

Investigation of security-related routing issues in IoT Networks



By

Muhammad Mohsin Ashraf

(Registration No: 00000363696)

School of Electrical Engineering and Computer Science (SEECS)

National University of Sciences & Technology (NUST)

Islamabad, Pakistan

(2024)

Investigation of security-related routing issues in IoT Networks



By

Muhammad Mohsin Ashraf

(Registration No: 00000363696)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Master in Information Security

Supervisor: Sana Qadir

School of Electrical Engineering and Computer Science

National University of Sciences & Technology (NUST)

Islamabad, Pakistan (2024)

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Investigation of security-related routing issues in IoT Networks" written by Muhammad Mohsin Ashraf, (Registration No 363696), of SEECs has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.


Signature: _____  _____

Name of Advisor: Dr. Sana Qadir

Date: 06-Dec-2024

HoD/Associate Dean: _____  _____

Date: 06-Dec-2024

Signature (Dean/Principal): _____  _____

Date: 06-Dec-2024


National University of Sciences & Technology
MASTER THESIS WORK


We hereby recommend that the dissertation prepared under our supervision by: (Student Name & Reg. #) Muhammad Mohsin Ashraf [363696]


Titled: Investigation of security-related routing issues in IoT Networks


be accepted in partial fulfillment of the requirements for the award of Master of Science (Information Security) degree.

Examination Committee Members

1. Name: Ayesha Kanwal Signature: 
27-Dec-2024 11:33 AM

2. Name: Farzana Jabeen Signature: 
27-Dec-2024 11:33 AM

Supervisor's name: Sana Qadir Signature: 
27-Dec-2024 1:31 PM



Mehdi Hussain
HoD / Associate Dean


27-December-2024

Date

COUNTERSIGNED

30-December-2024

Date

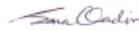


Muhammad Ajmal Khan
Principal

Approval


It is certified that the contents and form of the thesis entitled "Investigation of security-related routing issues in IoT Networks" submitted by Muhammad Mohsin Ashraf have been found satisfactory for the requirement of the degree

Advisor : Dr. Sana Qadir

Signature:  _____


Date: 06-Dec-2024

Committee Member 1:Ms. Ayesha Kanwal

Signature:  _____

06-Dec-2024

Committee Member 2:Dr Farzana Jabeen

Signature:  _____

Date: 06-Dec-2024

AUTHOR'S DECLARATION

I hereby declare that this submission titled "Investigation of security-related routing issues in IoT Networks" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEecs or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEecs or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: Muhammad Mohsin Ashraf

Student Signature: *M Ashraf*

Date: 06-Dec-2024

Certificate for Plagiarism

It is certified that PhD/M.Phil/MS Thesis Titled "Investigation of security-related routing issues in IoT Networks" by Muhammad Mohsin Ashraf has been examined by us. We undertake the follows:

- a. Thesis has significant new work/knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled/analyzed.
- d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC plagiarism Policy and instructions issued from time to time.

Name & Signature of Supervisor

Dr. Sana Qadir

Signature : 

DEDICATED TO
MY FAMILY

ACKNOWLEDGEMENTS

I want to express my deepest gratitude to all those who have supported and guided me throughout the journey of completing this thesis.

First and foremost, I am profoundly grateful to my advisor, Dr. Sana Qadir, for their unwavering support, insightful guidance, and constant encouragement. Her expertise and dedication have been instrumental in shaping the direction and quality of this research.

I sincerely thank the committee members, Ma'am Ayesha Kanwal, and Ma'am farzana Jabeen, for their valuable feedback, constructive criticism, and time dedicated to reviewing my work.

To my family, your love, patience, and unwavering belief in me have been my most significant source of strength. Thank you for always being there for me through the highs and lows of this journey.

Lastly, I am grateful to all the researchers and scientists whose work has inspired and paved the way for this study.

Thank you all for your contributions, support, and encouragement. This achievement would not have been possible without you.

Table of Contents

List of Figures.....	x
List of Tables	xi
List of Abbreviations	xii
Abstract.....	xiii
Chapter 1: Introduction.....	1
1. Introduction	1
1.1 Background.....	1
1.2 Growth of IoT	1
1.3 Motivation.....	2
1.4 Problem Statement	3
1.5 Research Objectives.....	3
Chapter 2: Literature Review	4
2. Literature Review.....	4
2.1 Background.....	4
2.1.1 IoT Attacks	5
2.2 Review of Work on Black Hole Attack	9
2.3 Review of Work on Worm Hole Attack	13
Summary.....	19
Chapter 3: Methodology.....	20
3.1 Methodology Used for Blackhole Attack Detection and Mitigation	20
3.1.1 Overview	20
3.1.2 Environment and Setup	20
3.1.3 Normal Network Operation	21
3.1.4 Implementation of Blackhole Attack	22
3.1.5 Detection and Mitigation Mechanism.....	23
3.1.5.1 Flowchart of AOMDV.....	24
3.2 Methodology Used for Wormhole Attack Detection and Mitigation	27
3.2.1 Overview	27
3.2.2 Environment and Setup	27
3.2.3 Normal Network Operation	29
3.2.4 Implementation of Wormhole Attack.....	29
3.2.5 Detection and Mitigation Mechanism.....	31
3.2.5.1 Flowchart of IDSAODV.....	31
Summary.....	33
Chapter 4: Data Analysis and Results.....	35

4. Results.....	35
4.1 Results for Blackhole Attack	35
4.1.1 Data Collection	35
4.1.2 Data Analysis	36
4.1.3 Comparative Analysis Across Both Scenarios	41
4.2 Results for Wormhole Attack	44
4.2.1 Data Collection	44
4.2.2 Data Analysis	45
4.2.3 Comparative Analysis Across Both Scenarios	50
4.3 Comparison and Discussion.....	53
4.3.1 Comparison of Blackhole Attack.....	53
4.3.2 Comparison of Wormhole Attack.....	54
Summary	54
Chapter 5: Conclusion and Future Work.....	56
5.1 Conclusion	56
5.1.1 Limitations	58
5.2 Future Work.....	58
References:.....	59
APPENDIX A: Script for the Blackhole Attack.....	62
APPENDIX B: Script for the Detection and Mitigation of Blackhole Attack.....	71
APPENDIX C: Script for the Wormhole Attack	81
APPENDIX D: Script for the Detection and Mitigation of Worm hole Attack.....	88

List of Figures

Page No.

Figure 1.1: IoT Devices Growth Ratio	2
Figure 2.1: IoT Device Vulnerabilities ratio.....	4
Figure 2.2: Blackhole Attack Diagram	5
Figure 2.3: Wormhole Attack Diagram	6
Figure 2.4: Sinkhole Attack Diagram	7
Figure 2.5: DDoS Attack Diagram	8
Figure 2.6: Jamming Attack Diagram.....	9
Figure 3.1: Normal Network.....	22
Figure 3.2: Blackhole Attack.....	23
Figure 3.3: Flowchart AOMDV Protocol	25
Figure 3.4: Detection and Mitigation of Blackhole	26
Figure 3.5: Normal Network.....	29
Figure 3.6: Wormhole Attack	30
Figure 3.7: Flowchart of IDSAODV Protocol.....	32
Figure 3.8: Detection and Mitigation of Wormhole	33
Figure 4.1: PDR of 11 Nodes Network.....	37
Figure 4.2: PDR of 20 Nodes Network.....	38
Figure 4.3: Throughput of 11 Nodes Network	39
Figure 4.4: Throughput of 20 Nodes Network	39
Figure 4.5: Packet Loss of 11 Nodes Network	40
Figure 4.6: Packet Loss of 20 Nodes Network	41
Figure 4.7: Average Throughput	42
Figure 4.8: Average Packet Delivery Ratio	43
Figure 4.9: Average Packet Loss	44
Figure 4.10: PDR of 25 Nodes Network.....	46
Figure 4.11: PDR of 30 Nodes Network.....	47
Figure 4.12: Throughput of 25 Nodes Network	48
Figure 4.13: Throughput of 30 Nodes Network	48
Figure 4.14: Packet Loss of 25 Nodes Network	49
Figure 4.15: Packet Loss of 30 Nodes Network	50
Figure 4.16: Average Throughput	51
Figure 4.17: Average Packet Delivery Ratio	52
Figure 4.18: Average Packet Loss	52

List of Tables

	Page No.
Table 2.1: Comparison of Related Studies for Blackhole Attack	16
Table 2.2: Comparison of Related Studies for Blackhole and Wormhole Attacks.....	17
Table 2.3: Comparison of Related Studies for Wormhole Attack	18
Table 3.1: Parameters of Blackhole Simulation.....	21
Table 3.2: Parameters of Wormhole Simulation.....	28
Table 4.1: Comparison of Blackhole Attack Mitigation Mechanism with Existing Work.....	54
Table 4.2: Comparison of Wormhole Attack Mitigation Mechanism with Existing Work.....	54

List of Abbreviations

Abbreviation	Description
MANET	Mobile Ad Hoc Network
PDR	Packet Delivery Ratio
AODV	Ad hoc On-demand Distance Vector
AOMDV	Ad hoc On-demand Multipath Distance Vector
NS-2.35	Network Simulator version 2.35
UDP	User Datagram Protocol
MAC	Media Access Control
IDSAODV	Intrusion Detection System AODV
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
ACK	Acknowledgment
PLR	Packet Loss Ratio
TNR	Transmission Network Range
CBR	Constant Bit Rate
PDS	Packet Delivery Speed
WORMHOLE	Wormhole Attack
BLACKHOLE	Blackhole Attack

Abstract

The rapid growth of Internet of Things (IoT) networks has brought significant advancements in sectors such as healthcare, smart homes, and industrial automation. However, this expansion also presents critical security challenges, particularly at the network layer. This research focuses on two significant attacks, namely blackhole and wormhole attacks, that disrupt routing in IoT networks, leading to packet loss, and reduced throughput. In blackhole attacks, malicious nodes falsely claim the best route, only to drop all received packets, causing severe packet loss and reduced packet delivery ratio. Wormhole attacks, on the other hand, create deceptive shortcuts by establishing a tunnel between colluding nodes, misleading the routing protocol. The study proposes enhancements to existing routing protocols, specifically the Ad hoc On-demand Multipath Distance Vector and Intrusion Detection System AODV protocols, aiming to detect and mitigate these attacks effectively. By leveraging multipath routing and anomaly detection techniques, the modified protocols improve the resilience of IoT networks. Key performance metrics such as packet delivery ratio, throughput, and packet loss were used to evaluate the effectiveness of the proposed solutions. Simulation experiments conducted using NS-2.35 demonstrate that the enhanced protocols significantly improve network performance in the presence of both blackhole and wormhole attacks. The results show a substantial improvement in packet delivery ratio and throughput, indicating successful detection and mitigation of malicious activities, thereby ensuring secure and reliable communication in IoT networks.

Chapter 1: Introduction

1. Introduction

1.1 Background

The Internet of Things (IoT) refers to the network of physical devices embedded with sensors, software, and other technologies that connect and exchange data with other devices and systems over the Internet. This concept has rapidly evolved over the past two decades, revolutionizing industries by facilitating seamless connectivity between devices, allowing for smarter environments and enhanced operational efficiency. IoT is increasingly integrated into numerous sectors, such as healthcare, transportation, manufacturing, agriculture, and smart cities, where real-time monitoring and data-driven decision-making are essential [1].

IoT devices collect, exchange, and analyze data through wireless networks, enabling automation and intelligent operations in various domains. For instance, IoT devices continuously monitor patient vitals in innovative healthcare and transmit this data to healthcare providers for immediate analysis and action [2]. In industrial settings, IoT systems can detect potential machinery failures before they occur, reducing downtime and enhancing productivity. Despite these advantages, IoT networks are prone to many security risks due to the inherent vulnerabilities in their architecture, communication protocols, and resource constraints [3].

1.2 Growth of IoT

The exponential growth of IoT is evident from the increasing number of connected devices worldwide. According to recent estimates, the number of IoT devices is projected to reach over 75 billion by 2025, fueled by advancements in wireless communication technologies like 5G, edge computing, and artificial intelligence [4]. The adoption of IoT devices spans a wide range of industries, including smart homes, agriculture, smart cities, healthcare, logistics, and autonomous vehicles [5].

Figure 1.1 illustrates the steady rise of IoT-connected devices globally from 2015 to 2025, with the base increasing from 15.41 billion in 2015 to an anticipated 75.44 billion by 2025. This growth underscores the significant role IoT plays in transforming various sectors.

The concept of IoT, first popularized in the late 1990s, has transformed significantly with

the proliferation of low-cost sensors, ubiquitous internet connectivity, and cloud computing. Today, IoT enables devices to communicate autonomously, transforming how individuals, businesses, and governments operate. For example, in agriculture, IoT sensors help monitor soil moisture, weather conditions, and crop health, improving yield and reducing water waste. Similarly, IoT devices are used in transportation vehicle-to-vehicle (V2V) communication, enhancing traffic management, safety, and efficiency [6].

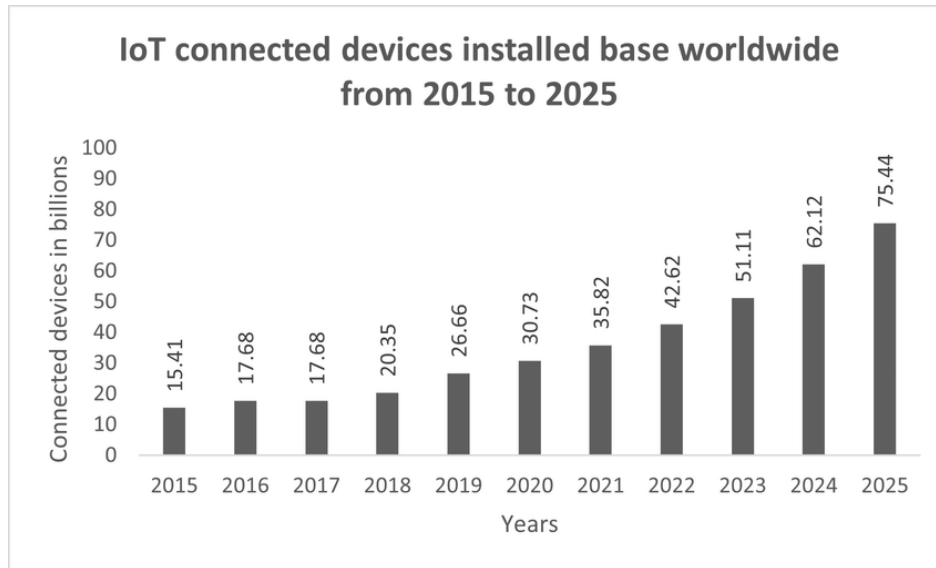


Figure 1.1: IoT Devices Growth Ratio

However, this massive deployment of interconnected devices creates a larger attack surface for cybercriminals. The diversity of devices, each with varying levels of security, coupled with the lack of standardized security protocols, significantly increases the vulnerability of IoT ecosystems to cyberattacks [7].

1.3 Motivation

The rapid growth of IoT devices and their integration into critical systems has made IoT networks an attractive target for attackers. IoT devices are deployed with minimal security, making them vulnerable to various network layer attacks [1]. Traditional security protocols, often too resource-intensive for IoT devices, are unsuitable for such environments. The need for lightweight, scalable security solutions that protect IoT devices from network layer attacks is more pressing than ever, especially in high-stakes industries such as healthcare and industrial automation [7].

High-profile attacks, such as the Mirai botnet, demonstrate the potential for IoT networks

to be exploited on a massive scale. These incidents emphasize the importance of developing effective and efficient security protocols to prevent network layer attacks, which can disrupt communication, steal sensitive data, and cause widespread service outages. This research aims to contribute to the growing body of work to improve IoT network security by developing mitigation strategies for common network layer attacks, such as black holes and wormholes [5].

1.4 Problem Statement

Although considerable progress has been made in the area of IoT security, existing approaches still fall short when it comes to effectively detecting and mitigating network attacks without negatively impacting crucial performance aspects such as throughput and packet loss. These performance metrics are essential for the smooth operation of IoT networks, where devices are often resource-constrained. Current security solutions fail to adequately address specific threats like wormhole and black hole attacks, leaving networks susceptible to disruptions. As the frequency and sophistication of these attacks continue to grow, the need for a more proactive security framework becomes critical. Such a solution must detect and mitigate wormhole and black hole attacks and maintain optimal network performance, minimizing impacts on throughput and packet delivery. This underscores the urgent need for innovative security mechanisms to protect IoT networks while preserving their essential performance.

1.5 Research Objectives

- Analyze the effect of blackhole and wormhole attacks on the performance of IoT networks.
- Survey the existing methods for the detection and mitigation of blackhole and wormhole attacks to identify their limitations.
- Propose and implement proactive detection and mitigation mechanisms for blackhole and wormhole attacks.
- Evaluate the performance of the detection and mitigation mechanisms in terms of throughput, packet loss, and packet delivery ratio.

Chapter 2: Literature Review

2. Literature Review

2.1 Background

As the number of IoT devices increases, the number of attacks on these systems has grown exponentially. This is depicted in Figure 2.1, which highlights the growth of IoT device attacks. IoT networks are particularly vulnerable due to the diverse and constrained nature of devices that often lack built-in security mechanisms [4]. Cyberattacks on IoT networks can target various communication layers, with the network layer being among the most vulnerable. Attacks such as black holes, wormholes, sinkholes, Distributed Denial of Service (DDoS), and jamming have been increasingly observed in IoT networks, resulting in severe disruptions and data breaches [5].

For example, the 2016 Mirai botnet attack leveraged unsecured IoT devices, such as cameras and routers, to launch a massive DDoS attack that disrupted internet services across the United States. Similarly, blackhole and wormhole attacks have also been prominent. One well-known attack occurred in 2010 when a large-scale blackhole attack affected mobile ad-hoc networks (MANETs) in military applications, compromising critical communications during a tactical operation. Likewise, the "Wormhole-Sybil Attack" was observed in 2018, where attackers created a wormhole tunnel to bypass security protocols in smart grid systems, leading to significant disruptions in service. These incidents highlight the need for more robust security mechanisms in IoT networks, particularly as these networks become integrated into critical infrastructure such as healthcare, transportation, and industrial control systems.

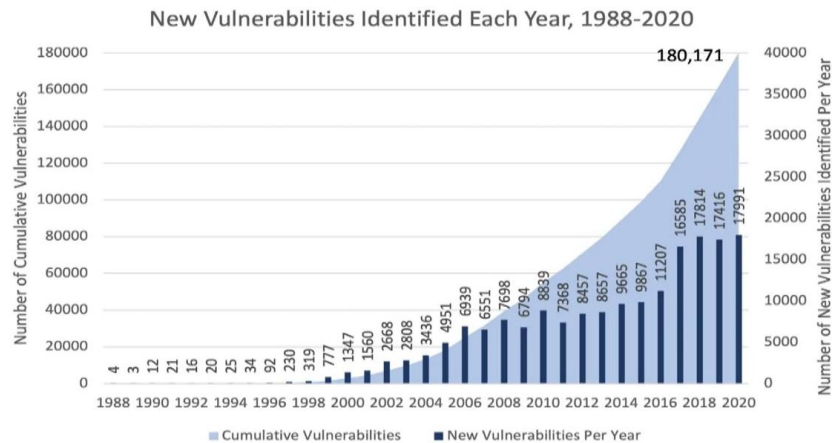


Figure 2.1: IoT Device Vulnerabilities ratio

2.1.1 IoT Attacks

2.1.1.1 Black Hole Attack

Black hole attacks are among IoT systems' most common and dangerous network layer attacks. In a black hole attack, a malicious node falsely claims to have the shortest path to the destination node, luring all traffic towards it. Once the malicious node receives the data packets, it discards them, causing a "black hole" in the network [8].

As shown in Figure 2.2 [44], the sender node (S) initiates communication by broadcasting a Route Request (RREQ) to find the shortest path to the destination node (D). The malicious node (B), acting as a black hole, immediately sends a false Route Reply (RREP 1), claiming a shorter path and attracting all traffic towards itself. As a result, the sender believes Node B has the best route, and data packets are sent to it.

While other legitimate nodes also respond (RREP 2), their replies are ignored due to Node B's deceptive response. The malicious node (B) then drops the packets instead of forwarding them, creating a "black hole" that disrupts communication and causes significant packet loss.

This attack severely impacts the network by causing packet loss, increased latency, and reduced overall throughput. In IoT environments, where devices have limited resources, detecting and mitigating black hole attacks is particularly challenging [32]. Such attacks can significantly disrupt communication, leading to data loss and delays in critical systems like healthcare monitoring or industrial automation [10].

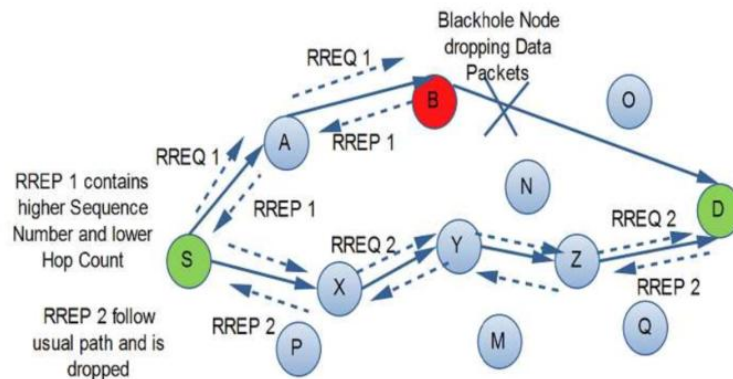


Figure 2.2: Blackhole Attack Diagram

2.1.1.2 Wormhole Attack

Wormhole attacks pose a severe threat to IoT networks by creating a tunnel between two

malicious nodes, which allows them to relay packets between distant points in the network, effectively bypassing standard routing protocols [11]. This attack disrupts the network by making it appear like the two malicious nodes are neighbors, thus misrouting data and causing network congestion or delays. Wormhole attacks are complicated to detect because they do not alter the content of the data packets but instead manipulate the network's topology [31]. With their reliance on wireless communication, IoT networks are highly susceptible to wormhole attacks, which can lead to significant disruptions in service, especially in mission-critical applications like smart grids and healthcare systems [14].

In Figure 2.3 [45], malicious nodes M1 and M2 establish a direct tunnel (indicated by the red dashed line), creating a wormhole link that misleads the network. The source node (S) and destination node (D) are connected via intermediate nodes (N1-N8), but the wormhole between M1 and M2 causes the network to misroute packets, thinking that M1 and M2 are direct neighbors. This manipulation disrupts regular routing, leading to potential data delays or congestion, making detecting the attack challenging for the network.

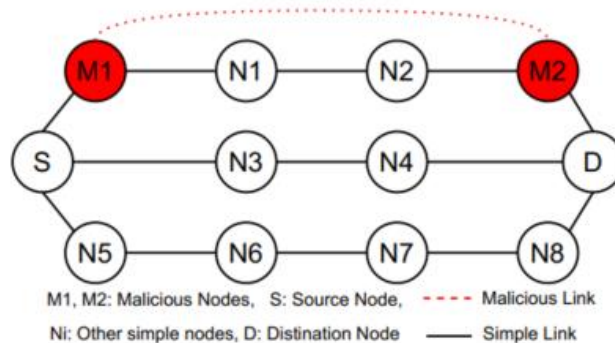


Figure 2.3: Wormhole Attack Diagram

2.1.1.3 Sinkhole Attack

In a sinkhole attack, a malicious node advertises itself as having the best route to a destination, attracting all surrounding nodes to route their traffic. Once the traffic is routed through the sinkhole, the attacker can selectively drop, modify, or intercept the packets, leading to data breaches and network malfunctions [15]. This type of attack is hazardous in IoT networks where critical systems, such as healthcare or industrial control devices, depend on continuous, reliable communication. Sinkhole attacks can disrupt the operation of these systems, leading to potentially catastrophic failures [30].

In Figure 2.4n[46], the central node acts as the sinkhole, attracting traffic from all nearby

nodes (shown by the orange arrows). The malicious node manipulates routing by falsely advertising the best path, causing surrounding nodes to send their data directly through it. This traffic redirection allows the attacker to control, alter, or drop packets as desired, causing significant disruptions to network performance and compromising the integrity of the communication.

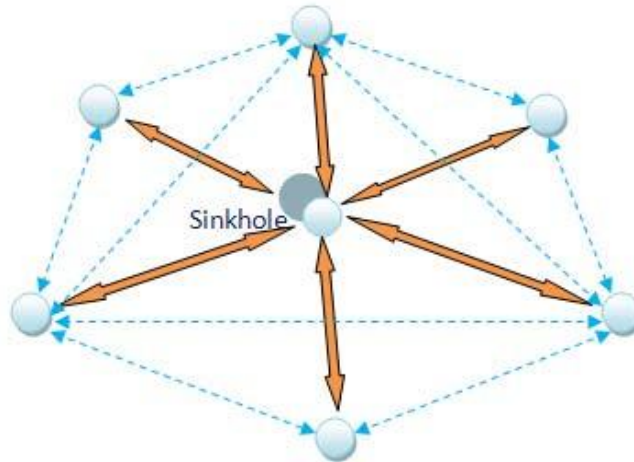


Figure 2.4: Sinkhole Attack Diagram

2.1.1.4 Distributed Denial of Service (DDoS) Attack

A Distributed Denial of Service (DDoS) attack occurs when many compromised IoT devices are used to overwhelm a target network or device with excessive traffic, effectively rendering it inoperable. DDoS attacks are devastating in IoT networks, where devices have limited processing power and cannot handle large amounts of traffic [41]. In the 2016 Mirai botnet attack, thousands of insecure IoT devices were hijacked and used to launch a DDoS attack that caused widespread internet service disruptions [28]. The sheer number of IoT devices makes them an ideal target for DDoS attacks, as even a tiny percentage of compromised devices can generate enough traffic to overwhelm a network [42].

In Figure 2.5 [47], the attacker uses a hierarchical structure to coordinate the DDoS attack. The attack starts with the attacker controlling handlers, which command a set of compromised devices known as zombies. The zombies collectively flood the victim with overwhelming traffic, causing the network to become unresponsive. This distributed approach enables the attacker to amplify the attack's impact by leveraging multiple compromised device layers.

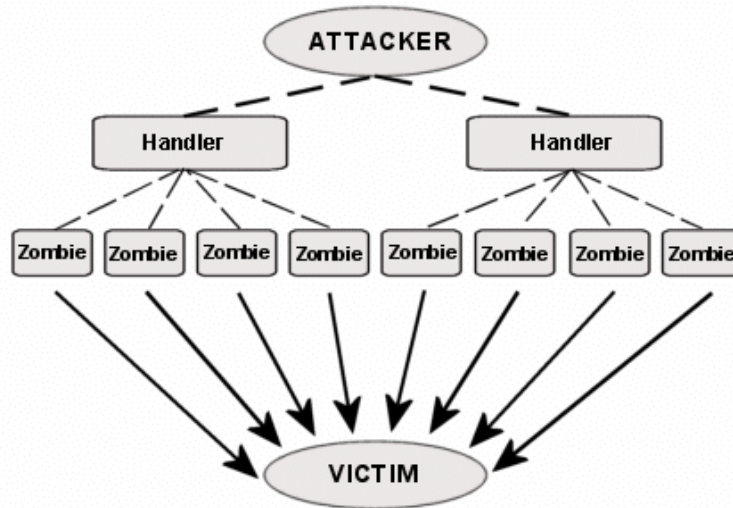


Figure 2.5: DDoS Attack Diagram

2.1.1.4 Jamming Attack

Jamming attacks occur when an attacker generates interference in the communication channel, preventing legitimate devices from transmitting or receiving data. IoT networks, particularly those using wireless communication protocols like Zigbee and Bluetooth, are vulnerable to jamming attacks [38]. In these networks, continuous communication is essential for maintaining normal operations, and jamming attacks can cause severe disruptions, leading to service outages in critical systems such as industrial automation or healthcare [39]. Jamming is often used with other attacks, such as DDoS or sinkhole attacks, to amplify their impact [18].

In Figure 2.6 [48], the jammer is located within the network, and its jamming signal extends across the jamming area (illustrated by the dashed boundary), impacting the communication of nearby sensor nodes. The jamming range indicates the distance over which interference is effective, blocking the ability of nodes within this range to send or receive data packets. This interference disrupts network communication, making it difficult for nodes to maintain normal operations.

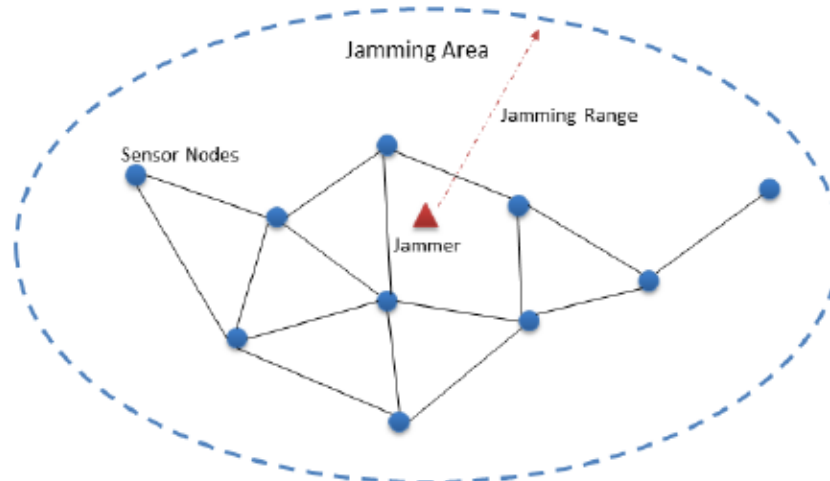


Figure 2.6: Jamming Attack Diagram

2.2 Review of Work on Black Hole Attack

Iraq Ahmad Reshi et al. researched to mitigate black hole attacks in IoT networks. Their study focuses on the challenges of securing the network layer in IoT, particularly against black hole attacks where malicious nodes drop all incoming packets, causing severe disruptions in network performance [2]. They employed the Ad hoc-on-demand Distance Vector (AODV) protocol, which plays a significant role in routing data across IoT devices. The study introduces a novel algorithm to detect and eliminate black hole nodes in the network. The algorithm works by creating a "Master Node" list containing all verified, non-malicious nodes and then systematically comparing all active nodes against this list. If a node fails to match the list, it is flagged as malicious and removed from the network. Additionally, a "sink node" monitors packet forwarding activities, ensuring that any node found to be discarding packets is promptly isolated. This mitigation approach ensures continuous packet delivery even in the presence of attacks.

The study utilizes NS2 and Simulink simulations to evaluate the effectiveness of their proposed algorithm. The results demonstrate a significant improvement in network performance metrics, particularly in the packet delivery ratio, which was restored to 98.21%, resembling an unaffected network. The simulations also show a remarkable increase in network throughput. This research addresses a critical gap by providing a lightweight, energy-efficient method for detecting and neutralizing black hole attacks in IoT networks. The algorithm's ability to dynamically update routing tables and bypass malicious nodes showcases its effectiveness in maintaining network stability without overburdening resource-constrained IoT devices [2].

Tauqeer Safdar et al. conducted a comparative study to analyze the effects of black hole and wormhole attacks on Cloud mobile ad-hoc networks (MANET) enabled IoT networks used for agricultural field monitoring [4]. The study highlights the significance of IoT devices and Cloud MANET monitoring agricultural fields, where nodes communicate without relying on a centralized infrastructure. However, these networks are vulnerable to attacks like blackhole and wormholes, which can degrade performance by disrupting the routing protocols. Using the AODV protocol, the researchers simulated both attacks to determine their impact on critical performance metrics such as throughput, packet delivery ratio, end-to-end delay, and jitter-sum. The study used Network Simulator-3 (NS-3) to simulate various scenarios of IoT nodes under attack, comparing the network's performance in normal and attack conditions.

The research results show that blackhole attacks, where malicious nodes drop packets, have a more detrimental effect on the packet delivery ratio, especially when there are fewer nodes, as the network has fewer alternative paths to route data. Wormhole attacks, on the other hand, involve the creation of a tunnel between malicious nodes to reroute traffic, resulting in higher throughput initially but with increased jitter and delay as the number of nodes increases. The study demonstrates that wormhole attacks are more harmful in terms of draining node resources, while blackhole attacks lead to more immediate packet loss. This comprehensive analysis provides valuable insights into the vulnerabilities of cloud-based IoT networks in agriculture and suggests that different attack types require different countermeasures to maintain network performance [4].

Mazoon Hashil Al Rubaiei et al. conducted a study focusing on the performance analysis of blackhole and wormhole attacks in mobile ad hoc networks (MANETs) [5]. These attacks are particularly harmful in MANETs due to the absence of centralized infrastructure, as each node serves as both a host and a router. Using the ad hoc on-demand distance vector (AODV) routing protocol, the researchers simulated these attacks in a network simulator (NS2) environment to understand their impact on network performance. Both blackhole and wormhole attacks aim to disrupt the network by preventing data packets from reaching their destination. In a black hole attack, the malicious node falsely claims to have the shortest path, capturing and dropping all the packets. In contrast, wormhole attacks involve creating a tunnel between two or more malicious nodes, which reroutes the traffic through this tunnel, resulting in dropped packets before they reach the intended destination.

The methodology employed in this study included modifying NS2's AODV protocol files

to simulate blackhole and wormhole attacks. Specific modifications were made to the AODV files for blackhole attacks to declare malicious nodes and prevent them from forwarding packets. For wormhole attacks, the researchers created a tunneling mechanism by modifying the link layer files to simulate the behavior of wormhole nodes. The study evaluated the effects of these attacks using performance metrics such as packet delivery ratio, end-to-end delay, and normalized routing load (NRL). The results indicated that blackhole attacks resulted in a higher packet drop rate due to the immediate routing of packets through the malicious node. In contrast, wormhole attacks caused higher end-to-end delays and increased routing load due to the complexity of creating tunnels between malicious nodes [5].

Muhammad Nasir Siddiqui et al. conducted a study to analyze the performance of blackhole and wormhole attacks in MANET-based IoT networks [1]. In this study, the researchers focused on the vulnerability of MANET-based IoT networks due to their infrastructure-less and self-organizing nature, making them susceptible to various denial-of-service attacks, such as blackhole and wormhole attacks. The primary aim of the research was to compare the impact of these two types of attacks on the network's performance, particularly in terms of packet delivery ratio, throughput, end-to-end delay, and jitter. The team implemented these attacks by modifying the Ad hoc On-demand Distance Vector (AODV) routing protocol in the NS-3 network simulator. It used the Flow Monitor module to gather data for analysis.

The methodology involved setting up a network simulation with varying numbers of nodes and introducing malicious nodes to simulate the blackhole and wormhole attacks. The malicious node falsely claims to have the best route for blackhole attacks and then drops all incoming packets. In contrast, wormhole attacks involved creating a tunnel between two malicious nodes to reroute and drop packets before they reached their destination. The study found that blackhole attacks caused a more significant reduction in the packet delivery ratio and throughput, as many packets were dropped immediately. In contrast, wormhole attacks resulted in higher end-to-end delay and jitter due to the tunneling process. Overall, the results indicated that while blackhole attacks had a more immediate impact on packet loss, wormhole attacks posed a more significant challenge regarding network delays and jitter, making them more disruptive to network performance [1].

S. Naveena et al. conducted research to analyze and mitigate black hole attacks in mobile ad hoc networks (MANETs) by employing a trust-based routing approach [23]. The study

addresses the critical security challenges posed by black hole attacks, where malicious nodes mislead the network by falsely advertising themselves as having the shortest route to the destination, only to drop all packets received. The authors implemented their proposed solution using the ad hoc on-demand distance vector (AODV) protocol. The trust-based scheme involves two stages: the data retrieval (DR) table phase and the route formation phase. In the DR phase, nodes collect and store routing information, including details about neighboring nodes and their forwarding behavior. The trustworthiness of each node is then calculated based on the ratio of successfully forwarded packets to the total number of packets that should be forwarded. A threshold is set to distinguish between trusted and untrusted nodes, and untrusted nodes are excluded from the routing process.

In the route formation phase, the network identifies a secure route to transmit data packets, ensuring the black hole nodes are avoided. The proposed scheme significantly enhances the packet delivery ratio, with the researchers achieving a PDR of 98%, demonstrating the system's efficiency in mitigating black hole attacks. The simulation was conducted using the NS-2.35 network simulator, with a setup consisting of 30 nodes. The results also indicated improved throughput and reduced delays, validating the effectiveness of trust-based routing in enhancing the security of MANETs. The study highlights the importance of such trust-based systems for maintaining reliable communication in MANET environments and suggests future work in optimizing energy consumption during detection [23].

Prabhakar Reddy B et al. conducted a study to address blackhole attacks in MANET networks by proposing an enhanced version of the ad hoc on-demand distance vector (AODV) routing protocol with built-in security mechanisms, termed AODV-BS [24]. The authors simulated the standard AODV and their proposed AODV-BS protocol under various network conditions, measuring the impact of blackhole attacks on key performance metrics such as packet delivery ratio, average end-to-end delay, normalized routing overhead, and throughput.

The results show that the AODV-BS protocol outperformed the standard AODV in mitigating blackhole attacks. Specifically, the PDR of AODV-BS under attack was approximately 85%, compared to 58% for the standard AODV. Similarly, AODV-BS reduced the average end-to-end delay and normalized routing overhead, improving overall network throughput even in the presence of blackhole nodes. This research highlights the effectiveness of integrating cryptographic verification and threshold evaluation mechanisms into existing MANET protocols

to enhance security without significantly impacting performance. The authors suggest further research on other MANET routing protocols and different types of attacks, such as wormholes or gray holes, for comprehensive network protection [24].

2.3 Review of Work on Worm Hole Attack

Marah Knaj et al. conducted a study to address wormhole attacks in MANETs using a hop count analysis technique to detect and mitigate such attacks' impact [25]. Wormhole attacks are a significant threat to MANETs, where malicious nodes create a hidden tunnel between them, allowing them to intercept and forward packets while bypassing legitimate routes. This leads to various network issues, including the loss and modification of packets. The authors used the NS-2.35 simulator to create a MANET environment using the AODV protocol. They measured the impact of wormhole attacks on critical network performance metrics, including Average throughput, packet delivery ratio, and average end-to-end, under both normal and attack scenarios.

The results indicated that the hop count analysis technique effectively mitigates the effects of wormhole attacks. Specifically, the technique improved the network's average throughput from 163.76 kbps (under attack) to 194.5 kbps and increased the PDR from 24.46% to 51.4% in the presence of two wormhole tunnels. However, there was an observed increase in the average end-to-end delay due to the additional time required to detect and avoid malicious paths. This research highlights the potential of hop count-based techniques to detect and mitigate wormhole attacks while maintaining acceptable performance levels in MANETs [25].

Mukul Shukla and Brijendra Kumar Joshi conducted a study to address wormhole attacks in MANETs by proposing a trust-based approach to detect and mitigate such attacks [8]. Wormhole attacks pose a significant threat to MANETs, where malicious nodes create a tunnel to falsely present themselves as having the shortest route, thereby intercepting and potentially disrupting network traffic. The authors introduced a trust-based mechanism, evaluating nodes based on parameters such as data rate and packet receiving time to identify and isolate malicious nodes. They used the NS-2 simulator to assess the impact of wormhole attacks on key performance metrics, including packet delivery ratio, throughput, and end-to-end delay.

The study's results showed that the trust-based approach significantly improved network performance in the presence of wormhole attacks. The PDR and throughput increased when using the trust-based scheme, returning to near-normal levels even under attack conditions. In contrast, the end-to-end delay remained relatively unaffected, with similar values observed in attacked and

unaffected network scenarios. This research demonstrates the efficacy of a trust-based approach in defending MANETs against wormhole attacks, offering a promising solution to enhance network resilience without compromising performance [8].

Ekin Ecem Tatar et al. conducted a study to address wormhole attacks in IoT-based networks, explicitly focusing on wireless sensor networks (WSNs) [11]. Wormhole attacks pose a severe threat in IoT networks, where malicious nodes create a tunnel between them, allowing them to intercept, drop, or manipulate data packets. This leads to severe communication disruption in the network. The authors employed the NS-2 simulator to analyze network performance under wormhole attack conditions, focusing on metrics such as packet delivery ratio and throughput, which were significantly degraded during attacks.

The results showed that the proposed mitigation strategies successfully restored network performance. Improvements in PDR and throughput were observed, indicating the effectiveness of the techniques in detecting and bypassing wormhole paths. This research emphasizes the importance of robust detection mechanisms and secure routing strategies in IoT-based WSNs to protect against wormhole attacks and maintain optimal network functionality. Future research could explore expanding these solutions to broader IoT applications [11].

Mohit Kumar Verma et al. conducted a study to address wormhole attacks in wireless sensor networks (WSNs) by surveying detection and prevention techniques [26]. Wormhole attacks are a critical threat to WSNs, where malicious nodes create a tunnel to intercept data packets, disrupting the routing process and preventing the data from reaching its intended destination. The authors reviewed various methods, such as packet encapsulation, packet relay, and out-of-band channels, which aim to detect and mitigate wormhole attacks by identifying the characteristics of malicious nodes and isolating them from the network.

The survey covered techniques like the wormhole geographic distributed detection (WGDD) algorithm, which uses hop counting to detect wormhole attacks, and the ad hoc on-demand multipath distance Vector (AOMDV) protocol, which incorporates round trip time (RTT) for attack detection. These methods were evaluated based on their accuracy, computational overhead, and applicability in static and dynamic network environments. The authors concluded that while these techniques are effective, there is a need for more efficient and adaptive approaches that reduce computational complexity and address the limitations of current methods in securing WSNs against wormhole attacks [26].

Zulfiqar Ali Zardari et al. conducted a study to address wormhole attacks in mobile ad hoc networks (MANETs) by proposing a lightweight detection and prevention technique [27]. The authors introduced a technique that calculates the average sequence number of the reply (RREP) packets in the AODV protocol. If the sequence number of a node exceeds the estimated average, the node is identified as malicious, and its traffic is discarded.

The study's results demonstrated that the proposed technique effectively detected wormhole attacks with minimal complexity and reduced overhead. The simulations, conducted using the NS-2 network simulator, showed that the method improved the Packet Delivery Ratio and network throughput compared to AODV under attack. Additionally, the proposed technique extended the network's lifetime by preserving the nodes' battery power. This research highlights the potential of using simple yet efficient methods to detect and mitigate wormhole attacks in MANETs without additional hardware [27].

Sankara Narayanan et al. conducted a study to address wormhole attacks in MANETs by proposing a Modified Secure AODV (MSAODV) protocol [9]. The authors introduced the MSAODV protocol, which uses packet forward ratio (PFR) and round-trip time (RTT) to detect wormhole attacks by evaluating individual nodes rather than the entire network. The protocol identifies malicious nodes by monitoring these metrics and effectively mitigates active and passive attacks.

The study's results, obtained through NS-2 simulation, showed that MSAODV outperformed existing protocols, such as the standard AODV and SAODV, regarding packet delivery ratio, end-to-end delay, and packet loss. MSAODV provided significantly reduced packet loss and delay while increasing PDR, even under attack conditions. The authors concluded that MSAODV effectively enhances the security of MANETs against wormhole attacks without the need for additional hardware. Future work could focus on comparing this method with other detection techniques to further improve performance [9].

Table 2.1: Comparison of Related Studies for Blackhole Attack

Source	Network	Routing Attack	Simulation	Benefits	Drawbacks	Mitigation
[2]	WSN	Black Hole	NS-2, Simulink	Analyzing the impact of the Black attack on IoT networks, propose a novel mitigation algorithm that improves network performance.	Maintaining an authentic node list and comparing all nodes do not scale in more extensive networks, increasing processing time and computational overhead.	Implementation of a novel algorithm that creates a list of authentic nodes compared with a network node and decides whether it is a malicious or genuine node.
[23]	MANET	Black Hole	NS-2	Propose a trust-based routing method that effectively improves packet delivery and mitigates Black Hole attacks.	Requires a higher computational overhead for trust value calculation; simulation is limited to small-scale network setups.	Use a DR table and trust-based values to identify and mitigate Black Hole attacks.
[24]	MANET	Black Hole	NS-2	The AODV-BS protocol integrates built-in security to counter Black Hole attacks, improving packet delivery and throughput.	Increased Average End-to-End Delay and Normalized Routing Load.	Uses cryptographic verification and threshold evaluation to identify and block malicious nodes.

Table 2.2: Comparison of Related Studies for Blackhole and Wormhole Attacks

Source	Network	Routing Attack	Simulation	Benefits	Drawbacks	Mitigation
[1]	MANET	Black Hole, worm Hole	NS-3	Provides a comparison of Blackhole and Wormhole attacks in terms of PDR, Throughput, and Delay.	Did not propose any mitigation techniques for the attacks.	N/A
[4]	MANET	Black Hole, worm Hole	NS-3	Evaluate the impact of attacks on Cloud MANET-enabled IoT networks, specifically for agricultural field monitoring.	Did not propose any mitigation techniques for the attacks.	N/A
[5]	MANET	Black Hole, Worm Hole	NS-2	Evaluates the performance of AODV protocol under the impact of attacks.	Did not propose any mitigation techniques for the attacks.	N/A

Table 2.3: Comparison of Related Studies for Wormhole Attack

Source	Network	Routing Attack	Simulation	Benefits	Drawbacks	Mitigation
[27]	MANET	Worm Hole	NS-2	Proposes a lightweight technique for detecting wormhole attacks, increasing the PDR and network lifetime	Slight decrease in throughput and PDR compared to normal AODV due to link failures.	Detects wormhole nodes by calculating the average sequence number of RREP packets and discarding paths with higher values.
[9]	MANET	Worm Hole	NS-2	Proposed MS-AODV protocol that improves security	It increased computational overhead due to RTT and PFR calculations for each node.	Detects active and passive wormhole attacks using RTT and PFR for each node without requiring extra hardware.
[11]	IoT	Worm Hole	NS-2	Provides a comprehensive study on the impact of wormhole attacks and evaluates their performance.	Did not propose any mitigation techniques for the attacks.	N/A
[26]	WSN	Worm Hole	N/A	Provides a detailed survey on wormhole attack detection and prevention techniques.	Did not propose any mitigation techniques for the attacks.	N/A
[25]	MANET	Worm Hole	NS-2	Successfully detects and mitigates the effect of wormhole attacks in MANETs using a hop count analysis technique.	Only focuses on the hop count. If a path with a low hop count is detected, it will mark that path as a wormhole attack.	The hop count analysis technique identifies wormhole tunnels by comparing hop counts across different routes.

Summary

Chapter 2 comprehensively reviews existing research on network security vulnerabilities in IoT networks, explicitly focusing on routing attacks such as black holes and wormholes. It explores various detection and mitigation techniques proposed in the literature, highlighting their strengths and limitations.

The chapter begins by detailing the challenges associated with these attacks, emphasizing how malicious nodes exploit routing protocols to disrupt communication, degrade performance, and cause packet loss in IoT environments. Each type of attack is illustrated with clear explanations and diagrams, helping to visualize their impact on network behavior.

The literature review shows trust-based mechanisms and machine-learning techniques are among the most effective methods for detecting and mitigating blackhole and wormhole attacks. Studies suggest that these techniques improve network performance by enhancing the PDR, increasing throughput, and reducing packet loss, albeit with varying complexity and computational overhead.

The review concludes with a comparative analysis of several studies demonstrating the evolution of security strategies in IoT networks. It is evident that while significant progress has been made in detecting and mitigating routing attacks.

Chapter 3: Methodology

3.1 Methodology Used for Blackhole Attack Detection and Mitigation

3.1.1 Overview

Security in MANETs remains critical due to their decentralized nature and dynamic node topology. Among the most severe threats is the blackhole attack, where a malicious node falsely advertises an optimal route to the destination, intercepting and discarding data packets. This attack results in significant packet loss, disrupting the network's regular operation and degrading performance.

In this research, the AOMDV routing protocol, widely used for its ability to maintain multiple paths between source and destination nodes, was enhanced to detect and mitigate blackhole attacks. The detection mechanism leverages route monitoring and sequence number analysis. At the same time, the mitigation strategy aims to restore the network's performance by improving the packet delivery ratio, enhancing throughput, and reducing packet loss.

The entire process, from detection to mitigation, was implemented and evaluated using the NS-2.35 simulator on Ubuntu 22.04. This section details the steps during the simulation and the methods employed to achieve blackhole detection and mitigation, creating a resilient MANET environment.

3.1.2 Environment and Setup

The simulation environment was configured to reflect a typical MANET scenario, with multiple nodes positioned within a designated simulation area. Two network setups were used: one with 11 nodes and another with 20 nodes, providing variation in network size. The environment was set up using NS-2.35 on Ubuntu 22.04, chosen for its robust ability to model network protocols and communication patterns. These configurations allowed for a thorough network behavior analysis under normal conditions and during blackhole attacks.

The network configuration was customized to model realistic communication conditions among the nodes. The mobility of the nodes, transmission range, and data flow patterns were carefully chosen to ensure that the simulation reflected a practical ad hoc network. Table 3.1 presents a summary of the network configuration parameters used in the simulation. It includes details such as the number of nodes, traffic patterns, routing protocol, and transport protocol. This

configuration served as a robust foundation for implementing the black hole attack and facilitated the analysis of the network's performance under both normal and attack conditions.

Table 3.1: Parameters of Blackhole Simulation.

Parameter	Value
Simulator	NS-2.35
Platform	Ubuntu 22.04
Simulation time	30 sec
Number of nodes	11,20
Number of blackhole nodes	1
Traffic	Constant bit rate (CBR)
Transmission range	1500*2500
Packet size	512 bytes
Routing protocol	AODV, AOMDV
Transport protocol	UDP
MAC layer	802.11

3.1.3 Normal Network Operation

The first simulation scenario represents the normal operation of the network using the AODV protocol. AODV dynamically establishes routes between the source and destination node only when needed. This protocol allows nodes to efficiently discover routes using RREQ and RREP messages without maintaining a global routing table, making it ideal for dynamic ad hoc networks.

In this scenario, the network operates without malicious interference, and all nodes cooperate in forwarding packets. Routes are established as needed, and data is transmitted from source to destination, leading to optimal packet delivery ratio and throughput performance.

To visualize the normal operation of the network, Figure 3.1 presents a screenshot from NS-2.35's Network Animator. The figure illustrates the source, destination, and intermediate nodes involved in the routing process. It shows the real-time data transmission path, highlighting how AODV dynamically establishes a route between the source and destination.

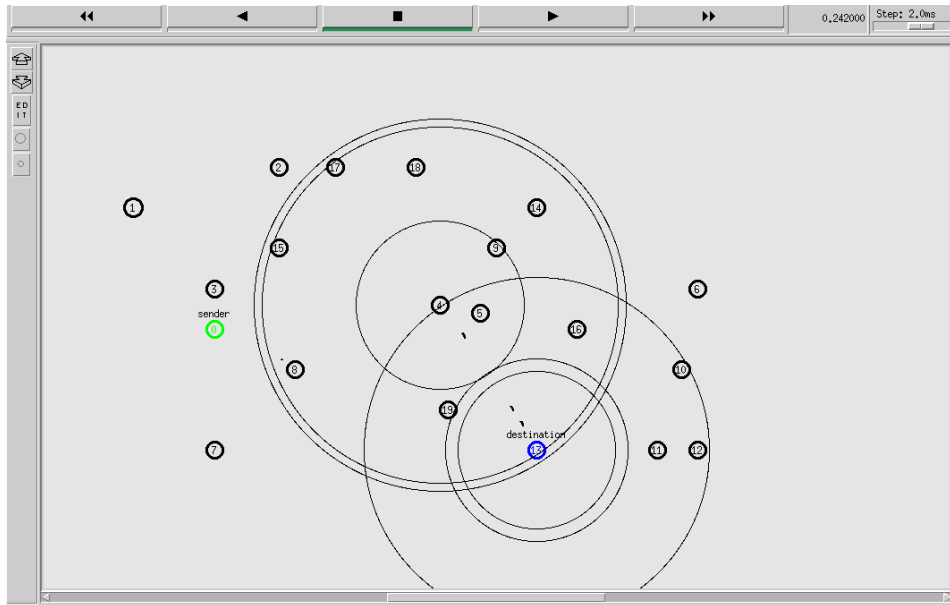


Figure 3.1: Normal Network

3.1.4 Implementation of Blackhole Attack

After establishing a baseline with normal operation, a blackhole attack was introduced. In this attack, a malicious node (blackhole) deceitfully claims to have the shortest path to the destination by sending a Route Reply (RREP) with an abnormally high sequence number. The source node, misled by this false information, selects the blackhole node as part of the optimal route, resulting in packet interception and loss.

The blackhole node does not forward any packets it receives. Instead, it drops all data packets, as seen in the sharp reduction in the packet delivery ratio and increased packet loss. The attack also negatively impacts throughput.

The network behavior under attack is captured in Figure 3.2, which shows the malicious blackhole node intercepting and discarding data packets.

The implementation code for simulating this blackhole attack scenario is provided in **Appendix A**. This appendix includes detailed simulation scripts and parameters used for modeling the attack in the network.

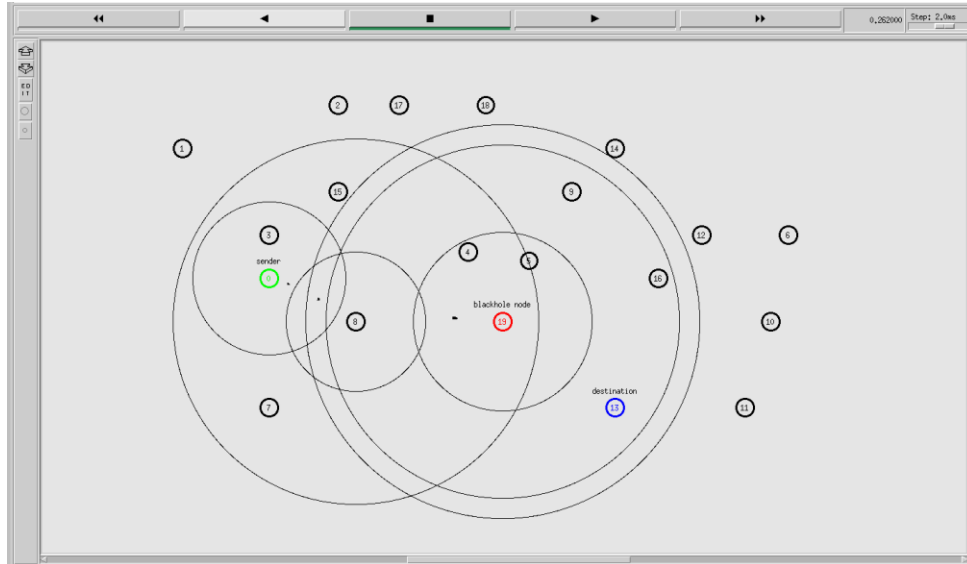


Figure 3.2: Blackhole Attack

As depicted in the figure, the source node unknowingly selects the blackhole node as part of the routing path, leading to a complete disruption in communication. The consistent packet loss and failure to reach the destination highlight the devastating effect of the blackhole attack, severely degrading the overall packet delivery ratio and throughput of the network.

3.1.5 Detection and Mitigation Mechanism

To counter the detrimental effects of the blackhole attack, the AOMDV protocol was modified to detect anomalies in the routing process and apply corrective measures. The detection mechanism is based on sequence number analysis and behavioral monitoring of RREP messages. The detection mechanism closely monitors the sequence numbers of incoming RREP messages. A node that consistently responds with abnormally high sequence numbers or repeatedly claims fresh routes raises suspicion. The protocol tracks the frequency and timing of these responses, identifying patterns indicative of blackhole behavior. Once a node is marked as suspicious, its route is further validated by sending a test data packet and waiting for an acknowledgment. The node is confirmed to be a black hole if the acknowledgment (ACK) is not received.

Upon detecting the presence of a blackhole node within the network, the modified AOMDV protocol promptly initiates a series of mitigation steps to minimize further disruption. These steps ensure the network quickly adapts and circumvents the malicious node, restoring stable communication between the source and destination nodes.

The first step involves broadcasting a RERR message, alerting all neighboring nodes to the

presence of the black hole. This ensures that the blackhole node is excluded from the route discovery process in subsequent routing decisions. Once neighboring nodes are informed, the routing tables across the network are updated, effectively isolating the blackhole node. This proactive update prevents any further routing attempts through the compromised node, ensuring that data packets do not continue to be intercepted or dropped.

In addition to excluding the blackhole node, the modified protocol leverages AOMDV's multipath routing capability, which inherently maintains multiple disjoint routes between the source and destination. By utilizing these multiple valid routes, the protocol ensures that communication can continue seamlessly, even after the malicious node is excluded from the network. This redundancy in path selection plays a critical role in preserving the integrity of communication and minimizing disruptions caused by such attacks.

3.1.5.1 Flowchart of AOMDV

The overall blackhole detection and mitigation is illustrated in Figure 3.3, providing a comprehensive visual representation of the modified AOMDV protocol. This flowchart captures the critical decision-making steps, from initial route discovery and detection of routing anomalies to the validation of routes and the subsequent avoidance of blackhole nodes. Each stage in the flowchart reflects the protocol's adaptive behavior in identifying and isolating malicious nodes, ensuring that data transmission occurs securely through legitimate paths. This diagram plays a vital role in understanding the inner workings of the enhanced AOMDV protocol, particularly in its ability to maintain secure and reliable routing in a dynamic and potentially hostile network environment. It is a crucial methodology component, offering insight into how the protocol mitigates threats while preserving network performance.

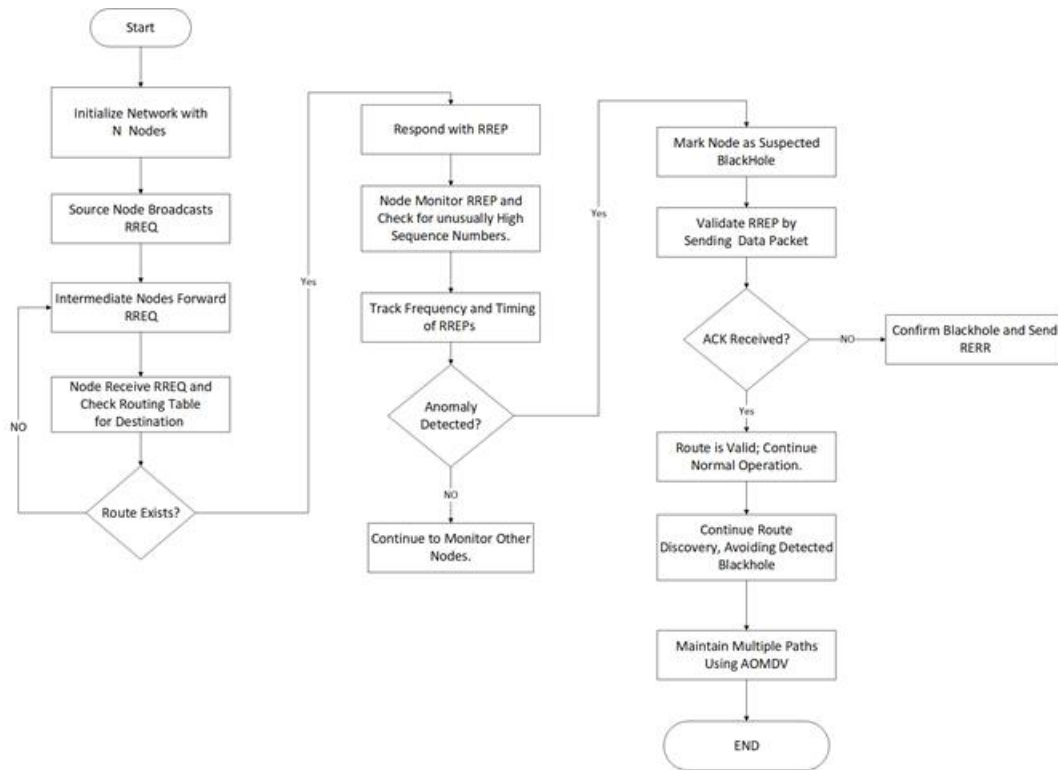


Figure 3.3: Flowchart AOMDV Protocol

As a result of these mitigation strategies, the network quickly recovers and re-establishes stable communication channels. Figure 3.4 illustrates the post-mitigation scenario, where the blackhole node has been effectively circumvented, and data packets resume flowing through legitimate and trusted routes. This visual representation captures how the protocol dynamically adapts, restoring the data flow after the malicious node has been avoided.

The implementation code for the detection and mitigation mechanism is provided in **Appendix B**. This appendix contains the detailed code scripts and configuration used to model the mitigation of blackhole attacks in the network.

Following the implementation of the blackhole detection and mitigation mechanism, a detailed evaluation was carried out to assess its overall effectiveness. The review was designed to observe the behavior of the network under three distinct conditions: during normal operation, under blackhole attack, and after the mitigation. Each phase provided insight into how the network responded to varying levels of security threats and how it recovered after corrective actions were taken.

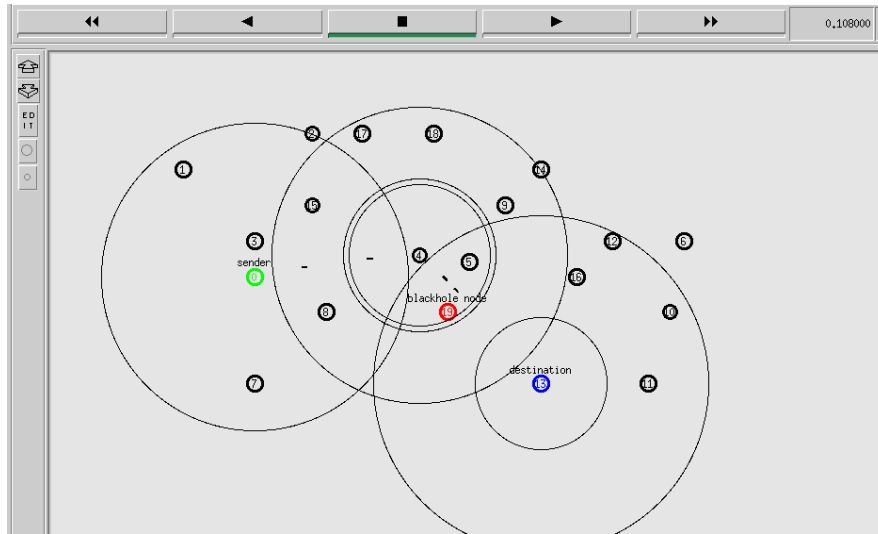


Figure 3.4:Detection and Mitigation of Blackhole

To thoroughly assess the impact of the blackhole detection and mitigation strategy, several key performance metrics were evaluated across the three phases of the network's operation: normal, under attack, and post-mitigation. The packet delivery ratio, which measures the proportion of successfully delivered packets, remained stable during normal operation but dropped significantly when the network was attacked, as the blackhole node intercepted and discarded data. After applying the mitigation strategy, the PDR showed a marked improvement, indicating that valid routes were re-established and data transmission resumed effectively. Similarly, throughput, which reflects the data transmission rate, was severely impacted during the attack but recovered once the blackhole node was isolated and legitimate routes were used. Packet loss was notably higher during the attack, as the malicious node dropped most packets; however, after mitigation, packet loss significantly decreased, demonstrating the protocol's success in avoiding the compromised route and maintaining reliable communication.

The overall blackhole detection and mitigation is illustrated in Figure 3.4, providing a comprehensive visual representation of the modified AOMDV protocol. This flowchart captures the critical decision-making steps, from initial route discovery and detection of routing anomalies to the validation of routes and the subsequent avoidance of blackhole nodes. Each stage in the flowchart reflects the protocol's adaptive behavior in identifying and isolating malicious nodes, ensuring that data transmission occurs securely through legitimate paths. This diagram plays a vital role in understanding the inner workings of the enhanced AOMDV protocol, particularly in its

ability to maintain secure and reliable routing in a dynamic and potentially hostile network environment. It is a crucial methodology component, offering insight into how the protocol mitigates threats while preserving network performance.

3.2 Methodology Used for Wormhole Attack Detection and Mitigation

3.2.1 Overview

In MANETs, nodes' decentralized nature and dynamic topology make the network susceptible to various security threats. Among these, the wormhole attack is hazardous, as it involves two colluding malicious nodes creating a tunnel between them to transmit data packets bypassing normal routing paths. This tunnel deceives the routing protocol by presenting a shortcut path that tricks the source node into forwarding packets through the malicious nodes, potentially leading to severe disruption in the network. The wormhole attack manipulates the normal route discovery process, bypassing legitimate nodes and causing the network to reroute traffic through the malicious wormhole tunnel, undermining the integrity of the network and leading to route hijacking, loss of connectivity, and packet misrouting.

We have modified the IDSAODV protocol to detect and mitigate wormhole attacks. The IDSAODV protocol introduces a mechanism to monitor specific routing behaviors, such as unexpected hop count reductions, abnormal sequence number manipulations, and suspiciously short delays between route requests and replies. By analyzing these anomalies, the protocol can detect wormholes and initiate mitigation steps to isolate and prevent further exploitation by malicious nodes. This methodology ensures the network remains robust and secure, even in wormhole attacks, by re-establishing legitimate communication routes and avoiding compromised paths. The entire detection and mitigation process was implemented using NS-2.35 on Ubuntu 22.04. The following sections describe the detailed steps to simulate and evaluate wormhole attack detection and mitigation, creating a resilient MANET environment capable of withstanding such security threats.

3.2.2 Environment and Setup

To simulate the wormhole attack and implement its detection and mitigation mechanism, two distinct network setups were configured using NS-2.35 on Ubuntu 22.04. The first setup involved a network of 20 nodes, with two of these nodes deliberately configured as wormhole

nodes, designed to create a malicious tunnel that would disrupt the normal route discovery process. The second setup expanded the network to 30 nodes, maintaining the same two wormhole nodes. These two setups allowed for a comprehensive evaluation of the wormhole attack and its detection under different network densities, providing insights into how the network behaves under normal conditions and when compromised by a wormhole attack. Using these varied configurations, the simulations captured the dynamics of MANETs with different node densities and assessed the efficiency of the detection and mitigation mechanisms in each scenario.

The network was configured to reflect practical communication scenarios accurately. Constant bit rate (CBR) traffic simulates continuous packet transmission between the source and destination nodes. The mobility model selected for the nodes represented random movements across a defined simulation area, creating realistic communication dynamics. Key parameters, including node mobility, transmission range, packet size, and simulation duration, were carefully chosen to ensure the network environment could effectively demonstrate both the wormhole attack and the efficiency of the detection mechanism. Table 3.2 outlines the network configuration parameters used in the simulation, including details such as the number of nodes, traffic patterns, routing protocol, and transport protocol. This setup established a solid foundation for executing the wormhole attack and allowed for the analysis of the network's behavior under both normal and attack scenarios.

Table 3.2: Parameters of Wormhole Simulation.

Parameter	Value
Simulator	NS-2.35
Platform	Ubuntu 22.04
Simulation time	30 sec
Number of nodes	25,30
Number of Wormhole nodes	2
Traffic	Constant bit rate (CBR)
Transmission range	1440*1000
Packet size	1500 bytes
Routing protocol	AODV, IDSAODV
Transport protocol	UDP
MAC layer	802.11

3.2.3 Normal Network Operation

The first phase of the simulation involved the network operating under normal conditions using the AODV protocol. The AODV protocol dynamically establishes routes between the source and destination nodes based on demand in this scenario. When a node initiates communication, it broadcasts an RREQ to its neighbors, and nodes send the RREP with a valid route to the destination. This process ensures that routes are established only when necessary, optimizing the network's efficiency and reducing unnecessary routing overhead.

Under normal operation, all nodes within the network cooperate in forwarding packets, and no malicious activities disrupt the routing process. The network successfully discovers and maintains routes, transmitting data from the source to the destination without interference. Figure 3.5 presents a screenshot from NS-2.35's Network Animator, visually depicting the network under normal conditions. It clearly shows the source and destination nodes, and the intermediate nodes involved in the routing process, with data packets being transmitted smoothly across the network. This scenario serves as the baseline for evaluating the wormhole attack's impact and the mitigation mechanism's effectiveness.

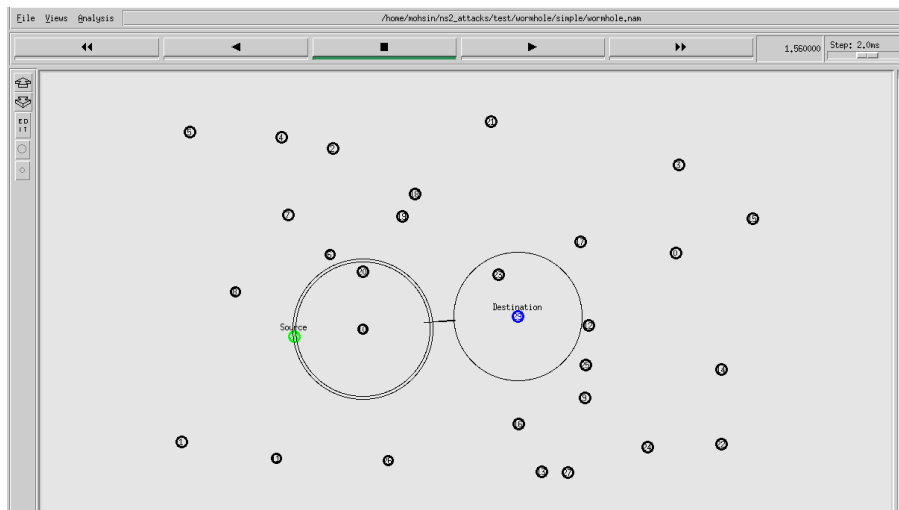


Figure 3.5: Normal Network

3.2.4 Implementation of Wormhole Attack

After establishing the baseline for normal network operation, the next phase of the simulation introduced a wormhole attack. In this attack, two malicious nodes were configured to

create a tunnel between them, bypassing the legitimate network topology. These wormhole nodes intercepted RREQ packets from one part of the network, tunneled them through their malicious link, and then replayed them on the other side of the network. This created a false appearance of a shorter and more efficient path to the destination. Consequently, the source node was misled into selecting this seemingly optimal but compromised route.

As a result of this manipulation, legitimate nodes were bypassed, and data packets were transmitted through the wormhole tunnel instead of following the correct multi-hop path. The wormhole nodes did not directly alter or drop the data packets. Still, their manipulation of the route discovery process allowed them to deceive the network into routing traffic through their tunnel, potentially leading to security breaches and disruptions in the network. Figure 3.6 captures this behavior through NS-2.35's Network Animator showing how the wormhole nodes establish a deceptive shortcut and disrupt the normal routing process. The visualization highlights the tunnel created by the wormhole nodes and how the normal network topology is bypassed.

The implementation code for simulating the wormhole attack is provided in **Appendix C**, detailing the simulation setup and parameters used to create the wormhole scenario within the network.

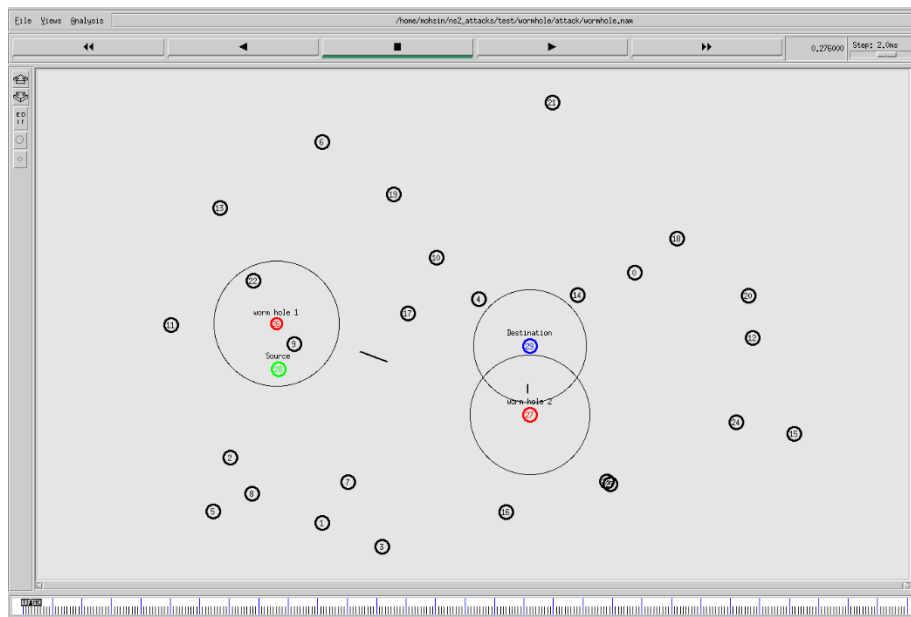


Figure 3.6: Wormhole Attack

3.2.5 Detection and Mitigation Mechanism

To counter the effects of the wormhole attack, the IDSAODV protocol was modified to include a detection and mitigation mechanism. This mechanism analyzes various parameters during the route discovery to identify suspicious behavior. The first aspect monitored is the hop count in the RREP messages. Under normal conditions, the hop count should reflect the legitimate intermediate nodes between the source and destination. Suppose the hop count is significantly lower than expected. In that case, it raises suspicion, as this may indicate that a wormhole artificially reduces the hop count by bypassing legitimate nodes through its tunnel.

In addition to hop count monitoring, the delay between the RREQ and RREP is also measured. Usually, the delay corresponds to the time taken for the request to propagate through multiple hops. However, when a wormhole is present, the delay may be unusually short, as the malicious nodes are tunneling the RREQ directly to their partner node, bypassing several legitimate hops. An unusually short delay serves as another indicator of a wormhole attack.

3.2.5.1 Flowchart of IDSAODV

The entire wormhole detection and mitigation process is depicted in the flowchart provided in Figure 3.7. This flowchart outlines the sequence of events within the IDSAODV protocol, from the initial route discovery process to monitoring anomalies such as abnormal hop counts, short delays, and inconsistent sequence numbers. The flowchart also details the steps taken once a wormhole is detected, including broadcasting the RERR message, excluding the wormhole nodes from routing tables, and re-establishing secure routes. This diagram is a crucial component of the methodology, visually representing the protocol's decision-making process and demonstrating how the network maintains secure communication even during a wormhole attack.

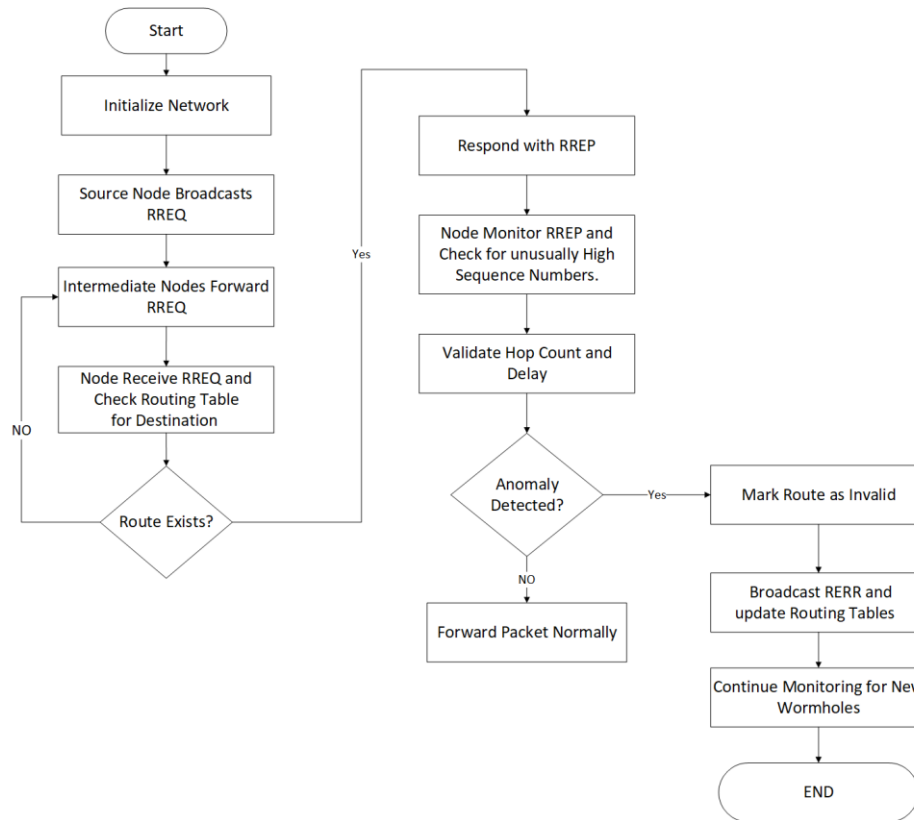


Figure 3.7: Flowchart of IDSAODV Protocol

The protocol also monitors the sequence numbers in RREP messages. Wormhole nodes may attempt to manipulate sequence numbers to make their route appear fresher or more reliable than others. By comparing the sequence numbers with expected values, the protocol can detect inconsistencies that signal potential manipulation by the wormhole nodes.

Upon detecting these anomalies, the protocol flags the route as compromised. The next step involves broadcasting a RERR message to inform neighboring nodes about the wormhole and prevent the compromised route from being used in future route discoveries. The network's routing tables are updated to exclude the wormhole nodes from subsequent communications, ensuring that data is routed through legitimate paths. Figure 3.8 illustrates the network after the wormhole attack has been detected and mitigated, showing how the protocol isolates the malicious nodes and reroutes traffic through secure paths.

The implementation code for detecting and mitigating the wormhole attack is provided in **Appendix D**. This appendix contains detailed code scripts and configurations used to model the

detection mechanism and its response within the network simulation.

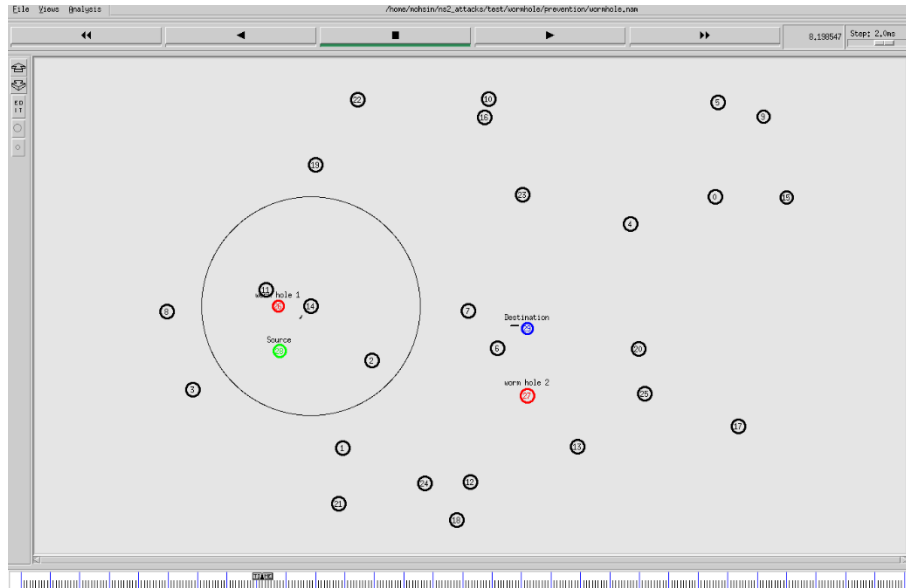


Figure 3. 8:Detection and Mitigation of Wormhole

The effectiveness of the wormhole detection and mitigation mechanism was evaluated by observing the network's behavior across three distinct phases: during regular operation, under wormhole attack, and after applying the mitigation strategy. The goal was to assess how the network responded to the wormhole attack and how quickly and effectively it recovered after the malicious nodes were identified and isolated. This evaluation provided insights into the robustness of the IDSAODV protocol in securing the network against wormhole attacks and ensuring that communication could continue even under threat.

Summary

In chapter 3, I investigated the blackhole and wormhole attacks and proposed detection and mitigation strategies to address these threats. Using the NS-2.35 simulator on Ubuntu 22.04, I modeled realistic MANET scenarios with varying node densities to study network behavior under normal conditions, during attacks, and after mitigation.

For blackhole attacks, the AOMDV routing protocol was enhanced to detect malicious nodes using sequence number analysis and route monitoring. Suspicious nodes were excluded from routing processes, and AOMDV's multipath capabilities ensured secure communication through alternative routes. For wormhole attacks, the IDSAODV protocol was modified to monitor

hop count abnormalities, sequence number inconsistencies, and delays in route replies. Detected wormhole nodes were isolated, and secure routes were re-established.

Throughout the chapter, I evaluated the protocols based on key performance metrics, such as packet delivery ratio, throughput, and packet loss, to demonstrate their effectiveness. These strategies successfully mitigated the attacks, restoring reliable and secure communication within the network.

Chapter 4: Data Analysis and Results

4. Results

4.1 Results for Blackhole Attack

This chapter analyzes network behavior under normal conditions, during a blackhole attack, and after applying a detection and mitigation mechanism. A MANET is highly vulnerable to various security threats due to its decentralized nature, dynamic topology, and limited resources. Among these threats, the blackhole attack is one of the most severe, leading to significant packet loss, degraded throughput, and reduced packet delivery ratios. This chapter provides an in-depth evaluation of how the proposed detection mechanism influences network performance under varying conditions.

The evaluation was conducted using NS-2.35, a widely used network simulator, which accurately models packet transmission, node mobility, and routing protocol behavior. The results were obtained through simulations under three distinct network conditions: normal operation, blackhole attack, and detection/mitigation. They were analyzed based on three critical performance metrics: packet delivery ratio, throughput, and packet loss. These metrics offer a holistic understanding of how effectively the detection and mitigation mechanism restores network integrity.

4.1.1 Data Collection

To thoroughly evaluate the impact of blackhole attacks and the proposed solution, two distinct simulation scenarios were designed:

Scenario 1: Consisted of 11 nodes operating over a 30-second simulation duration.

Scenario 2: Comprised of 20 nodes with a simulation time of 30 seconds.

For each scenario, three simulation scripts were developed:

Normal Network Script: This script was created to simulate a MANET operating without malicious interference, providing a baseline for performance measurement. It represented a typical network scenario where nodes establish and maintain routes using the AODV routing protocol.

Blackhole Attack Script: A blackhole node was introduced to simulate an attack scenario in this script. The blackhole node falsely claimed to have the shortest route to the destination, intercepting and dropping packets, causing a substantial degradation in network performance.

Detection and Mitigation Script: This script included the modified AOMDV protocol to

identify and circumvent the blackhole node. The protocol detects anomalies in sequence numbers, hop counts, and timing of RREPs (Route Reply messages) to mark suspicious nodes as potential black holes and update routing tables accordingly.

Data was collected using a sink agent configured to monitor incoming and outgoing packets at the destination node. The sink agent captured detailed metrics, including total packets received, sent, and bytes transmitted. These metrics were logged into three separate files corresponding to the standard network, attack scenario, and post-detection/prevention scenario. Each log file contained time-stamped entries to enable precise network behavior analysis over time.

The collected data was averaged across multiple tests runs to minimize variability and ensure statistical accuracy. Multiple runs also provided insights into the consistency of the detection mechanism's performance, further validating the results.

4.1.2 Data Analysis

A systematic approach was followed to analyze the collected network metrics. First, the data obtained from the simulations were processed to calculate values for PDR, throughput, and packet loss over the simulation period for each scenario. This involved aggregating the recorded values across multiple test runs to ensure statistical accuracy and reliability.

The data was further examined through trend analysis to interpret network behavior visually under varying conditions. Using Excel, line graphs were plotted for each scenario, displaying how PDR, throughput, and packet loss changed with time. This visual representation allowed for a more intuitive comparison of network performance during regular operation, under attack, and after detection and mitigation.

This comprehensive approach enabled a clearer understanding of the network's response to blackhole attacks and the relative effectiveness of the proposed detection and mitigation mechanism.

4.1.2.1 Packet Delivery Ratio (PDR)

The average PDR remained above 74% in the normal network, reflecting effective packet delivery. This high PDR is due to the dynamic establishment of routes between the source and destination nodes without interference. However, when the blackhole attack was introduced, the PDR dropped sharply to 0%, as the malicious node intercepted and discarded packets. This steep decline underscores the network's vulnerability to blackhole attacks and the need for a robust

detection mechanism.

After implementing the detection and mitigation mechanism, the PDR improved significantly, reaching 100% in both scenarios. This restoration indicates the success of the detection mechanism in identifying and avoiding the blackhole node, ensuring optimal packet delivery.

The formula for the PDR:

$$1. \text{ PDR} = \left(\frac{\sum \text{No of packets received}}{\text{No of Packets sent}} \right) \times 100$$

- **Results for 11 Nodes Scenario**

The initial set of simulations was performed with 11 nodes operating over a 30-second simulation duration. This scenario represents a small-scale MANET environment, where nodes frequently exchange routing information, making it susceptible to blackhole attacks. Figure 4.1 depict a graph comparing PDR across the three network states in the 11-node scenario.

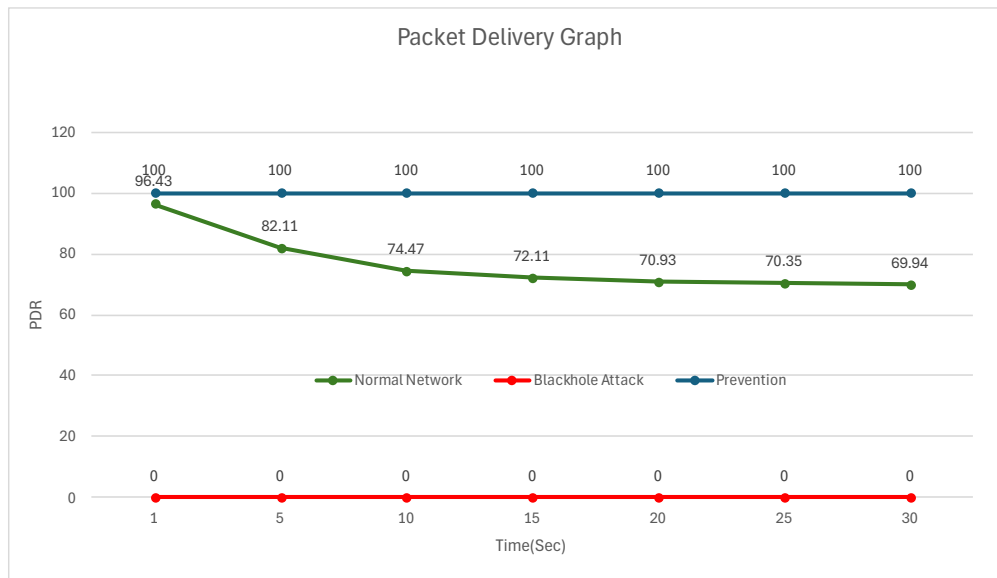


Figure 4.1: PDR of 11 Nodes Network

- **Results for 20 Nodes Scenario**

The second set of simulations was performed with 20 nodes over a 30-second simulation duration. Figure 4.2 presents a graph comparing PDR across the three network conditions in the 20-node scenario.

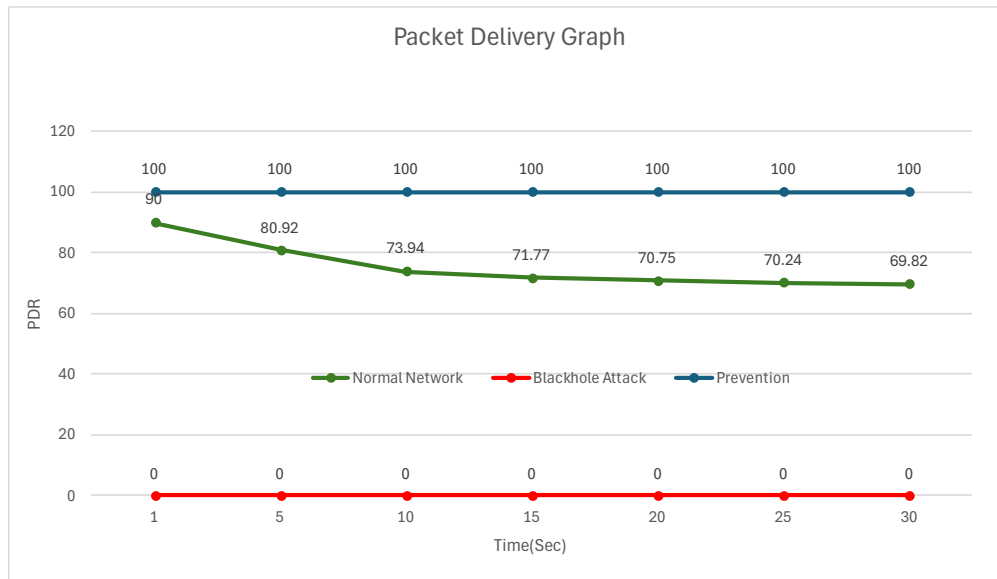


Figure 4.2: PDR of 20 Nodes Network

4.1.2.2 Throughput

In the normal network, throughput was stable, averaging around 233-234 kbps, indicating that the network efficiently transmitted data using available bandwidth. During the blackhole attack, throughput dropped drastically to kbps. This sharp drop occurred because the malicious node intercepted and discarded packets, disrupting the normal data flow.

The detection and mitigation mechanism significantly improved throughput to approximately 344.6 kbps in the 11-node scenario and 338 kbps in the 20-node scenario. This increase nearly restored the original performance levels observed in the normal network, demonstrating the robustness of the detection mechanism even under challenging conditions.

The formula for the Throughput:

$$2. \text{ Throughput (Kbps)} = \frac{\sum \text{No of bytes received} \times 8}{\text{Time} \times 1000}$$

- **Results for 11 Nodes Scenario**

The initial set of simulations was performed with 11 nodes operating over a 30-second simulation duration. Figure 4.3 provides a line graph illustrating the throughput trends across the three network states in the 11-node scenario.

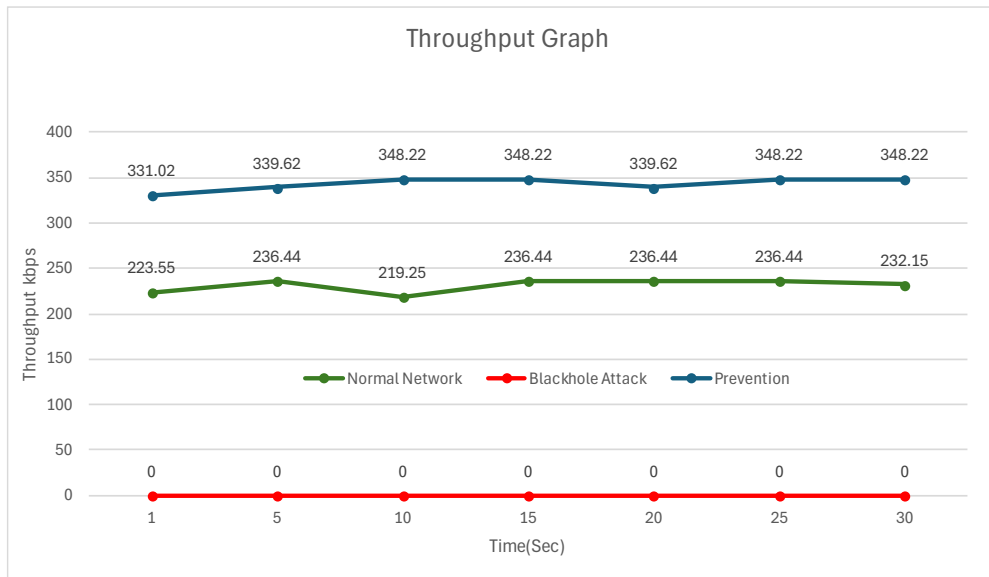


Figure 4.3: Throughput of 11 Nodes Network

- Results for 20 Nodes Scenario**

The second set of simulations was performed with 20 nodes over a 30-second simulation duration. Figure 4.4 will present a line graph comparing throughput across the three network conditions in the 20-node scenario.

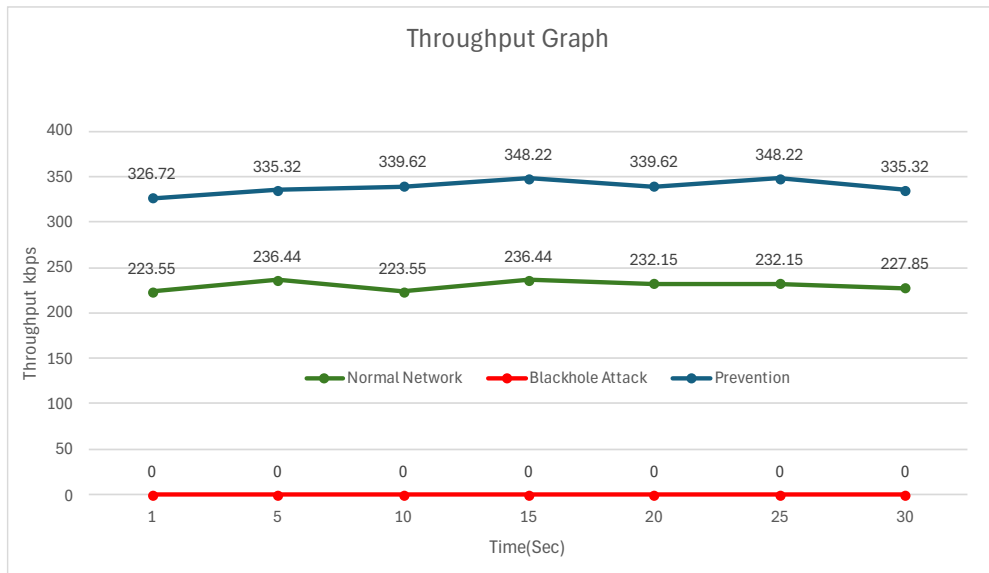


Figure 4.4: Throughput of 20 Nodes Network

4.1.2.3 Packet Loss

In the normal network, packet loss averaged around 24-25%, reflecting efficient data transmission. During the blackhole attack, packet loss surged to 100%, as the malicious node dropped all intercepted packets to disrupt communication. This significant increase in packet loss highlights the severe impact of blackhole attacks on MANETs.

After implementing the detection and mitigation mechanism, packet loss was effectively reduced to 0% in both scenarios, indicating successful attack mitigation. The mechanism managed to significantly lower packet loss, enhancing overall network reliability.

The formula for the Packet loss:

$$\text{Packet Loss Ratio} = \left(\frac{\sum \text{No of Packets lost}}{\text{No of Packets sent}} \right) \times 100$$

- **Results for 11 Nodes Scenario**

The initial set of simulations was performed with 11 nodes operating over a 30-second simulation duration. Figure 4.5 presents a line graph comparing packet loss across the three network conditions in the 11-node scenario.

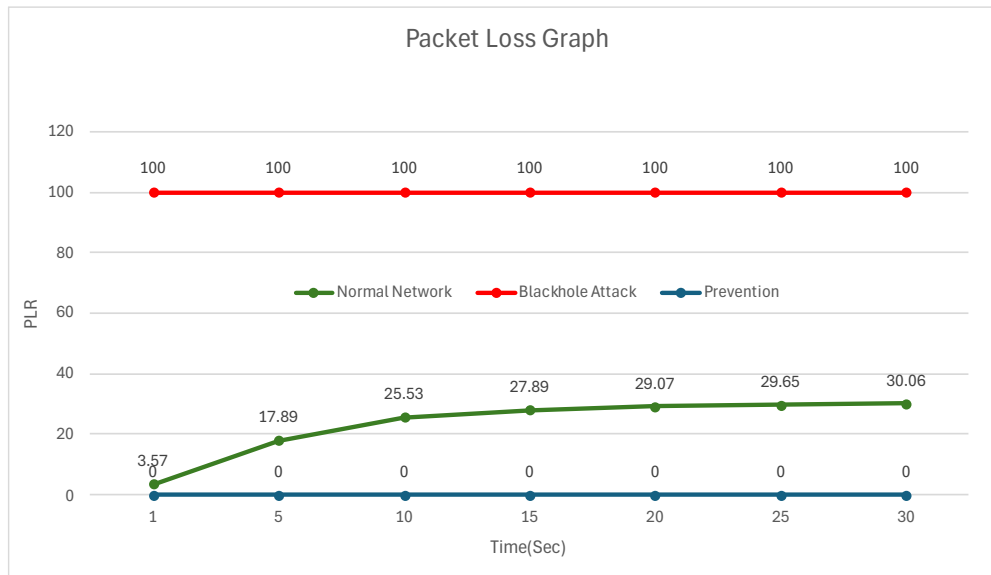


Figure 4.5: Packet Loss of 11 Nodes Network

- **Results for 20 Nodes Scenario**

The second set of simulations was performed with 20 nodes over a 30-second

simulation duration. Figure 4.6 displays a graph comparing packet loss across the three network conditions in the 20-node scenario.

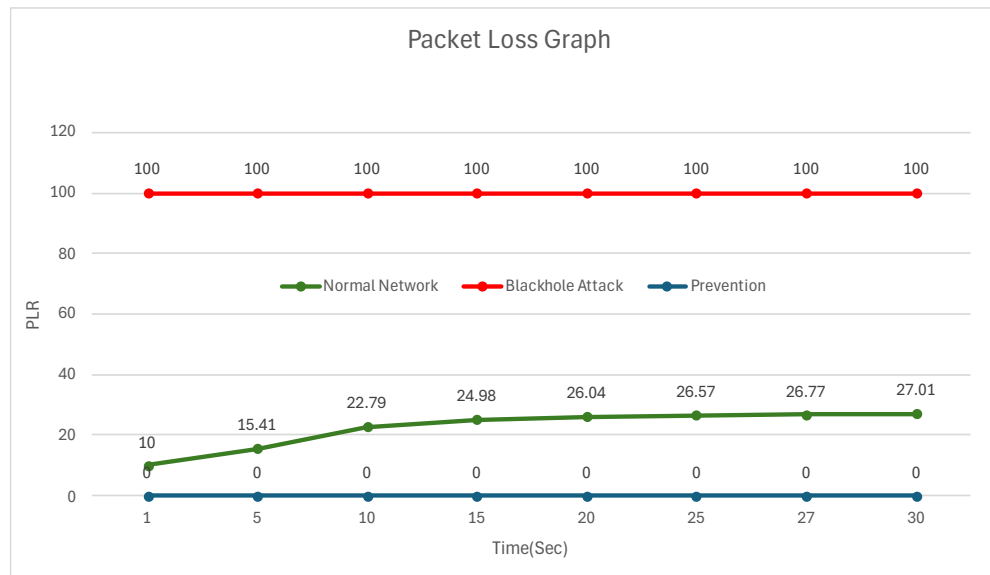


Figure 4.6: Packet Loss of 20 Nodes Network

4.1.3 Comparative Analysis Across Both Scenarios

The results across both scenarios showed consistent patterns:

PDR and throughput were high in the normal network environment, reflecting efficient communication with minimal packet loss, indicating smooth network performance without interference.

During the blackhole attack, these metrics plummeted: PDR dropped to zero, throughput was reduced to zero, and packet loss reached 100%. This significant degradation highlighted the disruptive impact of the blackhole attack on the MANET.

Implementing the detection and mitigation mechanism successfully mitigated the attack's impact, as seen in improved PDR and throughput metrics and reduced packet loss.

These consistent results across the 11-node/30-second and 20-node/30-second scenarios demonstrate the scalability and robustness of the proposed detection mechanism.

Visual representations of the results were created, using graphs to compare network behavior in the normal state, under attack, and following detection and mitigation, providing a

clear understanding of network stability across these conditions.

4.1.3.1 Average Throughput

Figure 4.7 presents a combined bar graph showing average throughput across the normal network, blackhole attack, and detection/mitigation in the 11-node and 20-node scenarios.

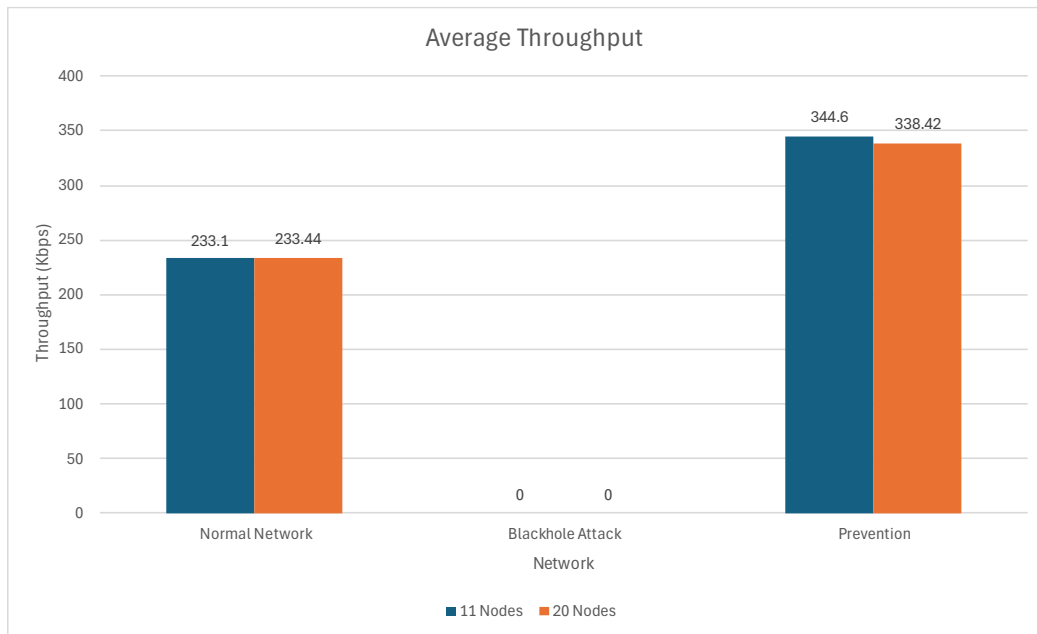


Figure 4.7: Average Throughput

4.1.3.2 Average PDR

Figure 4.8 shows a bar graph for average PDR trends across the three network states in the 11-node and 20-node scenarios. The graph highlights the severe drop in PDR during the attack, followed by a noticeable recovery once the detection mechanism is implemented.

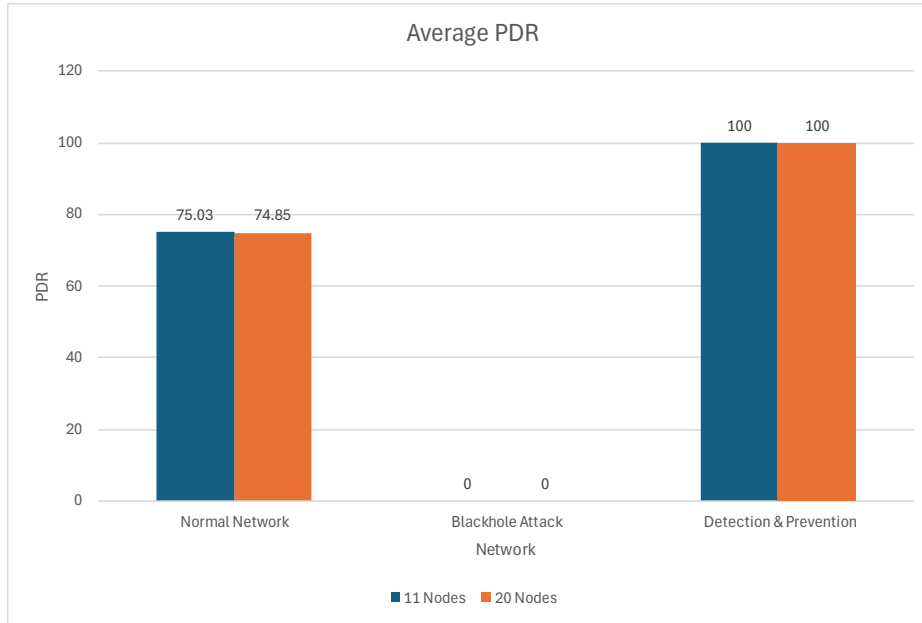


Figure 4.8: Average Packet Delivery Ratio

4.1.3.3 Average Packet Loss

Figure 4.9 presents average packet loss trends in the 11-node and 20-node scenarios, showing minimal packet loss in the normal network, a steep increase during the attack, and a significant reduction after detection. These graphical representations provide a comprehensive view of how the network performs under different conditions.

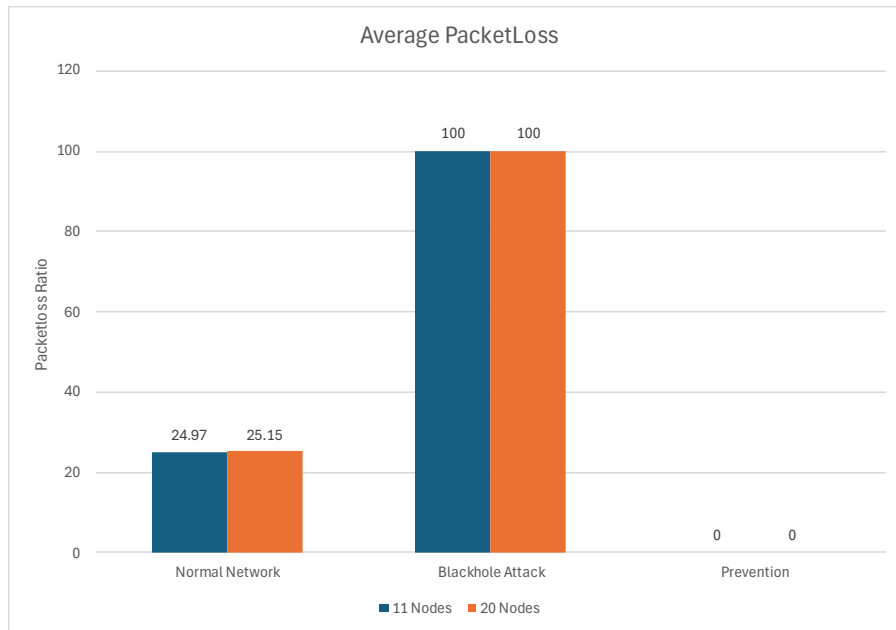


Figure 4.9: Average Packet Loss

4.2 Results for Wormhole Attack

This section explores the network behavior under normal conditions, during a wormhole attack, and after applying the IDSADOV detection and mitigation mechanism. Unlike blackhole attacks, wormhole attacks involve two colluding nodes, creating a direct communication tunnel that misleads the routing protocol by offering seemingly shorter paths. This chapter delves into how this deceptive routing impacts network performance and how IDSADOV mitigates the effects.

The analysis was performed using NS-2.35, a simulator known for accurately modeling packet transmission, node mobility, and routing protocol behavior. The evaluation focused on three key metrics—packet delivery ratio, throughput, and packet loss—across different network states. The simulations were conducted in two scenarios: one with 25 nodes and another with 30 nodes for 30 seconds. The collected metrics provide a comprehensive understanding of the IDSADOV mechanism’s effectiveness in detecting and mitigating wormhole attacks.

4.2.1 Data Collection

To thoroughly evaluate the impact of wormhole attacks and the proposed IDSADOV solution, two distinct simulation scenarios were developed:

Scenario 1: Consisting of 25 nodes over a 30-second simulation duration.

Scenario 2: Consisting of 30 nodes over the same 30-second duration.

For each scenario, three simulation scripts were implemented:

Normal Network Script: This script simulated a typical MANET operation using the AODV routing protocol without malicious interference. It served as a baseline to measure network performance under ideal conditions.

Wormhole Attack Script: This script introduced two colluding nodes that established a direct tunnel, creating false routes that attracted data packets through the tunnel, enhancing packet delivery ratio and throughput while minimizing packet loss.

Detection and Mitigation Script: This script incorporated the IDSADOV mechanism, designed to detect and mitigate the effects of wormhole attacks. IDSADOV identifies anomalies in route establishment, hop counts, and timing of route replies to flag suspicious nodes involved in tunneling and reroute data to maintain network integrity.

Data was collected using a sink agent at the destination node, configured to monitor incoming and outgoing packets. Metrics such as total packets sent, total packets received, and total bytes transmitted were recorded in three separate log files for normal network, wormhole attack, and detection/mitigation scenarios. The collected data was averaged across multiple simulation runs to ensure statistical accuracy and minimize variability.

4.2.2 Data Analysis

A systematic approach was adopted to analyze the collected network metrics. The data obtained from the simulations were processed to calculate PDR, throughput, and packet loss for each scenario. This process aggregated recorded values across multiple test runs to ensure statistical accuracy and reliability.

The data was further examined through trend analysis to interpret network behavior visually under varying conditions. Using Excel, line graphs were plotted for each scenario, displaying how PDR, throughput, and packet loss evolved. This graphical representation allowed for an intuitive comparison of network performance during normal operation, under wormhole attack, and after applying the IDSADOV mechanism.

This comprehensive approach provided a clearer understanding of the network's response to wormhole attacks and the effectiveness of the IDSADOV detection and mitigation mechanism.

4.2.2.1 Packet Delivery Ratio (PDR)

The average PDR remained above 90% in the normal network, reflecting optimal packet delivery. The high PDR was attributed to efficient routing protocols, which dynamically established routes between source and destination nodes without interference. However, the introduction of the wormhole attack caused the PDR to increase to 100% deceptively, as the tunnel path provided a direct route for packet delivery. This increase demonstrates how wormhole attacks exploit routing protocols to create false shortcuts, misleading nodes into higher packet delivery.

After implementing the IDSADOV mechanism, the PDR decreased slightly to around 93%. The reduction indicates successful detection of the wormhole tunneling effect, as the mechanism rerouted packets to avoid colluding nodes.

Formula for PDR:

$$PDR = \left(\frac{\sum \text{No of packets received}}{\text{No of Packets sent}} \right) \times 100$$

- **Results for 25 Nodes Scenario:**

The initial simulations were conducted with 25 nodes. Figure 4.10 presents a graph comparing PDR across the three network states in this scenario.

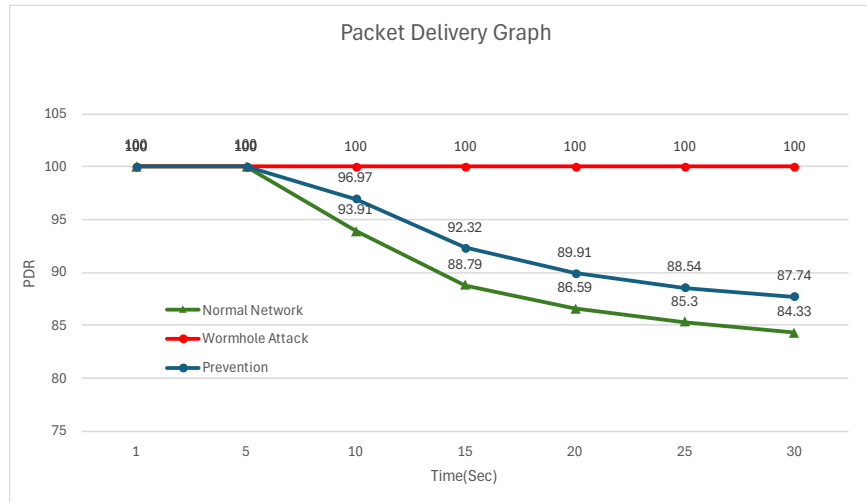


Figure 4.10: PDR of 25 Nodes Network

- **Results for 30 Nodes Scenario:**

The second set of simulations involved 30 nodes over a 30-second duration. Figure 4.11

shows a graph comparing PDR across the three network conditions in this scenario.

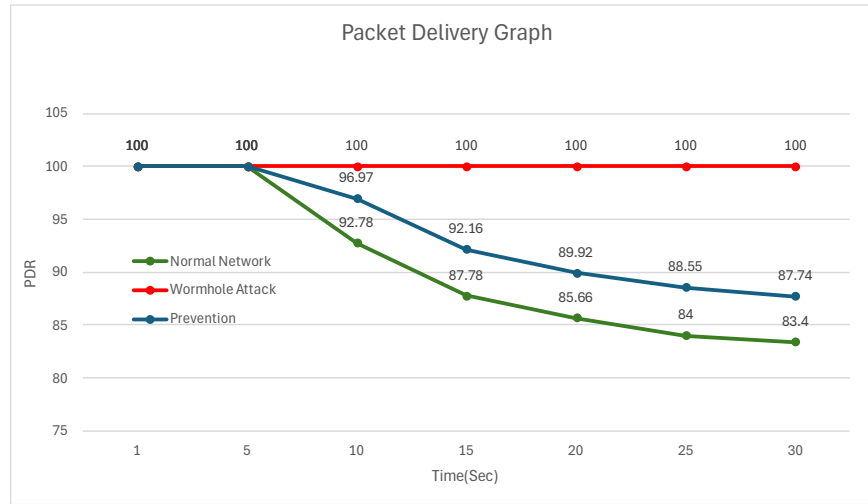


Figure 4.11: PDR of 30 Nodes Network

4.2.2.2 Throughput

In the regular network, throughput remained stable, averaging around 411-416 kbps. This high throughput indicates that the network efficiently transmitted data, utilizing available bandwidth effectively. During the wormhole attack, throughput increased significantly to around 518 kbps as packets were tunneled directly between colluding nodes, reducing route length and boosting transmission speed.

The IDSADOV mechanism, once activated, reduced throughput slightly to approximately 433 kbps. Compared to the wormhole attack state, this reduction demonstrates the mechanism's success in redirecting packets away from malicious paths, partially restoring normal throughput levels.

Formula for Throughput:

$$\text{Throughput (Kbps)} = \frac{\sum \text{No of bytes received} \times 8}{\text{Time} \times 1000}$$

- **Results for 25 Nodes Scenario:**

The initial simulations were conducted with 25 nodes operating over a 30-second duration. Figure 4.12 provides a line graph illustrating throughput trends across the three network states in

this scenario.

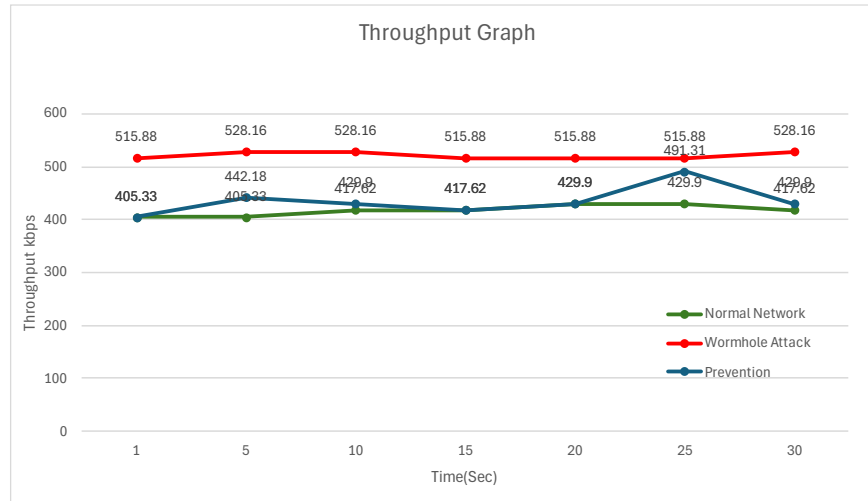


Figure 4.12: Throughput of 25 Nodes Network

- Results for 30 Nodes Scenario:**

The second set of simulations involved 30 nodes over a 30-second duration. Figure 4.13 shows a line graph comparing throughput across the three network conditions.

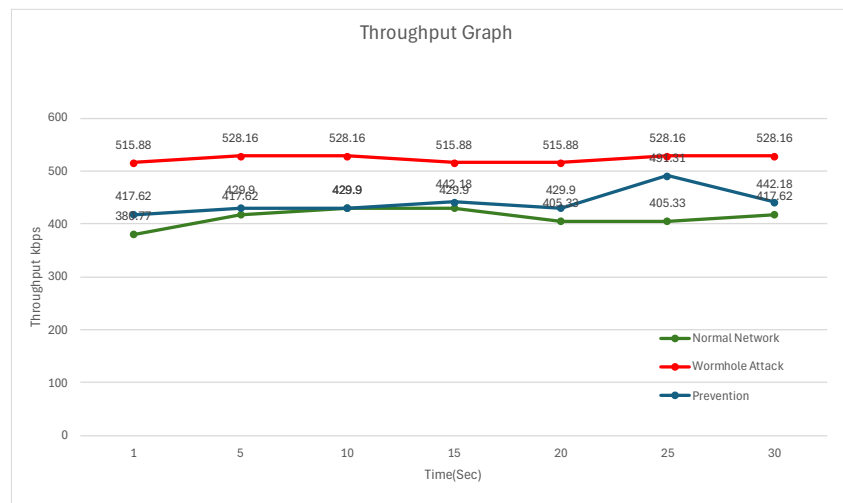


Figure 4.13: Throughput of 30 Nodes Network

4.2.2.3 Packet Loss

In the normal network, packet loss averaged around 8-9%, indicating efficient data transmission. However, during the wormhole attack, packet loss dropped dramatically to nearly zero, as the tunneled path allowed packets to reach their destination without being dropped. This

sharp decline in packet loss highlights the deceptive nature of wormhole attacks, where malicious nodes appear to improve network performance.

The IDSADOV mechanism effectively increased packet loss to approximately 6.5%, successfully mitigating the tunneling effect. The slight increase in packet loss is an acceptable trade-off necessary to maintain network integrity by rerouting packets away from colluding nodes.

The formula for Packet Loss:

$$\text{Packet Loss Ratio} = \left(\frac{\sum \text{No of Packets lost}}{\text{No of Packets sent}} \right) \times 100$$

- Results for 25 Nodes Scenario:**

The initial set of simulations involved 25 nodes over a 30-second duration. Figure 4.14 presents a line graph comparing packet loss across the three network conditions in this scenario.

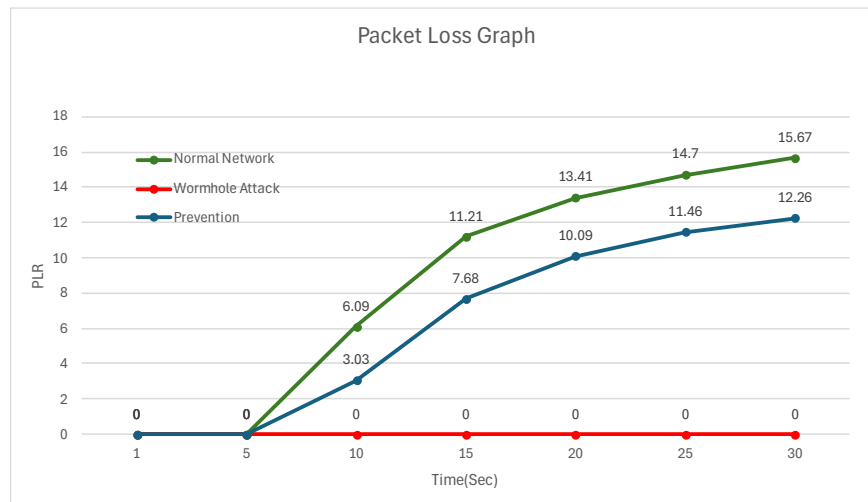


Figure 4.14: Packet Loss of 25 Nodes Network

- Results for 30 Nodes Scenario:**

The second set of simulations was conducted with 30 nodes over a 30-second. Figure 4.15 displays a graph comparing packet loss across the three network states.

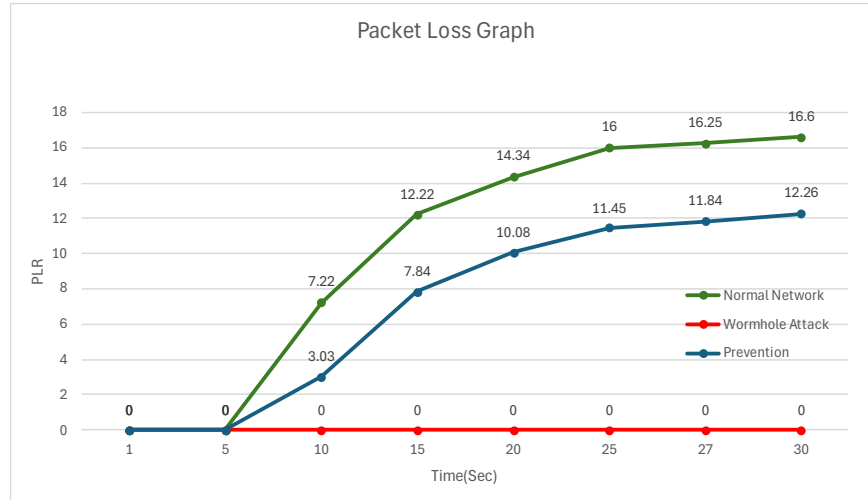


Figure 4.15: Packet Loss of 30 Nodes Network

4.2.3 Comparative Analysis Across Both Scenarios

The results across both scenarios exhibited consistent patterns, revealing the distinctive impact of wormhole attacks and the effectiveness of the IDSADOV detection and mitigation mechanism: PDR and throughput remained high in the normal network environment while packet loss was low, indicating smooth network performance without interference.

During the wormhole attack, the metrics showed an unusual improvement compared to the normal network. PDR increased to 100%, throughput rose to around 518 kbps, and packet loss nearly vanished, dropping to 0%. This enhancement reflects the deceptive nature of wormhole attacks, where colluding nodes create a false tunnel that misleads the routing protocol, resulting in a temporary boost in network performance.

Implementing the IDSADOV mechanism successfully mitigated the impact of the wormhole attack. PDR was restored to approximately 93%, throughput returned to around 433 kbps, and packet loss rose slightly to around 6.5%. These results indicate that the IDSADOV mechanism effectively detected and rerouted traffic from the malicious tunnel, restoring network integrity.

These consistent outcomes across the 25-node/30-second and 30-node/30-second scenarios confirm the scalability and robustness of the IDSADOV mechanism in detecting and mitigating wormhole attacks. The mechanism demonstrates its capability to maintain network performance even in larger, more dynamic setups.

Visual representations of the results were created using graphs to compare network behavior in the

normal state, under wormhole attack, and following detection and mitigation. These visual aids provide a clear understanding of how the network reacts to wormhole attacks and the subsequent restoration of normal operation, further reinforcing IDSADOV's effectiveness.

4.2.3.1 Average Throughput

Figure 4.16 presents a bar graph illustrating throughput trends across the regular network, wormhole attack, and detection/mitigation scenarios in the 20-node and 30-node cases. The graph confirms a noticeable increase in throughput during the attack, followed by consistent recovery after the IDSADOV mechanism is applied. This demonstrates that the detection mechanism can effectively adapt to larger network scales and restore throughput to near-normal levels.

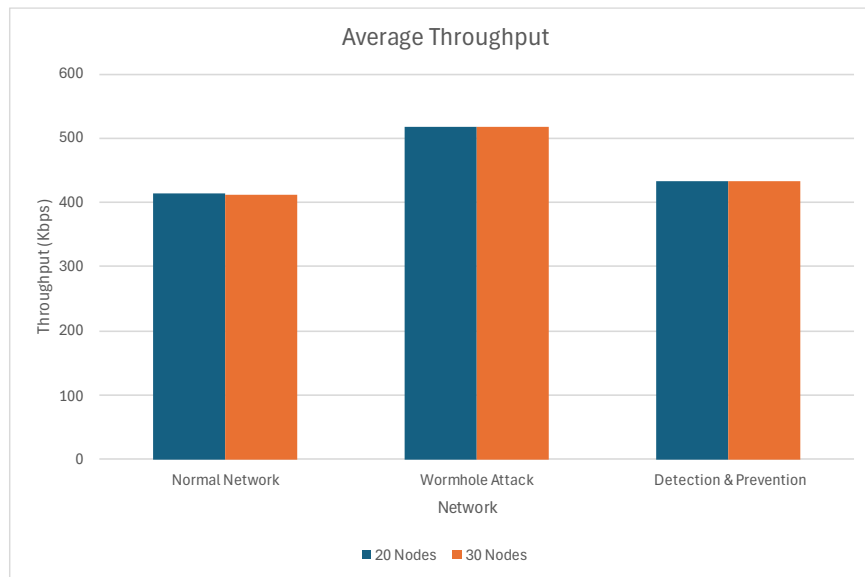


Figure 4.16: Average Throughput

4.2.3.2 Average PDR

Figure 4.17 shows a graph of PDR trends across the three network states in the 25-node and 30-node scenarios. The graph highlights the deceptive increase in PDR during the wormhole attack, followed by a noticeable stabilization of PDR once the IDSADOV mechanism is implemented, confirming its success in detecting and mitigating the attack.

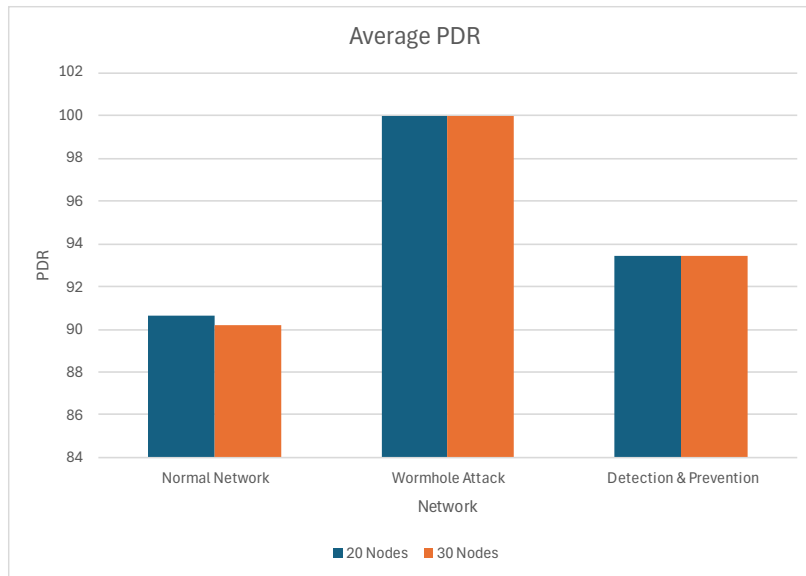


Figure 4.17: Average Packet Delivery Ratio

4.2.3.3 Average Packet Loss

Figure 4.18 presents packet loss trends across the 25-node and 30-node scenarios, showing minimal packet loss in the standard network, a dramatic decrease during the wormhole attack, and a moderate increase after applying the IDSADOV mechanism. These graphical representations provide a comprehensive view of network performance under different conditions, emphasizing the effectiveness of the IDSADOV mechanism in both small and large network setups.

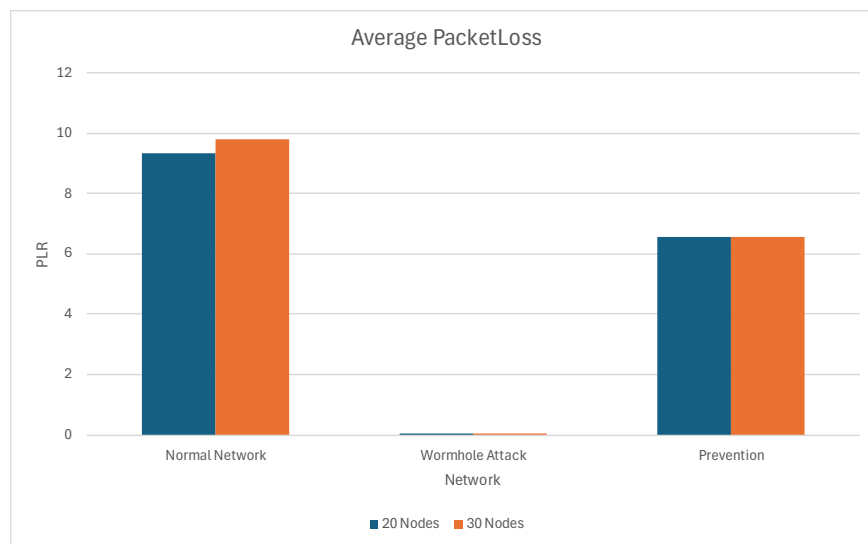


Figure 4.18: Average Packet Loss

4.3 Comparison and Discussion

Evaluating the performance of network security mechanisms is critical for understanding their effectiveness, particularly in dynamic and vulnerable environments like IoT networks. The comparative analysis in this section aims to offer a clear understanding of how the proposed detection and mitigation mechanisms perform against two significant types of attacks: blackhole and wormhole. We can identify our approach's strengths, weaknesses, and overall reliability in real-world scenarios by assessing key performance metrics.

The results from our proposed mechanisms are compared with those reported in existing studies. The comparison is organized into two segments: blackhole and wormhole attacks. For each attack type, we include comparative tables that illustrate how our solution performs relative to existing approaches across the specified metrics.

This analysis aims to demonstrate not only the improvements achieved by our approach but also to provide insights into the underlying strategies that contribute to better network performance. This comprehensive evaluation highlights how integrating advanced detection algorithms, multipath routing, and rapid response protocols can enhance network stability, minimize disruption, and sustain efficient communication, even in hostile environments.

4.3.1 Comparison of Blackhole Attack

The blackhole attack is known for its severe impact on network performance, causing drastic reductions in throughput and PDR while significantly increasing packet loss. In existing studies, throughput typically declines sharply during a blackhole attack, as the malicious node intercepts and discards packets instead of forwarding them. This results in significant communication disruptions. However, the proposed detection mechanism substantially improves throughput once the blackhole node is identified and isolated. By employing rapid detection and multipath routing, the network effectively reroutes data around the malicious node, achieving higher throughput than conventional methods.

Table 4.1 highlights a comparative analysis of the proposed method against three existing studies, focusing on blackhole attack mitigation in MANETs. While all approaches successfully mitigated the attack, the table emphasizes differences in their effectiveness across key performance metrics such as throughput, packet loss, and packet delivery ratio.

Table 4.1: Comparison of Blackhole Attack Mitigation Mechanism with Existing Work

Source	Routing Attack	Mitigation	Throughput (Kbps)	Packet loss (%)	PDR (%)
Proposed Method	Black Hole	Y	344	0	100
[24]	Blackhole	Y	281	15	85
[23]	Blackhole	Y	325	2	98
[2]	Blackhole	Y	350	1.79	98.21

4.3.2 Comparison of Wormhole Attack

The wormhole attack is a sophisticated network-layer threat that manipulates routing by creating a tunnel between two malicious colluding nodes, which misleads legitimate nodes into routing data through the tunnel. This comparison evaluates the performance of the proposed detection and mitigation mechanism against existing methods, focusing on three key metrics: throughput, packet delivery ratio, and packet loss under wormhole attack conditions.

Table 4.2 presents a comparison of the proposed method with several existing approaches for mitigating wormhole attacks in MANETs. The results emphasize the variability in the effectiveness of different strategies concerning throughput, packet loss, and packet delivery ratio.

Table 4.2: Comparison of Wormhole Attack Mitigation Mechanism with Existing Work

Source	Routing Attack	Mitigation	Throughput (Kbps)	Packet loss	PDR
Proposed Method	Wormhole	Y	433.58	6.55	93.45
[25]	Wormhole	Y	203.6	34.6	65.4
[9]	Wormhole	Y	N/A	25	75
[27]	wormhole	Y	158	N/A	0.16
[8]	Wormhole	Y	83.34	14	86

Summary

Chapter 4 extensively evaluates the network's behavior under blackhole and wormhole attacks, followed by implementing detection and mitigation mechanisms to counter these threats. The chapter highlights the vulnerability of MANETs to security breaches due to their decentralized

nature and dynamic topology. The analysis was carried out using the NS-2.35 simulator, allowing accurate network behavior modeling across normal, attack, and post-mitigation conditions.

The study explored two significant attacks, blackhole, and wormhole, and assessed the network performance based on three key metrics: PDR, Throughput, and Packet Loss. The results demonstrate a significant degradation in network performance during attacks, marked by a sharp decline in throughput and PDR and a substantial increase in packet loss. However, the proposed detection mechanisms for blackhole and wormhole attacks successfully mitigated these effects, leading to marked improvements in network stability and data delivery.

The proposed mechanism restored the PDR to 100% for the blackhole attack, significantly improving throughput to levels comparable to normal network conditions while reducing packet loss to 0%. The mitigation of the wormhole attack also yielded positive results, with the PDR stabilizing at around 93%, throughput recovering to 433.58 Kbps, and packet loss controlled at approximately 6.5%. The results confirmed that the proposed solutions could effectively maintain network integrity and performance across different attack scenarios, demonstrating robustness and scalability.

The comparative analysis further validated the effectiveness of the proposed mechanisms against existing studies. The proposed approach outperformed traditional methods regarding higher throughput, better PDR, and lower packet loss across both attack types. Visual graphs and comparative tables provided a comprehensive understanding of network performance under different conditions, reinforcing the practical applicability of the proposed detection and mitigation strategies.

Chapter 5: Conclusion and Future Work

5.1 Conclusion

The rapid growth of IoT networks across various sectors, such as healthcare, smart homes, and industrial automation, has created new opportunities and efficiencies. However, this growth also introduces significant security challenges, particularly at the network layer, where malicious attacks can severely disrupt communication and data integrity. This research specifically focused on two prominent attacks, namely blackhole and wormhole attacks, both of which target the routing mechanisms in IoT networks. These attacks can compromise the core communication processes, leading to substantial packet loss, reduced throughput, and degraded network reliability.

Blackhole attacks are one of the most damaging threats in IoT networks. These attacks involve malicious nodes falsely advertising themselves as having the best route to the destination, only to drop all received packets, disrupting everyday network communication and resulting in significant packet loss. This deceptive behavior leads to a drop in PDR, and compromises throughput. Similarly, wormhole attacks involve colluding malicious nodes and establishing a direct tunnel between each other, which misleads the routing protocol by creating a shortcut in the network. This results in the misdirection of packets and increased vulnerability to further attacks, such as replay or selective forwarding.

Given these security challenges, this research focused on developing effective mitigation strategies that enhance the resilience of IoT networks against these attacks. The study aimed to improve existing routing protocols by integrating enhanced detection and mitigation mechanisms, specifically targeting AOMDV and IDSADOV protocols. By leveraging multipath routing and anomaly detection, these protocols were designed to detect, isolate, and prevent malicious activities that compromise network integrity. The modified AOMDV protocol introduced a proactive detection mechanism that constantly monitors routing behaviors. At the same time, IDSADOV was designed to identify unusual patterns indicative of attacks, such as abnormal sequence numbers, hop counts, or timing discrepancies in route replies.

The methodology involved an extensive simulation using NS-2.35, a widely used network simulation tool, to model the behavior of IoT networks under different scenarios, including normal operation, under blackhole attacks, wormhole attacks, and after the implementation of the proposed mitigation mechanisms. The simulation parameters were carefully configured to

accurately represent IoT network behavior, considering node mobility, packet transmission, and dynamic routing factors. The evaluation was conducted across key performance metrics, including packet delivery ratio, throughput, and packet loss, to comprehensively assess the proposed solutions.

The simulation results revealed significant improvements in network performance when the enhanced protocols were employed. In the blackhole attack scenario, the PDR dropped to nearly 0% due to the malicious node dropping all received packets, confirming the attack's severe impact on network performance. However, after deploying the enhanced AOMDV protocol, the PDR improved drastically, reaching nearly 100% in most test cases. This substantial recovery indicates the success of the detection mechanism in accurately identifying and isolating blackhole nodes, thus mitigating further packet loss. The throughput, which had plummeted during the attack phase, was also restored to levels comparable to normal network operations, ensuring sustained communication.

Similarly, in the wormhole attack scenario, the colluding nodes created a deceptive tunnel that initially improved PDR and throughput by shortening the route. However, this deceptive advantage was mitigated once the IDSADOV mechanism was implemented. The IDSADOV protocol detected abnormal tunneling behavior by analyzing hop count anomalies and timing inconsistencies in route establishment. As a result, the PDR was adjusted to more realistic levels, averaging around 93%, which aligns with normal network conditions after the attack was mitigated. This adaptive response ensured reliable packet delivery and reduced the potential for further exploitation, such as replay attacks or selective forwarding. Additionally, the throughput was stabilized, maintaining consistent data transmission across the network. The protocols introduced some computational overhead, which was expected given the complexity of real-time attack detection and route recalculation.

This study contributes significantly to the existing body of knowledge on IoT security. It offers a detailed analysis of how specific routing attacks impact IoT networks and how protocol enhancements can mitigate them effectively. By addressing the blackhole and wormhole attacks, this research not only improves the security of IoT networks but also provides insights into the scalability and adaptability of routing protocols in hostile environments. Our results demonstrate significantly improved performance compared to existing studies, particularly in terms of higher throughput, lower packet loss, and a more consistent packet delivery ratio.

5.1.1 Limitations

In any research study, it's essential to recognize and articulate potential limitations. Identifying these constraints does not undermine the research but provides a more precise context for interpreting the results. It also serves as a foundation for future work, offering insights into areas where further exploration, testing, or improvements might be needed. Here are the specific limitations identified in this study:

- ❖ **Use of NS-2.35:** Although NS-3 offers more advanced features and active support, this study utilized NS-2.35 due to compatibility with specific simulation requirements. Such as the modification of the ADOV Protocol. This choice may limit the applicability of certain advanced functions that NS-3 could have provided.
- ❖ **Environmental Factors:** The simulations did not account for various environmental factors, such as physical obstacles or dynamic node mobility patterns, which could affect network behavior in actual implementations. This gap suggests that the simulation results may not fully reflect the complexities of real-world scenarios.
- ❖ **Need for Additional Fine-tuning:** The protocols evaluated in this study may require further refinement and testing to ensure their effectiveness in real-world conditions or when faced with different types of attacks.

5.2 Future Work

Building upon this research, future work will expand the scope of simulated attack scenarios to include more complex threats such as sybil and sinkhole attacks, common in IoT networks. By incorporating these additional attack types into the simulation, it could be possible to develop a more comprehensive understanding of how various malicious activities impact network performance and security. This broader simulation would contribute to creating a unified detection and mitigation technique that could safeguard IoT networks from a wide range of attacks. This integrated approach could simplify implementation, enhance response times, and optimize resource utilization, ensuring robust security across IoT networks.

Furthermore, transitioning to the latest version of NS-3 will be a strategic move in future efforts. Leveraging NS-3's advanced features and compatibility with modern protocols will allow for more realistic and precise simulations. This upgrade will enhance the accuracy of attack detection and mitigation strategies.

References:

1. M. N. Siddiqui, K. R. Malik, T. S. Malik. "Performance Analysis of Blackhole and Wormhole Attack in MANET Based IoT." *2021 IEEE International Conference on Digital Futures and Transformative Technologies (ICoDT2)*, 2021.
2. A. Reshi, S. Sholla, Z. A. Najjar. "Safeguarding IoT Networks: Mitigating Black Hole Attacks with an Innovative Defense Algorithm." *Journal of Engineering Research*, 2024.
3. S. D. Mali, K. Govinda. "A Study on Network Routing Attacks in IoT." *Materials Today: Proceedings*, 2023.
4. T. Safdar, M. N. Siddiqui, M. Mateen. "Comparison of Blackhole and Wormhole Attacks in Cloud MANET Enabled IoT for Agricultural Field Monitoring." *Security and Communication Networks*, 2022.
5. M. Alrubaiee, H. Shaker. "Performance Analysis of Black Hole and Worm Hole Attacks in MANETs." *International Journal of Communication Networks and Information Security*, 2022.
6. Amisha Parmar, V. B. Vaghela. "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol." *Procedia Computer Science*, 2016.
7. E. Elmahdi, S.-M. Yoo, K. Sharshembiev. "Secure and Reliable Data Forwarding using Homomorphic Encryption against Blackhole Attacks in Mobile Ad Hoc Networks." *Journal of Information Security and Applications*, 2020.
8. M. Shukla, B. K. Joshi. "A Trust-Based Approach to Mitigate Wormhole Attacks in Mobile Adhoc Networks." *IEEE International Conference on Communication Systems and Network Technologies*, 2021.
9. S. Sankara Narayanan, G. Murugaboopathi. "Modified Secure AODV Protocol to Prevent Wormhole Attack in MANET." *Concurrency and Computation: Practice and Experience*, 2018.
10. S.H. Jayachandra, R. Manjunatha, N. Hussain, B.U. Sujana, H.L. Gururaj, B. Ramesh. "Analysis of Black Hole Attack in Ad Hoc Network Using AODV and AOMDV Protocols." *Emerging Research in Computing, Information, Communication and Applications*, 2016.
11. E. E. Tatar, M. Dener. "Wormhole Attacks in IoT Based Networks." 6th International Conference on Computer Science and Engineering (UBMK), 2021.
12. N. Chaurasia, A. Singh. "A Survey on Wormhole Attack Detection Techniques in Wireless Sensor Networks." *Journal of Communications and Networks*, 2020.
13. M. Rafiqul Alam, A. P. Gupta. "RTT-TC: A Detection Scheme for Wormhole Attack Using Round Trip Time and Topological Comparisons." *Ad Hoc Networks Journal*, 2020.
14. G. Wazid, S. Das, A. M. Rao. "Detection and Prevention Techniques for Wormhole Attacks in MANET." *Journal of Communications and Networks*, 2019.
15. A.Parmar, V. B. Vaghela. "Wormhole Attack Prevention Using Adaptive Multipath Routing in Wireless Sensor Networks." *Procedia Technology*, 2017.
16. M. Sultana, M. Alam. "Impact of Wormhole Attacks on AODV Protocol Performance." *International Journal of Computer Science and Network Security*, 2021.
17. F. -E. Hachemi, M. Mana and B. A. Bensaber, "Study of the Impact of Sinkhole Attack in IoT Using Shewhart Control Charts," *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, Taipei, Taiwan, 2020, pp. 1-5, doi: 10.1109/GLOBECOM42002.2020.9322603.
18. C. Sharma, P. Singh. "Distributed Denial of Service Attack on IoT Networks and Its Mitigation." *Security and Privacy in the Internet of Things*, 2022.
19. S. Divya, V. Nithya. "Jamming Attacks in IoT Networks: A Survey." *International Journal of Computer Applications*, 2020.
20. F. Karray, M. Jmal. "A Survey on Routing Protocols and Security in IoT: Challenges and Solutions." *Sensors*, 2021.
21. Y. Qian, S. Li. "Mitigating Routing Attacks in Ad-Hoc IoT Networks: A Secure Routing

- Framework." *Journal of Communications and Networks*, 2020.
22. H. Kaur, S. Sharma. "Lightweight Intrusion Detection System for IoT: A Comprehensive Study." *Ad Hoc Networks Journal*, 2022.
 23. S. Naveena, C. Senthilkumar, T. Manikandan. "Analysis and Countermeasures of Black-Hole Attack in MANET by Employing Trust-Based Routing." 2020 6th International Conference on Advanced Computing & Communication Systems (ICACCS), 2020.
 24. P. Reddy B., B. Reddy, D. B. "The AODV Routing Protocol with Built-in Security to Counter Blackhole Attack in MANET." *Materials Today: Proceedings*.
 25. M. Knaj, F. Ghosna, M. Anbar, D.K. Voronkova, M. Nassr. "Detecting and Mitigating Wormhole Attack Effect in MANETs Based on Hop Count Technique." 2023 IEEE 5th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE) 2023.
 26. M. K. Verma, R. K. Dwivedi. "A Survey on Wormhole Attack Detection and Prevention Techniques in Wireless Sensor Networks." 2020 International Conference on Electrical and Electronics Engineering (ICE3-2020) 2020.
 27. Z. A. Zardari, K. A. Memon, R. A. Shah, S. Dehraj, I. Ahmed. "A lightweight technique for detecting and preventing wormhole attack in MANET." *EAI Endorsed Transactions on Scalable Information Systems* 2020.
 28. Y. Xie, "Machine Learning-Based DDoS Detection for IoT Networks," *Applied and Computational Engineering*, vol. 29, pp. 99-107, 2023, doi: 10.54254/2755-2721/29/20230972.
 29. S. Lushaba and S. Chindipha, "Investigating a Blackhole Attack Solution in Mobile Peer-to-Peer Networks with AODV Routing Protocol," 2023.
 30. L. Charles and J. Priyadarsini, "Sinkhole Detection in IoT Using Elliptic Curve Digital Signature," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, pp. 322-329, 2023, doi: 10.17762/ijritcc.v11i5.6620.
 31. R. O. Raji and A. M. Oyelakin, "Approaches for Solving Routing and Security Issues in Mobile Ad-Hoc Networks (MANETs): A Review," *Journal of Information Technology and Computing*, vol. 4, no. 2, pp. 20-30, 2023, doi: 10.48185/jitc.v4i2.930.
 32. A. Khan, R. Puree, B. Mohanta, and S. Chedup, "Detection and Prevention of Blackhole Attack in AODV of MANET," in *Proceedings of IEMTRONICS 2021*, pp. 1-7, 2021, doi: 10.1109/IEMTRONICS52119.2021.9422643.
 33. A. M. Eltahlawy, H. K. Aslan, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, "Detection of Sequence Number Attacks Using Enhanced AODV Protocol in MANETs," *Computers and Electrical Engineering*, vol. 118, Part B, 2024, Art. no. 109395, ISSN 0045-7906, doi: 10.1016/j.compeleceng.2024.109395.
 34. J. Cynthia, H. Parveen Sultana, M. N. Saroja, and J. Senthil, "Security Protocols for IoT," in *Ubiquitous Computing and Computing Security of IoT*, vol. 47, 2019, ISBN: 978-3-030-01565-7.
 35. A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A Review on the Security of IoT Networks: From Network Layer's Perspective," *IEEE Access*, vol. 11, pp. 71073-71087, 2023, doi: 10.1109/ACCESS.2023.3246180.
 36. A. Hasan, M. A. Khan, B. Shabir, A. Munir, A. W. Malik, Z. Anwar, and J. Ahmad, "Forensic Analysis of Blackhole Attack in Wireless Sensor Networks/Internet of Things," *Applied Sciences*, vol. 12, no. 22, Art. no. 11442, 2022, doi: 10.3390/app122211442.
 37. S. Ali, M. A. Khan, J. Ahmad, A. W. Malik, and A. ur Rehman, "Detection and Prevention of Black Hole Attacks in IoT & WSN," 2018 Third *International Conference on Fog and Mobile Edge Computing*, pp. 217-226, 2018, doi: 10.1109/FMEC.2018.8364068.
 38. A. A. Fadele, M. Othman, I. A. T. Hashem, et al., "A Novel Countermeasure Technique for Reactive Jamming Attack in Internet of Things," *Multimedia Tools and Applications*, vol. 78, pp. 29899–29920, 2019, doi: 10.1007/s11042-018-6684-z.
 39. N. Namvar, W. Saad, N. Bahadori, and B. Kelley, "Jamming in the Internet of Things: A Game-Theoretic Perspective," 2016 *IEEE Global Communications Conference (GLOBECOM)*, Washington, DC, USA, pp. 1-6, 2016, doi: 10.1109/GLOCOM.2016.7841922.

40. R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT", *Sustainable Engineering and Innovation*, vol. 3, no. 1, pp. 23-28, Jan. 2021.
41. P. Kumari and A. K. Jain, "A Comprehensive Study of DDoS Attacks over IoT Network and Their Countermeasures," *Computers & Security*, vol. 127, Art. no. 103096, 2023, ISSN 0167-4048, doi: 10.1016/j.cose.2023.103096.
42. R. Vishwakarma and A. K. Jain, "A Survey of DDoS Attacking Techniques and Defence Mechanisms in the IoT Network," *Telecommunication Systems*, vol. 73, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.
43. N. Sivanesan, A. Rajesh, and K. S. Archana, "ANFIS-RSOA Approach for Detecting and Preventing Network Layer Attacks in MANET," *Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advanced Studies (VISTAS)*.
44. Rushdi A. Hamamreh and Abdul-Rahman Salem, "Protocol to Avoid Multiple Black Hole Attacks in MANETs," *Journal of Advances in Computer Networks* vol. 4, no. 3, pp. 161-166, 2016
45. P. Bhale, D. Ray, S. Biswas and S. Nandi, "WOMN: WOrMhole Attack DetectioN and Mitigation Using Lightweight Distributed IDS in IoT Network," 2023 IEEE Guwahati Subsection Conference (GCON), Guwahati, India, 2023, pp. 01-06, doi: 10.1109/GCON58516.2023.10183505.
46. Gagandeep, & Aashima,. (2012). Study on Sinkhole Attacks in Wireless Ad hoc Networks. *International Journal on Computer Science and Engineering*. 4. 1078-1084.
47. Garg, Kanwal & Chawla, Rshma & Prof, Assoc. (2011). Detection of DDoS attacks using data mining. *International Journal of Computing and Business Research (IJCBR)*. 2.
48. Unsal, Emre & Çebi, Yalçin. (2013). DENIAL OF SERVICE ATTACKS IN WSN. 10.13140/2.1.4040.9929.

APPENDIX A: Script for the Blackhole Attack

```
set val(chan) Channel/WirelessChannel ;
set val(prop) Propagation/TwoRayGround ;
set val(netif) Phy/WirelessPhy ;
set val(mac) Mac/802_11 ;
set val(ifq) Queue/DropTail/PriQueue ;
set val(ll) LL ;
set val(ant) Antenna/OmniAntenna ;
set val(ifqlen) 50 ;
set val(nn) 20;
set val(rp) AODV;
set val(brp) blackholeAODV ;
set val(x) 1500 ;
set val(y) 2500 ;
set val(stop) 30 ;
set ns [new Simulator]
set tracefd [open blackhole.tr w]
set namtracefd [open wrlsaodv.nam w]
$ns trace-all $tracefd
$ns use-newtrace
$ns namtrace-all-wireless $namtracefd $val(x) $val(y)
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)

#GOD (General Operations Director)
create-god $val(nn)
$ns node-config -adhocRouting $val(rp) I will schedule some time for us to connect.
-llType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
```

```
-ifqLen $val(ifqlen) \  
-antType $val(ant) \  
-propType $val(prop) \  
-phyType $val(netif) \  
-channelType $val(chan) \  
-topoInstance $topo \  
-agentTrace ON \  
-routerTrace ON \  
-macTrace ON \  
-movementTrace ON \  

```

```
# Now configure and create the rest of the nodes
```

```
for {set i 0} {$i < $val(nn)} {incr i} {
```

```
  if {$i != 19} {
```

```
    set node_($i) [$ns node] ;
```

```
  }
```

```
}
```

```
$ns node-config -adhocRouting $val(brp)
```

```
set node_(19) [$ns node]
```

```
$node_(0) label "sender"
```

```
$node_(0) color "green"
```

```
$ns at 0.0 "$node_(0) color green"
```

```
$node_(13) label "destination"
```

```
$node_(13) color "blue"
```

```
$ns at 0.0 "$node_(13) color blue"
```

```
# *** Throughput Trace ***
```

```

set f0 [open thrpt.tr w]
puts $f0 "# Time (s) Throughput (Kbps)"
puts $f0 "color = red"
puts $f0 "thickness = 2.5"
puts $f0 "title_x = Time(s)"
puts $f0 "title_y = Throughput (Kbps)"
puts $f0 "title = Throughput Graph"
puts $f0 "lower_boundary = 5.000000"
puts $f0 "Color = Red"
puts $f0 "TITLE_LEGEND_POINT 2.0 6.25 1"
puts $f0 "Text 2.0 6.25"
puts $f0 " - Black Hole Attack"
puts $f0 "End_Text"
# *** Packet Loss Trace ***

```

```

set f1 [open pclos.tr w]
puts $f1 "# Time (s) PacketLoss "
puts $f1 "color = red"
puts $f1 "thickness = 2.5"
puts $f1 "title_x = Time(s)"
puts $f1 "title_y = PacketLoss Ratio"
puts $f1 "title = PacketLoss Graph"
puts $f1 "lower_boundary = 5.000000"
puts $f1 "Color = Red"
puts $f1 "TITLE_LEGEND_POINT 2.0 6.25 1"
puts $f1 "Text 2.0 6.25"
puts $f1 " - Black Hole Attack"
puts $f1 "End_Text"

```

```

set f2 [open pdr.tr w]
puts $f2 "# Time (s) Pakeket Delivery "

```

```
puts $f2 "color = red"
puts $f2 "thickness = 2.5"
puts $f2 "title_x = Time(s)"
puts $f2 "title_y = Paceket Delivery Ratio"
puts $f2 "title = Paceket Delivery Graph"
puts $f2 "lower_boundary = 5.000000"
puts $f2 "Color = Red"
puts $f2 "TITLE_LEGEND_POINT 2.0 6.25 1"
puts $f2 "Text 2.0 6.25"
puts $f2 " - Black Hole Attack"
puts $f2 "End_Text"
```

```
$node_(0) set X_ 400.0
$node_(0) set Y_ 1650.0
$node_(0) set Z_ 0.0
```

```
$node_(1) set X_ 300.0
$node_(1) set Y_ 1800.0
$node_(1) set Z_ 0.0
```

```
$node_(2) set X_ 480.0
$node_(2) set Y_ 1850.0
$node_(2) set Z_ 0.0
```

```
$node_(3) set X_ 400.0
$node_(3) set Y_ 1700.0
$node_(3) set Z_ 0.0
```

```
$node_(4) set X_ 630.0
$node_(4) set Y_ 1680.0
```


\$node_(4) set Z_ 0.0

\$node_(5) set X_ 700.0

\$node_(5) set Y_ 1670.0

\$node_(5) set Z_ 0.0

\$node_(6) set X_ 1000.0

\$node_(6) set Y_ 1700.0

\$node_(6) set Z_ 0.0

\$node_(7) set X_ 400.0

\$node_(7) set Y_ 1500.0

\$node_(7) set Z_ 0.0

\$node_(8) set X_ 500.0

\$node_(8) set Y_ 1600.0

\$node_(8) set Z_ 0.0

\$node_(9) set X_ 750

\$node_(9) set Y_ 1750

\$node_(9) set Z_ 0.0

\$node_(10) set X_ 980.0

\$node_(10) set Y_ 1600.0

\$node_(10) set Z_ 0.0

\$node_(11) set X_ 950.0

\$node_(11) set Y_ 1500.0

\$node_(11) set Z_ 0.0

\$node_(12) set X_ 900.0

\$node_(12) set Y_ 1700.0

\$node_(12) set Z_ 0.0

\$node_(13) set X_ 800.0

\$node_(13) set Y_ 1500.0

\$node_(13) set Z_ 0.0

\$node_(14) set X_ 800.0

\$node_(14) set Y_ 1800

\$node_(14) set Z_ 0.0

\$node_(15) set X_ 480

\$node_(15) set Y_ 1750

\$node_(15) set Z_ 0.0

\$node_(16) set X_ 850

\$node_(16) set Y_ 1650

\$node_(16) set Z_ 0.0

\$node_(17) set X_ 550

\$node_(17) set Y_ 1850

\$node_(17) set Z_ 0.0

\$node_(18) set X_ 650

\$node_(18) set Y_ 1850

\$node_(18) set Z_ 0.0

\$node_(19) set X_ 670.0

\$node_(19) set Y_ 1600

\$node_(19) set Z_ 0.0

set udp [new Agent/UDP]

\$udp set class_ 1

set sink [new Agent/LossMonitor]

\$ns attach-agent \$node_(0) \$udp

\$ns attach-agent \$node_(13) \$sink

```

set cbr [new Application/Traffic/CBR]
$cbr attach-agent $udp
$cbr set packetSize_ 512
$cbr set rate_ 335Kb
$ns connect $udp $sink
$ns at 0.0 "$cbr start"
$ns at 30.0 "$cbr stop"
$ns at 0.01 "$node_(19) label \"blackhole node\""
$node_(19) color "red"
$ns at 0.0 "$node_(19) color red"
for {set i 0} {$i < $val(nn)} {incr i} {
$ns initial_node_pos $node_($i) 20
}
for {set i 0} {$i < $val(nn)} {incr i} {
$ns at $val(stop) "$node_($i) reset"
}
# Initialize Flags
set holdrate1 0
set total_packets_sent 0
set total_packets_lost 0
set total_packets_received 0
proc record {} {
    global sink f0 f1 f2 total_packets_sent total_packets_lost total_packets_received
    set ns [Simulator instance]
    set time 0.99;
    # Get current statistics
    set bytes_received [$sink set bytes_]
    set packets_lost [$sink set nlost_]
    # Calculate packets received (assuming 512-byte packets)
    set packets_received [expr $bytes_received / 512]
    # Update total packets

```

```

set packets_sent [expr $packets_received + $packets_lost]
set total_packets_sent [expr $total_packets_sent + $packets_sent]
set total_packets_lost [expr $total_packets_lost + $packets_lost]
set total_packets_received [expr $total_packets_received + $packets_received]
set now [$ns now]
# Calculate and record throughput
puts $f0 "$now [expr (($bytes_received * 8) / ($time * 1000))]"
# Calculate and record packet loss ratio
if {$total_packets_sent > 0} {
    set packet_loss_ratio [expr (double($total_packets_lost) / $total_packets_sent)*100]
} else {
    set packet_loss_ratio 100
}
puts $f1 "$now $packet_loss_ratio"
# Calculate and record PDR
if {$total_packets_sent > 0} {
    set pdr [expr (double($total_packets_received) / $total_packets_sent) * 100]
} else {
    set pdr 0
}
puts $f2 "$now $pdr"
# Reset sink counters for next interval
$sink set bytes_ 0
$sink set nlost_ 0
$ns at [expr $now+$time] "record"
}
$ns at 0.0 "record"
$ns at $val(stop) "stop"
for {set i 0} {$i < $val(nn)} {incr i} {
    $ns at $val(stop) "$node_($i) reset"
}

```

```
proc stop {} {
  global ns tracefd f0 f1 f2 namtracefd
  # Close Trace Files
  close $f0
  close $f1
  close $tracefd
  close $namtracefd
  close $f2
  # Plot Recorded Statistics
  $ns flush-trace
  #exec xgraph out0.tr -geometry 800x400 &
  #exec xgraph lost0.tr -geometry 800x400 &
  exec nam wrlsaadv.nam &
  #exec awk -f pdr_sec.awk blackhole.tr &
  exit 0
}
puts "Starting Simulation..."
$ns run
```

APPENDIX B: Script for the Detection and Mitigation of Blackhole Attack

```
set val(chan) Channel/WirelessChannel ;
set val(prop) Propagation/TwoRayGround ;
set val(netif) Phy/WirelessPhy ;
set val(mac) Mac/802_11 ;
set val(ifq) Queue/DropTail/PriQueue ;
set val(ll) LL ;
set val(ant) Antenna/OmniAntenna ;
set val(ifqlen) 50 ;
set val(nn) 20;
set val(rp) AOMDV;
set val(brp) blackholeAODV ;
set val(x) 1500 ;
set val(y) 2500 ;
set val(stop) 30 ;

set ns [new Simulator]
set tracefd [open blackhole.tr w]
set namtracefd [open wrlsaodv.nam w]
$ns trace-all $tracefd
$ns use-newtrace
$ns namtrace-all-wireless $namtracefd $val(x) $val(y)
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)

#GOD (General Operations Director)
create-god $val(nn)
$ns node-config -adhocRouting $val(rp) \
-lIType $val(ll) \
-macType $val(mac) \
-ifqType $val(ifq) \
```

```
-ifqLen $val(ifqlen) \  
-antType $val(ant) \  
-propType $val(prop) \  
-phyType $val(netif) \  
-channelType $val(chan) \  
-topoInstance $topo \  
-agentTrace ON \  
-routerTrace ON \  
-macTrace ON \  
-movementTrace ON \  

```

Now configure and create the rest of the nodes

```
for {set i 0} {$i < $val(nn)} {incr i} {  
  if {$i != 19} {  
    set node_($i) [$ns node] ;  
  }  
}  
$ns node-config -adhocRouting $val(brp)  
set node_(19) [$ns node]  
  
$node_(0) label "sender"  
$node_(0) color "green"  
$ns at 0.0 "$node_(0) color green"  
  
$node_(13) label "destination"  
$node_(13) color "blue"  
$ns at 0.0 "$node_(13) color blue"
```

```
# *** Throughput Trace ***
```

```
set f0 [open thrpt.tr w]
puts $f0 "# Time (s) Throughput (Kbps)"
puts $f0 "color = blue"
puts $f0 "thickness = 2.5"
puts $f0 "title_x = Time(s)"
puts $f0 "title_y = Throughput (Kbps)"
puts $f0 "title = Throughput Graph"
puts $f0 "lower_boundary = 5.000000"
puts $f0 "Color = Blue"
puts $f0 "TITLE_LEGEND_POINT 2.0 6.5 2"
puts $f0 "Text 2.0 6.5"
puts $f0 " - Mitigation with IDS"
puts $f0 "End_Text"
```

```
# *** Packet Loss Trace ***
```

```
set f1 [open pclos.tr w]
puts $f1 "# Time (s) PacketLoss "
puts $f1 "color = blue"
puts $f1 "thickness = 2.5"
puts $f1 "title_x = Time(s)"
puts $f1 "title_y = PacketLoss Ratio"
puts $f1 "title = PacketLoss Graph"
puts $f1 "lower_boundary = 5.000000"
puts $f1 "Color = Blue"
puts $f1 "TITLE_LEGEND_POINT 2.0 6.5 2"
puts $f1 "Text 2.0 6.5"
puts $f1 " - Mitigation with IDS"
puts $f1 "End_Text"
```



```
# *** Packet delivery Trace ***
```

```
set f2 [open pdr.tr w]
puts $f2 "# Time (s)  Paceket Delivery "
puts $f2 "color = blue"
puts $f2 "thickness = 2.5"
puts $f2 "title_x = Time(s)"
puts $f2 "title_y = Paceket Delivery Ratio"
puts $f2 "title = Paceket Delivery Graph"
puts $f2 "lower_boundary = 5.000000"
puts $f2 "Color = Blue"
puts $f2 "TITLE_LEGEND_POINT 2.0 6.5 2"
puts $f2 "Text 2.0 6.5"
puts $f2 " - Mitigation with IDS"
puts $f2 "End_Text"
```

```
$node_(0) set X_ 400.0
$node_(0) set Y_ 1650.0
$node_(0) set Z_ 0.0
```

```
$node_(1) set X_ 300.0
$node_(1) set Y_ 1800.0
$node_(1) set Z_ 0.0
```

```
$node_(2) set X_ 480.0
$node_(2) set Y_ 1850.0
$node_(2) set Z_ 0.0
```

```
$node_(3) set X_ 400.0
$node_(3) set Y_ 1700.0
```

\$node_(3) set Z_ 0.0

\$node_(4) set X_ 630.0

\$node_(4) set Y_ 1680.0

\$node_(4) set Z_ 0.0

\$node_(5) set X_ 700.0

\$node_(5) set Y_ 1670.0

\$node_(5) set Z_ 0.0

\$node_(6) set X_ 1000.0

\$node_(6) set Y_ 1700.0

\$node_(6) set Z_ 0.0

\$node_(7) set X_ 400.0

\$node_(7) set Y_ 1500.0

\$node_(7) set Z_ 0.0

\$node_(8) set X_ 500.0

\$node_(8) set Y_ 1600.0

\$node_(8) set Z_ 0.0

\$node_(9) set X_ 750

\$node_(9) set Y_ 1750

\$node_(9) set Z_ 0.0

\$node_(10) set X_ 980.0

\$node_(10) set Y_ 1600.0

\$node_(10) set Z_ 0.0

\$node_(11) set X_ 950.0
\$node_(11) set Y_ 1500.0
\$node_(11) set Z_ 0.0

\$node_(12) set X_ 900.0
\$node_(12) set Y_ 1700.0
\$node_(12) set Z_ 0.0

\$node_(13) set X_ 800.0
\$node_(13) set Y_ 1500.0
\$node_(13) set Z_ 0.0

\$node_(14) set X_ 800.0
\$node_(14) set Y_ 1800
\$node_(14) set Z_ 0.0

\$node_(15) set X_ 480
\$node_(15) set Y_ 1750
\$node_(15) set Z_ 0.0

\$node_(16) set X_ 850
\$node_(16) set Y_ 1650
\$node_(16) set Z_ 0.0

\$node_(17) set X_ 550
\$node_(17) set Y_ 1850
\$node_(17) set Z_ 0.0

\$node_(18) set X_ 650
\$node_(18) set Y_ 1850
\$node_(18) set Z_ 0.0

```

$node_(19) set X_ 670.0
$node_(19) set Y_ 1600
$node_(19) set Z_ 0.0

set udp [new Agent/UDP]
$udp set class_ 1
$ns attach-agent $node_(0) $udp
set sink [new Agent/LossMonitor]
$ns attach-agent $node_(13) $sink

set cbr [new Application/Traffic/CBR]
$cbr attach-agent $udp
$cbr set packetSize_ 512
$cbr set rate_ 335Kb
$ns connect $udp $sink

$ns at 0.0 "$cbr start"
$ns at 30.0 "$cbr stop"

$ns at 0.01 "$node_(19) label \"blackhole node\""
$node_(19) color "red"
$ns at 0.0 "$node_(19) color red"

for {set i 0} {$i < $val(nn)} {incr i} {
$ns initial_node_pos $node_($i) 20
}

for {set i 0} {$i < $val(nn)} {incr i} {
$ns at $val(stop) "$node_($i) reset"
}

```

```

# Initialize Flags

set holdrate1 0

set total_packets_sent 0
set total_packets_lost 0
set total_packets_received 0

proc record {} {
    global sink f0 f1 f2 total_packets_sent total_packets_lost total_packets_received
    set ns [Simulator instance]

    set time 0.99;#Set Sampling Time to 0.9 Sec

    # Get current statistics
    set bytes_received [$sink set bytes_]
    set packets_lost [$sink set nlost_]

    # Calculate packets received (assuming 512-byte packets)
    set packets_received [expr $bytes_received / 512]

    # Update total packets
    set packets_sent [expr $packets_received + $packets_lost]
    set total_packets_sent [expr $total_packets_sent + $packets_sent]
    set total_packets_lost [expr $total_packets_lost + $packets_lost]
    set total_packets_received [expr $total_packets_received + $packets_received]

    set now [$ns now]

    # if {$now < 0.9} {

```

```

    # Schedule the next record without writing any data
#   $ns at [expr $now + $time] "record"
#   return
#}

# Calculate and record throughput
puts $f0 "$now [expr (($bytes_received * 8) / ($time * 1000))]"

# Calculate and record packet loss ratio
if {$total_packets_sent > 0} {
    set packet_loss_ratio [expr (double($total_packets_lost) / $total_packets_sent)*100]
} else {
    set packet_loss_ratio 100
}
puts $f1 "$now $packet_loss_ratio"

# Calculate and record PDR
if {$total_packets_sent > 0} {
    set pdr [expr (double($total_packets_received) / $total_packets_sent) * 100]
} else {
    set pdr 0
}

puts $f2 "$now $pdr"

# Reset sink counters for next interval
$sink set bytes_ 0
$sink set nlost_ 0

$ns at [expr $now+$time] "record"
}

```

```

$ns at 0.0 "record"

$ns at $val(stop) "stop"

for {set i 0} {$i < $val(nn) } {incr i} {
$ns at $val(stop) "$node_($i) reset"
}

proc stop {} {

global ns tracefd f0 f1 f2 namtracefd

# Close Trace Files

close $f0
close $f1
close $f2
close $tracefd
close $namtracefd

# Plot Recorded Statistics
$ns flush-trace
#exec xgraph out0.tr -geometry 800x400 &
#exec xgraph lost0.tr -geometry 800x400 &
exec nam wrlsaadv.nam &
#exec awk -f pdr_sec.awk blackhole.tr &
exit 0
}
puts "Starting Simulation..."
$ns run

```

APPENDIX C: Script for the Wormhole Attack

```
# Define Simulation Parameters
set val(chan) Channel/WirelessChannel
set val(prop) Propagation/TwoRayGround
set val(netif) Phy/WirelessPhy
set val(mac) Mac/802_11
set val(ifq) Queue/DropTail/PriQueue
set val(ll) LL
set val(ant) Antenna/OmniAntenna
set val(ifqlen) 50
set val(nn) 30
set val(rp) AODV
set val(x) 1440
set val(y) 1000
set val(stop) 30.0
# Initialize the Simulator
set ns [new Simulator]
# Setup Topography Object
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)

# Create "God" Object
create-god $val(nn)
# Open Trace Files
set tracefile [open out.tr w]
$ns trace-all $tracefile
set f0 [open out2.tr w]
set f1 [open lost2.tr w]
set f2 [open pdr.tr w]
set namfile [open wormhole.nam w]
```



```

$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x) $val(y)
# Create Wireless Channel
set chan [new $val(chan)]
# Configure Node Parameters
$ns node-config -adhocRouting $val(rp) \
    -llType $val(ll) \
    -macType $val(mac) \
    -ifqType $val(ifq) \
    -ifqLen $val(ifqlen) \
    -antType $val(ant) \
    -propType $val(prop) \
    -phyType $val(netif) \
    -channel $chan \
    -topoInstance $topo \
    -agentTrace ON \
    -routerTrace ON \
    -macTrace ON \
    -movementTrace ON

# Throughput Trace
puts $f0 "# Time (s) Throughput (Kbps)"
puts $f0 "color = red"
puts $f0 "thickness = 2.5"
puts $f0 "title_x = Time(s)"
puts $f0 "title_y = Throughput (Kbps)"
puts $f0 "title = Throughput Graph"
puts $f0 "lower_boundary = 5.000000"
puts $f0 "Color = Red"
puts $f0 "TITLE_LEGEND_POINT 2.0 6.25 1"
puts $f0 "Text 2.0 6.25"
puts $f0 " - Worm Hole Attack"

```

```

puts $f0 "End_Text"
# Packet Loss Trace
puts $f1 "# Time (s) PacketLoss"
puts $f1 "color = red"
puts $f1 "thickness = 2.5"
puts $f1 "title_x = Time(s)"
puts $f1 "title_y = PacketLoss Ratio"
puts $f1 "title = PacketLoss Graph"
puts $f1 "lower_boundary = 5.000000"
puts $f1 "Color = Red"
puts $f1 "TITLE_LEGEND_POINT 2.0 6.25 1"
puts $f1 "Text 2.0 6.25"
puts $f1 " - Worm Hole Attack"
puts $f1 "End_Text"

# Packet Delivery Trace
puts $f2 "# Time (s) Packet Delivery"
puts $f2 "color = red"
puts $f2 "thickness = 2.5"
puts $f2 "title_x = Time(s)"
puts $f2 "title_y = Packet Delivery Ratio"
puts $f2 "title = Packet Delivery Graph"
puts $f2 "lower_boundary = 5.000000"
puts $f2 "Color = Red"
puts $f2 "TITLE_LEGEND_POINT 2.0 6.25 1"
puts $f2 "Text 2.0 6.25"
puts $f2 " - Worm Hole Attack"
puts $f2 "End_Text"
# Initialize Nodes
for {set i 0} {$i < $val(nn)} {incr i} {
    if {( $i == 12) || ( $i == 13) || ( $i == 14) || ( $i == 15)} {

```

```

        continue
    }
    set node [$ns node]
    $node set X_ [expr rand()*$val(x)]
    $node set Y_ [expr rand()*$val(y)]
    $node set Z_ 0.0
    $ns initial_node_pos $node 25
}

# Set Specific Nodes as Source and Destination
set n12 [$ns node]
$n12 set X_ 299; $n12 set Y_ 400; $n12 set Z_ 0.0
$ns initial_node_pos $n12 25
$n12 color green
$ns at 0.0 "$n12 color green"
$ns at 0.0 "$n12 label Source"

set n13 [$ns node]
$n13 set X_ 850; $n13 set Y_ 450; $n13 set Z_ 0.0
$ns initial_node_pos $n13 25
$n13 color blue
$ns at 0.0 "$n13 color blue"
$ns at 0.0 "$n13 label Destination"

# Configure Wormholes
set n14 [$ns node]
$n14 set X_ 295.0; $n14 set Y_ 500.0; $n14 set Z_ 0.0
$ns initial_node_pos $n14 25
$n14 color red
$ns at 0.0 "$n14 color red"
$ns at 0.01 "$n14 label \"worm hole 1\""

set n15 [$ns node]
$n15 set X_ 850; $n15 set Y_ 300; $n15 set Z_ 0.0
$ns initial_node_pos $n15 25

```

```

$n15 color red
$ns at 0.0 "$n15 color red"
$ns at 0.01 "$n15 label \"worm hole 2\""
[$n14 set ll_(0)] wormhole-peer [$n15 set ll_(0)]
[$n15 set ll_(0)] wormhole-peer [$n14 set ll_(0)]

# Setup UDP Connection
set udp0 [new Agent/UDP]
$ns attach-agent $n12 $udp0
set sink [new Agent/LossMonitor]
$ns attach-agent $n13 $sink
$ns connect $udp0 $sink
$udp0 set packetSize_ 1500

# Setup CBR Application over UDP
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $udp0
$cbr0 set packetSize_ 1500
$cbr0 set rate_ 512Kb
$cbr0 set random_ null
$ns at 0.0 "$cbr0 start"
$ns at 30.0 "$cbr0 stop"
# Initialize Flags
set holdrate1 0
set total_packets_sent 0
set total_packets_lost 0
set total_packets_received 0
# Record Throughput, Packet Loss, and PDR
proc record {} {
    global sink f0 f1 f2 total_packets_sent total_packets_lost total_packets_received
    set ns [Simulator instance]

```

```

set time 0.99

set bytes_received [$sink set bytes_]
set packets_lost [$sink set nlost_]
set packets_received [expr $bytes_received / 1500]
set packets_sent [expr $packets_received + $packets_lost]
set total_packets_sent [expr $total_packets_sent + $packets_sent]
set total_packets_lost [expr $total_packets_lost + $packets_lost]
set total_packets_received [expr $total_packets_received + $packets_received]
set now [$ns now]
puts $f0 "$now [expr (($bytes_received)*8)/(($time*1000))]"
if {$total_packets_sent > 0} {
    set packet_loss_ratio [expr (double($total_packets_lost) / $total_packets_sent)*100]
} else {
    set packet_loss_ratio 0
}
puts $f1 "$now $packet_loss_ratio"

if {$total_packets_sent > 0} {
    set pdr [expr (double($total_packets_received) / $total_packets_sent) * 100]
} else {
    set pdr 0
}
puts $f2 "$now $pdr"

$sink set bytes_ 0
$sink set nlost_ 0

$ns at [expr $now+$time] "record"
}
$ns at 0.0 "record"

```

```
# Schedule Stop Procedure
$ns at $val(stop) "stop"
# Termination Procedure
proc stop {} {
    global ns tracefile f0 f1 f2 namfile
    close $f0
    close $f1
    close $f2
    close $tracefile
    close $namfile
    $ns flush-trace
    exec nam wormhole.nam &
    exit 0
}
puts "Starting Simulation..."
$ns run
```

APPENDIX D: Script for the Detection and Mitigation of Worm hole Attack

```
# Define Simulation Parameters
set val(chan) Channel/WirelessChannel
set val(prop) Propagation/TwoRayGround
set val(netif) Phy/WirelessPhy
set val(mac) Mac/802_11
set val(ifq) Queue/DropTail/PriQueue
set val(ll) LL
set val(ant) Antenna/OmniAntenna
set val(ifqlen) 50
set val(nn) 30
set val(rp) idsAODV
set val(x) 1440
set val(y) 1000
set val(stop) 30
set val(wormholes) 2

# Initialize the Simulator
set ns [new Simulator]

# Setup Topography
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)

# Open the NS Trace File
set tracefile [open out.tr w]
$ns trace-all $tracefile

# Open Trace Files for Metrics
```

```
set f0 [open out2.tr w]
puts $f0 "# Time (s) Throughput (Mbps)"
puts $f0 "color = blue"
puts $f0 "thickness = 2.5"
puts $f0 "title_x = Time(s)"
puts $f0 "title_y = Throughput (Kbps)"
puts $f0 "title = Throughput Graph"
puts $f0 "lower_boundary = 5.000000"
puts $f0 "Color = Blue"
```

```
set f1 [open lost2.tr w]
puts $f1 "# Time (s) PacketLoss"
puts $f1 "color = blue"
puts $f1 "thickness = 2.5"
puts $f1 "title_x = Time(s)"
puts $f1 "title_y = PacketLoss Ratio"
puts $f1 "title = PacketLoss Graph"
```

```
set f2 [open pdr.tr w]
puts $f2 "# Time (s) Packet Delivery"
puts $f2 "color = blue"
puts $f2 "thickness = 2.5"
puts $f2 "title_x = Time(s)"
puts $f2 "title_y = Packet Delivery Ratio"
puts $f2 "title = Packet Delivery Graph"
```

```
# Open NAM Trace File
```

```
set namfile [open wormhole.nam w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x) $val(y)
```



```

# Create Wireless Channel
set chan [new $val(chan)]

# Configure Node Parameters
$ns node-config -adhocRouting $val(rp) \
    -llType $val(ll) \
    -macType $val(mac) \
    -ifqType $val(ifq) \
    -ifqLen $val(ifqlen) \
    -antType $val(ant) \
    -propType $val(prop) \
    -phyType $val(netif) \
    -channel $chan \
    -topoInstance $topo \
    -agentTrace ON \
    -routerTrace ON \
    -macTrace ON \
    -movementTrace ON

# Initialize Nodes
for {set i 0} {$i < $val(nn)} {incr i} {
    if {( $i == 12) || ( $i == 13) || ( $i == 14) || ( $i == 15)} {
        continue
    }
    set node [$ns node]
    $node set X_ [expr rand()*$val(x)]
    $node set Y_ [expr rand()*$val(y)]
    $node set Z_ 0.0
    $ns initial_node_pos $node 25
}

# Set Up Specific Nodes as Source and Destination
set n12 [$ns node]

```

```
$n12 set X_ 299; $n12 set Y_ 400; $n12 set Z_ 0.0
$ns initial_node_pos $n12 25
$n12 color green
$ns at 0.0 "$n12 color green"
$ns at 0.0 "$n12 label Source"
```

```
set n13 [$ns node]
$n13 set X_ 850; $n13 set Y_ 450; $n13 set Z_ 0.0
$ns initial_node_pos $n13 25
$n13 color blue
$ns at 0.0 "$n13 color blue"
$ns at 0.0 "$n13 label Destination"
```

```
# Configure Wormholes
```

```
set n14 [$ns node]
$n14 set X_ 295.0; $n14 set Y_ 500.0; $n14 set Z_ 0.0
$ns initial_node_pos $n14 25
$n14 color red
$ns at 0.0 "$n14 color red"
$ns at 0.01 "$n14 label \"worm hole 1\""
```

```
set n15 [$ns node]
$n15 set X_ 850; $n15 set Y_ 300; $n15 set Z_ 0.0
$ns initial_node_pos $n15 25
$n15 color red
$ns at 0.0 "$n15 color red"
$ns at 0.01 "$n15 label \"worm hole 2\""
```

```
[$n14 set ll_(0)] wormhole-peer [$n15 set ll_(0)]
[$n15 set ll_(0)] worm
```