

MINIMIZING BLACK HOLE ATTACK IN MOBILE AD HOC NETWORK WITH ANOMALY BASED IDS APPROACH

BY:

WORKU AYALEW MESELE



A thesis Submitted to

Department of Computer Science and Engineering

School of Electrical Engineering and Computing

Presented in Partial Fulfillment of the Requirement for Degree of
Master's in **Computer Science and Engineering**

Office of Graduate studies

Adama Science and Technology University

Adama, October, 2019

MINIMIZING BLACK HOLE ATTACK IN MOBILE AD HOC NETWORK WITH ANOMALY BASED IDS APPROACH

WORKU AYALEW MESELE

Advisor: KETEMA ADERE (PhD)



A thesis Submitted to

Department of Computer Science and Engineering
School of Electrical Engineering and Computing

Presented in Partial Fulfillment of the Requirement for Degree of
Master's in Computer Science and Engineering

Office of Graduate studies

Adama Science and Technology University

Adama, October, 2019

APPROVAL BY BOARD OF EXAMINERS

We, the undersigned members of the Board Examiners of the final open defense by **Worku Ayalew** have read and evaluated his Thesis entitled “**Minimizing Black Hole Attack in Mobile Ad Hoc Network with Anomaly Based IDS Approach**” and examined the candidate. This is, therefore to certify that the thesis has been accepted in partial fulfillment of the requirement of the Degree of Master’s in **Computer Science and engineering**

Advisor

Signature

Chairperson

Signature

Internal Examiner

Signature

External Examiner

Signature

DECLARATION

I hereby declare that this MSC thesis is my original work and has not been presented as a partial degree requirement for a degree in any other university and that all sources of materials used for the thesis have been duly acknowledged.

Name: _____

Signature: _____

This MSC thesis has been submitted for examination with my approval as thesis advisor

Name: Dr Ketema Adere G

Signature: _____

Date of submission: _____

ACKNOWLEDGEMENT

I would like to thank the Almighty God who helped me to succeed in all my life long learns. Next, I would like to give my most sincere and wholehearted gratitude to my Advisor Dr. Ketema Adere G and also Dr. Satish Kumar, Dr. Mesfin Abebe, Dr. Ing Frezewd, Dr. Tilahun M For their valuable assistance in providing their genuine, professional advice. I glad to thank all my friends, who are positive all the time to help me with all the idea and knowledge we have shared. I also express my heart full thanks to all those who have made their own contributions to accomplish this study.

TABLE OF CONTENT

ACKNOWLEDGEMENT	iii
TABLE OF CONTENT	iv
LIST OF FIGURES	viii
LIST OF TABLES	ix
ACRONYMS AND ABBREVIATIONS	x
ABSTRACT	xii
CHAPTER ONE	1
INTRODUCTION	1
1.1 Background	1
1.2 Motivation	3
1.3 Statement of the problem	4
1.4 Significance of the Study	4
1.5 Objective of the Study	5
1.5.1 General Objective	5
1.5.2 Specific Objective	5
1.6 Research Methodology	5
1.6.1 Research Framework	6
1.6.2 Network Simulator	6
1.7 Scope and Limitation of the Study	7
1.7.1 Scope of the Study	7
1.7.2 Limitation of the Study	7
1.8 Organization of the Thesis Work	8
CHAPTER TWO	9
LITERATURE REVIEW AND RELATED WORK	9
2.1 Literature Review of Mobile Ad Hoc Network	9
2.2 Routing Protocol Classification in MANET	9
2.2.1 Reactive Routing Protocols	10
2.2.1.1 AODV Routing Protocol	11

2.2.1.2	AOMDV ROUTING PROTOCOL.....	11
2.2.1.3	DSR Protocol.....	13
2.2.2	Proactive Routing Protocols	14
2.2.2.1	Destination Sequence Distance Vector Protocol.....	14
2.2.3	Hybrid Routing Protocol	14
2.2.3.1	Zone Routing Protocol	14
2.2.3.2	Zone-Based on Hierarchical Link State Routing Protocol.....	14
2.3	MANET Attacks.....	15
2.3.1	Passive Attack.....	17
2.3.2	Active Attack	17
2.3.2.1	Nature of Black Hole Attack.....	17
2.3.2.1.1	Single Black Hole Attack	18
2.3.2.1.2	Cooperative (Multiple) Black Hole Attack	19
2.3.3	Intrusion Detection System	19
2.3.3.1	Signature Based Intrusion Detection System	20
2.3.3.2	Anomaly Based Intrusion Detection System	20
2.3.3.3	Specification Based Intrusion Detection System	20
2.4	Trace Graph	21
2.5	Mobility Model.....	21
2.5.1	Reference Point Group Mobility	22
2.5.2	Random Waypoint Mobility Model	22
2.5.3	Freeway Mobility Model	23
2.5.4	City Section Mobility Model.....	24
2.6	RELATED WORK.....	25
2.6.1	Summarization of Related Works.....	27
2.6.2	Gap of Related Works	28
CHAPTER THREE		29
PROPOSED SOLUTION OF STUDY		29
3.1	Proposed Solution to Minimize Black Hole Attack	29
3.1.1	Pseudo Code for Proposed Algorithm	30
3.2	The Architecture of the Proposed Solution	31

3.2.1	Flow Chart Diagram for Proposed ABIDS Algorithm to Reduce BHA	34
3.2.2	AOMDV Modification	36
CHAPTER FOUR	37
SIMULATION OF THE PROPOSED SOLUTION	37
4.1	Simulation Scenario.....	37
4.2	Working Environment	37
4.3	Four Scenarios Evaluated under AOMDV Routing Protocol in MANET	37
4.3.1	Simulating and Analyzing Standard AOMDV Scenario	38
4.3.2	Simulating and Analyzing AOMDV Scenario with SBHA	38
4.3.3	Simulating and Analyzing AOMDV RP Scenario with MBHA	39
4.3.4	Simulate and Analyze AOMDV RP Scenario with ABIDS Approach	39
4.4	Core Implementation	40
4.5	Simulation of AOMDV with ABIDS Proposed Algorithm.....	42
4.6	Simulation Model	42
4.7	Simulation Parameter	43
4.8	Performance Metrics.....	48
4.8.1	Qualitative Metrics	48
4.8.2	Quantitative Metrics	48
4.8.2.1	Throughput	49
4.8.2.2	Jitter	49
4.8.2.3	End-to-End delay.....	49
4.9	Simulation Result and Discussion	49
4.9.1.1	Throughput	50
4.9.1.2	Jitter	54
4.9.1.3	End-to-End Delay.....	57
4.9.2	Summary of Result	58
I).	Throughput.....	58
II).	Jitter	58
III).	End-to-End Delay.....	58
CHAPTER FIVE	60
SUMMARY, CONCLUSION AND FUTURE WORK	60

5.1 Conclusion	60
5.2 Summary of Contribution	60
5.3 Future Work.....	61
Reference	62
Appendixes	66
Appendix I. Sample TCL File (.tcl) for ABIDSAOMDV Scenario.....	66
Appendix II. Sample Trace File (.tr) of ABIDSAOMDV Scenario	69
Appendix III. Source Code to Add Black Hole Attack	71
Appendix IV. Sample Source Code to Reduce BHA	72

LIST OF FIGURES

Figure 1. 1: MANET for Rescue Operation	2
Figure 1. 2: Mobile Ad Hoc Network Structure	3
Figure 2. 1: Routing Protocol classification in MANET.....	10
Figure 2. 2: Route Discovery Process in AOMDV Protocol	12
Figure 2. 3: Classification of Attacks in MANET.....	16
Figure 2. 4: Single Black Hole Attack in MANET	18
Figure 2. 5: Cooperative (Multiple) Black Hole Attack in MANET	19
Figure 2. 6: Trace Graph Diagram Window	21
Figure 2. 7: Reference Point Group Mobility.....	22
Figure 2. 8: Random Waypoint Mobility Model.....	23
Figure 2. 9: Freeway Mobility Model	23
Figure 2. 10: City Section Mobility Model	24
Figure 3. 1: Architecture of Proposed Solution.....	32
Figure 3. 2: Flow Chart Diagram of Proposed ABIDS Algorithm.....	34
Figure 4. 1: Standard AOMDV in MANET	45
Figure 4. 2: AOMDV Protocol with SBHA in MANET	46
Figure 4. 3: AOMDV Scenario with MBHA in MANET	47
Figure 4. 4:AOMDV with ABIDS Proposed Algorithm in MANET.....	48
Figure 4.5. a: Standard AOMDV simulation.....	51
Figure 4.5. b: AOMDV with Single Black Hole Attack	52
Figure 4.5. c: AOMDV with Multiple Black Hole Attack	53
Figure 4.5. d: AOMDV Modification with ABIDS.....	54
Figure 4.6. a: Standard AOMDV Simulation	55
Figure 4.6. b: AOMDV with Single Black Hole Attack	55
Figure 4.6. c: AOMDV with Multiple Black Hole Attack	56
Figure 4.6. d: AOMDV Modification with ABIDS.....	56
Figure 4.7. a: Standard AOMDV Simulation	57
Figure 4.7. b: Modification of AOMDV with ABIDS Proposed Algorithm.....	58

LIST OF TABLES

Table 2. 1: Fields of RREQ and RREP	13
Table 2. 2: Classification of Attacks per Layer	20
Table 2. 3: Summarization of Related Works	27
Table 4. 1: Set up of Simulation Parameters	44
Table 4. 2: Comparison of Various Scenario Results.....	59

ACRONYMS AND ABBREVIATIONS

ABIDS:	Anomaly Based Intrusion Detection System
AGT:	Agent
AODV:	Ad Hoc on-demand Distance Vector
AOMDV:	Ad hoc on-demand Multipath Distance Vector
BHA:	Black Hole Attack
CBR:	Constant Bit Rate
DoS:	Denial of Service
DSDV:	Destination Sequence Distance Vector
DSN:	Destination Sequence Number
DSR:	Dynamic Source Routing
DT:	Device Tampering
E2E:	End-to-End Delay
GUI:	Graphical User Interface
ID:	Identification
IEEE:	Institute of Electrical and Electronics Engineering
IN:	Intermediate Node
IP:	Internet Protocol
MANET:	Mobile Ad hoc Network
MBRA:	Multiple Black Hole attack
MCN:	Multi-hop Cellular Network
MID:	Malicious Node ID

MNT:	Manipulation of Network Traffic
NHN:	Next Hop Node
NID:	Node ID
NS2:	Network Simulation Two
OLSR:	Optimized Link State Routing protocol
PDA:	Personal Digital Assistant
PDR:	Packet Delivery Ratio
RERR:	Route Error
RP:	Routing Protocol
RQ:	Research Question
RREP:	Route Reply
RREQ:	Route Request
SBHR:	Single Black Hole Attack
ST:	Simulation Tool
TCP:	Transfer Control Protocol
TCL:	Tool Command Language
TGP:	Throughput for Generating Packet
TORA	Temporarily Ordered Routing Algorithm
TSP:	Throughput for Sending Packet
TRP:	Throughput for Receiving Packet
UDP:	User Datagram Protocol
WAN:	Wireless Ad Hoc network
ZRP:	Zone Routing Protocol

ABSTRACT

Mobile Ad hoc Network suffers from many attacks due to a lack of centralized authorized system. In the existing works, the protection mechanisms of a network from attacks are by using only encryption-decryption software and firewalls, which have less security. Since MANET has no authorized system, it exposes too many attacks such as jellyfish attack, the man in the middle attack, selfish node attack, wormhole attack, Dos attack, Sybil attack, and black hole attack. Among those attacks, black hole attack is a realistic and difficult attack in MANET. It against network integrity, confidentiality, and availability by absorbing and dropping data packets in the network while the sender node sends to the destination node. Due to the interruption of the black-hole attack, data packets cannot reach to the target node. Black Hole Attack damage mobile nodes by sending a forged RREP immediately to the sender node before the receiver node reply. In this thesis work, we evaluate the impact of single black hole attack as well as multiple black hole attack and minimize its consequence by applied Anomaly based IDS approach under Ad hoc on Demand Multipath Distance Vector to improve the performance of MANET. As we have seen, the simulation result using NS2 the proposed ABIDS approach is an efficient approach to reduce black hole attack in terms of Jitter, Throughput, and End to end delay. This regards the performance of AOMDV protocol is improved in MANET because of using the proposed ABIDS approach.

Key Words: MANET, SBHA, MBHA, ABIDS, AOMDV, and BHA

CHAPTER ONE

INTRODUCTION

This chapter initially describes the general introduction to MANET and BHA. Then, it explains the overall objective of the study, methodology, motivation, scope, limitation of the thesis, and statement of the problem addressed in this thesis work. Finally, describe the organization of the thesis.

1.1 Background

MANET is an infrastructure-less network technology, which is suitable to configure for emergencies like natural disasters and other community service area. Mobile nodes dynamically moved in MANET and the connection between nodes can change continuously. In MANET, nodes have limited battery life and high-energy consumption. The security issue is concerned for effective communication and data forwarding between different nodes. Mobile nodes in MANETs are free in acquiring and enter the network dynamically. Mobile Nodes or any network devices such as laptops, MP3 players can form a random network structure, by configuring dynamically with one another within the network. These nodes have the power to configure themselves because of their self-configuration ability [1][2].

The term ad hoc denotes the configuration of a network for a particular purpose, often-wireless network applications. It is an infrastructure-less wireless-network. It can configure anywhere easily and less costly in terms of infrastructure cost. Lack of the central system and sink node makes the network operations more complex than other types of wireless networks such as cellular networks or wireless local area networks. The high increment of customer, cheaper, smaller, and lot of powerful mobile devices, MANET became one of the quickest growing areas of Wireless Networks. Mobile nodes will act as host/router on this network simultaneously [3]. In today's world, there are many MANET applications on practice because mobile nodes can enter the network randomly at any time. Various types of MANET importance incorporates those emergency activities, for instance, volcano eruption, flood, and earthquake. Data packet transmitted from the sender node to the receiver node through suitable network components. In addition to the above advantages in MANET, the communication can use in Military application among the soldiers, vehicles, and headquarters of the military. The commercial environment is also MANETs application to share the daily updates of authority works among sectors [4], [5].

The black hole attack is a denial of service attack, which can degrade the performance of MANET. This attack node forwards a fake RREP to the sender node instead of a real reply. BHA may cause to numerous damage network operations in MANET. In this thesis work, the researcher proposes a new algorithm to minimize the consequence of BHA using Anomaly Based IDS approach under AOMDV routing protocol in MANET. The main aim of this study is to improve security by minimize BHA and evaluate the consequence of single as well as cooperative BHA. The new proposed algorithm enables to detect and minimize BHA in MANET under AOMDV routing protocol [1][6].

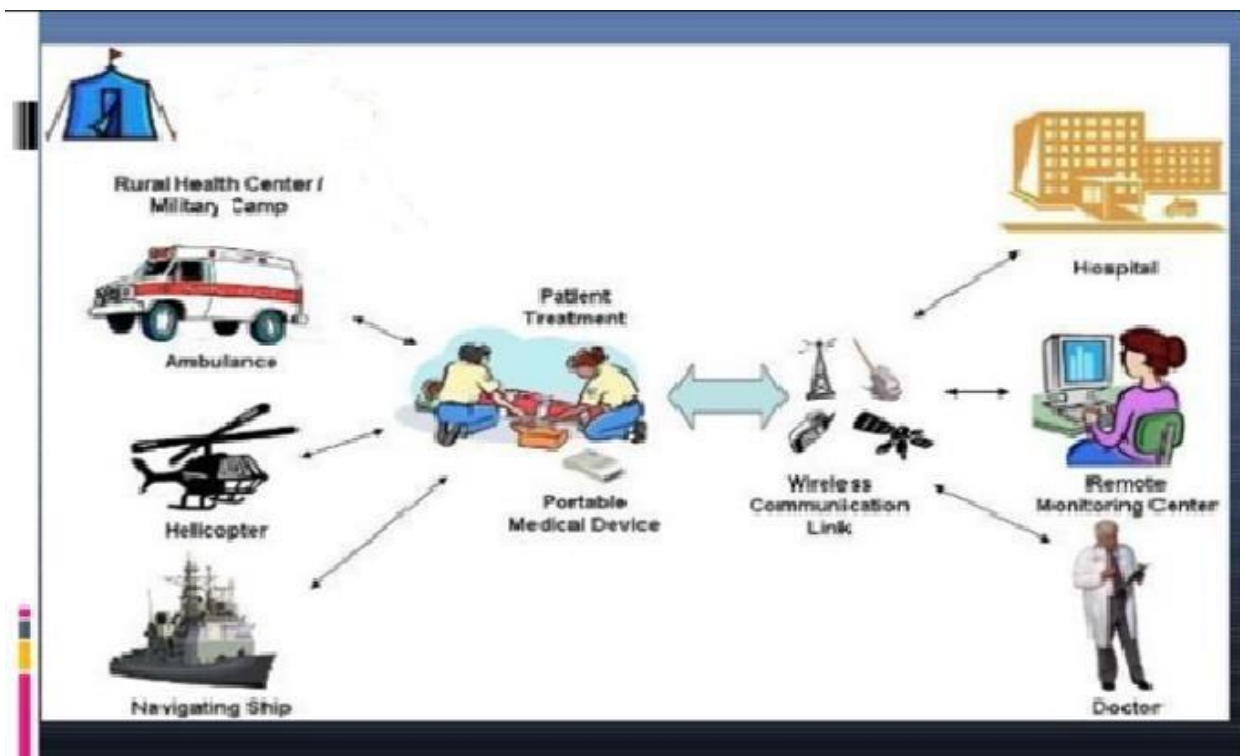


Figure 1. 1: MANET for Rescue Operation [6]

The nature of mobile devices in Ad Hoc is autonomous Failure of a communication link in MANET frequently because of the mobility of the nodes dynamically within a short period of time [7]. The size of MANET depends on the number of mobile devices that are connected to the network topologies dynamically [8].

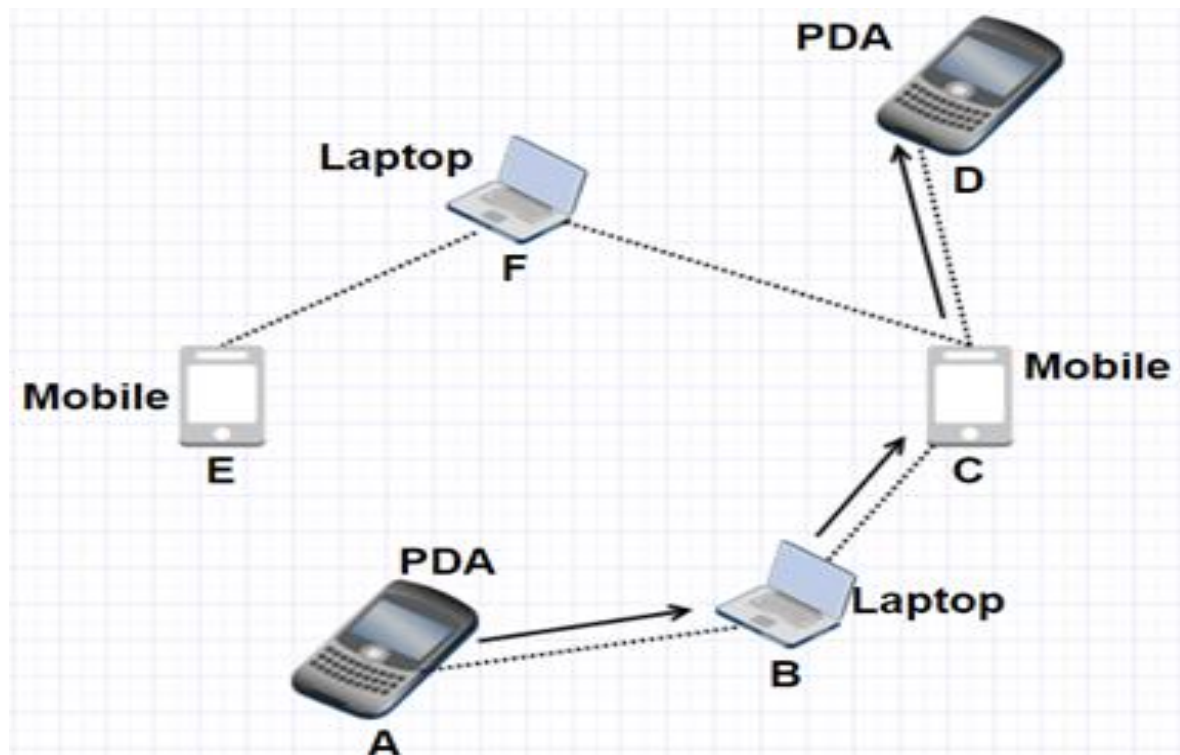


Figure 1. 2: Mobile Ad Hoc Network Structure [8]

1.2 Motivation

MANET is one of an infrastructure-less wireless network without any central authority to monitor any network activity. A number of issues exist in MANET regarding security, performance, confidentiality, and reliability. Due to its security limited, mobility, no fixed infrastructure and scalability, it suffers from any network problems. Nowadays the usage of wireless network increased day to day rapidly. Ad hoc Network is a hot academic research area to improve its performance. Since it is a researchable area in terms of minimizing BHA to improve the network performance for efficient communication [9].

The black-hole attack is a DoS network layer attack, which can drop a large number of packets within the Ad hoc network. Because of the nature of the attacker, the researcher is motivated to investigate the consequence and minimize its impact. To improve the network performance and ensure the security, the researcher has been modified the AOMDV routing protocol in MANET. Since MANET is an emerging technology, it is vulnerable due to its dynamic topology and other fundamental characteristics [10].

1.3 Statement of the problem

The security issue is the main concern for integration, availability, and performance of the Network. BHA is an active attack, which affects network operations. When the sender node forwards RREQ to the neighbor nodes through on multiple routes, due to the presence of BHA the malicious node sends a false reply with highest DSN. A major statement of problem on this thesis is that black hole attack drops data packet by claiming a fresh route to the receiver node. When the RREQ reaches to malicious nodes, the malicious node immediately sends fake RREP to the sender node then the sender node sends data packets to malicious node [11].

BHA in MANET can cause vast degradation of network performance because it drops packets before reach to the target node. Massive loss of packets occurs with the existing of BHA by having a modified highest sequence number. This thesis work examines the impacts of BHA including how much this attack interrupts the communication of nodes under AOMDV routing protocol in MANET. Previous researches conducted on BHA in MANET on different IDS approach under AODV, DSR and DSDV Protocols. This study regards proposed the security mechanism in MANET under AOMDV routing protocol to minimize black-hole attack by using ABIDS approach [12]. The effect of single and multiple black hole attacks are not investigated in previous works using this proposed approach.

1.4 Significance of the Study

This study simulates single and co-operative black hole attack with AOMDV routing protocol in MANET and examines its consequences. The simulation would be performed on under standard AOMDV routing protocol, with SBHA, with MBHA, and with ABIDS proposed an approach using real simulation tool, which is NS2. Hereafter, this study would be reduced the impact of black hole attack to safeguard information and network security under reactive protocol in MANET using ABIDS approach. The significance of this study is to reduce BHA using ABIDS proposed approach under AOMDV protocol in MANET to improve security goals such as network performance and network reliability for its application area. The simulation of the thesis work evaluates in terms of those performance metrics like Throughput of (sending, receiving and generating packets), Jitter, packet dropping time and end-to-end delay.

Research Question

RQ1: How to evaluate and simulate SBHA, MBHA and Standard AOMDV in MANET?

RQ2: How to the proposed algorithm minimizes the effect of BHA under AOMDV in MANET?

RQ3: How to determine the efficiency of the proposed solution to minimize BHA under AOMDV routing protocol using quantitative performance metrics such as throughput of sending and receiving packets, end to end delay and jitter?

1.5 Objective of the Study

1.5.1 General Objective

The aim of the thesis is to minimize black hole attack and study its consequence on AOMDV Routing Protocol in MANET by using Anomaly Based IDS approach.

1.5.2 Specific Objective

- To analyze the effect of black hole attack in MANET
- Simulating standard AOMDV routing protocol, AOMDV with single, multiple black hole attack through NS2 tool.
- Reduce BHA under AOMDV RP in MANET using the proposed Anomaly Based Intrusion Detection Approach.
- To compare the proposed solution simulation result with the standard AOMDV

1.6 Research Methodology

There are a number of methods used in order to achieve this proposed work to its objectives. These are:

- Collecting papers, thesis, journals, conference document and other useful resource on a black hole attack and its mitigation method
- Investigating the collected resource and understand its core idea
- Exercising and understand about NS2 for this study to make effective simulation
- Reviewing MANET behavior and its acts when it is under attack or not
- Applying an Anomaly based IDS method to reduce black hole attack on MANET
- Modify the AOMDV Protocol by Using IDS-AOMDV proposed algorithm
- The work is simulating by NS2 because it is discrete event simulator provides simulation for TCP, Routing and multicast protocols.

1.6.1 Research Framework

Research framework briefly describes the individual steps that we follow throughout the study. It used as a guide for researchers to define the framework of the thesis. This study contains mainly four phases. **Phase 1** investigates different IDS methods to detect minimize SBHA with reactive protocols in MANET. **Phase 2** implemented under a normal environment i.e the standard AOMDV Routing protocol without any single as well as cooperative BHA. **Phase 3** states the simulation analysis of the effect in MANET with the presence of single as well as cooperative BHA on different scenarios independently. **Phase 4** in this phase, we simulate and analyze AOMDV Protocol with a proposed solution to minimize BHA in MANET in the same simulation network environment. After simulating the module using the proposed anomaly-based IDS algorithm to minimize BHA, we evaluate the simulation result. Finally, compares the results found from Phase2, phase 3 and phase 4 then the performance of proposed solution to minimize BHA would be evaluated on ns2 using in terms of different performance metrics such as throughput of sending, receiving, generating packets, end to end delay and jitter [13].

1.6.2 Network Simulator

Network simulation is a free source network simulator, and it is compatible to run on different platforms such as Unix operating system, Linux system, and Mac system [14]. Network simulator is an object-oriented simulator, which written in C++ and OTCL as frontend. Tool Command Language is a front-end language used to write TCL scripts for network simulation. NS2 is an open-source tool and widely used for network researchers to simulate various network types and routing protocols such as TCP, UDP, FTP, and traffic sources like CBR on different networks. The researcher simulated the simulation using the latest version of ns2, which is 2.35 [14], [15].

Simulator	Qualnet	OMNET++	NS2	Opnet	J-sim
Language Supported	Parse c C++	C++	C++/OTCL	C++/Java	Java
Licensed	Commercial	Open source	Open source	Commercial	Open source
GUI support	Excellent	Good	Poor	Excellent	Good
Time taken to learn	Very easy	Moderate	Long	Long	Moderate
Platform	Linux	Linux, Mac-OS , Unix	Unix, Mac-OS Window	Window, Linux and Solaris	Math lab

1.7 Scope and Limitation of the Study

1.7.1 Scope of the Study

This work mainly focuses on minimizing and investigate the consequence of single as well as multiple BHA under AOMDV routing protocol in MANET. Anomaly Based Intrusion Detection Approach applied to minimize black hole attack. The simulation result of the study evaluated after the simulation took place on SBHA, MBHA, and standard AOMDV scenarios.

1.7.2 Limitation of the Study

Many issues are concerned with the performance of MANET like remaining energy, network lifetime and security. This thesis does not incorporate other attacks, such as worm whole attack, jellyfish attack, selfish node attack, spoofing attack, slide-channel attack, and man of the middle attack.

1.8 Organization of the Thesis Work

This thesis organized into five Chapters. Those chapters describe briefly different topics. The first chapter briefly described about the background and introduction of the thesis work. The second chapter focuses on literature reviews of the basic nature of BHA, detection mechanism, and prevention of BHA on different reactive protocols like AODV, DSR, DSDV, AOMDV and related works in MANET area. The third chapter describes the proposed solution architecture of the study and the detailed algorithm using flow chart diagram to reduce BHA. The fourth chapter describes the simulation result and discussion of the study. Finally, the fifth chapter describes the, summary of contribution, conclusion and future work in this research area.

CHAPTER TWO

LITERATURE REVIEW AND RELATED WORK

2.1 Literature Review of Mobile Ad Hoc Network

This chapter focuses to review nature of MANET, security issues that affect MANET operation and nature of protocols. The researcher reviewed various papers on MANET area, which conducted to minimize and prevent single as well as multiple black hole attacks with different Routing protocols such as DSR, DSDV, AODV, and AOMDV. In MANET, some of the routing protocols are DSR, AODV, AOMDV, DSDV, TORA, and ZRP [16].

2.2 Routing Protocol Classification in MANET

Routing is a way of choosing a route in a network to transfer the data packet from the sender node to the receiver node. The growth in industry MANET was rapid in the 1990s. There was a demand for a new set of protocols and strategies for efficient communication in the infrastructure-less mobile network. Because of the limited resources and mobility of mobile nodes in the wireless networks, the existing TCP/IP structure is modified and refined for efficient function in MANET. Routing is an important topic and a challenging task in MANET, which gained the attention of the researchers to conduct researches on it. The categorization of routing in MANET protocol shown below (Figure 2.1). Because of their functionality, routing protocols mainly categorized into three. Those routing protocols are Reactive, Proactive and Hybrid protocols [17], [18]. Insecure and improper routing will not only degrade ad hoc network performance but also exposed to various security attacks.

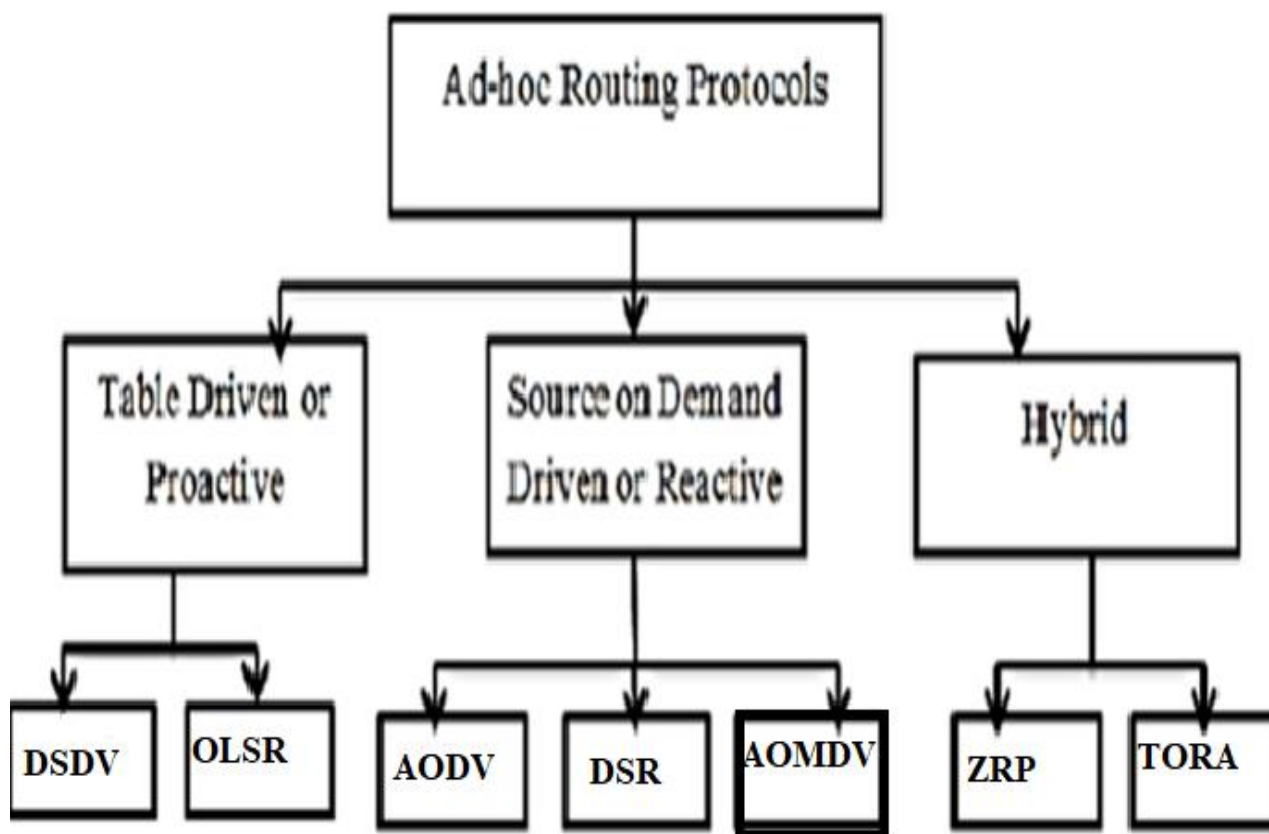


Figure 2. 1: Routing Protocol classification in MANET [18]

2.2.1 Reactive Routing Protocols

This type of routing protocol does not maintain the network topology information. In a reactive routing protocol, the correct path is required during packet transmission or communication. In a reactive routing protocol, the routes are currently in use within the network. These types of protocols also known as on Demand Routing Protocols. It has no information before defined for routing. To determine a new route whenever a transmission is necessary, a source node requests for the route discovery phase. The flooding algorithm is the base to route discovery mechanism, which implements the technique that the node transmits the data packet to its neighbor nodes and also sends the data packet to intermediate nodes repeatedly till the packets reached to destination node [18], [19]. AODV, DSR, DSDV, and AOMDV are some of the reactive routing protocols.

2.2.1.1 AODV Routing Protocol

AODV is simple, efficient, and an effective routing protocol for MANET, which has dynamic topology. AODV has smaller routing overheads as compared with DSR and DSDV routing protocols. AODV is a combination of both Dynamic Source Routing and Destination Sequence Distance Vector. AODV routing protocol shares the most important concepts from DSR and DSDV routing protocols. AODV determines a route to a target only when a node wants to send to that receiver node. The Protocol consists of two phases (Mesut Günes et al) [20].

I. Route Discovery packet (RREQ, RREP message)

II. Route Maintenance packet (RRER, Hello message)

2.2.1.2 AOMDV ROUTING PROTOCOL

An ad hoc on-demand distance vector routing protocol is a multipath routing protocol in MANET. It works based on, on-demand of route protocol when it is essential to send the data packet from the sender node to the receiver node. AOMDV is an extension of the Destination Sequence Distance Vector protocol. DSDV creates a small network. Every node in a DSDV routing protocol wants to maintain whole routes for every destination within the mobile network. The main advantage of AOMDV is to reduce the number of RREQ broadcasts. RREQ broadcasts continuously until reach to the target node. Once finish the routing process, the sender node and the target node can be communicated and send the packets between them. When any node knows a link break or crash, Route Error (RERR) sent to all other nodes. The hello message is used for detecting and monitoring links to a neighbor [21].

When all the routes fail in AOMDV, route discovery is required to establish communication between nodes. Its advantage is to manage the load on the network and avoid the impact of congestion and increase integrity, security, and reliability of the ad hoc network [22].

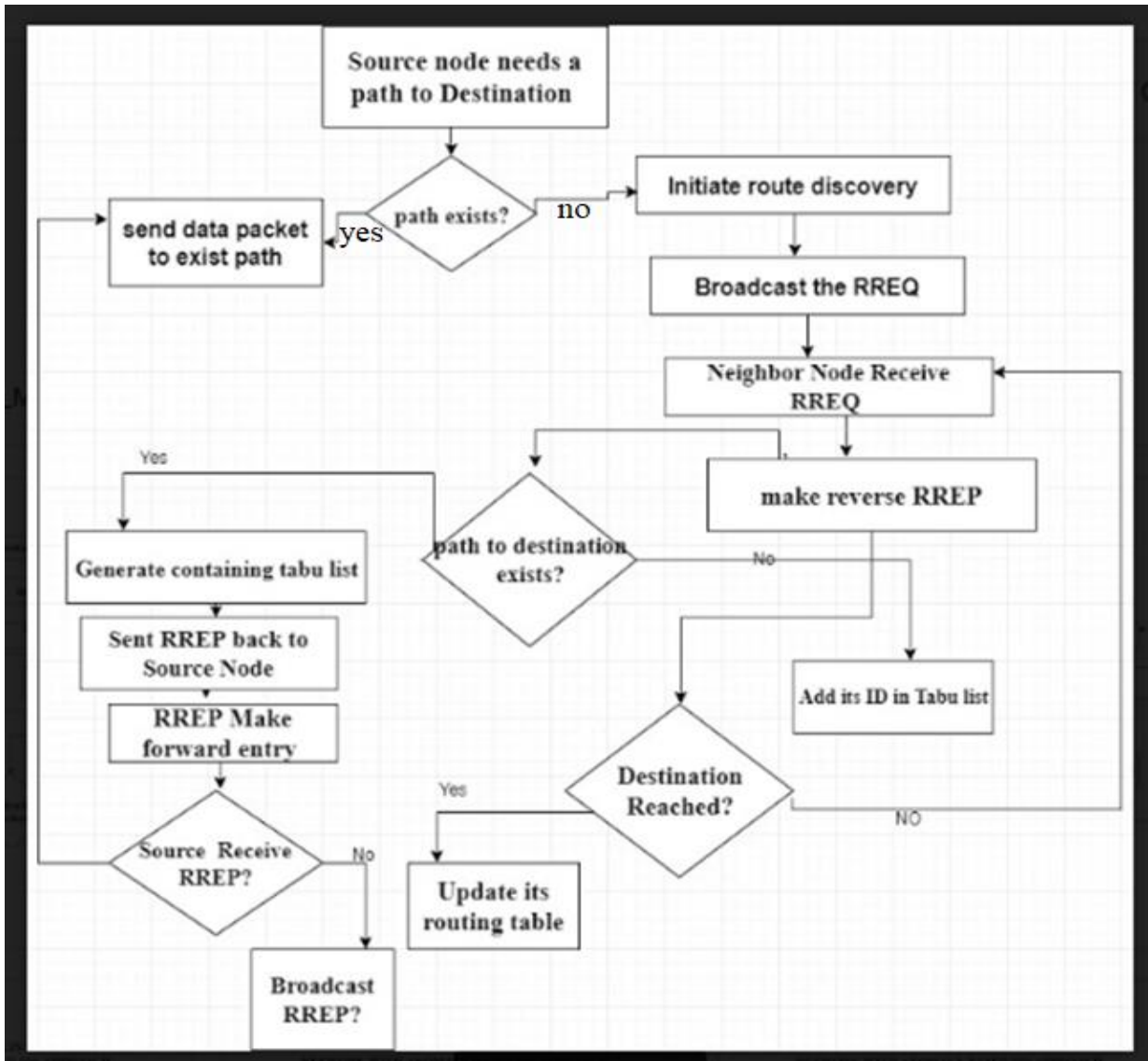


Figure 2. 2: Route Discovery Process in AOMDV Protocol [22]

AOMDV creates multiple link-disjoint and loop-free paths. AOMDV routing protocol consists of two types of phases. A route update rule is used to established and maintain multiple loop-free at each node and a distributed protocol to find link-disjoint paths.

- Route Discovery (RREQ, RREP Message)
- Route Maintenance (RRER, Hello Message) [22].

Table 2. 1: Fields of RREQ and RREP

RREQ	RREP
Source Address	Destination Address
Source Sequence Number	Hop count
Destination Address	Destination Sequence Number
Destination Sequence Number	Source Address
Hop count	Lifetime

I). Advantages of AOMDV protocol

- It creates a path on demand
- It maintains connectivity
- Fast and recovery from failures
- It creates a loop-free route

II). Disadvantages of AOMDV

The drawback of using AOMDV protocol, it has more message overheads during route discover because of having a large number of routes. In this reactive protocol, the receiver node replies to numerous RREQ in a longer overhead and numerous RREP to single RREQ may lead to less network operation[23].

2.2.1.3 DSR Protocol

Dynamic Source Routing is a routing protocol, which designed for specifically in multi-hop wireless mobile devices. DSR permits the network to self-configuring and self-organizing, without any need of existing network infrastructure. In DSR RREQs data packet flooded throughout the network when the source node sends packets to the destination node. If the receiving node is not the destination node, route request receiving nodes rebroadcast the packets

to other intermediate nodes. Due to its simplicity, DSR is a well-known reactive protocol for Ad hoc networks, which is originally developed by Johnson, Maltz, and Broch [24].

2.2.2 Proactive Routing Protocols

This type of protocol is known as a table-driven protocol in which all the route information maintained in the routing table. The packets transferred over the network in a specified way and predefined route in the routing table. In a proactive routing protocol, the data transmission has done faster but the routing overhead is high because all the routes defined before transmitting the data packets to the receiver node. DSDV, OLSR protocols are examples of Proactive Routing protocols (Optimized Link State Routing) [25].

2.2.2.1 Destination Sequence Distance Vector Protocol

DSDV routing protocol is a proactive routing algorithm in MANET. In DSDV protocol, every node i keeps for each destination x , if $d_{ik}(x)$ equals $\min_i \{d_{ij}(x)\}$. In this manner, the shortest path is selected along x [26].

2.2.3 Hybrid Routing Protocol

The hybrid protocol is the combinations of reactive routing protocol and table deriving routing protocols. This type of protocol can be beneficial from both of these routing protocols. Because of this searching routing process is quick in the routing Zone. ZHLS, ZRP, and SHARP protocols are some of Hybrid Routing Protocols [26].

2.2.3.1 Zone Routing Protocol

As its name indicates zone routing protocol focused based on the zone concept. The aim of ZRP is to solve a problem by combing both properties of on-demand and table-driven routing protocols. Therefore, Zone Routing Protocol reduces the scope of a proactive routing protocol. ZRP is easy to maintain routing information in a limited zone. Nodes, which are further each other, can be reached using reactive routing [27].

2.2.3.2 Zone-Based on Hierarchical Link State Routing Protocol

Due to different approaches to the routing protocol, Zone based on HLSRP is a hierarchical protocol. This protocol categorized into non-overlapping zones. In ZHLS all the network nodes configure two routing tables, such as the intra-zone routing table and inter-zone routing table [27].

2.3 MANET Attacks

The security issue is a researchable issue in MANET, because of its exposure to different network attacks. Since MANET has no administrator for the sake of security, it can be affected easily by different attacks. The performance of the network is indispensable for effective communication between different mobile nodes in MANET. There are various types of network attacks, which can interrupt network behavior. Attacks are network intruders that could degrade the performance, availability, and integrity of MANET. Attacks mainly categorized into two main classifications of attacks, known as passive and active attack. A passive attack achieves information transfer in the network without changing and disturbing the network operation. The active attack causes to damage the entire network performance because of, its highly dropped data packets in MANET. Generally, the active attack can easily identify and easy to prevent through different prevention mechanisms such as encryption-decryption, signature-based intrusion detection, specification-based IDS and the threshold value. The distributed operation, dynamic topology, and resource constrain are some of the unique characteristics of that exist in MANET, which increase the vulnerability of this network [28]. Diagrammatically the classification of attacks in MANET describes in figure 2.3 [26].

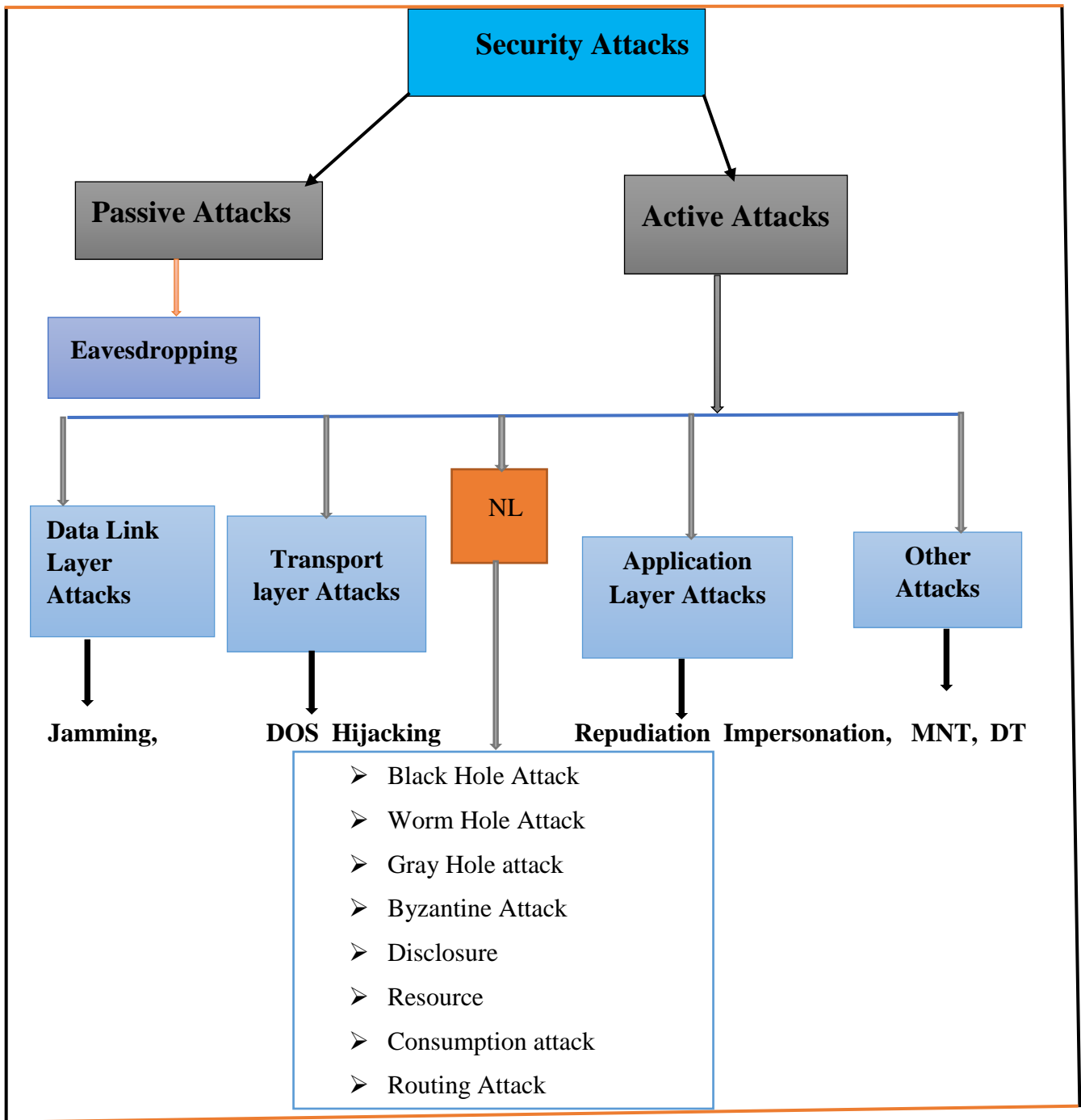


Figure 2. 3: Classification of Attacks in MANET [26]

2.3.1 Passive Attack

This type of attack is hard to recognize and to prevent easily as compared with an active attack. The passive attack can get easily the information in MANET, which does not intend to disrupt network operations. Those attacks, just to intrude the information communication within the network without any modification and fabrication of information. The detection of this type of attack is difficult because neither the critical network functions nor the system resources are physically affected to prove the intrusions [29]. Those attacks interrupt information transmission in MANET [30],[31].

2.3.2 Active Attack

An active attack is a realistic attack, which attempts to disturb or demolish the communication within node devices in MANET. It causes a series changed to the quality of operation in the network. Those attacks can be recognized and prevent easily in the network. In MANET malicious node and unwanted nodes are interrupt the performance, availability, accuracy, integrity, and security within the network [30].

2.3.2.1 Nature of Black Hole Attack

Black Hole is an astronomic term, which is the region of space in a gravitational field and it is a powerful and not even light. It is an active attack, which can be, interrupt the network operations. Due to its nature, it can claim during route discovery the sender node has a fresh route from a sender node to the receiver node. BHA always replay forged information with the highest destination sequence number to the source node. When a node intrudes with BHA, the malicious node replies a forged RREP to the sender node. The sender assumes that the route is the shortest path then broadcast packet contents to the target node but before reach, to the destination node, the packet would drop. The routing wrongful conduct degrades the network performance by dropping the information packet or capturing the data packets in the network[9].

- ✓ The BHA send false route information.
- ✓ BHA that passes through malicious nodes will drop all data.
- ✓ The sender continuously tried to send data even there is a failure number of times by malicious node.

BHA is a realistic attack and can interrupt the communication operation between nodes in MANET. The impact of BHA is to increase the traffic congestion, high drop packets low

throughput to send, receive and generate packets in a network. A malicious node drops data packets instead of transmits to the destination node. The intention of the malicious node is to disturb the pathfinding process by delivered the fake route replay packets for the source node. Due to the existing of BHA in AOMDV routing protocol, the malicious node sent the fake route replay (with a fake highest destination sequence number) to the sender node by claiming fresh route has a sufficient fresh route to the receiver node. Therefore, all packets will be sent through the malicious node and then data packets will be swallow or dropped [26]. The black-hole attack mainly classified as single and cooperative BHA.

2.3.2.1.1. Single Black Hole Attack

SBHA claims itself as a real route to the target node than the other routes. When the sender sends a data packet to the receiver node, the malicious node drops and does not send to any neighboring nodes [32], [5]. In SBHA only a single malicious node is involved in MANET [33].

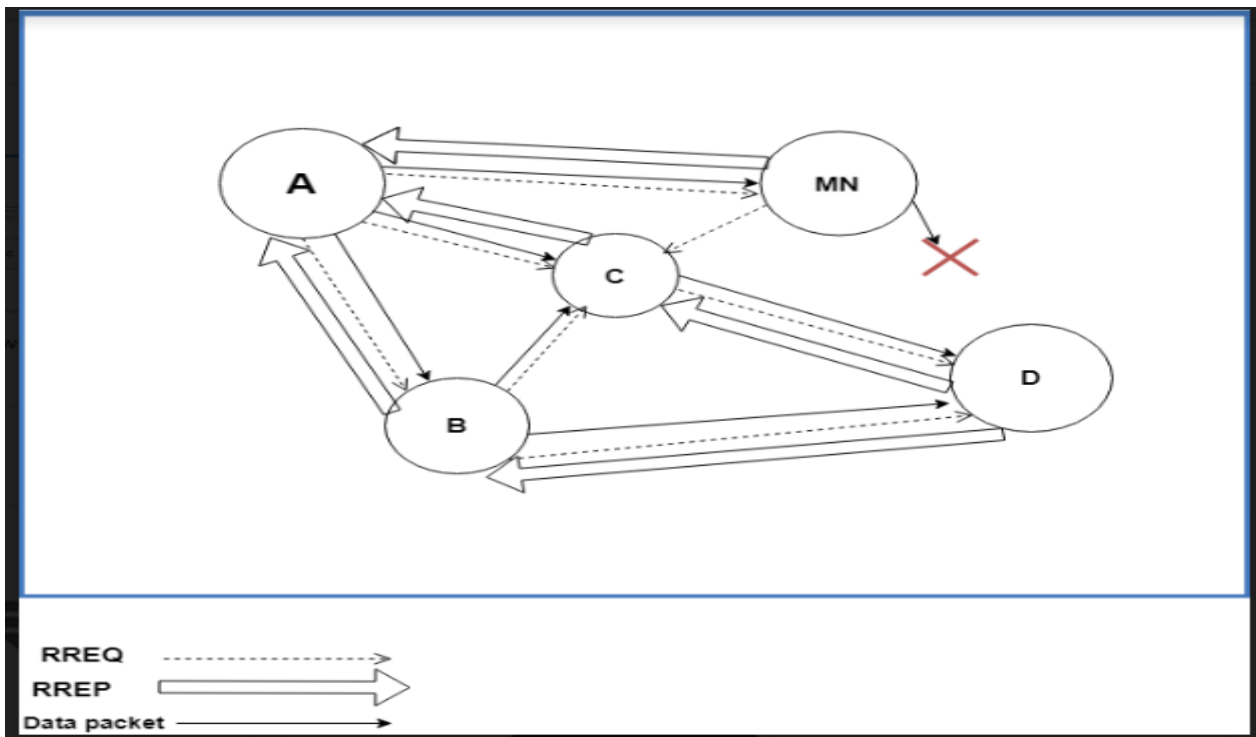


Figure 2. 4: Single Black Hole Attack in MANET [33]

2.3.2.1.2. Cooperative (Multiple) Black Hole Attack

This attack intrudes two or more mobile nodes by working together in the simulation network environment. This type of BHA causes series damage in MANET operation performance. The malicious nodes wrongly replay to route request by claiming the route to the destination node then data packets are dropped [1], [5].

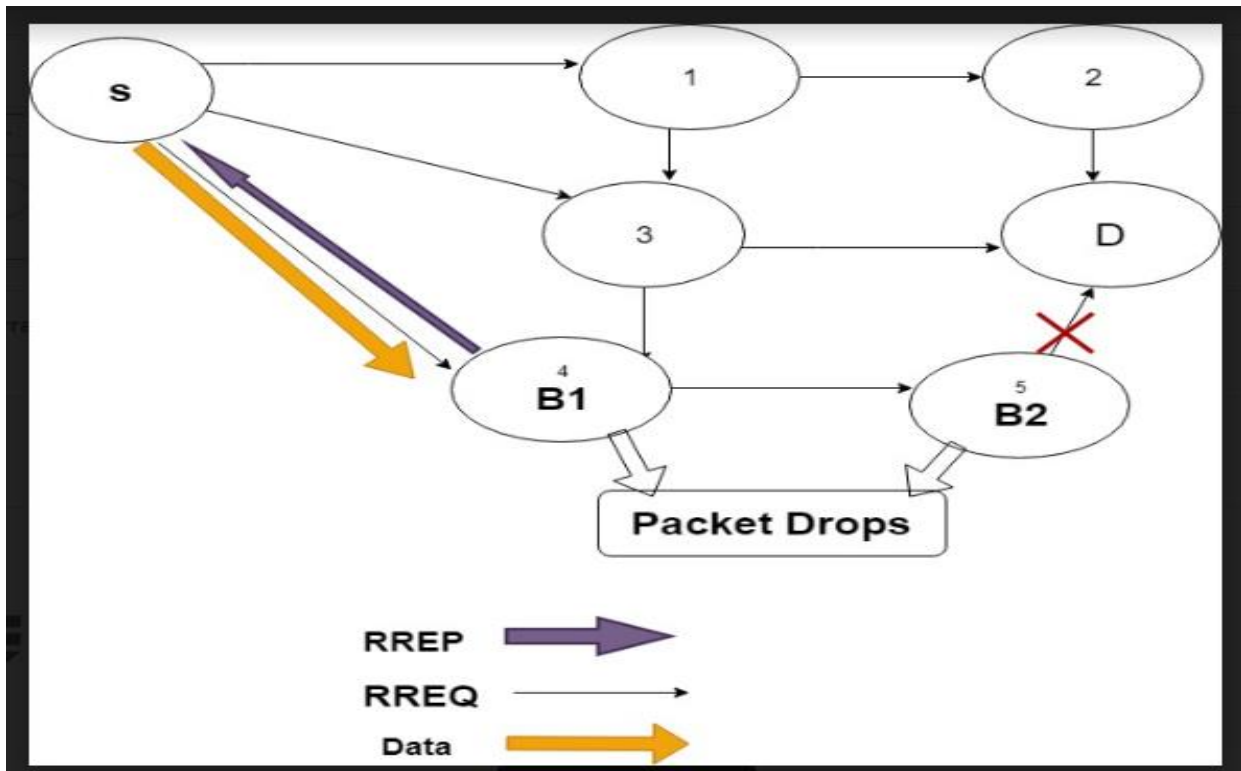


Figure 2. 5: Cooperative (Multiple) Black Hole Attack in MANET [5]

2.3.3 Intrusion Detection System

Intrusion detection approach is the process of controlling any abnormal activity that occurs in a MANET network, which threatens violations of computer security system or standard security system. Different IDS system has a vital role in analyzing and minimizing attacks for possible effective network operation. IDS categorized into two major categories. Network-based IDS, which runs on a network, and obtained data from malicious nodes and Host-based IDS which acquires the data through hope rating system's log files that run on the node [34][35]. Depending on the detection systems used, host-based IDS categorized into three main categories as listed below.

2.3.3.1 Signature Based Intrusion Detection System

This approach compares the known threats with unknown threats to investigate events for recognizing intrusion activity. It is a very vital approach to distinguish known threats but is mostly unsuccessful in detecting unknown threats and any other different known threats. Signature Based Intrusion Detection System cannot detect and understand complex communications, so it cannot detect most attacks that include various events [36].

2.3.3.2 Anomaly Based Intrusion Detection System

It is a type of intrusion detection approach which enables to distinguish and can prevent the unknown threats or novel activity of intrusion in MANET. Anomaly Based IDS approach enables to monitor the characteristics of the different activity of attacks. The IDS compares the feature of current activity to a threshold associated with the static routing table information. Anomaly Based Intrusion Detection Approach is an effective mechanism to detect and mitigate a novel intruder [37], [38].

2.3.3.3 Specification Based Intrusion Detection System

It describes a collection of constraints that explain the accurate operation of a program or protocol. It checks the program with respect to well-defined constraints. This IDS approach enables to identify previously unknown attacks [39]. Attackers can also be classify based on as per the layer at which the attack happens as shown in the table 2.2.

Table 2. 2: Classification of Attacks per Layer

Layers	Attackers
Application Layer	Data corruption ,Repudiation
Transport Layer	Session Hijacking, SYN Flooding
Network Layer	Black-hole, Gray hole, wormhole, byzantine, Sybil and Jellyfish
Link Layer	Fabrication, Interception, and Modification
Physical Layer	Sniffing and Jamming

2.4 Trace Graph

Mostly NS-2 users use trace graph, which is an essential tool to analyze and simulate the outcome of scenario based on different network performance metrics. It avoids the need to configure and run Perl/AWK scripts for the trace file. The screen of the trace graph shown on figure 2.6.

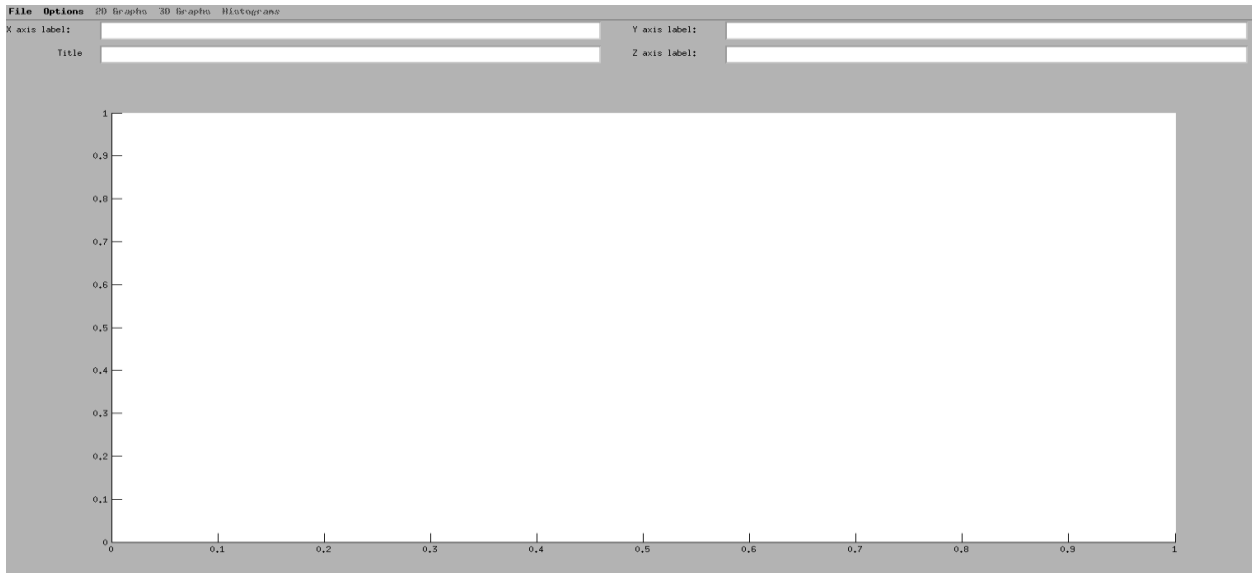


Figure 2. 6: Trace Graph Diagram Window [40]

Trace graph contains the following features.

- ✓ Trace graph can support 238 graphs on different depending upon different parameters in the 2-dimensional area.
- ✓ Trace graph supports 12 graphs 3 Dimension
- ✓ Jitters, delay, processing times round trip time, throughput graphs and statistics can be plotted with trace graph [40].

2.5 Mobility Model

Mobility model is the movement of mobile nodes and it describes how the velocity, location, and connectivity of nodes are dynamically changed at any time. These mobility models are necessary to determine the simulation whenever new changing techniques and environments are applied on mobile devices to get a worthy performance and prominent connectivity in MANET [41]. Some of the mobility models listed as follows.

2.5.1 Reference Point Group Mobility

This mobility model denotes the random motion of a set of mobile devices and in this mobility; there is a random motion individually within the group. Each group contains one leader and a number of members. The mobility of the entire group determined by the behavior of the leader [41].

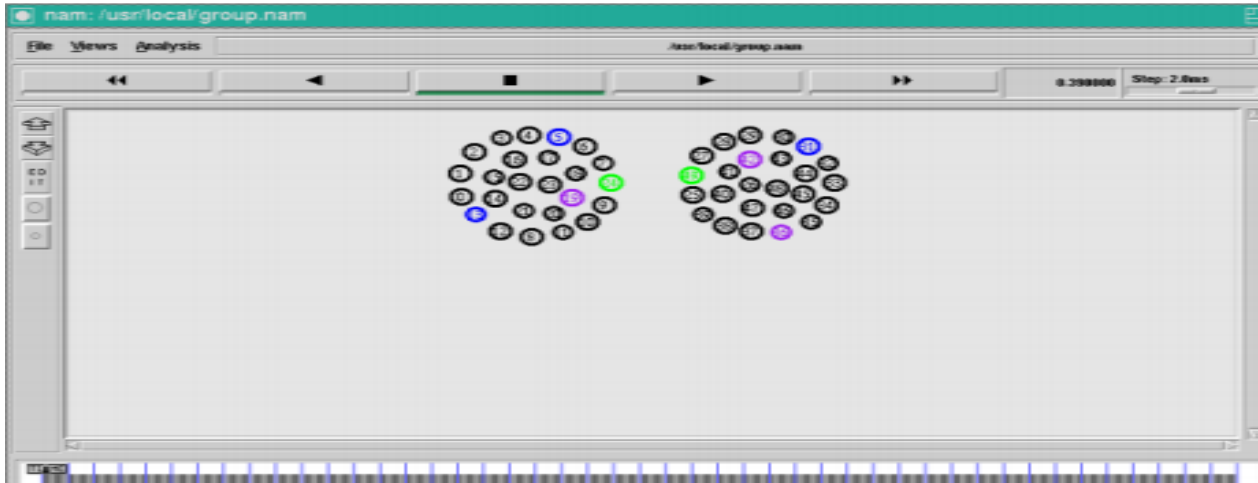


Figure 2. 7: Reference Point Group Mobility [41]

2.5.2 Random Waypoint Mobility Model

In MANET, RWP mobility model is a good mobility model in a wireless network. This model creates a real mobility model in which moves to the random point in the specific network with certain area and moves to a random point. Researcher's commonly choice RWP mobility model because of its simple model to implement and enabling a long run simulation to consider all allocation and node interaction. RWP already implemented in network simulation two and used to implement different network protocols. RWP model simulation starts with the distribution nodes easily in the simulation area [41], [42].

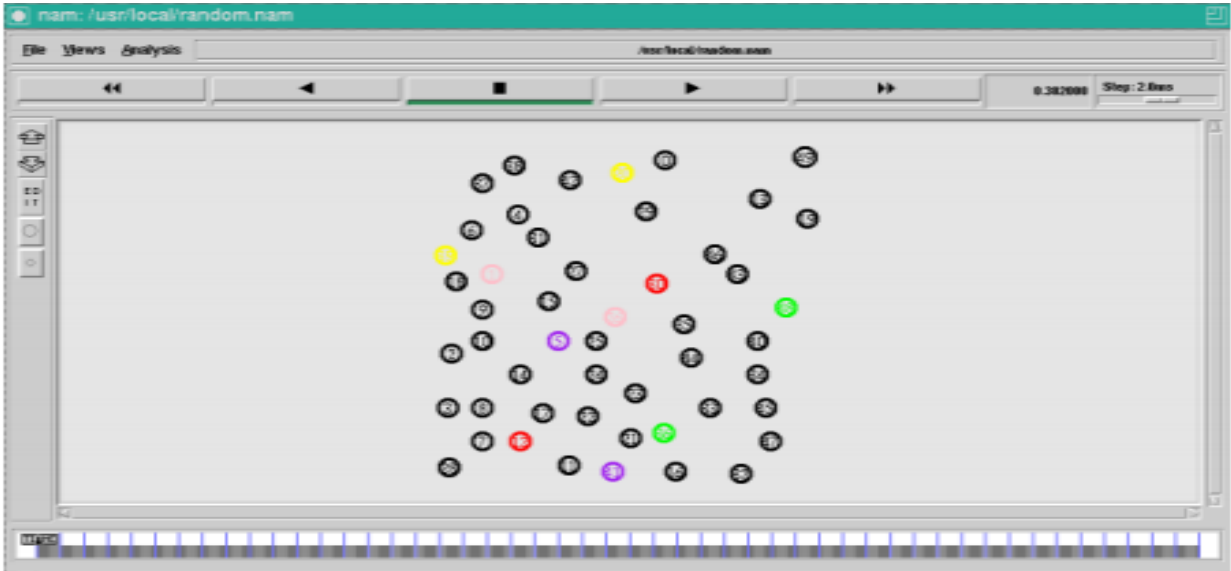


Figure 2. 8: Random Waypoint Mobility Model [42]

Among these mobility models for this study, we have used Random Waypoint Mobility model because of its simplicity and reliability for MANET research.

2.5.3 Freeway Mobility Model

This model follows the motion character of mobile devices freely. There are several freeways on the map and each freeway has paths in both directions.

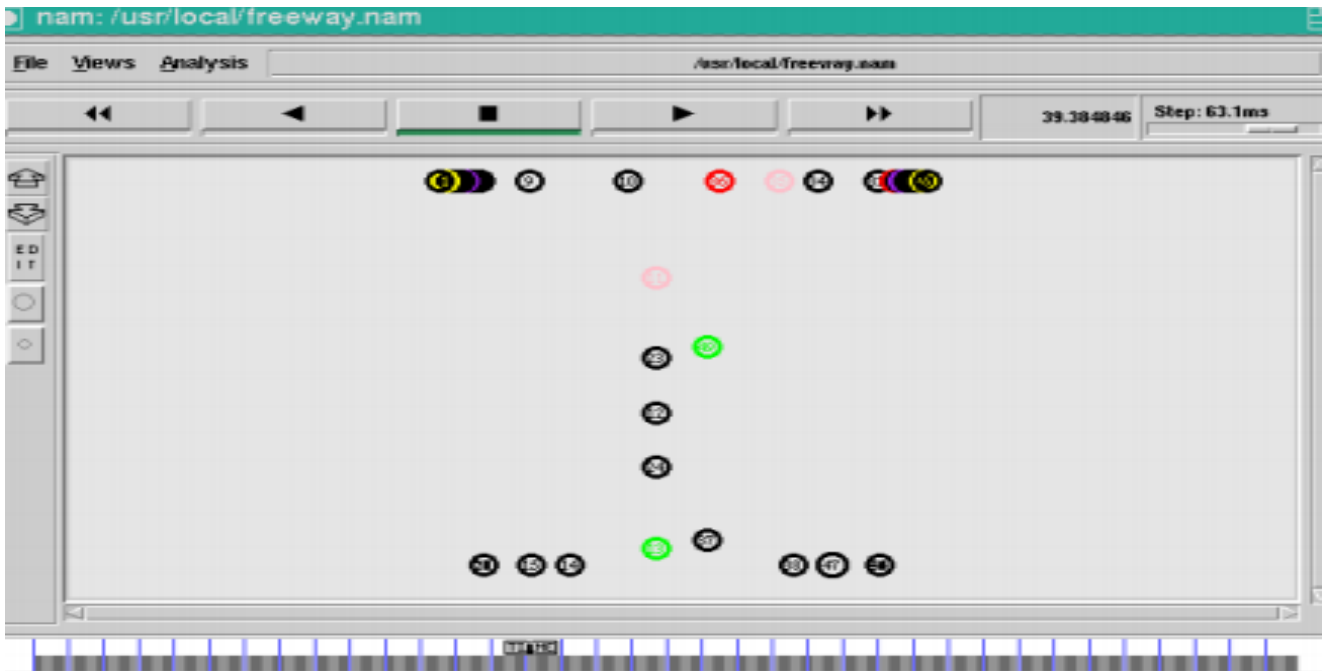


Figure 2. 9: Freeway Mobility Model [41]

2.5.4 City Section Mobility Model

This mobility model gives a realistic movement to nodes located within specific city sections, by restricted to polar coordinate characteristics of mobile devices. CSM model has a map, which contains vertical and horizontal streets. In this model, the mobile device is free to move along the horizontal and vertical lines in the grid at the intersection of vertical and horizontal streets, the mobile node can turn left and right dynamically.

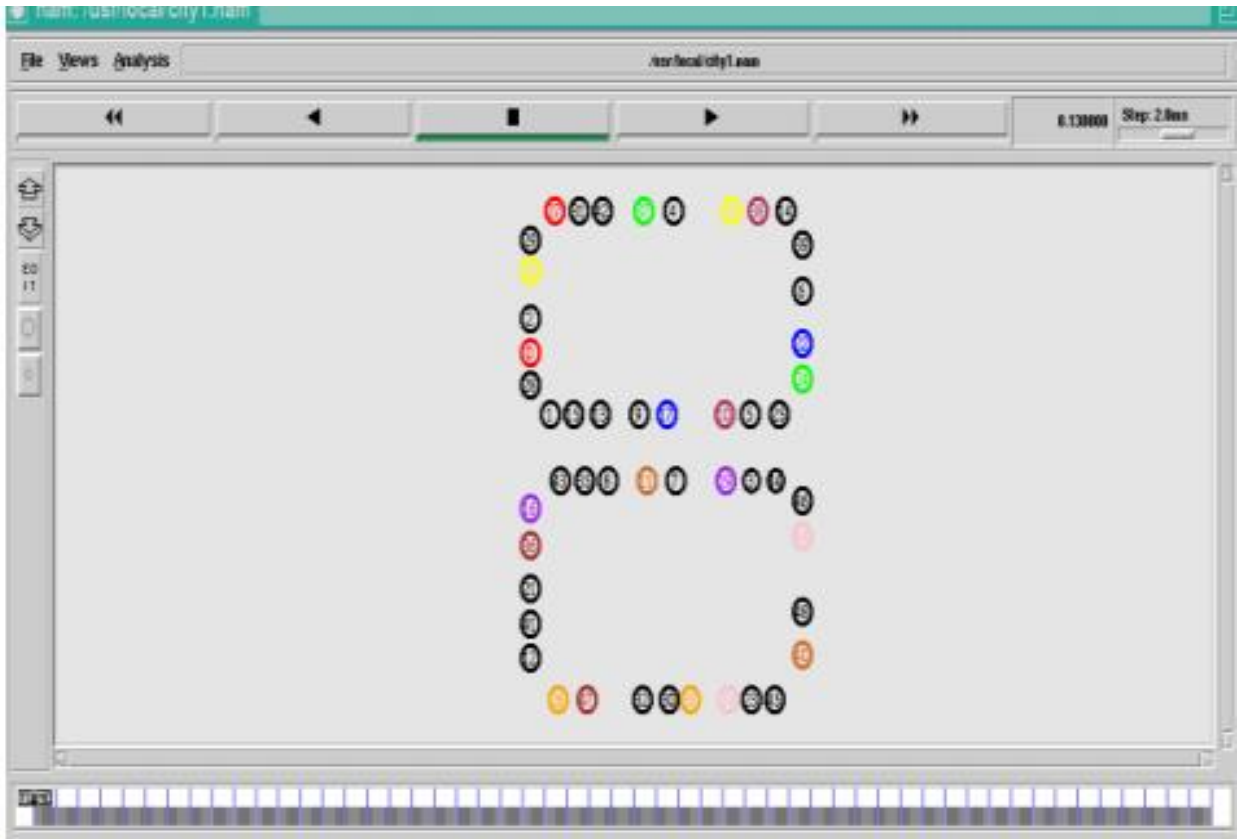


Figure 2. 10: City Section Mobility Model [41]

2.6 RELATED WORK

S. Amutha and Kannan Balasubramanian proposed an algorithm, which has two steps such as checking the difference between the sequence number of the source node and target node. then transfer the data packets in secured route. When the malicious node sends RREP to the sender node with HDSN, than that is in the Routing Table. Compare the source sequence number with the DSN, if it has much more differences between them. it is possible to conclude that the node is the malicious node and discard that entry from the Routing Table [43].

In this work written by Semih Dokurer which title is “SIMULATION OF BHA IN WAN” describes the MANET and the impact of BHA in different views and its impact on the communication in ad hoc network. The main goal of the researcher is to investigate the causes of the initial point of the attack. It allows the attacker to attract all sending packet and drop those data packets. This thesis uses AODV Routing Protocol is the important protocol for finding a path from source to the destination in an ad hoc network. All mobile nodes work in cooperation using the routing control messages to find the path to the destination node. For establishing a path to the destination route requests, route replay, route errors these control messages are required. The writer of this thesis work describes a BHA node absorbs the network traffic and how drops all packets [44].

Dynamic Training Intrusion Detection Scheme for BHA in MANETs, In this paper the writer propose an anomaly detection scheme using a dynamic training method in which the training data is updated at a specific time intervals. The result of the simulation shows the efficiency compared to the conventional scheme with the writer proposed scheme. However, in MANET where the network state changes regularly, the predefined normal state may not accurately reflect the present network topology. In this paper, the researcher uses a reactive routing protocol, which is AODV to analyze the impact of BHA. The destination sequence numbers changed through simulation then, a feature is select in order to define the standard state from the behavior of BHA. In every given time interval the researcher describes a new training technique for high accuracy detection by changing the data and adaptively describing the regular state based on the MANET environment [45].

Neetika Bhardwaj writes the succeeding proposed methodology and Rajdeep Singh, detection and avoidance of BHA in AOMDV protocol in MANETS. In this work, the proposed solution approach implements by sending the data packet through all possible routes, after sending a

random number of packets, the algorithm detects the existence of BHA in Ad hoc network, then destination node is changed to receive packets [32].

In this study, the writer uses Dynamic supply Routing (DSR) protocol, which is on-demand routing protocol. The researcher stated DSR protocol is the combination of two major phases: route discovery and route maintenance phases. Whenever any node wants to send information, before sending the data packet first it checks the route cache for the route to the destination. If it has the correct route to the receiver node, then it uses it otherwise initiate a route discovery process first by broadcasting the RREQ packet, which contains the source address and destination address. RREP is generated whenever RREQ reaches to destination node [46]. The efficiency of suggested techniques as the throughput of the network does not decay in the presence of the black holes [47].

This proposed a new method, it uses a trust-based multipath AOMDV routing protocol combined with a soft encryption methodology, securely transfer messages with different nodes security scheme for MANETs. More precisely, the researcher approach consists those steps: Message Encryption: whereat the source node, Message routing: where the message parts are routed separately through different trust-based multiple paths using a novel node disjoint AOMDV routing protocol and Message Decryption: where the destination node decrypts the message parts to recover the original message [48] .

2.6.1 Summarization of Related Works

Table 2. 3: Summarization of Related Works

<i>Title and Author</i>	<i>Protocol</i>	<i>Simulator</i>	<i>Result of the study</i>	<i>Study Gap</i>	<i>Conference & Publication year</i>
Neetika Bhardwaj And Rajdeep Singh “DETECTION AND AVOIDANCE OF BH IN AOMDV PROTOCOL”	AOMDV	NS-2	The Proposed technique increases the Packet Delivery Ratio	The result of this work evaluates only in terms of PDR but not incorporates other parameters.	International Journal of Application or IE 2014
“Solution To BHA In AODV Routing Protocol ”Written by Ahmed Ibrahim And Nagy Ezaki	AODV	NS-2	A black-hole node cannot decrypt RREQ message and avoid the Black Hole attack. The result of the proposed protocol gives higher security by packet scoring highest packet delivery ratio.	Uses CESAR cipher algorithm can be easily decrypted Performance Evaluation only measured by PDR. No throughput or packet loss is calculated.	JCS A20 15,Department of Computer, Science Arab Academy for Science, Technology &Maritime Transport, Egypt
Semih Dokurer “Simulation Of Black Hole Attack In Wireless Ad-Hoc Networks”	AODV	NS-2	IDSAODV highly detect and remove the attack and decreases total packet	Sometimes this technique doesn't work to conduct more research	A MASTER'S THESIS in CE Atılım University by Semih Dokurer September 2006

Avoidance Of Black hole Attack In	AOMDV	Ns2	PDR and throughput near to the original Values as there were no	calculated to identify the performance	Management(IJ AIEM) May,2014
-----------------------------------	-------	-----	---	--	------------------------------

AOMDV Protocol Manets”			Malicious nodes in the Network. Even the number of malicious nodes increased new approach Produced the same results.	metrics of the proposed work in terms of different mobility and no of node	M.Tech, CS Department, Punjab Technical University, Kapurthala, Punjab, India
Improving AOMDV Protocol, against Blackhole Attacks proposed By Naresh Kumar, et	AOMDV	Ns2	The experimental results show a minimum routing overhead.	Failed to protect cooperative black hole attack	ICCCCM 2013

2.6.2 Gap of Related Works

The researchers reviewed several related papers regarding on MANET and the behavior of Attacks particularly black-hole attack. Numerous researches are conducted on AODV, DSDV and DSR routing protocols using different techniques such as encryption-decryption, fuzzy logic, signature-based IDS, specification-based IDS, and anomaly-based IDS methods. Various techniques are applied to detect and avoid different attacks under different RP in MANET. No researches are conducted Under AOMDV protocol to mitigate single as well as cooperative black hole attack using anomaly-based IDS approach. In this thesis work, the researcher have selected the anomaly-based IDS approach to evaluate the consequence and minimize the effect of BHA. Because of BHA is a realistic attack, it can drop a large number of packets in the AOMDV routing protocol. Among the related works that we have reviewed, there is no effective mitigation technique on single and multiple black hole attack, using anomaly-based IDS approach.

CHAPTER THREE

PROPOSED SOLUTION OF STUDY

3.1 Proposed Solution to Minimize Black Hole Attack

In this study, we have proposed a solution to analyze the effect of black hole attack and minimize its effect. The proposed solution implemented based on the modification of AOMDV routing protocol using anomaly-based IDS approach. In this proposed approach, the researchers focused on the RREP destination sequence number that sends from any intermediate or destination node to the source node. In the routing table, RREP information checks using the proposed, Anomaly Based IDS Approach under AMODV routing protocol in MANET. Instead of receiving all RREP packets from any intermediate nodes, the source node receives RREP only that comes from the destination node.

In the First step, the sender node broadcasts RREQ to all intermediate nodes. When an intermediate node accepts RREQ and if the receiver is a destination node, then it quickly replies to the sender node with the reverse address. The intermediate node rebroadcast to its neighbor node. When the intermediate RREQ reaches to a malicious node, the node replies RREP with the highest sequence number. When RREP broadcast to the intermediate node, the proposed algorithm first checks RREP sequence number in routable then the algorithm determines whether accepted or not. In the proposed approach, RREP from the attacker node always greater than routing table sequence number. The proposed algorithm checks and rejects the new RREP that comes from a malicious node. If the routing table is NULL, it updates the table with the fresh route. If the fresh RREP sequence number is less than the maximum sequence number in the routing table OR fresh RREP sequence number is equal to the maximum sequence number in the routing table then update the routing table with fresh RREP.

To detect and minimize the impact of SBHA and MBHA under AOMDV Routing Protocol in MANET, the researchers have modified different routing functions in aomdv.cc file. The solution that we propose the design to reduce BHA using the approach based on modifying the existing Receive Reply (packet p) and Receive request functions. In AOMDV, the source node receives the first route reply, which comes from any node. BHA node always sends route reply with the highest destination sequence number to the sender node.

3.1.1 Pseudo Code for Proposed Algorithm

1. initialize rrep from malicious node is the first route reply packet with HDSNo
2. SN broadcast RREQ
3. If(RREQ reach to destination){
4. Rrep_reply ();
5. }
6. If(RREP sends to source node){
7. Rrep_lookup(nsaddr, rrepid);
8. }
9. Return
10. Else If(rredsno \geq rrepdsno, in routing table){
11. Rrep comes from malicious node
- 12. Black hole attack is exist**
13. Rrep_remove(nsaddr, rrepid)
14. Mitigate BHA
15. }
16. Else if(rrep_dsno $<$ rt_dsno){
17. Rrep_purge()
18. Update route table
19. Data packet reach to destination node
20. End if
21. }

3.2 The Architecture of the Proposed Solution

The proposed architecture is a design to minimize single as well as multiple BHA under AOMDV protocol in MANET. The source node discovers the route to the destination node, by sending route request if a malicious node is existing in the network, which replies false route reply to the source node. The source node assumes that the RREP is coming from the destination node, and then it sends data packets to the malicious node. The data packet is dropped when the malicious node receives from the source node. The proposed solution architecture describes how to integrate and reduce the impact of a malicious node using Anomaly Based Approach. In the existing routing protocol, there is no rule to detect and discarded the malicious route reply.

Based on the proposed architecture in AOMDV routing protocol, the source node broadcasts RREQ packet to the intermediate through multiple routes, then rebroadcast RREQ to other intermediate nodes with their own address. When the malicious node receives route request, it sends a forged route reply (RREP) message to the source node. ABIDS checks RREP destination sequence number in the routing table. If the RREP with HDSN immediately discarded from the routing table. When the malicious node DSN remove, the sender sends the packet to the other fresh route for effective communication. This approach is implemented by using modification AOMDV protocol. The researcher has reduced BHA with anomaly-based intrusion detection approach. Figure 3.1 shows the proposed architecture, which describes the overall architecture of the Anomaly Based IDS approach.

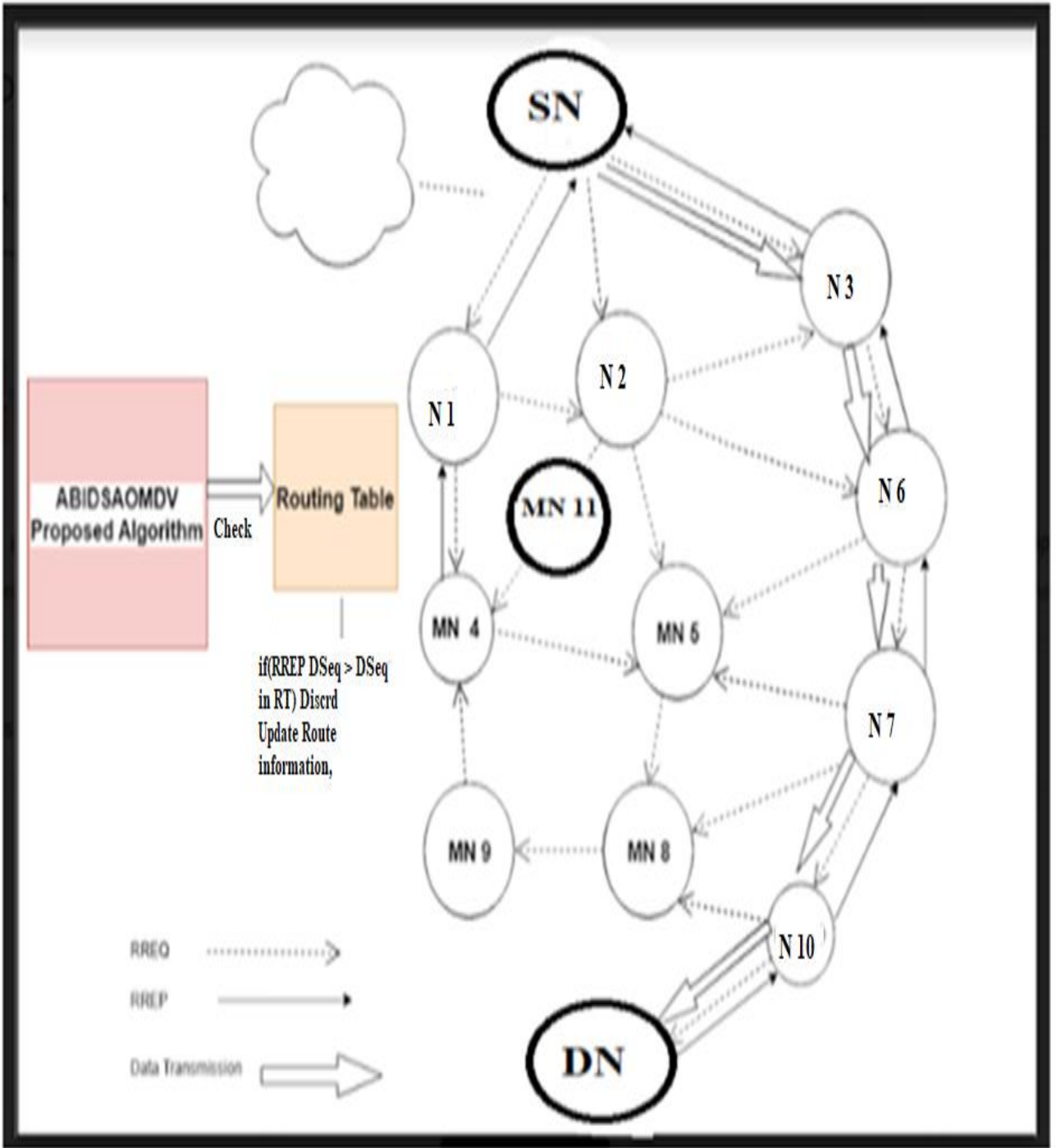


Figure 3. 1: Architecture of Proposed Solution

To achieve the specified objective, the researchers proposed an architecture by using anomaly-based IDS approach to minimize the effect of black hole attack under AOMDV RP in MANET. The proposed solution architecture describes the IDS System of preventing and mitigating of black hole Attack with the proposed algorithm. In the proposed architecture, MN indicates a malicious node. As you can see, the four malicious nodes, which are incorporated in the architecture that effects cooperatively the proposed network because of their nature. When the sender node broadcasts RREQ to neighbor nodes including malicious nodes then, the forged RREP created to send the source node. The proposed algorithm compares RREP information with the existed routing table information by using the modification n of the AOMDV protocol. Then if RREP comes from malicious node immediately remove from the route information and receive the fresh route RREP that comes from normal nodes.

The proposed solution architecture proposes to mitigate the impact of BHA under AOMDV routing protocol in MANET. ABIDS approach applied in the AOMDV routing protocol. To mitigate BHA using the proposed solution, the researcher has used a host-based IDS method specifically anomaly-based intrusion detection approach. The reason to select Anomaly-based IDS approach is, it can detect and reduce the previous unknown attacks and the novel attacks. The proposed solution architecture implemented by modifying the existing AOMDV routing protocol in MANET. The proposed solution simulated on the simulation network environment with the existing black hole attack then improve network performance by detecting and mitigating the impact of black hole attack. The figure 3.2 discussed in detail how to discard the false RREP that delivered from abnormal nodes and sends data packets through a fresh route to the destination node.

3.2.1 Flow Chart Diagram for Proposed ABIDS Algorithm to Reduce BHA

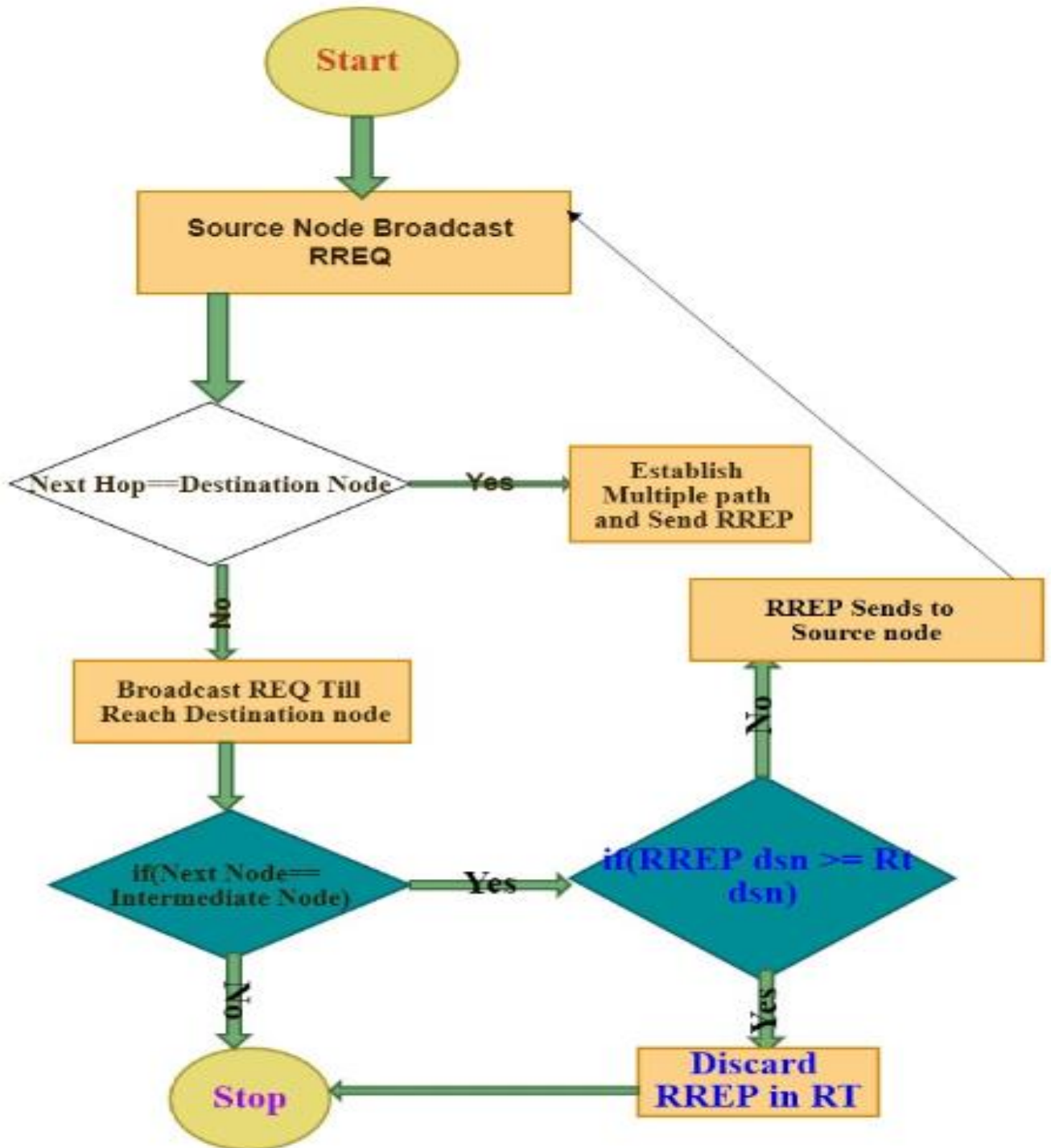


Figure 3. 2: Flow Chart Diagram of Proposed ABIDS Algorithm

The following steps are the description of the Proposed Algorithm using Anomaly Based Intrusion Detection System Approach.

Step 1: Send RREQ messages to all neighboring nodes to discover a real route for data packet transmission.

Step 2: If the Next Node is DN immediately sends RREP, otherwise rebroadcast the request to the neighbor node until reach to destination node found

If next node == DN

{ send RREP to Source node

Else

IN Rebroadcast RREQ }

Step 3: if the RREQs reaches to destination node then select, the target node delivers the RREP to the source node.

Step 4: The proposed ABIDS Approach compare RREP DSN with Routing Table sequence number in AOMDV routing protocol to check whether the RREP packet is from the normal or malicious node.

Step 5: if the attacker exists in the selected path, it sends immediately a forged RREP to the sender node. If RREP SNO greater than routing table Seqno the node is abnormal node RREP will be discarded.

Step 6: Intrusion Detection System (IDS) verify if RREP DSN less or equal to the routing table sequence number the source node would transfer data to the target node.

Step 7: If routing information matched then transfer real data to the receiver node by selecting the shortest routing path.

Step 8: Applied the proposed approach, change the route table information and block that RREP then, finds the new path in order to forward data packets and the new fresh route for effective communication.

Step 9: End

3.2.2 AOMDV Modification

To minimize the impact of BHA using ABIDS approach through the following procedures, we have changed some routing functions under the AOMDV reactive routing protocol.

Step 1. Cloning AOMDV routing protocol to ABIDSAOMDV in ns-2.3.5 directories then change all files in the cloned ABIDSAOMDV routing protocol

Step 2. Storing process

Adding RREP messages and update the routing table by using “rrep_insert” function

Step 3. Recognize and minimize Black Hole Attack

Focusing route reply messages by using “rrep_lookup” function.

Eliminating route reply messages with HDSNo by using “rrep_delete” function

Update function by using “rrep_purge” function can update routing table periodically.

To detect and minimize the impact of BHA in the proposed simulation network topology, we have modified AOMDV routing protocol in mobile ad hoc network using ABIDS approach.

CHAPTER FOUR

SIMULATION OF THE PROPOSED SOLUTION

4.1 Simulation Scenario

The simulation section discusses how to analyze and evaluate the consequence of SBHA and MBHA under AOMDV routing protocol in MANET and how to minimize its effect by using anomaly-based IDS approach. To achieve this study, the researcher is modified the standard AOMDV routing protocol under normal and abnormal environment. Simulation is performed using NS2 to minimize the impact of BHA under this protocol in MANET.

4.2 Working Environment

To demonstrate this thesis, the researcher has used some software tools such as Ubuntu 16.04 platform, NAM and Trace Graph to analyze the result through different network performance metrics. There are different types of tools to show the result of the trace file generated by ns2 graphically. Some of those graphical tools are Xgraph, NS2 wireless trace analyzer, Gnuplot, and trace graph. In this thesis work, a trace graph used to analyze and evaluate graphically the trace file result, because it has the ability to support various trace file formats and it is an open-source graphical tool. Trace graph is compatible on different environments such as Linux, Unix, Window and MAC Os system[49].

The flavor of Linux used for this work is Ubuntu, which used to simulate four scenarios and analysis of those scenarios result. The reason that we have chosen this operating system to this scenario simulation is it is suitable and robust platforms for ns2. Secondly, the Linux system has more security than other operating systems [40].

4.3 Four Scenarios Evaluated under AOMDV Routing Protocol in MANET

This work mainly focuses on the evaluation of the existing AOMDV RP without BHA, with BHA and anomaly-based IDS approach to minimize the impact of BHA. This study considers the comparisons of modules under AOMDV routing protocol to accomplish the objective

- ✓ First, simulate and analyze the AOMDV routing Protocol scenario without BHA
- ✓ Second, simulate and analyze the AOMDV routing Protocol scenario with SBHA
- ✓ Third, simulate and analyze AOMDV routing Protocol scenario with MBHA
- ✓ Fourth, simulate and analyze the AOMDV routing Protocol scenario with the proposed ABIDS approach.

4.3.1 Simulating and Analyzing Standard AOMDV Scenario

To simulate and analyze AOMDV routing protocol scenario without any BHA, the researchers has used some steps to implement the simulation scenario. To analyze standard AOMDV routing protocol scenario, first, TCL script is created based on the proposed network environment. There are some files such as aomdv.cc, rqueue.cc, rqueue.h, aomdv_packet.h in AOMDV directory. The researcher modify files in the AOMDV routing protocol using two methods. These methods are cloning method by changing all function and variable names and the other method is as it is without Change the name of any function, variable and other files in AOMDV protocol. For this thesis work, the researchers analyzed the performance of AOMDV routing protocol in both methods. The researcher did not use the cloning method in the first three modules, but in the proposed approach, the cloning method is applied.

4.3.2 Simulating and Analyzing AOMDV Scenario with SBHA

To simulate and analyze AOMDV routing protocol scenario with SBHA, first, SBHA is added to the proposed network. To apply SBHA under AOMDV routing protocol, modification is implemented in aomdv.cc and aomdv.h files. On this simulation scenario, the effect of SBHA analyzes by creating a TCL script on the simulation network environment. There are some files such as aomdv.cc, rqueue.cc, rqueue.h, aomdv.h, packet.h under AOMDV directory. The researchers have modified aomdv.cc and aomdv.h files in AOMDV routing protocol without cloning method, by added the new source code into different functions to create SBHA. The rt_resolve function checks the received packet belongs to RREQ, RREP, and RERR. In this scenario, the modification in AOMDV routing protocol applied using the following simple code and then the malicious node would drop packets before reach to the destination node.

```
If(attacker ==true)
{
Drop(P,DROP_RTR_ROUTE_LOOP);
Return 0;
}
```

4.3.3 Simulating and Analyzing AOMDV RP Scenario with MBHA

To simulate and analyze AOMDV routing Protocol scenario with the presence of MBHA, first, added BHA into five nodes on the proposed network environment. To evaluate the performance of AOMDV routing protocol with MBHA, analyze its impact by creating a TCL script on a simulation network environment. Simulate the consequence of MBHA using modification without changing functions and variable names under AOMDV routing protocol in the ns-2.35 directory. In this thesis work, the impact of MBHA simulated and evaluated under AOMDV RP in MANET without using the cloning method.

4.3.4 Simulate and Analyze AOMDV RP Scenario with ABIDS Approach

To simulate the proposed algorithm, we have used the without cloning method and cloning method. In the first method in ns2 directory, modification is implemented on the proposed network simulation environment by simply added new source code without changing route function or variable names. In the second method, the simulation is implemented by changing the routing function and variable names in the AOMDV directory. First, AOMDV changed to new ABIDSAOMDV routing protocol using the cloning method then modify all files in a new protocol such as aomdv.cc to abidsaomdv.cc, aomdv.h to abidsaomdv.h, aomdv_packet.h to abidsaomdv_packet.h and so on. BHA is added to the simulation network environment then applies the proposed ABIDS algorithm to reduce its impact. ABIDS proposed algorithm could minimize the impact of SBHA as well as MBHA using the anomaly-based approach under AOMDV protocol in MANET. We have modified “\tcl\lib\ ns-lib.TCL file” in ns2 directories in this step agents are implemented as the following procedure.

```
abidsaomdv {  
  
    Set ragent ($self create-sibaomdv-agent $node)  
  
    }  
  
    Simulator instproc create-abidsaomdv-agent {node}  
  
    Set ragent (new Agent/ABIDSAOMDV ($node node-addr))  
  
    $self at 0.0 “$ragment start”  
  
    $node set ragent_ $ragment  
  
    Return $ragment }  
}
```

The second step is modified “\makefile” in “ns-2.35”. After the implementation, we have compiled ns-2 to create object files by adding the following lines of code.

```
Aomdv/abidsaomdv_logs.o amodv/abidsaomdv.o
```

```
Aomdv/abidsaomdv_rtable.o amodv/abidsaomdv_rqueue.o
```

The two object files are created In the makefile, we have changed abidsaomcv.cc and abidsaomdv.h files. In this scenario “recv” function in abidsaomdv/abidsaomdv.cc sends the packet to “recvabidsaomdv”.

Incoming packets

```
Switch (ah->ah_type) {
    Case1:ABIDSAOMDVTYPE_RREQ:
        recvRequest(p); break;
    Case 2:ABIDSAOMDVTYPE_RREP:
        recvReply(p);
        break;
    Case 3:ABIDSAOMDVTYPE_RERR:
        recvError(p);
        break;
    Case 4: ABIDSAOMDVTYPE_HELLO:
        recvHello(p);
        break;
    default: fprintf(stderr, "Invalid AOMDV type (%x)\n", ah->ah_type);
    exit(1);
}
```

4.4 Core Implementation

After setting up the simulation environment, ns2 installed on Linux Os then compare the four modules ie NORAOMDV, SBHAAOMDV, MBHAAOMDV and ABIDSAOMDV under AOMDV routing protocol. Ns2 requires script file to run on this script file written in a Tool Command Language. This section describes the basic script file which is written in Tool Command Line is given below.

```
set val(chan) Channel/Wireless Channel
```

```
set val(prop) Propagation/Two Ray Ground
```

```
set val(netif) Phy/Wireless Phy
```

```

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) 26 nodes
set val(rp) AOMDV ;# routing protocol
set val(x) 1000 ;# X dimension of topography
set val(y) 1000 Y dimension of topography
set val(stop) 100.0 ;# time of simulation end
#Create a ns simulator set ns (new Simulator) #Setup topography object
set topo (new Topography)
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
#Open the NS trace file
set trace file (open out.tr w) $ns trace-all $tracefile
#Open the NAM trace file
set namfile (open out.nam w)
$ns namtrace-all $namfile
$ns namtrace-all-wireless
$namfile $val(x) $val(y)
set chan (new $val(chan)) #Create wireless channel
*****Definin Random Mobility *****#
#Random mobility for all the nodes
for{ set i 0} {$i < 26} {incr i} {
set node_($i) [$ns node]
$node_($i) random motion 1
}#Create 26 nodes set n ($ns node) $n
set X_ 663
$n set Y_ 484
$n set Z_ 0.0
$ns initial_node_pos $n 30 #Definition of Agent types set udp (new Agent/UDP)
set cbr (new Application/Traffic/CBR)
'finish' procedure proc finish {} {

```

```

global ns trace file name file
$ns flush-trace close $tracefile close $namfile
exec nam noraomdv.nam& exit 0 } for {set i 0} {$i < $val(nn)} {incr i} {
$ns at $val(stop) "\n$i reset" }
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ";
$ns halt" $ns run

```

4.5 Simulation of AOMDV with ABIDS Proposed Algorithm

To minimize the impact of BHA, we have modified the AOMDV routing protocol by applying the proposed algorithm using the cloning method and without cloning method. In the cloning method, we copied all files in AOMDV routing protocol to ABIDSAOMDV. In the newly cloned protocol directory the purge function, receive RREP function and remove RREP function added in abidsaomdv.cc and abidsaomdv.h files. We have also modified the different functions in aomdv.cc and aomdv.h to examine the consequence of SBHA and MBHA under AOMDV routing protocol in MANET without the cloning method. As we have discussed the algorithm with its description in the proposed solution section. The thesis accomplished with the simulation of standard AOMDV and AOMDV with BHA, then minimizes BHA using Anomaly Based Intrusion Detection Approach.

4.6 Simulation Model

To analyze the simulation scenario, first, a simulation network environment is created by using a TCL script. In the thesis work, we have configured MANET topology with UDP connection type and other network parameters. The simulation environment 1000m by 1000m area is chosen in X and Y span because we assume that the mobility of mobile nodes in Z span is zero. To simulate BHA the selected routing protocol is AOMDV routing protocol in MANET model. After this network configuration and design of the network, the researchers have created different objects ns and number of nodes. RWP mobility model is selected for this thesis study because of its simplicity and easy to implement. In this network simulation, the CBR application generates constant packets through this UDP connection. To this simulation, we have set 512 bytes long packet size is chosen and the packet generates with 0.1s interval.

4.7 Simulation Parameter

In this simulation scenario, a simulation is simulated on a network topology dimension of 1000m x 1000m and 26 nodes randomly. The nodes will be moving within the network space according to the random placement model. In random mobility, each node will be moving to a random location within the specified network area. In this network simulation, we have used UDP connection and the tests performed on CBR under 512-packet size. The simulation did not use TCP connection for the simulation, because in TCP connection the source node will stop the connection if the TCP ACK packets not receive. The four scenarios that are evaluated based on different parameter values. We have set up parameters in table 4.1 because of those lists of reasons.

Ns-2.35, which is the latest version of NS-2.

AOMDV routing protocol:- On this protocol we have evaluated those scenarios such as normal AOMDV, AOMDV with SBHA, AOMDV with MBHA and AOMDV with ABIDS proposed approach. We have considered the area of school of electrical engineering and computing to configure network topology environment. We have selected the CBR traffic type for this simulation because it enables to adopt any type of data. The effect of SBHA and MBHA are selected for this simulation because black hole attack in the proposed network in the form of single as well as multiple. In this simulation, black hole attack is selected because it is an active attack that can be dropped large amount of data packets. Ubuntu platform is used for this simulation, due to its portability for NS-2. RWP mobility model is selected for this simulation because of its simplicity and suitability for MANET researches. Trace graph is selected because it can take any trace file format without any configuration PRL or AWK files. We have taken 26 number of nodes and 100ms in this network environment for effective network communication.

Table 4. 1: Set up of Simulation Parameters

Parameter	Value
Simulator	NS-2.35
Routing Protocol	NORAOMDV,SBHAAMDV,MBHAAOMDV and ABIDSAOMDV
Network area	1000*1000
Traffic type	CBR
SBHA,MBHA	1,5 respectively
Attack Type	Black Hole Attack
Platform	Ubuntu 16.04
mobility	Random Waypoint
Graphing Utility	Trace Graph
Connection Type	UDP
Number of nodes	26
Simulation time(ms)	100ms

By using table, 4.2 the simulation set up the following simulation results are simulated using NAM Window.

Figure 4.1 shows a simulation scenario with 26 number of nodes in a normal network environment under AOMDV routing protocol. As you observe from the simulation window, all nodes are normal nodes without BHA. In this simulation, the data packet reaches the destination node under AOMDV routing protocol in MANET. This regards, there is a small number of packet dropped and it has high throughput for sending, receiving, generating packets and low end-to-end delay.

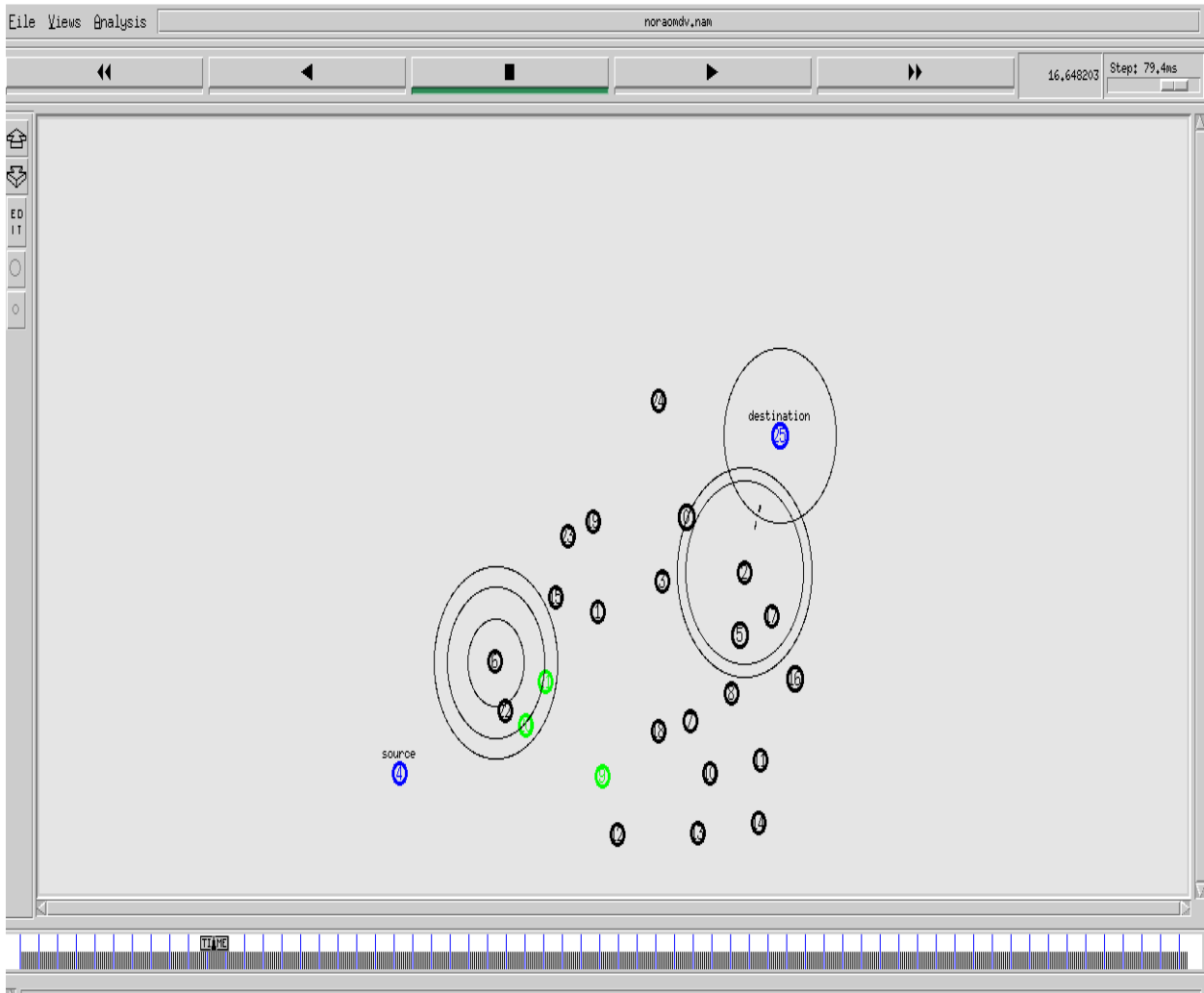


Figure 4. 1: Standard AOMDV in MANET

Figure 4.2 shows a simulation scenario with 26 number of nodes in a normal network environment with SBHA. In this simulation, as you observed from a simulation window, node 15 is a malicious node, which affected by SBHA. It drops a packet that comes from the sender node. In this simulation, the source node cannot reach the destination node safely because of the existing of SBHA under AOMDV routing protocol in MANET. The simulation has a high amount of dropped packets, low throughput for sending, low throughput for receiving and generating packets relatively compared with normal AOMDV routing protocol scenario.

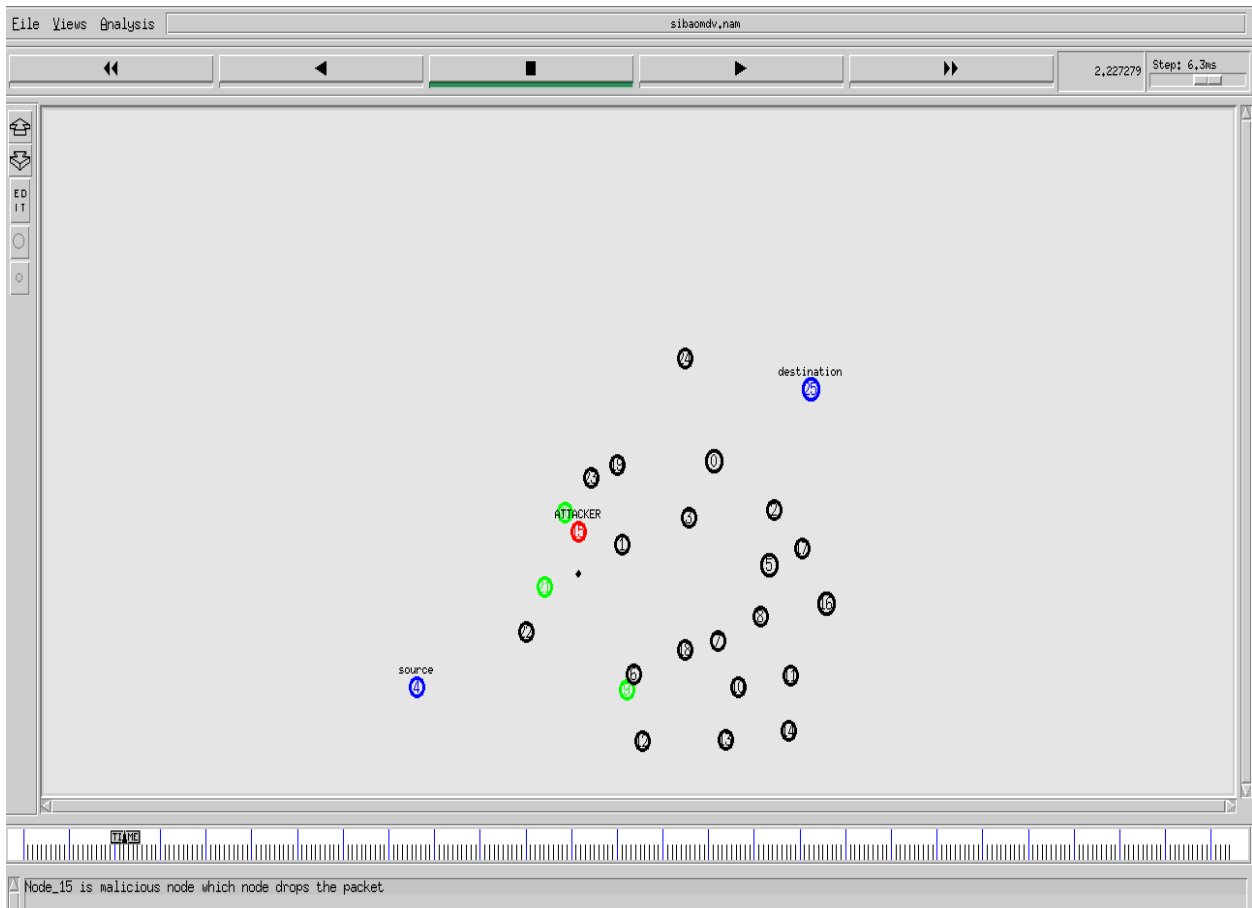


Figure 4. 2: AOMDV Protocol with SBHA in MANET

The figure 4.3 shows a simulation scenario with 26 number of mobile nodes in a MANET environment. In this examination as you observe on a simulation window, node 15, 17, 18, 19 and 22 are a malicious node, which affected by BHA then those nodes drop a data packets that come from sender node. On simulation environment, a data packet cannot reach a destination node because of MBHA exists in the given scenario in MANET. The scenario has a high amount of dropped data packet but a low-performance metrics in terms of throughput for sending, throughput for receiving and generating packets.

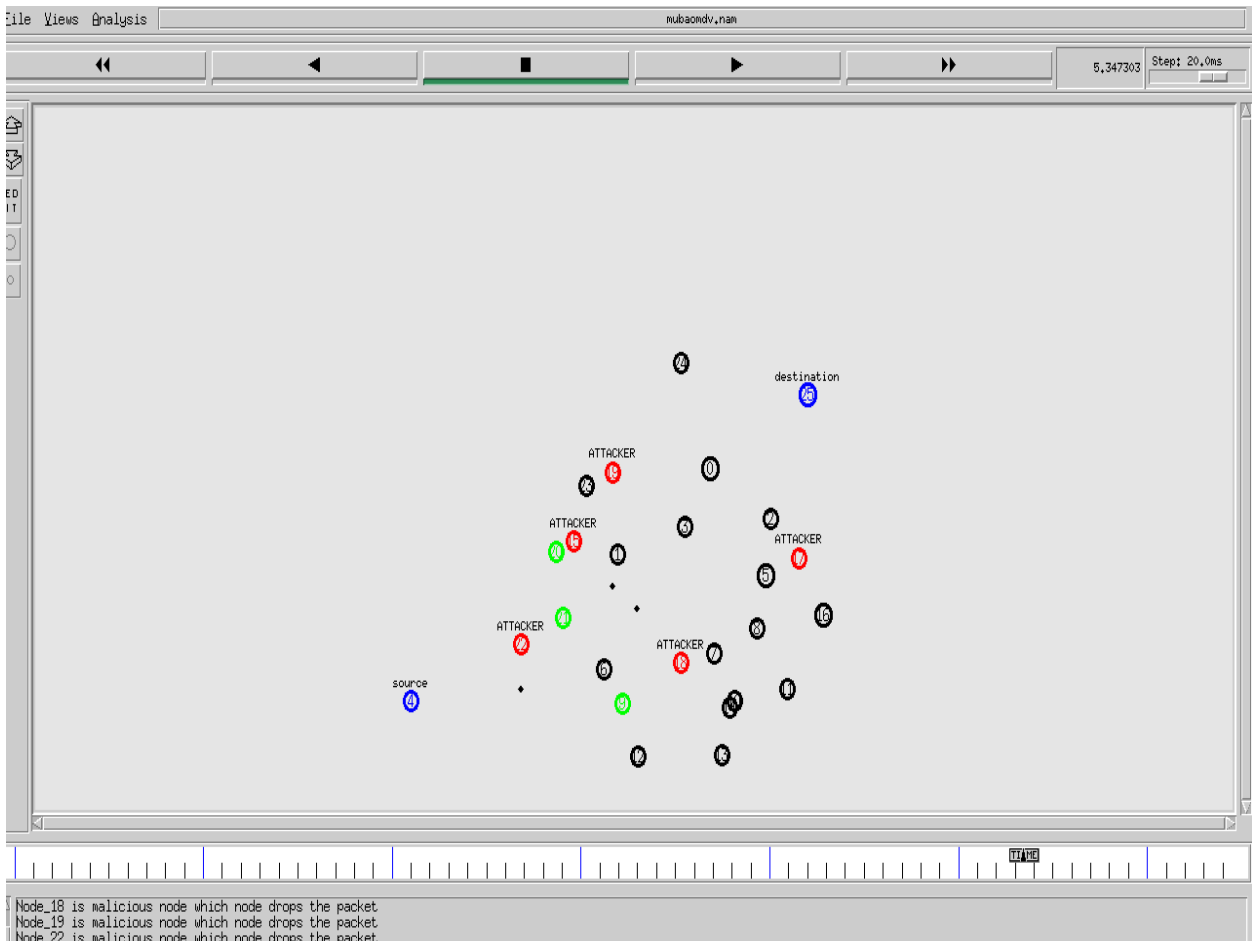


Figure 4. 3: AOMDV Scenario with MBHA in MANET

The figure 4.4 shows a simulation scenario with 26 number of mobile nodes under AOMDV routing protocol with ABIDS Proposed Algorithm in MANET. In this scenario, as you observe on a simulation window, node 15, 17, 18, 19 and 22 are attacker nodes but due to applying the proposed, anomaly-based IDS approach, the data packets can reach to the target node under AOMDV protocol in MANET. In this module, it has a good result in terms of throughput, jitter and end-to-end delay than the other simulation scenarios.

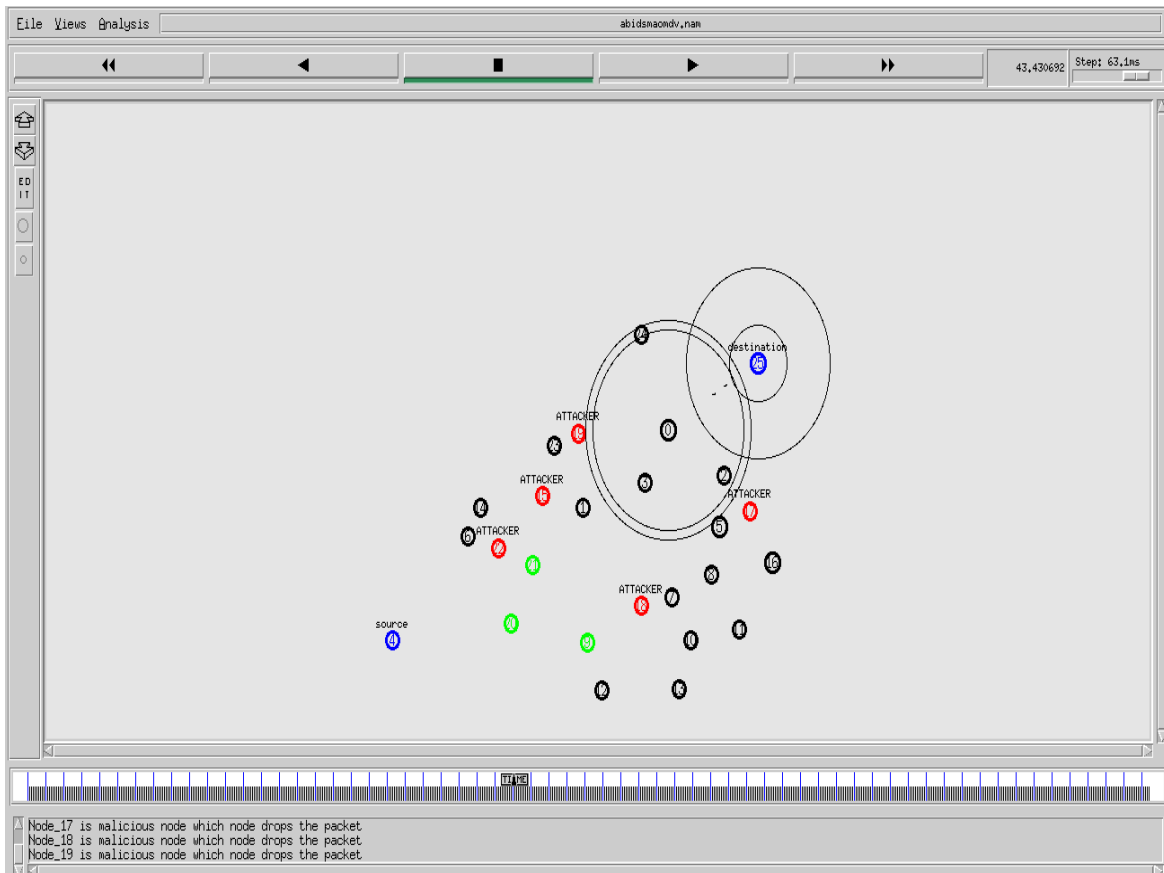


Figure 4. 4: AOMDV with ABIDS Proposed Algorithm in MANET

4.8 Performance Metrics

Qos consists of a set of constraints between sender and receiver, the connection must grantee the required communication between them. There are two major categories of performance metrics in routing protocols under MANET. Those qualitative and quantitative metrics are described below [50].

4.8.1 Qualitative Metrics

The qualitative metrics is a type of performance metrics, which measured by observation without any metrics or statistics. Some of the qualitative metrics are loop-freedom, route stability, on-demand, scalability, integrity, and reliability [50].

4.8.2 Quantitative Metrics

The focus of quantitative measurement measured by a metric or statistics. Some of the qualitative metrics are an end-to-end delay, Throughput, overhead, packet delivery ratio,

mobility and packet loss [13]. In this thesis work, we have utilized the following performance metrics to compare the four simulation scenarios.

4.8.2.1 Throughput

- ✓ **Throughput of Generate packets:-** measures the number of packets generates within a given time interval.
- ✓ **Throughput of sending packets:-** measures the number of packets sent within a given time interval.
- ✓ **Throughput of receiving packets:-** represents the packets received by the receiver within a given time interval.
- ✓ **Throughput of packet dropping:-** measures the number of data packet dropped on the scenario within a total simulation time.

4.8.2.2 Jitter

Jitter is a measurement of performance metrics in the given network, the higher value of jitter leads to a high-performance problem. It is the difference /fluctuation between nodes [51], [52]. It described as the variation of received packets in the network within a time. Due to the presence of attack in MANET, the source node will attempt to send the packets in a continuous manner to the receiver node but the receiver node may face some problems to receive the packets continuously in the network.

4.8.2.3 End-to-End delay

All possible delays in the network including latency retransmission by intermediate nodes, route discovery, processing delay, queuing delay and propagation delay. Represent the time taken from the sending time to receiving time from the sender node to the receiver node.

4.9 Simulation Result and Discussion

In this study, the researcher is simulated and analyzed the four scenario modules such as standard AOMDV Routing Protocol, AOMDV with SBHA, AOMDV with MBHA routing protocol and AOMDV with ABIDS proposed approach on the same simulation network environment. The simulation gives the following result using tracegraph202 in terms of throughput, Jitter, and End-to-End Delay. The scenario results such as standard AOMDV, with single as well as multiple BHA and proposed ABIDSAOMDV algorithm on the proposed network topology shows graphically and tabular form. In this work, the impact of BHA under

AOMDV routing protocol would be evaluated using the given parameter set-ups. Based on our simulation result in the simulation network environment single as well as multiple BHA degrade the performance of the network. As you observe from the simulation result, SBHA has less effect than MBHA. When SBHA exists in network topology, it gives less throughput to send, receive, jitter and generate a packet, but when MBHA exists in a simulation network, the performance of the network was more degrade because in this case BHA works cooperatively. The consequence of single, as well as MBHA under AOMDV routing protocol in MANET, describes graphically. In terms of the following quantitative performance metrics to measure simulation results.

4.9.1.1 Throughput

- a) Throughput of Generate packets
- b) Throughput of Sent packets
- c) Throughput of Received packets
- d) Throughput of packet dropping

Discussion of Results in terms of Throughput

From the discussion of each graph, it is clear that throughput of sending, receiving and generating packets evaluated on different scenario modules. Figure 4.5.d shows the AOMDV routing protocol with ABIDS proposed solution gives a better result. The proposed approach gives a good simulation result in terms of throughput for sending, receiving and generating packets on the simulation network environment. The throughput of sending, receiving and generating packets are very low under AOMDV with MBHA. In this scenario, even no transmission occurs at the beginning of simulation time. The proposed ABIDSAOMDV routing protocol scenario has a high throughput than AOMDV with SBHA, MBHA, and standard AOMDV routing protocol.

Figure 4.5.a shows the throughput of sending, receiving, generating and dropping packets of standard AOMD scenario. In the standard AOMDV scenario, there is a high throughput of sending, receiving, and generating packet because in this simulation environment there is no BHA. In this scenario module, the simulation result is better than the other SBHA and MBHA scenario modules. At the initial time around 0.01sec, throughput is high then, it becomes suddenly decrease. The simulation time between 18-23 sec throughputs suddenly decreases and again suddenly rises and then it becomes consistent throughout the simulation time.

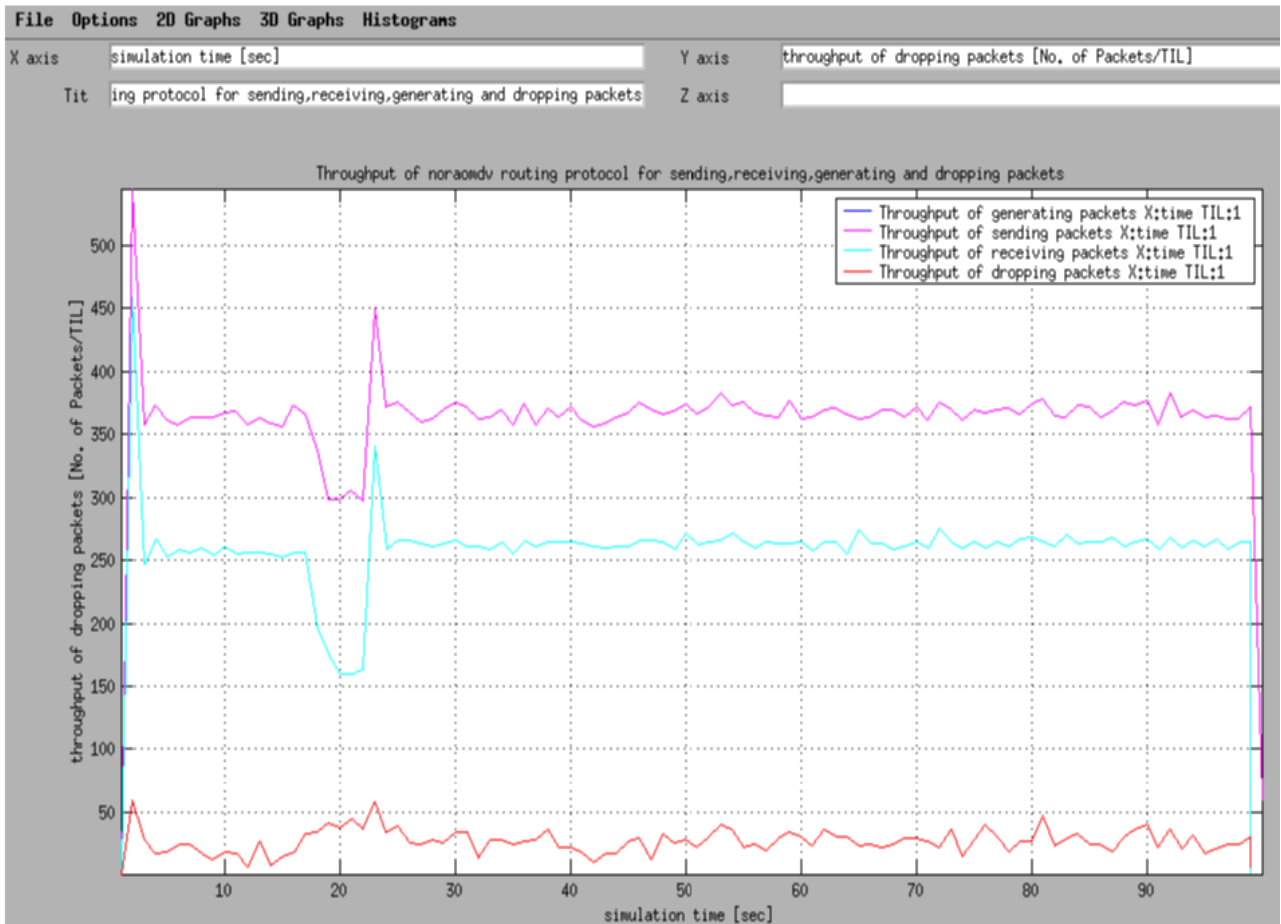


Figure 4.5. a: Standard AOMDV simulation

Figure 4.5.b shows the throughput of sending, receiving, packet dropping and generate packets in AOMDV RP with SBHA. In this scenario, the throughput of sending, receiving, dropping and generating packet less than standard AOMDV scenario because SBHA involved in this simulation. At the initial simulation, time from 0.1 to around 0.10 throughput suddenly rises, then it becomes sharply decrease again rise up and then it almost remains constant.

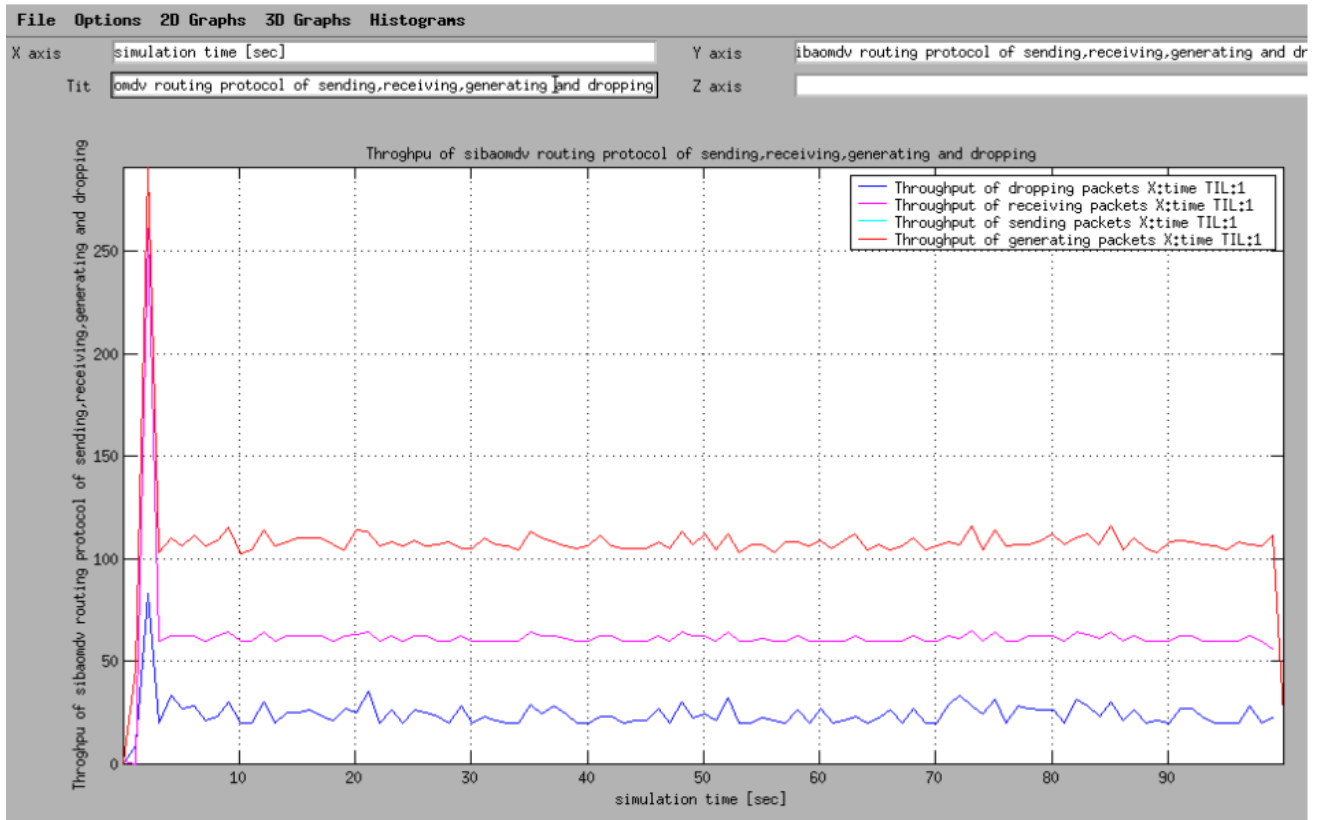


Figure 4.5. b: AOMDV with Single Black Hole Attack

Figure 4.5.c shows that throughput for Send, Received and Generate packets of AOMDV RP with MBHA has a minimum throughput. As you have seen on the above simulation graph, the throughput of sending, receiving and generating packet is very less than the standard AOMDV, SBHAAOMDV, and ABIDSAOMDV scenarios, because of cooperative BHA. Due to the existence of cooperative BHA, at the beginning of simulation time throughput to send, receive and generate packets has very less value but at some point of time interval in the simulation time there is sudden increase then suddenly over decrease around 79% of time interval throughput is very low.

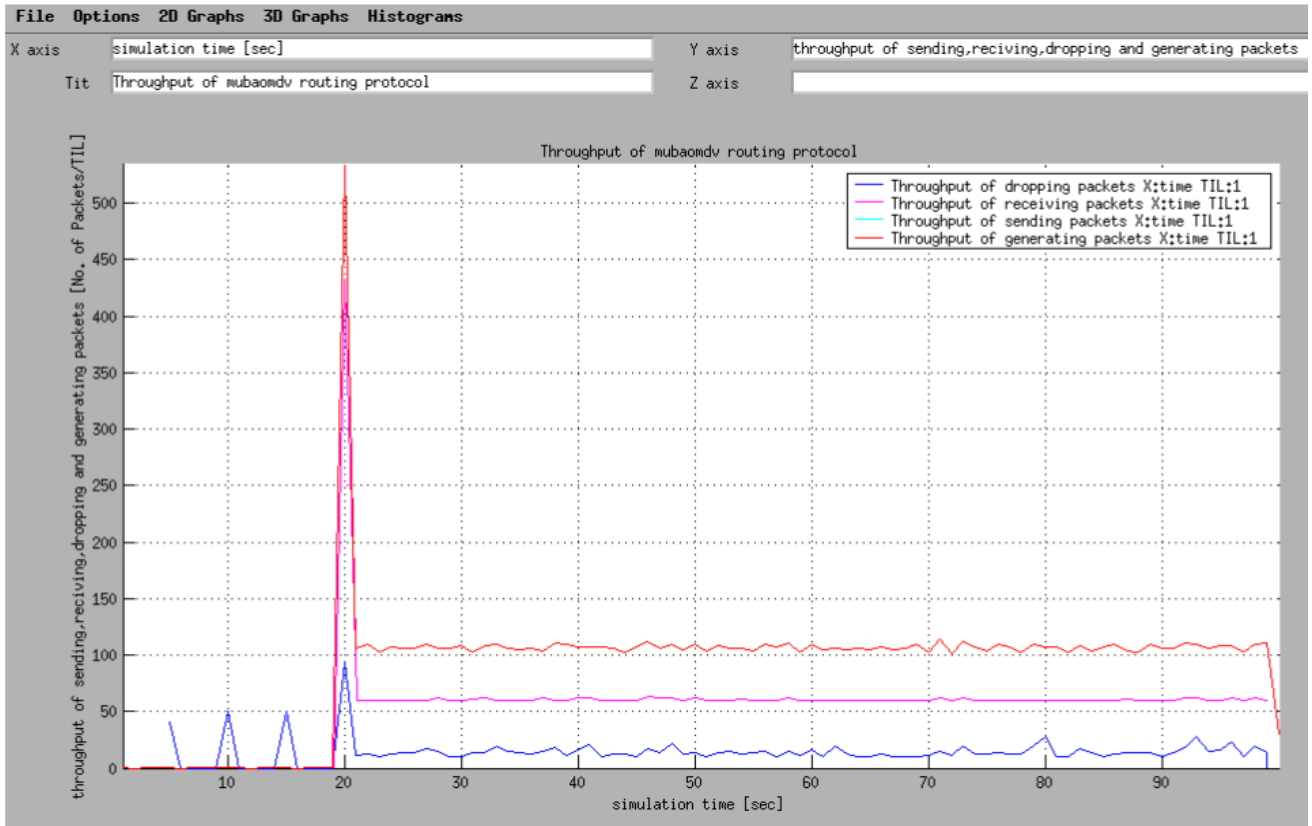


Figure 4.5. c: AOMDV with Multiple Black Hole Attack

Figure 4.5.d shows the throughput of the packet in AOMDV RP with ABIDS Approach. In the proposed ABIDSAOMDV routing protocol scenario, the throughput of sending, receiving and generating packet is higher than standard AOMDV, AOMDV with SBHA and MBHA, because of the proposed algorithm. In this scenario, throughput is constant and very high in all simulation time interval.

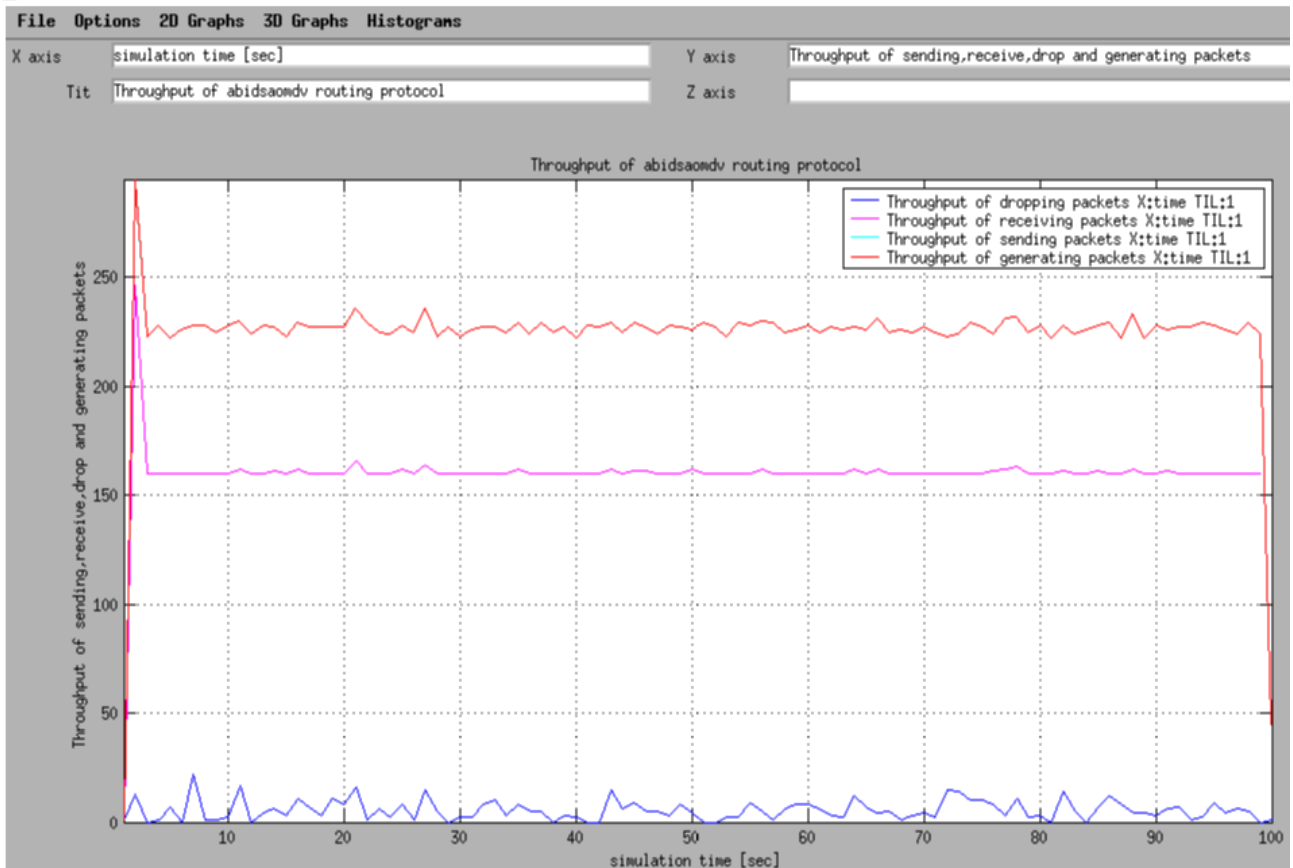


Figure 4.5. d: AOMDV Modification with ABIDS

4.9.1.2 Jitter

Discussion of Results in Terms of Jitter

As you see, from the simulation graph, the simulation result varies in terms of jitter in different scenario modules. Figure 4.6.d shows the proposed AOMDV Routing Protocol module, which has less jitter than the other three modules. Due to the presence of ABIDS algorithm, it minimizes impact of BHA. Whereas Figure 4.6.b and Figure 4.6.c show, a scenario with single and multiple BHA respectively have a high result in terms of jitter. Based on this analysis SBHA and MBHA have the highest impact for communication and any other networking activities on proposed network topology. Due to the effect of BHA in a simulation network, jitter has a high value in those two scenario modules.

Figure 4.6.a shows the scenario environment to simulate standard AOMDV RP without BHA, as you observe from the graph jitter is less than SBHA and MBHA scenarios. From the simulation graph, jitter is high, in the simulation time interval around 0.03 to around 0.08 sec.

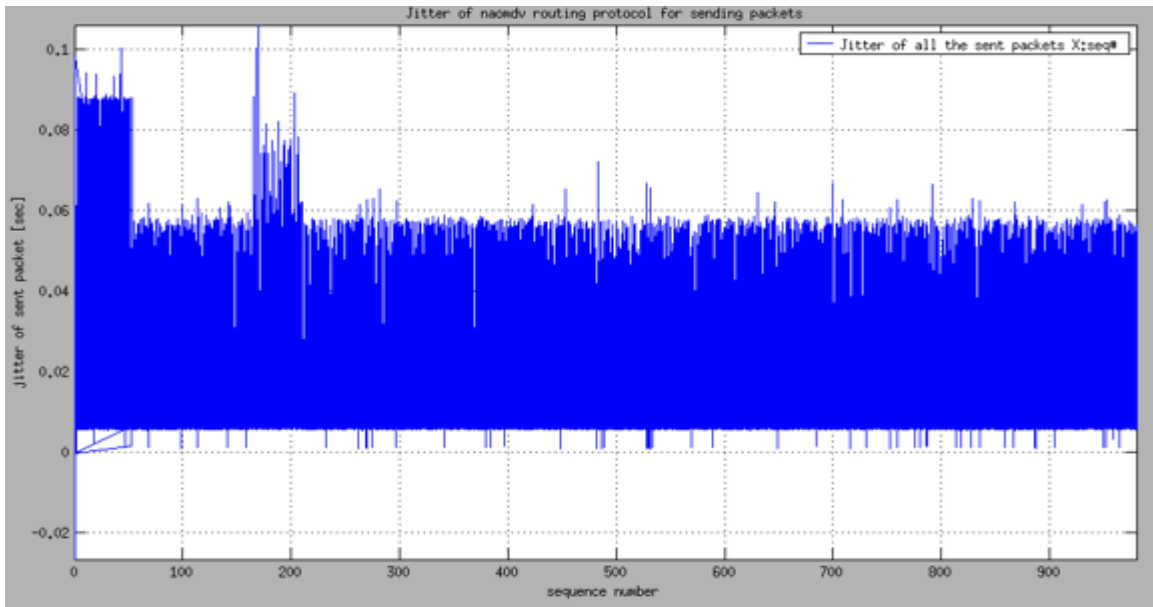


Figure 4.6. a: Standard AOMDV Simulation

Figure 4.6.b and Figure 4.6.c show the graph on the simulation of AOMDV RP with SBHA and AOMDV RP with MBHA have a high jitter value from 0.02 to 0.09 sec. In this scenario, jitter has a high impact on the performance of the network in the given simulation environment.

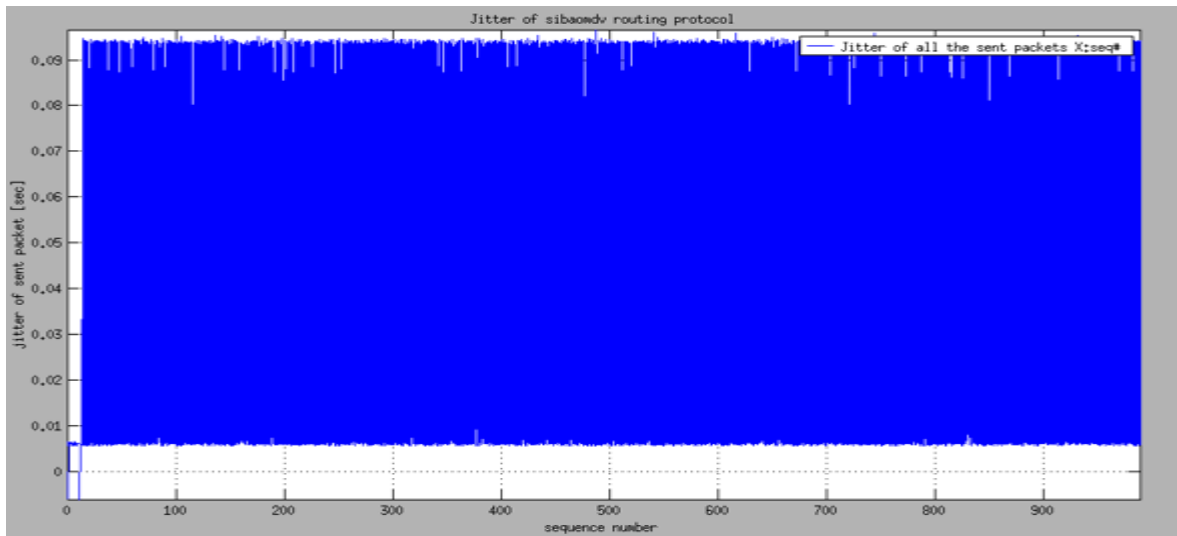


Figure 4.6. b: AOMDV with Single Black Hole Attack

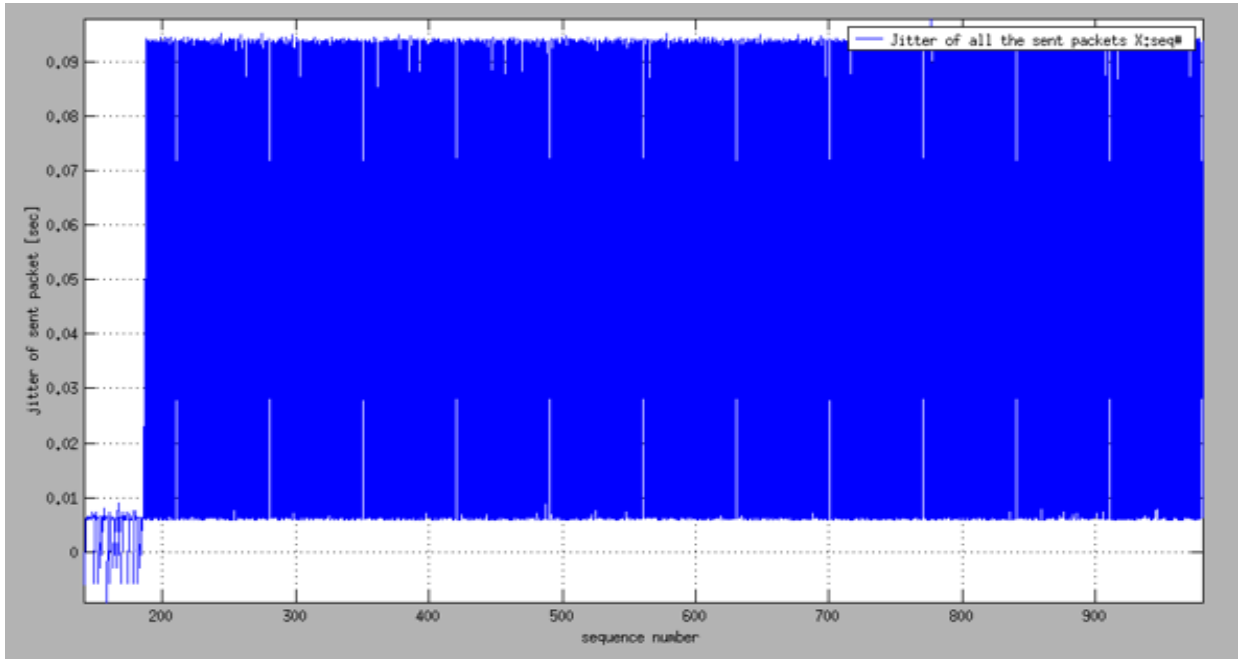


Figure 4.6. c: AOMDV with Multiple Black Hole Attack

Figure 4.6.d shows that the jitter in the proposed ABIDSAOMDV routing protocol scenario has less value in the proposed network topology. As we observe from the simulation graph, the effect of jitter is on the simulation scenario, because of the ABIDS proposed Approach.

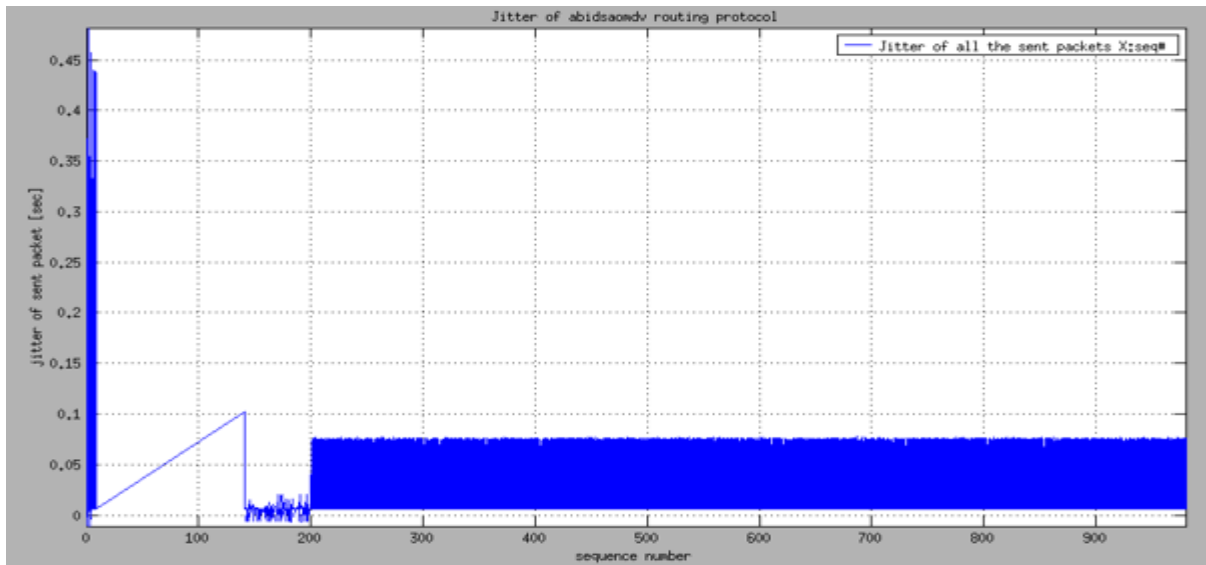


Figure 4.6. d: AOMDV Modification with ABIDS Approach

4.9.1.3 End-to-End Delay

Discussion of Results in Terms of E2E Delay

From the simulation graphs, the researcher observed that the impact of SBHA and MBHA in different scenario modules in terms of E2E delay. The result of E2E delay does not calculated in a simulation environment with the presence of SBHA and MBHA, because the data packet is dropped before arrive to the target node. Figure 4.7.a shows E2E delay graph in standard AOMDV RP scenario, it has in consistent graph with increment of throughput. Figure 4.7.b shows low end-to-end delay in AOMDV with ABIDS Approach simulation scenario. At some points, E2E delay is increase sharply relatively with the increment of throughput, then again gradually decrease. It is possible to conclude that, the proposed approach scenario has a less E2E delay.

Figure 4.7.a shows that end-to-end delay is high initially and then it decreases suddenly, then it rises for a short time. In this scenario, the simulation result in terms of end-to-end delay shows inconsistent graph throughout the simulation time. End to end delay gradually increase as the throughput increases and it has lack of consistency.

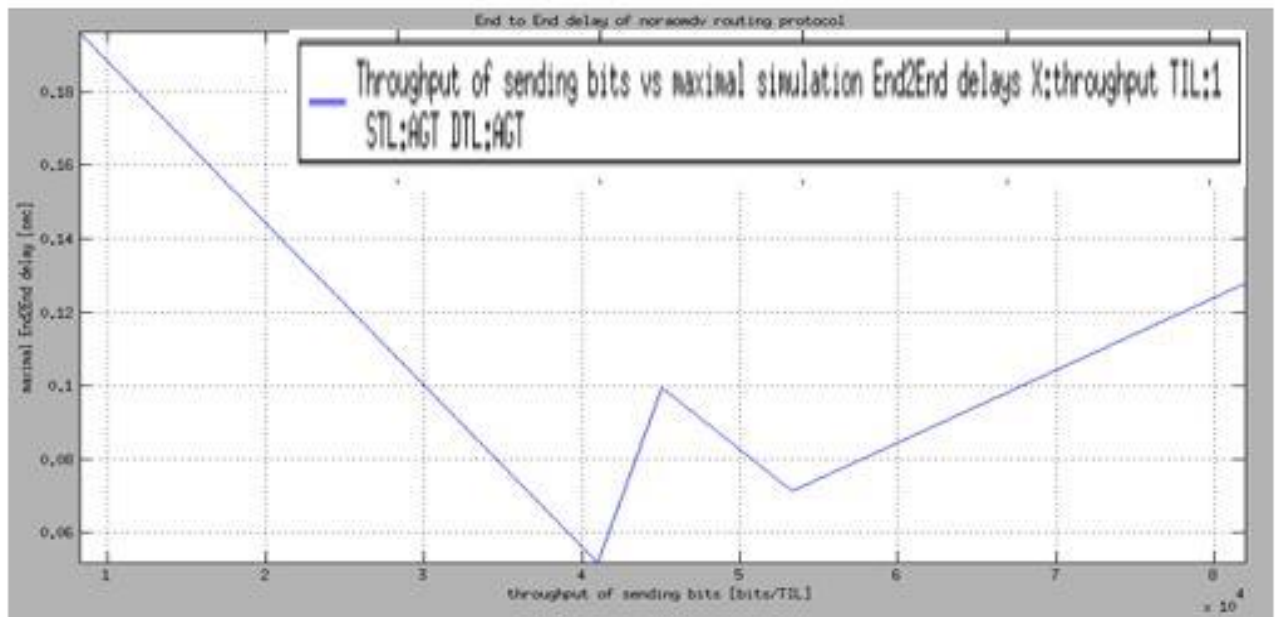


Figure 4.7. a: Standard AOMDV Simulation

Figure 4.7.b shows that the end-to-end delay of the proposed algorithm scenario, which is less than the standard AOMDV scenario because of ABIDS Approach. In the proposed network environment, end-to-end delay is inconsistent throughout the total simulation time.

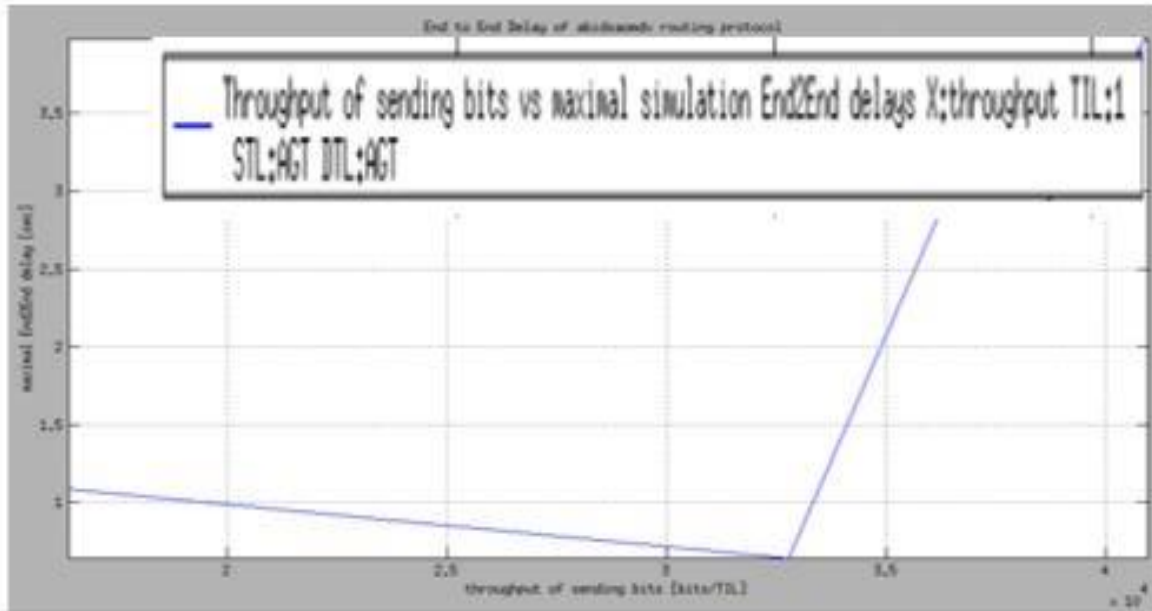


Figure 4.7. b: Modification of AOMDV with ABIDS Proposed Approach

4.9.2 Summary of Result

Simulation result on scenarios evaluates using quantitative performance metrics to compare the simulation results on the proposed simulation environment. The researcher described the scenario module results in tabular form, using the following metrics, such as throughput of (sending, receiving, packet dropping and generating packets), Jitter and end-to-end delay.

I). Throughput

- Throughput of Generate packets
- Throughput of Sent packets
- Throughput of Received packets

II). Jitter

III). End-to-End Delay

Table 4.2 shows the brief comparison of the simulation result in different scenarios. The researcher evaluated and analyzed the simulation result of the four scenario modules based on

the performance metrics such as throughput, E2E delay, DP time and jitter. The simulation result of AOMDV with Proposed Algorithm gives a better result than other simulation scenarios.

Table 4. 2: Comparison of Various Scenario Results

Modules	TGP(High is Better)	TSP(High is Better)	TRP(High is Better)	Jitter	E2E(Low is Better)	DP(Low is Better)
NORAOMDV	High and inconsistent	High and inconsistent	High and inconsistent	Low and inconsistent	High and inconsistent delay	low and inconsistent
SBHAAOMDV	Medium and consistent	Medium and consistent	Medium and consistent	High and consistent	Low packet drop time	High inconsistent
MBHAAOMDV	low and inconsistent	low and inconsistent	Low and inconsistent	High and consistent	Low packet drop time	High and inconsistent
ABIDSAOMDV Proposed Algorithm	Very High and consistent	Very High and consistent	Very High and consistent	Very low and inconsistent	Low and inconsistent delay	Very Low and consistent

CHAPTER FIVE

SUMMARY, CONCLUSION AND FUTURE WORK

5.1 Conclusion

This thesis work describes the detail about how to minimize black hole attack and analyze the effect of SBHA as well as MBHA scenarios. Anomaly-based IDS approach is applied to reduce the impact of BHA under AOMDV routing protocol in MANET. The researchers have investigated the effect of SBHA, MBHA under AOMDV routing protocol and compare with the standard AOMDV routing protocol. BHA is an active attack, which can highly degrade the performance of the network in the simulation environment. The researchers maximized the performance of MANET on the environment with the existing of BHA simulation area using the proposed approach.

Standard AOMDV routing protocol, SBHAAOMDV, MBHAAOMDV, and ABIDS proposed approach are simulated through different performance metrics. The simulation result on the proposed ABIDSAOMDV routing protocol scenario is a good result in terms of throughput of sending, generating and receiving packets than standard AOMDV scenario and with BHA. ABIDSAOMDV routing protocol scenario has less Jitter, End-to-End delay, and high throughput because of the mitigation of BHA. Based on the simulation results, the researcher can conclude that ABIDS approach is an effective approach to minimize the impact of BHA on a proposed network topology environment. Generally, simulation is implemented in four cases scenario (without attacks, with a single attack, with multiple attacks and attacks with ABIDS).

5.2 Summary of Contribution

In MANET, the security issue is the main concern issue to achieve network operations safely. To improved security in MANET under AOMDV routing protocol, the researchers have developed an effective mechanism to mitigate the impact of black hole attack using anomaly-based IDS approach. The nature of BHA and its effect on the network performance under reactive protocol explained in detail. Since BHA is an active attack, it drops a large amount of data packets under the existing multipath routing protocol. In this work, first, the researcher analyzed the standard AOMDV routing protocol without the existing of single as well as multiple black hole attack in Mobile Ad hoc network. Anomaly-based IDS approach is an

approach, which is an effective technique to overcome both single and cooperative black hole attack.

This study simulates single as well as cooperative BHA under AOMDV routing protocol and evaluate its effect in MANET under a healthy environment and unhealthy environment. The main contribution of this study is to improve security, network performance and network reliability for safeguarding information on its application area using ABIDS under AOMDV routing protocol in MANET.

- ✓ Simulate the performance of existing standard AOMDV protocol
- ✓ Simulating and analyzing the impact of SBHA under existing AOMDV protocol
- ✓ Simulating and analyzing the effect of MBHA under existing AOMDV protocol
- ✓ Minimize the effect of BHA using ABIDS approach under existing AOMDV routing protocol

In this thesis work, due to the proposed solution network performance is improved in terms of some quantitative performance metrics.

5.3 Future Work

The security issue is the main issue to improve the performance of AOMDV routing protocol in MANET. In the future work, ABIDS approach applied on other attacks to effective mitigation. In this study, Throughput, jitter, and an end-to-end delay are the performance metrics used to evaluate and analyze the effectiveness of the proposed approach in this study.

- ✓ To further studies, recommend simulating and analyzing using those performance metrics such as energy consumption, link failure, and congestion problems.
- ✓ In the future work distributed black hole attack will evaluate and mitigate it under AOMDV routing protocol in MANET.
- ✓ We recommend future researchers, this real-time simulation will be implemented on the real application area
- ✓ ABIDS approach will apply to mitigate other attacks in MANET

Reference

- [1] K. S. Arathy and C. N. Sminesh, "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET," *Procedia Technol.*, vol. 25, no. Raerest, pp. 264–271, 2016.
- [2] T. Prasanna, "Overview of Proactive Routing Protocols in MANET," no. April 2014
- [3] N. P. John and A. Thomas, "Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review," vol. 2, no. 9, pp. 1–6, 2012.
- [4] E. E. Khin and T. Phyu, "Impact of Black Hole Attack on AODV Routing Protocol," *Int. J. Inf. Technol. Model. Comput.*, vol. 2, no. 2, pp. 9–17, Jun. 2014.
- [5] N. Panda and B. Kumar Pattanayak, "Energy aware detection and prevention of black hole attack in MANET," *Int. J. Eng. Technol.*, vol. 7, no. 2.6, p. 135, 2018.
- [6] B. Patel and K. Trivedi, "A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET," vol. 5, no. 3, pp. 2816–2818, 2014.
- [7] F. Mohammed, O. Mohamed, and E. Abdellah, "The Impact of Black-Hole Attack on AODV Protocol," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 2, pp. 20–24, 2014.
- [8] L. Mejaele and E. Oketch Ochola, "Effect of varying node mobility in the analysis of black hole attack on MANET reactive routing protocols," *2016 Inf. Secur. South Africa - Proc. 2016 ISSA Conf.*, pp. 62–68, 2016.
- [9] S. P. Medhi, "BLACKHOLE ATTACK ON MANET AND ITS," no. March, pp. 3–8
- [10] K. Patel and A. Thoke, "A Details Survey on Black-hole and Denial of Service Attack over MANET Environment," pp. 1377–1381, 2016.
- [11] N. Kalia, "Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol," vol. 8, no. 5, pp. 160–174.
- [12] A. Rai, R. Tewari, and S. Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," *Int. J. ...*, no. 4, pp. 265–274, 2010.
- [13] R. Ramdhany and G. Coulson, "MANETkit: A framework for MANET routing protocols," *Ad-Hoc Sens. Wirel. Networks*, vol. 10, no. 4, pp. 301–316, 2010.

- [14] L. Hogie, P. Bouvry, and F. Guinand, “An overview of MANETs simulation,” *Electron. Notes Theor. Comput. Sci.*, vol. 150, no. 1, pp. 81–101, 2006.
- [15] L. E. Quispe, S. C. Alto, and L. M. Galan, “Assessment Of Throughput Performance Under NS2 In Mobile Ad Hoc Networks (MANETs).”
- [16] S. Lalar, “Security in MANET : Vulnerabilities , Attacks & Solutions,” 2014.
- [17] S. K. Gupta and R. K. Saket, “Performance Metric Comparison of AODV and DSDV Routing Protocol In MANETs Using NS-2,” *Ineternational J. Res. Rev. Appl. Sci.*, vol. 7, no. 3, pp. 339–350, 2011.
- [18] D. E. Mustafa Ahmed and O. O. Khalifa, “A Comprehensive Classification of MANETs Routing Protocols,” *Int. J. Comput. Appl. Technol. Res.*, vol. 6, no. 3, pp. 141–158, 2017.
- [19] R. U. Khan and A. Vijayalakshmi, “Shell Script to Clone AODV Routing Protocol in Network Simulator - 2,” vol. 7, pp. 17–23, 2018.
- [20] A. Topics, B. Awerbuch, and C. Science, “Ad hoc On Demand Distance Vector (AODV) Routing Protocol,” pp. 1–67.
- [21] E. E. Lawrence and R. Latha, “RESEARCH ARTICLE A Comparative Study of Routing Protocols for Mobile Ad-Hoc Networks,” vol. 3, no. 11, pp. 46–53, 2014.
- [22] P. Aggarwal and E. Pranab Garg, “AOMDV Protocols in MANETS : A Review I.”
- [23] A. R. Rao, N. Muralivishnu, K. V Swathi, K. Hanisha, and N. Anand, “Performance Evaluation of DSR , AOMDV and ZRP Routing Protocols in MANETS by using NS2,” vol. 5, no. 1, pp. 711–714, 2014.
- [24] B. Patel and S. Srivastava, “Performance analysis of zone routing protocols in Mobile Ad Hoc Networks,” no. 0976, pp. 1–5, 2010.
- [25] S. H. Raut and H. P. Ambulgekar, “Proactive and Reactive Routing Protocols in Multihop Mobile Ad hoc Network,” vol. 3, no. 4, pp. 152–157, 2013.
- [26] S. Gour, “The Modified Secure AODV Routing Protocol for Black Hole Attack in Manet,” vol. 7, no. 2, pp. 8–17, 2016.

- [27] K. Raheja and S. K. Maakar, "A Survey on Different Hybrid Routing Protocols of MANET," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 5, pp. 5512–5516, 2014.
- [28] Y. Hu, A. Perrig, and D. B. Johnson, "Wormhole Attacks in Wireless Networks,"
- [29] S. Yadav, "Attacks in MANET," vol. 1, no. 3, pp. 123–126, 2012.
- [30] M. V Pawar and J. Anuradha, "Network Security and Types of Attacks in Network," *Procedia - Procedia Comput. Sci.*, vol. 48, no. June, pp. 503–506, 2015.
- [31] A. Mathematics, R. Request, and R. Reply, "Complete analysis of various attacks in manet," vol. 119, no. 15, pp. 1721–1727, 2018.
- [32] N. Bhardwaj and R. Singh, "Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs," *Int. J. Appl. or Innov. Eng. Manag.*, vol. 3, no. 5, pp. 376–383
- [33] S. Jain and S. R. Choudhary, "A SURVEY OF SINGLE BLACK HOLE ATTACK AND COLLABORATIVE BLACK HOLE IN MANET," pp. 242–250.
- [34] C. Obimbo and L. M. Arboleda-cobo, "An Intrusion Detection System for MANET," *Commun. Inf. Sci. Manag. Eng.*, vol. 2, no. 3, pp. 1–5, 2012.
- [35] K. J. Sarma, R. Sharma, and R. Das, "A Survey of Black Hole Attack Detection in Manet," pp. 202–205, 2014.
- [36] V. Kumar, "Signature Based Intrusion Detection System Using SNORT," no. April, 2015.
- [37] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *J. Comput. Sci.*, vol. 25, pp. 152–160, Mar. 2018.
- [38] D. Bolzoni and S. Etalle, "Approaches in anomaly-based intrusion detection systems."
- [39] P. Uppuluri and R. Sekar, "Experiences with Specification-based Intrusion Detection."
- [40] C. Science, "PERFORMANCE BASED COMPARATIVE ANALYSIS OF AODV , DSR AND DSDV PROTOCOLS w . r . t UDP and TCP," *Analysis*, no. July, 2009.
- [41] E. S. A. Ahmed, B. El, S. Ali, E. O. Osman, and T. A. M. Ahmed, "Impact of Different

- Mobility Models in MANETs Based on MAC 802 . 11,” vol. 1, no. 6, pp. 118–122, 2015.
- [42] B. Divecha, A. Abraham, C. Grosan, and S. Sanyal, “Impact of Node Mobility on MANET Routing Protocols Models .,” no. May 2014, 2007.
- [43] S. Amutha and K. Balasubramanian, “Australian Journal of Basic and Applied Sciences Detection and Prevention of Black Hole Attack on MANET Routing Protocols,” vol. 9, no. March, pp. 281–289, 2015.
- [44] D. K. K. K. Meenakshi, “Simulation of Black Hole Attack in Adhoc Network Using Ns2,” *Manager*, vol. 3, no. 1, pp. 942–945, 2000.
- [45] M. A. Naveena, “Dynamic Training Intrusion Detection Scheme for Blackhole Attack in MANETs,” vol. 2, no. 6, pp. 622–627, 2012.
- [46] K. Mahamuni and C. Chandrasekar, “Mitigate Black Hole Attack In Dynamic Source Routing (DSR) Protocol By Trapping,” vol. 10, no. 4, pp. 49–54, 2013.
- [47] E. Fazeldehkordi and O. Akanbi, “A Study of Black Hole Attack Solutions on AODV Routing Protocol in MANET Wireless Network Security : A Study of Black Hole Attack Solutions on AODV Routing Protocol in MANET By University Technology Malaysia Photonics Research Centre , University of Malay,” no. October, 2017.
- [48] X. Li, Z. Jia, P. Zhang, R. Zhang, and H. Wang, “Trust-based on-demand multipath routing in mobile ad hoc networks,” *IET Inf. Secur.*, vol. 4, no. 4, p. 212, 2010.
- [49] A. Hamidian, “A study of internet connectivity for mobile ad hoc networks in ns 2,” *Dep. Commun. Syst. Lund Inst. ...*, no. January, 2003.
- [50] H. Paul and P. D. Scholar, “Performance Evaluation of MANET Routing Protocols,” vol. 9, no. 4, pp. 449–456, 2012.
- [51] S. Hakak, S. A. Latif, F. Anwar, and M. K. Alam, “Impact of Key Factors on Average Jitter in MANET,” *Proc. 2014 First Int. Conf. Syst. Informatics, Model. Simul.*, pp. 219–223, 2014.
- [52] A. Mashal, V. R., and S. A., “Implementation and Analysis of AODV Routing Protocol with and without LTE Network,” *Int. J. Comput. Appl.*, vol. 171, no. 4, pp. 32–36, 2017.

Appendixes

Appendix I. Sample TCL File (.tcl) for ABIDSAOMDV Scenario

ABIDS to Minimize Black Hole 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) 26
set val(rp) AOMDV
set val(x) 1000
set val(y) 1000
set val(stop) 100.0
```

Initialization

```
#Create a ns simulator
set ns [new Simulator]
#Setup topography object
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)
#Open the NS trace file
set tracefile [open idsaomdv.tr w]
$ns trace-all $tracefile
#Open the NAM trace file
set namfile [open idsaomdv.nam w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x) $val(y)
set chan [new $val(chan)];#Create wireless channel
```

```

# Mobile Node Parameter Setup
#=====
$ns node-config -adhocRouting $val(rp) \
  -llType $val(ll)
  -macType $val(mac) \
  -ifqType $val(ifq) \
  -ifqLen $val(ifqlen) \
  -antType $val(ant) \
# Nodes Definition
#Create 26 nodes
set n0 [$ns node]
$n0 set X_ 663
$n0 set Y_ 484
$n0 set Z_ 0.0
$ns initial_node_pos $n4 30
set n25 [$ns node]
$n25 set X_ 28
$n25 set Y_ 120
$n25 set Z_ 0.0
$ns initial_node_pos $n25 30
# Multiple Black Hole Nodes
#Definition of Agent types
$ns at 0.0 "$n4 label source"
$ns at 0.0 "$n25 label destination"
$n15 color red
$ns at 0.0 "$n15 color red"
$ns at 0.0 "$n15 label ATTACKER"
$n17 color red
$ns at 0.0 "$n17 color red"
$ns at 0.0 "$n17 label ATTACKER"
$n18 color red

```

```
$ns at 0.0 "$n18 color red"
$ns at 0.0 "$n18 label ATTACKER"
$n19 color red
$ns at 0.0 "$n19 color red"
$ns at 0.0 "$n19 label ATTACKER"
$n22 color red
$ns at 0.0 "$n22 color red"
$ns at 0.0 "$n22 label ATTACKER"
#=====
$ns at 1.0 "[$n15 set ragent_] blackhole"
$ns at 0.5 "[$n22 set ragent_] blackhole"
$ns at 0.5 "[$n17 set ragent_] blackhole"
$ns at 0.5 "[$n18 set ragent_] blackhole"
$ns at 0.5 "[$n19 set ragent_] blackhole"
set udp0 [new Agent/UDP]
$ns attach-agent $n4 $udp0
set cbr0 [new Application/Traffic/CBR]
$cbr0 set packetSize_ 512
$cbr0 set interval_ 0.1
$cbr0 attach-agent $udp0
set null1 [new Agent/Null]
$ns attach-agent $n25 $null1
$ns connect $udp0 $null1
$ns at 1.0 "$cbr0 start"
```

```

for {set i 0} {$i < $val(nn)} {incr i} {
  $ns at $val(stop) "\n$i reset" }
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ; $ns hal"
$ns run

```

Appendix II. Sample Trace File (.tr) of ABIDSAOMDV Scenario

```

s 1.000000000 _4_ AGT --- 0 cbr 512 [0 0 0 0] ----- [4:0 25:0 32 0] [0] 0 0 r 1.000000000 _4_ RTR --- 0 cbr 512 [0 0 0 0] -----
[4:0 25:0 32 0] [0] 0 0
s 1.000000000 _4_ RTR --- 0 AOMDV 52 [0 0 0 0] ----- [4:255 -1:255 30 0] [0x2 0 1 [25 0] [4 4]] (REQUEST)
s 1.000135000 _4_ MAC --- 0 AOMDV 110 [0 ffffffff 4 800] ----- [4:255 -1:255 30 0] [0x2 0 1 [25 0] [4 4]] (REQUEST)
r 1.001015831 _22_ MAC --- 0 AOMDV 52 [0 ffffffff 4 800] ----- [4:255 -1:255 30 0] [0x2 0 1 [25 0] [4 4]] (REQUEST)
r 1.001040831 _22_ RTR --- 0 AOMDV 52 [0 ffffffff 4 800] ----- [4:255 -1:255 30 0] [0x2 0 1 [25 0] [4 4]] (REQUEST)
s 1.006991105 _22_ RTR --- 0 AOMDV 52 [0 ffffffff 4 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
s 1.007566105 _22_ MAC --- 0 AOMDV 110 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)

```

r 1.008446399 _21_ MAC --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008446759 _15_ MAC --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008446863 _20_ MAC --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008446885 _9_ MAC --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008446937 _4_ MAC --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008471399 _21_ RTR --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008471759 _15_ RTR --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008471863 _20_ RTR --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008471885 _9_ RTR --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008471935 _1_ RTR --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
r 1.008471937 _4_ RTR --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [22:255 -1:255 29 0] [0x2 1 1 [25 0] [4 4]] (REQUEST)
s 1.011041696 _15_ RTR --- 0 AOMDV 52 [0 ffffffff 16 800] ----- [15:255 -1:255 28 0] [0x2 2 1 [25 0] [4 4]] (REQUEST)
s 1.011276696 _15_ MAC --- 0 AOMDV 110 [0 ffffffff f 800] ----- [15:255 -1:255 28 0] [0x2 2 1 [25 0] [4 4]] (REQUEST)
r 1.012156881 _20_ MAC --- 0 AOMDV 52 [0 ffffffff f 800] ----- [15:255 -1:255 28 0] [0x2 2 1 [25 0] [4 4]] (REQUEST)
r 1.012157003 _23_ MAC --- 0 AOMDV 52 [0 ffffffff f 800] ----- [15:255 -1:255 28 0] [0x2 2 1 [25 0] [4 4]] (REQUEST)
r 1.012157014 _1_ MAC --- 0 AOMDV 52 [0 ffffffff f 800] ----- [15:255 -1:255 28 0] [0x2 2

[25 0] [4 4] (REQUEST)

r 1.012157095 _21_ MAC --- 0 AOMDV 52 [0 ffffffff f 800] ----- [15:255 -1:255 28 0] [0x2

2 1 [25 0] [4 4] (REQUEST)

Appendix III. Source Code to Add Black Hole Attack

```
//This Blackhole Attack-code is added by worku |
int
AOMDV::command(int argc, const char*const* argv) {
    if(argc == 2) {
        Tcl& tcl = Tcl::instance();

        if(strncasecmp(argv[1], "id", 2) == 0) {
            tcl.resultf("%d", index);
            return TCL_OK;
        }

        if(strcmp(argv[1], "blackhole")==0) {
            attacker=true;
            return TCL_OK;
        }
    }

void
AOMDV::rt_resolve(Packet *p) {
    struct hdr_cmn *ch = HDR_CMN(p);
    struct hdr_ip *ih = HDR_IP(p);
    aomdv_rt_entry *rt;

    if(attacker==true)
    {
        printf("packet dropped by node Number %d is %d \n",index,t_count++
        drop(p,DROP_RTR_ROUTE_LOOP);
    }
}
```

```

// Newly Code Added line to send RREP with highest Dseqno from black hole attack By worku
|
if(seqno%2) seqno++;
sendReply(rq->rq_src,          //ip destination
          0,                   // Hop count
          index,               //(RREQ) destination ip adress
          4294967295,         //the highest Destination seqno
          MY_ROUTE_TIMEOUT,   // life time
          rq->rq_timestamp,    // timestamp
          ih->saddr(),         // next hop
          rq->rq_bcast_id,     //broadcast id to identify this rout discovery
          ih->saddr());
          Packet::free(p);
}

```

Appendix IV. Sample Source Code to Reduce BHA

Void

```

ABIDSAOMDV::recvReply(Packet *p) {
AbidsaomdvBroadcastRREP * r = rrep_lookup(rp->rp_dst);
if(NH == index) {
if (r == NULL) {
count = 0;
rrep_insert (rp->rp_dst);
} else {
r->count ++;
Count = r->count;}
UPDATE ROUTE TABLE
} else {
Forward (p); } }
void
ABIDSAOMDV:: rrep_insert(nsaddr_t id) {
BroadcastRREP *r = new BroadcastRREP (rrepid);
assert(r);
r->expire = CURRENT_TIME + BCAST_ID_SAVE;

```

```

r->count ++;
LIST_INSERT_HEAD(&rrephead, r, link);
}
void
ABIDSAOMDV::rrep_lookup(nsaddr_t id) {
    BroadcastRREP *r = rrephead.lh_first;
    for( ; r; r = r->link.le_next) {
        if (r->dst == rrepid)
            Return r; }
    Else {
        return NULL; }
    void
    ABIDSAOMDV::rrep_purge() {
        BroadcastRREP *r = rrephead.lh_first;
        BroadcastRREP *rn;
        }
    If (rrep_seqno > rt_seqno){
        ABIDSAOMDV::remove_rrep();
    Else if (rrep_seqno < rt_seqno || rrep_seqno == rt_seqno)
        Forward (p);
    Else if (rt_table==null){
        Return update rt_table; }
    } }

```