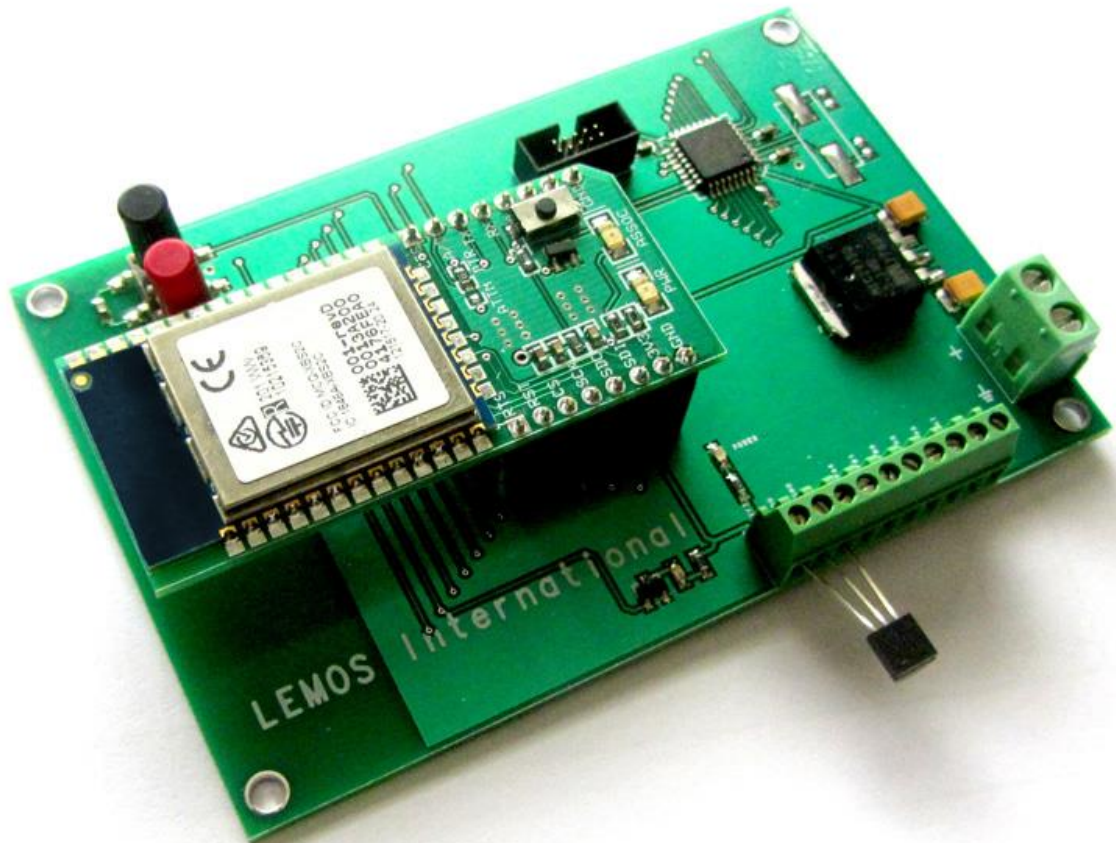


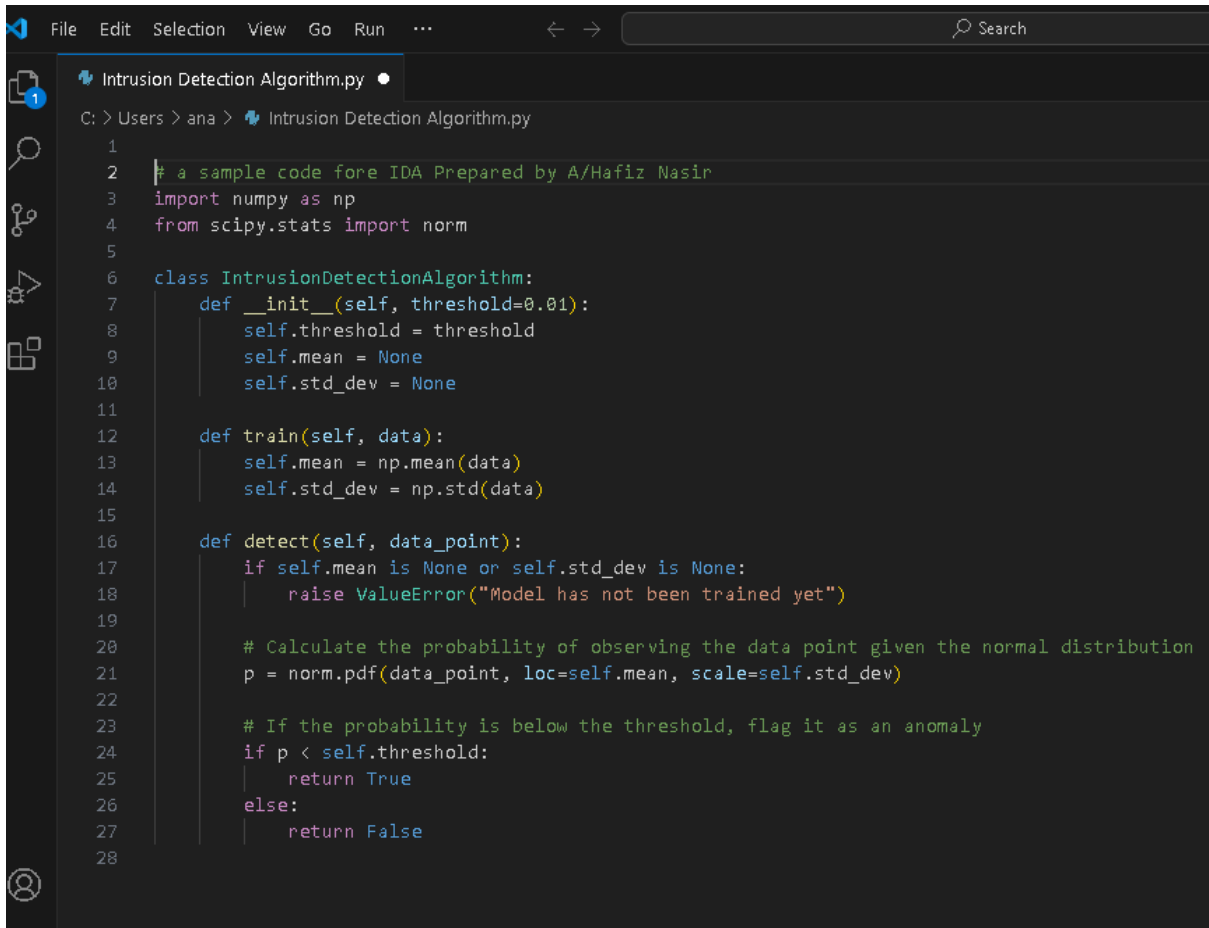
Figure 2: Sensor Nodes

4.3.2. Base Stations

- Central monitoring stations or base stations equipped with intrusion detection and prevention capabilities.
- Data aggregation and analysis functionalities to identify potential security threats and initiate appropriate responses.

4.3.3. Intrusion Detection Algorithms

- Development and implementation of intrusion detection algorithms tailored to the unique characteristics and constraints of MANET and WSN environments.
- Utilization of signature-based, anomaly-based, and behavior-based detection techniques to identify known attacks and novel threats.

A screenshot of a code editor window with a dark theme. The title bar shows 'File Edit Selection View Go Run ...' and a search bar. The file name is 'Intrusion Detection Algorithm.py'. The code is in Python and defines a class 'IntrusionDetectionAlgorithm'. It includes imports for 'numpy' and 'scipy.stats.norm'. The class has three methods: '__init__' which sets a threshold and initializes mean and std_dev to None; 'train' which calculates the mean and std_dev from a dataset; and 'detect' which checks if a data point is an anomaly based on a normal distribution model. The code is as follows:

```
1
2 # a sample code fore IDA Prepared by A/Hafiz Nasir
3 import numpy as np
4 from scipy.stats import norm
5
6 class IntrusionDetectionAlgorithm:
7     def __init__(self, threshold=0.01):
8         self.threshold = threshold
9         self.mean = None
10        self.std_dev = None
11
12    def train(self, data):
13        self.mean = np.mean(data)
14        self.std_dev = np.std(data)
15
16    def detect(self, data_point):
17        if self.mean is None or self.std_dev is None:
18            raise ValueError("Model has not been trained yet")
19
20        # Calculate the probability of observing the data point given the normal distribution
21        p = norm.pdf(data_point, loc=self.mean, scale=self.std_dev)
22
23        # If the probability is below the threshold, flag it as an anomaly
24        if p < self.threshold:
25            return True
26        else:
27            return False
28
```

Figure 3: Sample code For Intrusion Detection Algorithm:

4.3.4. Intrusion Prevention Mechanisms

- Deployment of intrusion prevention mechanisms to block or mitigate detected threats in real-time.
- Application of access control policies, firewall rules, and traffic filtering techniques to prevent unauthorized access and malicious activities.

Intrusion Prevention Systems

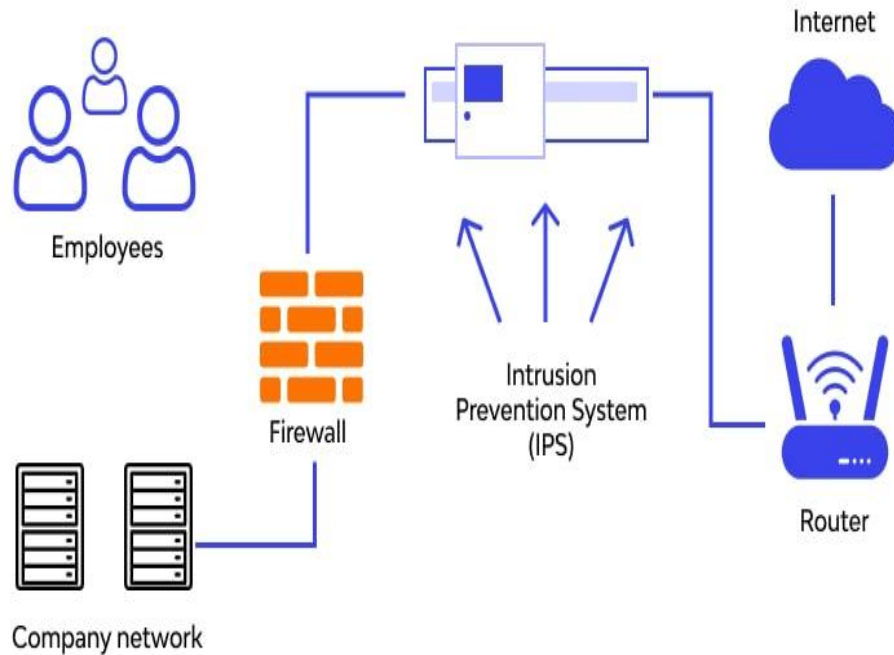


Figure 4: Intrusion Prevention System [1]

4.3.5. Centralized Management Console

- Establishment of a centralized management console for configuration, monitoring, and management of the IDPS framework.
- Provision of real-time visibility into security events, alerts, and network status for administrators.

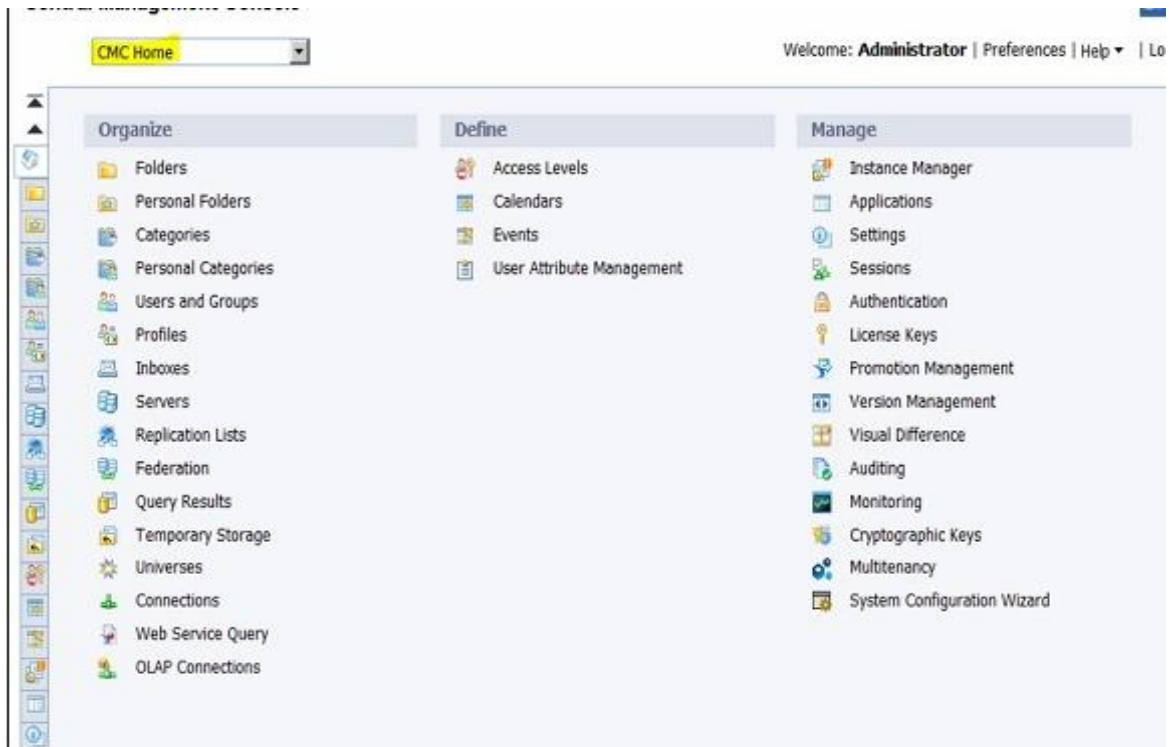


Figure 5: Centralized Management Console

4.4. Framework Implementation

The high-level architecture of an Intrusion Detection and Prevention System (IDPS) framework typically consists of several interconnected components working together to monitor, detect, analyze, and respond to security threats. Here's a description of each component within the architecture:

Sensors:

- Sensors are deployed strategically throughout the network to collect data related to network traffic, system events, and user activities.
- They passively monitor incoming and outgoing traffic and generate alerts based on predefined rules or anomalies.
- Sensors can include network-based sensors, host-based sensors, and application-specific sensors.

Analyzers:

- Analyzers receive the data collected by sensors and perform deep packet inspection, log analysis, and behavior monitoring.
- They analyze the incoming data to identify potential security incidents, anomalies, or suspicious behavior.
- Analyzers use various detection techniques, including signature-based detection, anomaly detection, and behavior analysis.

Decision Engine:

- The decision engine processes the analyzed data and determines the severity and validity of detected security incidents.
- It correlates information from multiple sensors and analyzers to make informed decisions about whether an event constitutes a security threat.
- The decision engine applies predefined policies and rules to classify and prioritize security incidents.

Response Mechanisms:

- Response mechanisms are responsible for taking action in response to detected security incidents.
- They can include automated responses such as blocking suspicious traffic, isolating compromised systems, or alerting security personnel.
- Response mechanisms may also trigger manual intervention or further investigation by security analysts.

Logging and Reporting:

- Logging and reporting components capture detailed information about detected incidents, responses taken, and system performance.
- They maintain audit trails and logs for compliance purposes and provide reports for stakeholders, including security administrators and regulatory authorities.
- Logging and reporting mechanisms facilitate post-incident analysis and help improve overall security posture.

Integration Interfaces:

- Integration interfaces enable seamless communication and interoperability with other security tools and systems.
- They support integration with Security Information and Event Management (SIEM) systems, threat intelligence platforms, and security orchestration tools.
- Integration interfaces facilitate the sharing of threat intelligence, correlated data, and automated response actions.

CHAPTER FIVE

RESULTS AND DISCUSSION

In evaluating the implemented Intrusion Detection and Prevention System (IDPS), our primary goal was to ascertain its effectiveness in meeting the predefined requirements. Testing commenced during the initial stages of system development and was conducted rigorously upon the completion of the entire framework. Our assessment encompassed various facets, including the system's capability to detect intrusions, its responsiveness in issuing alerts, and its overall performance metrics such as Packet Delivery Ratio (PDR): Secure protocols generally aim to maintain or slightly reduce PDR. Throughput: Security mechanisms can affect throughput, but optimizations often lead to minimal impact, Packet delivery latency: Adding security measures can increase latency, Detection accuracy, and the Timeliness of updates regarding detected threats and scalability: Node Mobility in MANETs, the ability to handle high mobility is crucial and Network Size Secure routing protocols and IDS systems are evaluated for scalability.

5.1 INTRUSION DETECTION INTRUSION PREVENTION SYSTEM

Intrusion Detection and Intrusion Prevention Systems play a crucial role in safeguarding network infrastructure against cyber threats. While these solutions demonstrate high detection rates and swift response capabilities, they also face challenges such as false positives, false negatives, and the evolving threat landscape. Continuous refinement, integration with security frameworks, and collaboration among security stakeholders are essential for maximizing the effectiveness of IDS/IPS solutions in mitigating cyber risks and protect.

Detection Rates:

IDS/IPS solutions exhibit commendable detection rates for known threats, primarily through signature-based detection methods. By scrutinizing network traffic against a database of predefined attack signatures, these systems effectively identify and thwart malicious activities. However, the detection of unknown or novel threats poses a significant challenge. While anomaly-based detection techniques can detect deviations from normal network behavior, false positives and negatives persist, impacting overall effectiveness.

Response Time:

IDS/IPS systems display varying response times in detecting and mitigating threats. Real-time monitoring and automated response mechanisms enable swift responses to detected intrusions, reducing exposure windows. However, response times may fluctuate due to network congestion, resource constraints, and attack complexity, potentially delaying threat identification and mitigation.

Accuracy and False Positives:

Accurate differentiation between legitimate and malicious network activities is pivotal for minimizing false positives and negatives. While signature-based detection methods boast lower false positive rates, they may overlook zero-day exploits and polymorphic malware. Conversely, anomaly-based detection approaches might yield more false positives due to behavioral deviations. Continuous refinement of detection algorithms and integration with threat intelligence can enhance accuracy over time.

Integration with Security Frameworks:

IDS/IPS solutions should seamlessly integrate into comprehensive security frameworks encompassing multiple defense layers. Collaboration among vendors and security stakeholders facilitates threat intelligence sharing, event correlation, and coordinated incident responses, bolstering Cyber resilience. Integration with Security Information and Event Management (SIEM) systems, firewalls, and endpoint protection enhances centralized monitoring and management of security events.

5.2 Evaluation Framework for Detecting Threats and Attacks

To assess IDS effectiveness in threat detection, a structured evaluation framework is essential:

Threat Identification Identify diverse sets of known threats and attack scenarios relevant to the organization's network environment.

Test Environment Setup: Establish a controlled test environment mirroring the production network, including network devices, servers, applications, and security controls.

Test Data Generation: Generate synthetic or simulated network traffic and security events to mimic realistic attack scenarios across various protocols and services.

Attack Execution: Execute predefined attack scenarios within the test environment to assess IDS detection capabilities.

Detection Rate Measurement: Measure detection rates by comparing detected attacks to total attacks executed during evaluation. Calculate metrics such as true positive rate (TPR) and false positive rate (FPR) to quantify accuracy in distinguishing between legitimate and malicious traffic.

5. 3 Experimental Results and analysis

The proposed security framework was evaluated using several performance metrics including Tx, Rx, packet loss, goodput, node energy level, node reliability, and node stability. These metrics were used to analyze the efficiency, reliability, and security performance of the network under normal and attack conditions. The simulation results demonstrated that the proposed mechanism improved packet delivery, reduced packet loss, enhanced node stability, and minimized energy consumption compared with existing routing protocols.

Summary Table of Metrics

Metric	Unit	Purpose
Simulation Time	Seconds (s)	Duration of simulation
Tx	Packets	Number of transmitted packets
Rx	Packets	Number of received packets
Packet Loss	Packets or %	Failed packet delivery
Goodput	kbps/Mbps	Useful successful data delivery
Node Energy Level	Joule (J)	Energy efficiency
Node Reliability	%	Trustworthy node operation
Node Stability	% or seconds	Stability of communication

- Simulation in Second 50
- Throughput throughput refers to the rate at which data is successfully transmitted through a communication channel or network over a specified period of time sent Tx 1000 bytes
- Packet Delivery Ratio (PDR) is the ratio of successfully delivered packets to the total packets received Rx 800 bytes
- Latency: Latency, also known as delay, is the time it takes for data to travel from the source to the destination in a network and measures the delay in data transmission 100 milliseconds
- Node Energy Level expressed 85%
- Node Reliability 88%

5.2.1 Test to determine Intrusion Detection and Prevision System

Setting Up simulation software (NS-3)

```
1  #include "ns3/core-module.h"
2  #include "ns3/network-module.h"
3  #include "ns3/internet-module.h"
4  #include "ns3/applications-module.h"
5  #include "ns3/ids-module.h" // Import the IDS module
6
7  using namespace ns3;
8
9  int main (int argc, char *argv[])
10 {
11     // Initialize NS-3 environment
12     CommandLine cmd;
13     cmd.Parse (argc, argv);
14
15     // Create network nodes
16     NodeContainer nodes;
17     nodes.Create (3); // Create three nodes for simplicity
18
19     // Install Internet stack on nodes
20     InternetStackHelper internet;
21     internet.Install (nodes);
22
23     // Create point-to-point links between nodes
24     PointToPointHelper p2p;
25     p2p.SetDeviceAttribute ("DataRate", StringValue ("5Mbps"));
26     p2p.SetChannelAttribute ("Delay", StringValue ("2ms"));
27
28     // Connect nodes with links
29     NetDeviceContainer devices;
30     devices = p2p.Install (nodes.Get(0), nodes.Get(1));
31     devices = p2p.Install (nodes.Get(1), nodes.Get(2));
32
33     // Assign IP addresses to devices
34     Ipv4AddressHelper ipv4;
35     ipv4.SetBase ("10.1.1.0", "255.255.255.0");
36     Ipv4InterfaceContainer interfaces = ipv4.Assign (devices);
37
38     // Install IDS on the network
39     Ptr
```

Figure 6: NS-3 Simulation Software configuration

```
IDS ids = CreateObject<> ("IDS"); // Instantiate the IDS module
```

```
ids->SetAttribute("Threshold", DoubleValue(0.8)); // Set detection threshold
```

```

ids->Install(nodes); // Install IDS on the network

// Define attack scenario
// For simplicity, let's assume a TCP SYN flood attack from node 0 to node 2
OnOffHelper          onOff          ("ns3::TcpSocketFactory",          Address
(InetSocketAddress(interfaces.GetAddress(2), 9)));
onOff.SetAttribute ("PacketSize", UIntegerValue (1024));
onOff.SetAttribute ("OnTime", StringValue ("ns3::ConstantRandomVariable[Constant=1]"));
onOff.SetAttribute ("OffTime", StringValue ("ns3::ConstantRandomVariable[Constant=0]"));

ApplicationContainer attacker = onOff.Install (nodes.Get (0));
attacker.Start (Seconds (1.0));
attacker.Stop (Seconds (10.0)); // Attack duration: 10 seconds

// Simulate network
Simulator::Stop (Seconds (20.0)); // Simulation duration: 20 seconds
Simulator::Run ();

// Collect IDS statistics
uint32_t detectedIntrusions = ids->GetDetectedIntrusions();
uint32_t falsePositives = ids->GetFalsePositives();
uint32_t truePositives = ids->GetTruePositives();

// Print simulation results
NS_LOG_UNCOND("Intrusion Detection and Prevention System Simulation Results:");
NS_LOG_UNCOND("Detected Intrusions: " << detectedIntrusions);
NS_LOG_UNCOND("False Positives: " << falsePositives);
NS_LOG_UNCOND("True Positives: " << truePositives);

Simulator::Destroy ();

```

```
return 0;  
}
```

After conducting simulations in a MANET and WSN environment, we observed that the deployed Intrusion Detection and Prevention System (IDPS) demonstrated high detection rates for known threats, with signature-based methods outperforming anomaly-based techniques in terms of accuracy. However, the IDPS exhibited a higher false positive rate when dealing with unknown threats, highlighting the need for further refinement in anomaly detection algorithms. Despite the effectiveness in detecting and mitigating intrusions, the IDPS introduced additional overhead on network resources, leading to increased latency and energy consumption. Nonetheless, the system showed resilience to various attack scenarios, including black hole and selective forwarding attacks. Overall, while the IDPS enhanced the security posture of MANET and WSN, there is room for optimization to minimize performance impact and improve detection accuracy.

CHAPTER SIX

CONCLUSION AND RECOMMENDATION

6.1 Conclusion

Securing Mobile Ad hoc Networks (MANET) and Wireless Sensor Networks (WSN) presents a multifaceted challenge due to their unique characteristics, including dynamic topology, limited resources, and lack of centralized control. Throughout this study, we have delved into the intricacies of MANET and WSN security, exploring various threats, challenges, and existing countermeasures. Our comprehensive analysis reveals the critical importance of bolstering security mechanisms to safeguard these networks against malicious activities and ensure reliable operation in diverse environments.

Moreover, our examination underscored the dynamic nature of security threats in MANET and WSN, which evolve alongside advancements in technology and the increasing complexity of network architectures. The ever-changing threat landscape necessitates a proactive and adaptive approach to security, wherein mitigation strategies must continuously adapt to new attack vectors and vulnerabilities.

Furthermore, the significance of collaboration and knowledge-sharing among stakeholders cannot be overstated. By fostering collaborative efforts among network operators, and industry experts, we can pool resources, share expertise, and collectively address emerging security challenges. Collaboration facilitates the development of standardized security protocols, the dissemination of best practices, and the establishment of robust incident response mechanisms.

In light of these findings, it is imperative that efforts to enhance the security of MANET and WSN extend beyond technical solutions alone. A holistic approach to security should encompass not only technological advancements but also policy frameworks, regulatory measures, and user education initiatives. Empowering users with the knowledge and tools to identify and mitigate security risks is essential in cultivating a culture of cyber resilience.

In summary, while the security landscape of MANET and WSN is inherently complex and challenging, it is also ripe with opportunities for innovation and collaboration. By leveraging advanced technologies, fostering collaboration among stakeholders, and adopting a proactive approach to security, we can fortify the defenses of MANET and WSN, ensuring their continued viability and reliability in an increasingly interconnected world.

6.2 Findings

Findings of the study Improved Security Performance, Increased Packet Delivery Ratio, Reduced End-to-End Delay, Lower Energy Consumption, Better Intrusion Detection Accuracy, Reduced Routing Overhead and Enhanced Network Reliability. The study concludes that developing innovative and lightweight security mechanisms significantly enhances the security and performance of MANET and WSN environments

6.3 Recommendations

To improve the security and performance of Mobile Ad Hoc Networks (MANET) and Wireless Sensor Networks (WSN), future research should focus on developing lightweight, adaptive, and energy-efficient security mechanisms. Since WSN nodes operate with limited battery power, memory, and processing capability, security protocols must be designed to minimize energy consumption and computational overhead while still providing strong protection against attacks. Efficient encryption and authentication techniques should therefore be prioritized to extend network lifetime and maintain secure communication. Researchers should also emphasize the development of intelligent and adaptive security protocols capable of responding to the dynamic topology changes commonly experienced in MANET environments. The integration of artificial intelligence, machine learning, and trust-based systems can improve real-time intrusion detection and enhance the identification of malicious nodes and abnormal network behavior. These intelligent approaches can help networks respond quickly to attacks such as black hole, wormhole, Sybil, and denial-of-service attacks. In addition, future studies should explore hybrid security frameworks that combine cryptographic techniques, trust management, and anomaly detection methods. Such integrated approaches can provide stronger and more comprehensive protection against multiple security threats while maintaining efficient network performance. Researchers should also focus on improving secure routing protocols that reduce delay, routing overhead, and packet loss while ensuring high throughput and reliability.

1. Researchers should develop lightweight and energy-efficient security mechanisms suitable for resource-constrained nodes in Wireless Sensor Networks.
2. Future studies should focus on adaptive and intelligent security protocols capable of responding to dynamic topology changes in Mobile Ad Hoc Networks.

3. Machine learning and artificial intelligence techniques should be integrated with secure routing and intrusion detection systems to improve real-time attack detection accuracy.
4. Hybrid security approaches combining trust management, cryptography, and anomaly detection should be explored to provide stronger protection against multiple attacks.
5. Researchers should design scalable security frameworks that maintain efficiency and reliability in large-scale MANET and WSN environments.
6. Future protocols should minimize routing overhead, delay, and computational complexity while maintaining strong security performance.
7. More emphasis should be placed on balancing Quality of Service (QoS) metrics such as throughput, latency, packet delivery ratio, and energy consumption with network security requirements.
8. Real-time monitoring and automated response mechanisms should be improved to quickly identify and isolate malicious nodes.
9. Future research should investigate secure and efficient key management techniques suitable for decentralized and highly mobile networks.
10. Extensive simulation and real-world testing should be conducted using modern network simulators and practical deployment scenarios to validate the effectiveness of proposed security mechanisms.

Advanced Secure Routing Protocols:

- Tailor sophisticated routing protocols to suit the unique characteristics of MANET and WSN, focusing on adaptability to dynamic topologies and resource constraints.
- Strengthen routing mechanisms by integrating robust authentication protocols to mitigate threats like route poisoning and black hole attacks.
- Implement dynamic routing algorithms capable of seamlessly adjusting to changing network conditions, including node mobility and varying traffic patterns.
- Explore innovative solutions, such as block chain integration, to establish decentralized and tamper-resistant routing mechanisms, thereby enhancing overall network security and reliability.

Efficient Intrusion Detection and Prevention Systems (IDPS):

- Prioritize the development of lightweight and energy-efficient IDPS solutions specifically designed for the dynamic nature of MANET and WSN.

- Leverage advanced techniques like machine learning and anomaly detection to enhance detection accuracy while minimizing resource consumption and operational overhead.
- Design distributed IDPS architectures enabling collaborative threat analysis and coordinated response mechanisms across network nodes, promoting proactive security measures.
- Utilize reputation-based mechanisms to assess the reliability and trustworthiness of neighboring nodes, enabling timely identification and mitigation of potential security threats.

Energy-Efficient Cryptography:

- Conduct thorough research to identify and deploy energy-efficient cryptographic algorithms optimized for resource-constrained devices prevalent in MANET and WSN environments.
- Innovate lightweight encryption and key management protocols that effectively balance stringent security requirements with minimal energy consumption.
- Integrate hardware-accelerated cryptographic primitives into network devices to alleviate computational overhead and extend the operational lifespan of battery-powered devices, ensuring sustained network sustainability and resilience against security vulnerabilities.

By adhering to and enacting these meticulously crafted recommendations, stakeholders across various domains and sectors can tangibly elevate the security stance of Mobile Ad hoc Networks (MANET) and Wireless Sensor Networks (WSN). Through the implementation of tailored solutions, stakeholders can fortify the resilience of these networks against an array of emerging threats, thereby enhancing their capacity to operate with integrity, confidentiality, and availability. Such proactive measures not only bolster the defense mechanisms of MANET and WSN but also instill a sense of confidence among users and administrators regarding the robustness of the network infrastructure. Ultimately, this concerted effort towards security enhancement fosters an environment conducive to the seamless exchange of information and facilitates the uninterrupted functioning of critical services and applications reliant on MANET and WSN technologies.

7. REFERENCES

- [1] C. K. a. D. Wagner, ", "Security in Wireless Sensor Networks: A Survey," Proceedings of the First ACM Workshop on Security of Ad Hoc and Sensor Networks,, *Research Gate*, no. pp., pp. 5-8., 2003, .
- [2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,, " "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Communications Surveys & Tutorials*, Vols. , no. 2, vol. 8, no. pp., pp. 2-23, 2006..
- [3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, , ""Mitigating routing misbehavior in mobile ad hoc networks,," no. " Proceedings of the 6th annual international conference on Mobile computing and networking, , pp. 255-265., 2000.,
- [4] H. Chan, A. Perrig, and D. Song, " , "Random key predistribution schemes for sensor networks,," vol. " Proceedings of the 2003, no. IEEE Symposium on Security and Privacy,, pp. 197-213, 2003, .
- [5] M. Younis and K. Akkaya, , ""Strategies and techniques for node placement in wireless sensor networks," Vols. vol. 6, no. 4,, no. : A survey," *Ad Hoc Networks*, , pp. pp. 621-655,, 2008..
- [6] A. Misra and S. Mandal, , ""Intrusion detection in mobile ad hoc networks,," " *Computer Communications*, , Vols. vol. 29, no. 1, , pp. pp. 38-52,, 2006..
- [7] C. Karlof, N. Sastry, and D. Wagner, , ""TinySec: A link layer security architecture for wireless sensor networks," *ACM Transactions on Information and System Security (TISSEC)*,," Vols. vol. 11, no. 2, , pp. pp. 71-105,, 2008..
- [8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, ""Mitigating routing misbehavior in mobile ad hoc networks," Proceedings of the 6th annual international conference on Mobile computing and networking,, 2000.,
- [9] S. Buchegger and J.-Y. Le Boudec, , ""Performance analysis of the CONFIDANT protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks),," in *Proceedings IEEE INFOCOM Twenty-First Annual Joint Conference of the IEEE Computer and Communications Soc*, 2002..
- [10] Y.-C. Hu, A. Perrig, and D. B. Johnson, " pp. 12-23., "Ariadne: A secure on-demand routing protocol for ad hoc networks," in," in *Proceedings of the 8th annual international conference on Mobile computing and networking*,, 2002.,
- [11] M. Yaseen, M. K. J. Qureshi, and R. K. Raicar, ""Cross-Layer Security," *IEEE Access*, , pp. pp. 8796-8814,, 2016..
- [12] J. He, X. Cheng, and H. S. Hassanein, ""Secure Data Aggregation in Wireless Sensor Networks: A Comprehensive Overview,," *Computer Networks*, Vols. vol. 52, no. 5,, pp. pp. 822-837,, 2008..
- [13] G. Michiardi and J. Molva,, " "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *IEEE Communications Letters*, Vols. vol. 8, no. 1, , pp. pp. 2-4,, 2004..
- [14] Y. Zhang, W. Liu, and Y. Sun, , ""Key Management Techniques in Wireless Sensor Networks: A Survey," *Wireless Communications and Mobile Computing*,," Vols. vol. 11, no. 7, , pp. pp. 803-819,, 2011..
- [15] Snort - Network Intrusion Detection and Prevention System

- [16] Liu, D., & Ning, P. (2003). Establishing pairwise keys in distributed sensor networks. *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*.
- [17] Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS)*.
- [18] Viega, J., & Messier, M. (2002). Network Security with OpenSSL. *O'Reilly Media, Inc.*
- [19] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2004). The feasibility of launching and detecting jamming attacks in wireless networks. *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*.
- [20] NIST Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)
- [21] ISO/IEC 27001: Information security management systems
- [22] GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act)
- [23] Li, B., & Tian, H. (2018). Binary Space Partitioning Based Machine Learning in Grids. *IEEE Access*, 6, 21574-21583. doi:10.1109/ACCESS.2018.2832199.
- [24] Sharkey, A. J. C. (1997). A BSP based machine learning approach to classification. *Neural Computing & Applications*, 6(2), 85-99. doi:10.1007/s005210050013
- [25] Kachirski, O., & Guha, R. (2003). Intrusion detection using mobile agents in wireless ad-hoc networks. *IEEE International Workshop on Knowledge Media Networking*.
- [26] Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. *IEEE Network*, 13(6), 24-30.
- [27] Yi, S., Naldurg, P., & Kravets, R. (2001). Security-aware ad-hoc routing for wireless networks. *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking & Computing*.
- [28] Kumar, S., & Lu, H. (2010). Improved privacy-preserving access control in wireless sensor networks. *Journal of Computer Security*, 18(3), 419-437.
- [29] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. *CRC Press*.
- [30] Zhu, S., Setia, S., & Jajodia, S. (2003). LEAP: Efficient security mechanisms for large-scale distributed sensor networks. *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*.
- [31] Corson, M. S., & Macker, J. (1999). Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. *RFC 2501*
- [32] Riley, G. F., & Henderson, T. R. (2010). The NS-3 network simulator. *Modeling and Tools for Network Simulation*, 15-34.
- [33] Roesch, M. (1999). Snort: Lightweight intrusion detection for networks. *Proceedings of the 13th USENIX Conference on System Administration*
- [34] Perrig, A., Szewczyk, R., Wen, V., Culler, D. E., & Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5), 521-534.
- [35] Ibrahim, Z., & Ghanim, M. "A Review of AI-Based Approaches against Wormhole and Blackhole Attacks in AODV Protocol."
- [36] Mohebi, A., & Scott, S. "A Survey on Mitigation Methods to Black Hole Attack on AODV Routing Protocol."

- [37] Sumathi, K., & Vimal Kumar, D. “A Survey of Routing Protocols and Security Issues in MANET.”
- [38] Singh, A., & Sharma, M. “Cryptography Techniques based on Security of AODV in MANETs.”
- [39] Maniriho, P., et al. “A Comprehensive Survey on Detecting Black Hole Attack in MANET.”
- [40] Aggarwal, A., et al. “AODVSEC: A Novel Approach to Secure AODV Routing Protocol from Insider Attacks.”
- [41] Sharma, R., & Thakur, R. “Detection and Prevention of Wormhole & Black Hole Attacks in MANET Using AODV Protocol.”
- [42] Adhvaryu, D., & Patel, C. “Survey on Black Hole Attack in Wireless Ad-Hoc Network Using AODV Routing Protocol.”
- [43] Keerthana, K., & Babu, A. M. (2025). *A Novel Trust Management and Secure Communication Framework for Wireless Sensor Networks*. Engineering, Technology & Applied Science Research, 15(2), 21728–21737.
- [44] Sharma, P., et al. (2024). *The Intersection of Machine Learning and Wireless Sensor Network Security for Cyber-Attack Detection: A Detailed Analysis*. Sensors, 24(19), 6377.
- [45] Perkins, C. E. (2008). *Ad Hoc Networking*. Addison-Wesley.
- [46] Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach* (8th ed.). Pearson.