DEBRE BERHAN UNIVERSITY

COLLEGE OF COMPUTING

Dual Security Based Ad-hoc On-Demand Distance Vector Algorithm to Detect and Mitigate Black Hole and Gray Hole Attacks in Mobile Ad-hoc Networks

Dagne Alemu Kebede

Supervised By

Esubalew Yitayal (Ph.D.)

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Networking and Security

Debre Berhan, Ethiopia

January, 2021

DEBRE BERHAN UNIVERSITY

COLLEGE OF COMPUTING

DEPARTMENT OF INFORMATION TECHNOLOGY

Dual Security Based Ad-hoc On-Demand Distance Vector Algorithm to Detect and Mitigate Black Hole and Gray Hole Attacks in Mobile Ad-hoc Networks

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Networking and Security

Dagne Alemu Kebede

Advisor: Esubalew Yitayal (Ph.D.)

Debre Berhan, Ethiopia

January, 2021

Approval Page

This M.Sc. Thesis proposal is entitled with Dual Security Based Ad-hoc On-Demand Distance Vector Algorithm to Detect and Mitigate Black Hole and Gray Hole Attacks in Mobile Ad-hoc Networks.

The following examiners have approved it:

Advisor:

Esubalew Yitayal (Ph.D.) Sign ---------- Date ----------

External Examiner:

---------- Sign ---------- Date ----------

Internal Examiner:

---------- Sign ---------- Date ----------

Chairperson:

---------- Sign ---------- Date ----------

DECLARATION

I am Dagne Alemu, a student in the College of Computing, University of Debre Berhan, aware of my responsibility, the penal law, declare and certify with my signature that my thesis entitled *Dual Security Based Ad-hoc On-Demand Distance Vector Algorithm to Detect and Mitigate Black Hole and Gray Hole Attacks in Mobile Ad-hoc Networks* is entirely the result of my original work and this is not done in another university. I have faithfully and accurately cited all my sources. Every serious effort has been made to avoid any plagiarism in the preparation of this thesis.

Declared By:

Name: Dagne Alemu

Sign: ----------

Date: ----------

This thesis has been submitted for examination with my approval as a university advisor.

Confirmed By:

Name: Esubalew Yitayal (Ph.D.)

Sign: ----------

Date: ----------

Dedication

This thesis work is dedicated to my family.

Dagne Alemu

Acknowledgments

First and foremost, praises and thanks to God, the Almighty, for His showers of blessings throughout my research work to complete the research successfully.

I would like to thank my advisor, Esubalew Yitayal (Ph.D.), for his guidance, direction, patience, and continuous encouragement throughout the time of my thesis research.

I would like to express my respectful thanks to my families, without their support and encouragement I would have not been here today. They have always been with me supporting, helping, and appreciating my journey to be a better man.

Finally, my thanks go to all the people who have supported me to complete the research work directly or indirectly.

Abstract

A Mobile Ad-hoc Network (MANET) is characterized as an ad hoc network that utilizes mobile nodes that are self-assertively located. In a MANET, it is expected that all of the nodes cooperate to move data packets in a multi-hop design. However, some malicious nodes don't cooperate with other nodes and disturb the network through bogus routing information. This activity prompts security challenges because MANET has no mechanism to identify malicious nodes. This study focuses on detecting and mitigating data packet dropping malicious nodes, which are black hole and gray hole attacks. A black hole is a malicious node that absorbs all data packets by advertises false routing information in route discovery operation, and the gray hole attack advertises true route information but changes behavior in the actual data transmission. To overcome these security challenges different researchers have developed different algorithms. In this paper, we have proposed a Dual Security based Ad-hoc On-Demand Distance Vector Algorithm (DS-AODV) based on the destination sequence number of RREPs and data packets to detect and mitigate black hole and gray hole attacks during route discovery operation and actual data transmission. The modifications to the AODV protocol and justify the solution with appropriate implementation and simulation using NS-2.35. The performance of our DS-AODV algorithm shows that in the case of black hole attacks 83.6 % and smart gray hole attacks 81.3% average detection rate. Hence, our analysis shows the improvement in Packet Delivery Ratio and Normalized Routing Overhead. In the case of a black hole attacks are improved by 10.7% and 30.9%, respectively than MBDP-AODV algorithm, and 6.4% and 6.11%, respectively than DDBG-AODV algorithm. In the case of smart gray hole attacks are improved by 4.27% and 1.38%, respectively than the DDBG-AODV Algorithm.

Keywords: *AODV, Black Hole Attack, Data Packet, DS-AODV, Mobile Ad-hoc Network, Sequence Number, Smart Gray Hole Attack*

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AODV	Ad-hoc On-Demand Distance Vector
CBR	Constant Bite Rate
DARPA	Defense Advanced Research Project Agency
DDBG	Dual Attack Detection for Black and Gray Hole Attacks
DFV	Data Forwarding Value
DoS	Denial of Service
DS-AODV	Dual Security-AODV
DSDV	Destination Sequenced Distance Vector
DSR	Dynamic Source Routing
FNR	False Negative Rate
FPR	False Positive Rate
GUI	Graphical User Interface
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	Media Access Control
MANET	Mobile Ad-hoc Network
MBDP	Mitigating Black Hole effects through Detection and Prevention
NAM	Network Animator

NS-2	Network Simulator Version 2
NS-3	Network Simulator Version 3
OLSR	Optimized Link State Routing
OTCL	Object-Oriented Variant of Tool Command Language
PDR	Packet Delivery Ratio
QoS	Quality of Service
RERR	Route Error Packet
RREP	Route Reply Packet
RREQ	Route Request Packet
TORA	Temporary Ordered Routing Algorithm
UDP	User Datagram Protocol
ZRP	Zone Routing Protocol

Chapter 1 Introduction

In this chapter, the basic introduction of the research background, the motivation of the study, the statement of the problem, objectives, scope, limitations and significance of the study are discussed. Also, the organization of the thesis is discussed in this chapter.

1.1 Background

The wireless ad-hoc network is a type of computer network that allows the device to communicate with one another through the wireless connection [1]. The major characteristics of ad-hoc networks are lack of fixed infrastructure, multi-hop communication by cooperative sending of the packet and the utilization of shared wireless links [2]. As the ad-hoc network is bound to these characteristics, Mobile Ad-Hoc Network (MANET) is an infrastructure-less, self-made and self-composed ad-hoc network of mobile nodes that are interconnected with each other over a wireless link. Due to wirelessly link, MANET is a significant piece of correspondence innovation, devices communicate with each other and route information to a remote end without the guide of any fixed infrastructure [3].

In a MANET, the nodes taking part in the route between the source and the destination node to accomplish the routing activity, each node has two roles, i.e., as a host and as a router to send data packets. A basic design of MANET routing protocols is the assumption that the entirety of its nodes works genuinely and cooperatively [4]. To do that, they require a standard routing protocol like Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). These are not intended to manage security threats. In the absence of incorporating security management with dynamic topology features, MANET faces security issues [5, 6] and is highly vulnerable to a variety of attacks [7]. The major attacks that disturb the standard behavior and affect the performance of networks are a black hole, gray hole, wormhole, selfish-node misbehaving, Sybil, etc. [8]. Among these attacks, black holes and gray holes come under a dangerous variety of Denial-of-Service attacks (DoS) [9].

In a black hole attack, the attacker node imitates a destination node by sending a false route reply packet to a source node that starts a route discovery process by creating a fake destination sequence number to promote itself as a fresher node and absorbs all data packets then drops them [10]. In

the gray hole attack, the attacker node may behave as a normal node initially during the route discovery operation and then may change its state to malicious during actual data transmission [5].

Nowadays, ongoing works in DoS attack mitigation are fundamentally centered on anomaly-based techniques. Numerous anomaly-based techniques were proposed in the recent past to mitigate the black hole and gray hole attacks. Among these techniques cryptography based, sequence number based, trust based, acknowledgment based, clustering based and IDS based are popular [11]. In this paper, we propose a dual security based method to secure the AODV routing protocol against black and gray hole attacks. The detection mechanism works during the route discovery phase as well as during the data transmission phase. If the attacker node misbehaves maliciously during the route discovery phase by sending a fake destination sequence number, then the detection mechanism in the route discovery phase will detect the attacker node. If the attacker node acts normal during the route discovery phase and once after getting route path begins showing up maliciously by dropping data packets, then additionally the detection mechanism in the data transmission phase will detect the attacker node.

1.2 Motivation of the Study

Nowadays, MANETs have gotten particularly significant. Since, it tends to implement an infrastructure-less connection, which is helpful to expand the conventional fixed infrastructure network. However, due to the advancement of MANET, it has given new challenges. Such challenges come up due to technological changes. Those challenges are security, multipath routing, bandwidth constraint, QoS issues and compromised nodes. Among those lists of challenges, security is an open area of research, which is not fully addressed still now it needs more research work. The design of conventional MANET routing protocols is not considered a security. Because of this reason, MANET security is one of the major issues.

To forward the data packet to the targeted node, a malicious node free route path is required. Among those malicious nodes, the black hole and the gray hole are data packet dropping attacks. Therefore, securing the network is significant for forwarding data packets correctly from the node to the neighbor node without any data packet loss. There are many existing security mechanisms to detect black hole and gray hole attacks in the related work, yet at the same time, security issues exist, not completely tended to the issues in MANET. The constraints of the existing security

mechanism give inspiration for us to propose the dual security based black hole and gray hole attack detection and mitigation algorithm based on AODV in MANET.

1.3 Statement of the Problem

In a MANET, all nodes are independent of each other and they behave like a router/host or like both a router and a host at the same time [12]. Due to its dynamic nature, routing in MANET is difficult. A fundamental issue arising in MANET routing regarding security attacks is the selection of the correct path between any two nodes. All the nodes are assumed cooperative and trustworthy in the routing protocols such as AODV and DSR [4]. However, these conventional routing protocols are vulnerable to different sorts of attacks since it depends on the assumption that all nodes will cooperate, it has been structured without security mechanism consideration [13, 14]. The problem here is to send and receive data packets through the route across the nodes that may have malicious nodes in it that will drop the data packets [15]. Previously the works done on MANET focused on different security attacks. Among these attacks, the black hole and the gray hole attack involved in MANET is evaluated based on reactive routing protocol like AODV. Some of the designed detection mechanisms are not covering all kinds of packet drop attacks under various networking scenarios.

In [16], the authors have proposed an algorithm for securing MANET from a black hole node. In this algorithm, the authors assumed that the malicious node adds an arbitrary maximum number of 100 to the source sequence number. If the difference of destination sequence number and source sequence number greater than 100, then the node is a black hole node. However, as the behaviors of a black hole in MANET, which is difficult to set arbitrary number because the black hole node generates RREP by adding a random number. Therefore, this algorithm fails to detect malicious nodes when the difference of destination sequence number and source sequence number less than 100, and it cannot detect the malicious node that sends true RREP.

The authors have proposed a dynamic threshold approach called Mitigating Black Hole effects through Detection and Prevention (MBDP-AODV) algorithm [17]. The MBDP-AODV algorithm mitigates a malicious (black hole) node in the route discovery operation that sends false RREP. According to this algorithm, unlike in AODV, the destination node sends back RREP for all the received RREQ packets to the source node. After the source node receives a minimum of three RREPs, it calculates the average and standard deviation value of the destination sequence number

(D_Seqno) in RREPs. The standard deviation value is taken as the threshold value. If the threshold (standard deviation) is greater than the average value, then the detection mechanism starts, else the algorithm is considered there is no malicious node in the network. If the D_Seqno in the RREP packet is greater than the threshold value, the node is considered a black hole node. However, the MBDP-AODV algorithm fails in some conditions, these are listed as follows.

The drawbacks of the MBDP-AODV algorithm are:

- If the dispersion value of the destination sequence number in the RREP between the malicious node and normal node is small, then this algorithm fails to detect malicious nodes. Because the standard deviation is less than the average value.
- Even the dispersion value of the destination sequence number in the RREP between the malicious node and normal node is high, but if RREQ by the source node to a destination node is assigned a higher destination sequence number, then this algorithm fails to detect malicious nodes.
- If the malicious node behaves normally by sending true RREP during route discovery operation and behaves maliciously during actual data packet transmission, then this algorithm fails to detect it i.e., Smart gray hole attack.
- High routing overhead due to the destination node sends multiple RREPs.

In this paper, we propose a method to overcome the stated problems by considering any dispersion value of the destination sequence number in RREPs in route discovery operation and data packets in actual data transmission.

1.4 Research Questions

This study is to present the dual security based algorithm for MANETs to overcoming the limitations of algorithms presented in related work. Hence, this research work attempts to answer the following research questions:

1. What are the possible network conditions that allow a malicious node (black hole and gray hole) to get a route path in MANETs?
2. Which existing security based MANET routing protocol is more efficient for the detection and mitigation of black hole and gray hole attack to enhance the performance of MANETs?

3. How to design a dual security based algorithm using the destination sequence number of RREPs in the route discovery operation and data packets in the actual data transmission for detecting and mitigating the black hole and gray hole attacks?
4. What are the performance metrics to evaluate the proposed algorithm?

1.5 Objective of the Study

1.5.1 General Objective

The general objective of this study is to develop a dual security based algorithm that detects and mitigates malicious nodes launching black hole and gray hole attacks for MANET based on AODV protocol.

1.5.2 Specific Objectives

To achieve the general objective, the following specific objectives are identified.

- Carryout literature review on conventional and security based routing protocol of MANETs.
- Select the appropriate simulation tool.
- Identify appropriate performance metrics for the evaluation of the proposed algorithm against the existing one.
- To implement the black hole and smart gray hole attacks in the AODV routing protocol.
- To develop dual security based black hole and gray hole attack detection and mitigation algorithm in route discovery operation and data packet transmission for MANETs.
- To implement the proposed algorithm under the AODV algorithm.
- To evaluate the performance of the proposed algorithm against the existing one, concerning the black hole and smart gray hole attacks.

1.6 Scope and Limitation of the Study

The scope of this study is delimited to develop a dual security based algorithm using the destination sequence number of RREPs and data packets. It analyzes MANETs under the black hole and smart gray hole attacks, which affect the performance of a MANET. In this study, among other routing protocols, AODV is selected. The performance metrics used for comparison and analysis of the results are Detection Rate, False Positive Rate, False Negative Rate, Packet Delivery Ratio, and

Normalized Routing Overhead. The scope of the study is also delimited to a maximum of 30 mobile nodes and a simulation area of 1000m x 1000m. The limitation of this study is the sequence number based gray hole attack is not evaluated in the simulation.

1.7 Significance of the Study

In this work, black hole and gray hole attacks are considered misbehavior. In particular, this paper addresses the problem of routing misbehavior by designing a dual security based mechanism for black hole and gray hole attacks. This mechanism prevents a malicious node from dropping data packets. The major contributions of the proposed method to the existing method are summarized as follows:

- It increases the detection rate of the black hole for any dispersion value of D_Seqno in RREP and gray hole attacks.
- It adds one level of security mechanism to the existing one, which is the data transmission phase for detecting and mitigating the effects of the black hole and the gray hole (particularly nodes with smart gray hole attacks) in the network.
- Detect and mitigate both the black hole and gray hole nodes.
- Minimize Routing Overhead.

1.8 Organization of the Thesis

The rest of this thesis is organized as follows: Chapter 2 literature review and related work for MANET security regarding black and gray hole attacks were presented. It also describes the basic concept of the MANET, the techniques to mitigate MANET attacks, and a detailed description of related work that is done in this research area. Chapter 3 describes the proposed dual security based algorithm for the detection and mitigation of black hole and gray hole nodes from the network. Furthermore, the proposed algorithm flowchart and the algorithm of the proposed protocol is introduced. Chapter 4 describes the implementation and performance analysis of the proposed algorithms as well as present the result analysis based on the simulation results obtained. Finally, the conclusion and future work are discussed in Chapter 5.

Chapter 2 Literature Review

In this chapter, the basic concept of wireless networking, ad hoc network, vulnerability and challenges of the MANET, routing protocol of MANET, security attacks and the defense mechanism of security attack are discussed. Also, related work for black hole and gray hole attack detection mechanisms in route discovery operation, actual data packet transmission and both in route discovery operation and actual data packet transmission are discussed.

2.1 Wireless Networks

Throughout the years, the development of mobile devices has refined the world and it has got one of the most discussed topics in the computer world. A computer network is a group of two or more devices that are connected to the sharing of resources with a physical or wireless connection. Because of the dependence on the framework, the networks can be divided into two main categories, which are wired and wireless networks. Wireless networks provide flexibility in which nodes are associated through the wireless connection. The popularity of wireless innovation becomes expanded and a new paradigm has been characterized by utilizing this innovation in the networking domain [18]. The wireless network is getting well known because of its capacity to permit various nodes to communicate simultaneously while keeping up their mobility [19]. It is comparatively simpler to install rather than wired networks. There is nothing to stress over pulling the cables in walls and roofs and it can configure according to the need of the users.

Based on the dependency of infrastructure, the wireless network can be divided into two i.e., Infrastructure-based networks and infrastructure-less networks [20, 21]. In infrastructure-based networks, the network has a fixed base station under centralized administration [22]. In infrastructure-less networks, the mobile nodes act as routers, the networks that do not have an access point or fixed base station and these mobile nodes build route paths dynamically among themselves to make their network. Ad-hoc networks come under this kind of network, as they do not depend on centralized administration [20].

2.2 Ad-Hoc Networks

An ad-hoc network is a decentralized wireless network, which has no infrastructure. The nodes are allowed to join and left from the networks and the duration of the established route path in the network for a short duration [23]. Unlike traditional wireless networks, the nodes are associated

with one another through a wireless link. A node can fill in as a router to advance the information to the neighbor nodes. Consequently, this sort of network is called infrastructure-less networks. These networks have no centralized organization. The ad-hoc networks can manage the node with any breaking down or any progressions that it experiences because of topology changes. At whatever point a node in the network is down or leaves the network that causes the connection between the nodes is broken. The nodes in the network just request for new routes and new connections are set up as a Mobile Ad-Hoc Network [18].

2.3 Overviews of Mobile Ad-hoc Networks (MANETs)

The name of MANET was known as a packet radio network, which was introduced by Defense Advanced Research Project Agency (DARPA) in 1970 and the Internet Engineering Task Force (IETF) starts the working group of MANET in 1996, with the goal to normalized IP routing protocol functionality appropriate for wireless routing applications [24]. MANET is a self-creating network formed automatically by an arrangement of at least two nodes. The Nodes are devices i.e., Mobile phone, laptop and a personal computer that is participating in the network and is mobile.

In the current situation, due to flexibility and ease of use wherever and whenever, many real-time applications use MANET, such as a military operation, crisis management and personal area network [25, 26]. In a MANET, the connections are imparting bidirectional. The direct communication of the source node and the destination node is showing up when the destination node is under the transmission scope of the source node unless communicating with each via the intermediate nodes between them because the transmission scope in MANET is limited [27]. The topology is performed by the connectivity of the nodes with each other in the network. Due to their self-configuration, the nodes can configure themselves. One of the challenging and interesting research areas is routing protocols. Because many routing protocols have been proposed for MANETs, i.e., AODV, OLSR, DSR, etc.

An example of MANET is shown in Figure 2.1. It depicts a MANET wherein every mobile node is independent to move toward any path, causing successive fluctuation in a joint. It comprises an independent collection of mobile nodes where the nodes may associate and detach the network periodically. The mobile nodes dynamically change and each mobile node plays out an assembly just as a router to transmit the information. The devices utilized in MANET are compelled to energy, memory, battery and data transmission.

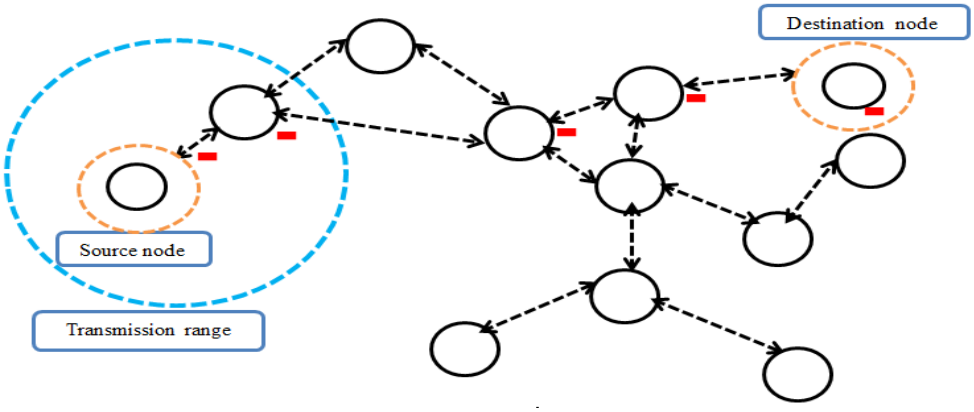


Figure 2. 1 Mobile Ad-hoc Network [28]

2.3.1 Vulnerabilities of MANET

In this section, we describe the different security vulnerabilities and weaknesses of wireless networks. The wireless medium is seen as more introduced to security attacks than the wired medium due to its weaknesses. These gained weaknesses of wireless connection make the MANETs significantly powerless. Keeping with or without the accommodation, the properties of MANETs are to such an extent that security is continually going to be an issue. These vulnerabilities can be listed in the following [24, 28, 29]:

- **Wireless Links:** Unlike wired networks, wireless networks are available to some other devices in the network, which makes the wireless connections inclined to security issues. The nodes utilizing wireless transmission joins makes the ad hoc network vulnerable to the malicious node, MANET is vulnerable to diverse kinds of attacks due to no clear secure boundary [7]. In MANET, nodes have the freedom to join and leave inside the network. A node can join a network automatically if the network is in the range of the node, thus it can communicate with other nodes in the network. Due to unsecured boundaries, MANET is more disposed to attacks.
- **Dynamic Topology:** The nodes in MANETs can move around freely and join or leave the network with no limitations that result in a frequent change in the network topology. Thus, there is no assurance concerning the delivery of packets or the presence of substantial paths prompting to the destination. MANET nodes are allowed to move randomly in the network. Hence, the network topology may change arbitrarily and quickly at unpredictable times. It

is hard to recognize a normal difference in the network topology and malicious node conduct in this powerful network condition.

- **Lack of Central Governing Body:** According to the meaning of MANETs, it doesn't have any central body to care for the general working of the network or to screen the malicious nodes. It doesn't have a concentrated administration instrument, for example, a server or the interruption identification framework, which leads to various vulnerability and security issues.

2.3.2 Challenges of MANET

The area of MANETs leads to the node to move openly in the wireless medium. For this reason, the nodes are leaving and entering the network freely. There is no centralized framework to deal with the activity of the procedure. The shortcoming of MANET is vulnerable to different challenges. Among those challenges, the following are listed [30, 31]:

- **Multi-Hop Routing:** In the multi-hop routing mechanism, the destination node can communicate with more than one node to perform routing. In a MANET, the nodes act as the host and router at the same time [12]. There is no fixed router, the routing algorithm utilized in MANETs have a presumption that each node ready to be a piece of the network is non-malicious and can help in routing the packets all through the networks.
- **Security:** In a MANET, nodes are associated with a wireless network. For any network, security is the primary concern and it turns out to be more challenging about MANET. MANET permits anybody to move freely in or out of the network and the device moves with one another in an open space, which uncovered the network exercises to the attackers.
- **Quality of Service (QoS):** The difficulty of QoS, which makes the MANET an additional challenging area. MANET is a wireless network and in correlation to wired connections, wireless connections experience more data loss, distortion, delays and vary in speed and capacity, which makes it hard to ensure the nature of the administration. As MANET follows dynamic topology, it is hard to have accurate data about the condition of networks and devices and it turns out to be considerably even more challenging to give the QoS.
- **Compromised Node:** Some of the attacks are to get access inside the network to get control over the node in the network using unfair means to carry out their malicious activities. The mobile node in MANET is free to move, join, or leave the network [19].

Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity.

- **Scalability of Network:** In a traditional network, where the network is built and each machine is connected to the other machine with the help of wire [1, 2]. The network topology and the scale of the network, while designing it defined in the beginning phase of the designing of the network. The case is quite opposite in MANETs because the nodes are mobile and due to their mobility in MANETs, the scale of the MANETs is changing. It is too hard to know and predict the number of nodes in the MANET in the future.

2.4 MANET Routing Protocols

In a MANET, there is no centralized administration framework; every mobile node works as a router [12]. Due to the unpredictable and dynamic nature of MANET, nodes do not have any earlier information about the topology. In this manner, nodes need to decide the topology. A node advertises its essence and listens to advertisements of its neighbors. This is the manner that a node finds its neighbors just as approaches to come to those. This activity is performed by routing. Therefore, routing is a major challenge in the environment where nodes are moving very frequently and the movement of a node may bring in an adjustment in the route. It is a procedure of exchanging data starting with one node and then onto the next node or it is the procedure wherein, the packets or messages will be sent from the source to the destination node in the mobile ad-hoc network, this directing procedure is performed by a routing protocol [12, 20].

Routing protocols are the basic piece of the MANET. They are answerable for recognizing the ideal way from a source node to a destination node in a particular MANET. Because of these different requirements alongside lively topology, the role of routing protocol is even more challenging. Routing protocols are used to organize the distinguishing proof of route path and transmission of packets from the source to the destination node through the intermediate node. In a MANET, there are many routing protocols accessible openly. All the accessible MANET routing protocols are classified into three different categories according to their functionality [32, 33, 34] i.e., Proactive (table-driven), reactive (on-demand) and hybrid routing protocols. The hierarchy of these protocols is shown in Figure 2.2.

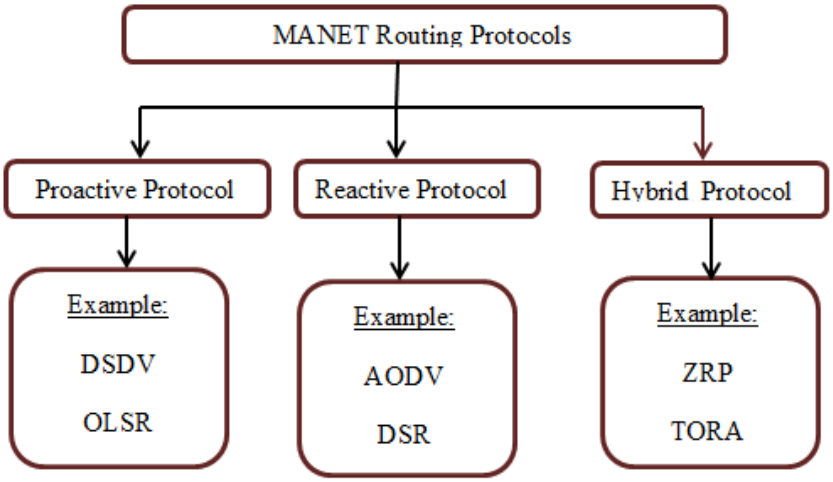


Figure 2. 2 Classification of MANET Routing Protocols [26]

2.4.1 Proactive Routing Protocols

A Proactive routing protocol is also called table-driven routing protocols, here the routing information of the mobile nodes is periodically exchanged and the network topology information is maintained in routing tables [35]. These tables are always updated to keep up up-to-date routing information from each node to every alternative node as the network topology changes. This activity leads to high overhead on the network comparatively over other routing protocols. Due to the high control overhead, the proactive routing protocol is not suitable for larger networks. This protocol works based on Link state and distance vector algorithms. DSDV is one of the most common proactive protocols in MANET [33].

2.4.2 Reactive Routing Protocols

In reactive routing protocol [35], there is no exchange of routing information periodically. It is also called an on-demand routing protocol. Each node builds its routing table that it can use to find a path to a destination. In contrast to the proactive routing protocol, the reactive routing protocol does not maintain routes but builds them on demand [32]. This leads to higher latency and less control overhead than with proactive protocols. The most well-known examples of the reactive routing protocol are AODV, DSR [33].

Typically, the reactive routing protocol has the following characteristics:

- Do not discover a route until requested.
- When attempting to discover the goal "on request", it utilizes a flooding method to engender the inquiry.

A reactive protocol finds a route on-demand by flooding the network with route request packets. These protocols have the following advantages:

- No big overhead for global routing table maintenance as in proactive protocols.
- The quick reaction for network restructure and node failure.

2.4.2.1 Ad hoc On-Demand Distance Vector (AODV) Routing Protocol

Ad hoc On-Demand Distance Vector [36] is a state of the art routing protocol for MANET, created as an enhancement to DSDV and DSR routing protocols. It is an on-demand routing protocol settled just when required. Until the communication of the node is established, it does not have any information about other nodes. Based on a regular time interval, the local connectivity information is maintained by each node by broadcasting HELLO packets. The local connectivity of the node maintains information about all the neighbors. The AODV protocol operates in two phases: Route Discovery and Route Maintenance [37]. In the AODV routing protocol, three control packets are utilized for performing routing activity i.e., Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) [38]. It utilizes RREQ and RREP in the route discovery phase and the RERR in the route maintenance phase.

Packet Type	Reserved	Hop Count
RREQID		
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Source Sequence Number		

(a) RREQ

Packet Type	Reserved	Hop Count
Destination IP Address		
Destination Sequence Number		
Source IP Address		
Lifetime		

(b) RREP

Packet Type	Reserved	DestCount
Unreachable Destination IP Address (1)		
Unreachable Destination Sequence Number (1)		
Additional Unreachable Destination IP Addresses (if needed)		
Additional Unreachable Destination Sequence Numbers (if needed)		

(c) RERR

Figure 2. 3 AODV Packet Formats

I. Route discovery

All the mobile nodes work in cooperation to discover the route path from source to destination. The transmission of real information is performed after the path is set up. It uses bidirectional connections for route discovery and route maintenance [27]. It utilizes a route discovery mechanism to locate the specific route in the network [20]. The source node initiates route discovery operation when it needs to communicate to another node in the network. The source node starts to broadcast the RREQ message to its neighbors when the requested route isn't available. The neighbor nodes receiving the RREQ message then must check whether the neighbor is the desired destination or not. The neighbor node sends RREP message to the source node through the backward connection, if it is the destination node. Unless it starts to rebroadcast the RREQ message to other nodes in the network until it reaches the intermediate node or destination node, which contains the fresh enough route to the destination [39]. Generally, when the node gets the RREQ message, there are two possibilities to return the RREP to the source node such that, if it is the node is a destination or if it has a fresh enough route to the destination. Therefore, to send RREP, it must consider the destination sequence number of the node.

II. Route Maintenance

It utilizes a route maintenance mechanism to keep up the routes that are effectively participating in the network [20]. During the process of sending the packets, the node will be monitoring its neighbor to know the neighbor node active or not. When an error is found in the active route by any node in that route, the node can immediately broadcast RERR packets to all of its reachable neighbors. The RERR message contains the list of the unreachable destinations for its loss of connectivity. When a source node receives RERR, it can initiate the route discovery.

2.4.2.2 Role of Sequence Number in AODV Routing Protocol

The AODV protocol varies from other on-demand routing protocols by utilizing a sequence number. In AODV, the highest destination sequence number demonstrates the freshness of the path. If the RREP is sent by an intermediate node if and only if its destination sequence number greater than the destination sequence number of RREQ unless it cannot send the route reply. If the RREP packet is sent by the destination, the sequence number of the node is further increased by one and gets unicasted back to the originator. When the source node receives RREP, if the node destination sequence number in its routing table is higher than the destination sequence number specified in the RREQ packets, the source node will update its routing table with the new RREP control message else, the RREP control message will be discarded. The source node may receive multiple RREPs; it will select one among those RREP having the highest destination sequence number. If the destination sequence number is equal, then it will select the RREP having the smallest hop count [40].

In Figure 2.4, suppose source node S broadcast RREQ for a neighboring node with a destination sequence number of destination node D. The intermediate node sends back RREP if it has a fresh route to the destination node else rebroadcast RREQ to neighboring nodes. In this figure, the intermediate node E sends back RREP indicates it has a fresh route to destination node D. The target destination node D sends back RREP.

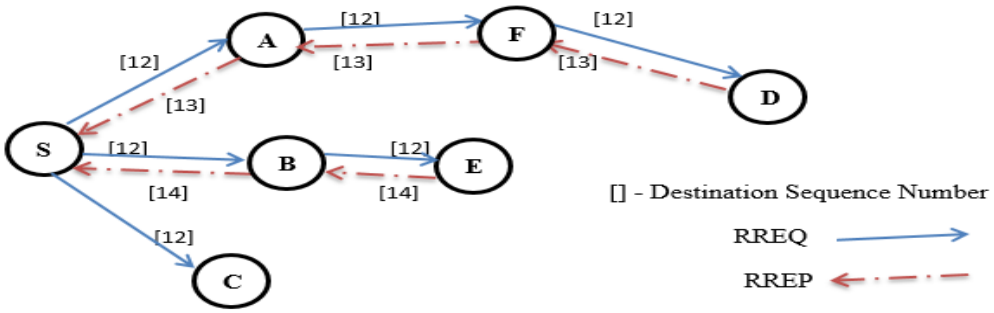


Figure 2. 4 AODV Working Principle [40]

After that, the source node S selects one RREP from the two by using the destination sequence number. According to AODV working principle, it selects the path S➔B➔E➔➔D, because it has a higher destination sequence number i.e., 14.

In this paper, the AODV routing protocol is selected as the base protocol because the black hole and gray hole attack properties center on the sequence number, it utilizes a destination sequence number for the determination of the best route [19]. It decides the path for data forwarding with a higher destination sequence number [5]. The destination sequence number of RREPs is used to propose an algorithm for detecting and mitigating black hole and gray hole attacks.

2.4.3 Hybrid Routing Protocols

A hybrid routing protocol is designed by combining the features of the proactive and reactive routing protocol. Inherent the advantages of the two protocols (reactive and proactive) routing protocols. Every node maintains each of the topology information at an interval of its zone. Proactive behavior is used within the routing zone of each node while reactive behavior is used for the nodes that are outside the routing zone [35]. Along these lines, a route to every destination at intervals a zone is built instantaneously, while a route discovery and a route maintenance strategy are required for a destination that is in alternative zones.

2.5 Security Concerns in MANET

In a MANET, there are some significant issues, such as security, routing, QoS and scalability of the network [30]. Among the issues of MANET, security turns into a major concern. Due to its characteristics like open medium, dynamically changing topology and any exercises performed without fixed infrastructure, MANET often suffers from security attacks. Besides, due to the inherited characteristics and dynamic nature of MANET, it is more powerless to be assaulted than

wired networks. Security in MANET is the most basic worry for the appropriate usage of the network [26].

The non-secure boundaries of the MANET [7] make it revered to different dangers like information leakage by eavesdropping or Denial of Services where the malicious node continues creating the bogus answers until where the node jams itself with the ceaseless answers from the malicious nodes. Due to the non-secure boundaries, the malicious nodes frequently get inside the network as a black hole, gray hole, wormhole, and jellyfish attackers and perform their malicious exercise. The significant security that should be satisfied for a reliable network is the accessibility of the network when required, the confidentiality and integrity of data, its verification of the genuine source and destination, and non-repudiation must be satisfied if the network is secure from the different kinds of assaults.

2.5.1 Classification of Attack

According to the disruptive behavior in wireless communication, attacks are broadly divided into two classes, i.e., Passive attacks and active attacks [26].

I. Passive Attack

In a passive attack, the attacker doesn't intrude on the typical activity of the routing protocol but attempts to attain and retrieve useful information by listening to the network [41]. The point of this attack is to work quietly to gather information by observing the network to launch active attacks in the future [18]. Distinguishing these kinds of attacks is very challenging because the operation of the routing is correctly working. Accordingly, it is hard to safeguard against passive attacks. Examples of passive attacks include eavesdropping, monitoring, and traffic analysis [8].

II. Active Attack

An active attack [35] intrudes on the ordinary activity of the protocol to gain unauthorized access for inserting, altering, and deleting the exchanging data packets. It limits the accessibility and authentication of the data exchanged in the ad-hoc network to different nodes. It tends to be malicious or selfish attacks. A malicious attack [41] expects to disrupt normal network operations, while a selfish attack focuses on the increase out of line portions of the constrained network assets, even at the costs of different nodes. Attacks that mostly occur that disturb the normal behavior of

the network are jamming, impersonating, modification, denial of service (DoS) and message reply. The active attack is easier to distinguish than the passive attack because the behaviors of the attacks are known. There are many attackers under active attack classification such as the Black hole, Gray hole, Wormhole and Jellyfish [8, 24].

- Black Hole Attacks: Attacker deceives other nodes by advertising itself as having the higher destination sequence number and shortest path to the node whose packets it needs to block in the network. A malicious node pretends to an intermediate node of a route to some given destinations. From this point, an attacker diverts all packets destined for itself.
- Gray Hole Attacks: The attacker in the route discovery phase participates in normal, but changes its behaviors to malicious in actual data transmission. In this way, selectively drop some portion of the incoming packets and then forward the remaining packets coming from the various nodes to their neighbors.
- Jellyfish Attacks: The attacker node presents a delay during packet sending. It is characterized by three classifications: Jellyfish Delay variance attack, Jellyfish periodic dropping attack, and Jellyfish reorder attack. In a delay variance attack, Packets are delayed in arbitrary order. Whereas periodic dropping attack, the attacker periodically drops the packet. Jellyfish reorder attack, reorders the transmission between a source node and a destination node.
- Wormhole Attacks: Attacker performs malicious exercises by two malicious nodes working together to make a tunnel between them to distort the widely used hop-count metric. Routing can be disrupted when routing control messages are tunneled, wormhole attacks could prevent the discovery of any routes other than through the wormhole.

In this paper, the algorithm focus on the two attacks: black hole and gray hole. The AODV routing protocol has weakness expose to the active attacker in different ways, i.e., the intruder modifies the message then forwards, drops the data packets and the attacker sends a faked message for the received routing message or the attacker sends a forged message without any intervention illustrated in Figure 2.5. Therefore, this paper focus on fake RREP in the route discovery operation and a data packet drop in the data transmission.

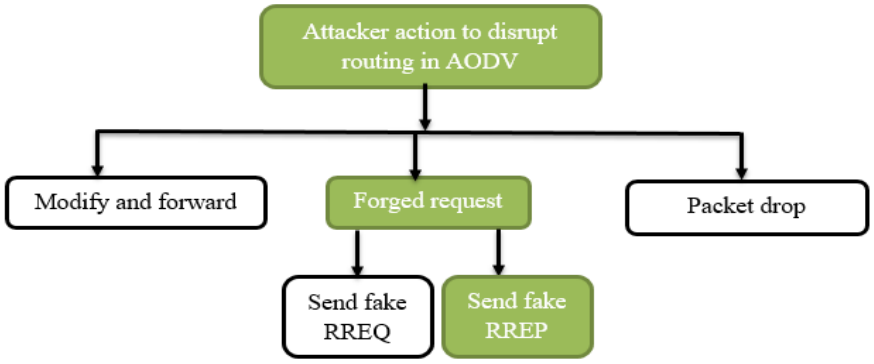


Figure 2. 5 Attacker Action to Disrupt Routing in the AODV Protocol [41]

2.5.2 Data Packet Dropping Attacks

The data packet dropping attack is a kind of DoS attack that a node in the network will drop the data packets [42]. DoS attack is an active attack that disturbs the ordinary activity of the route by producing bogus messages to expend other node resources. In the data packet dropping attack, the attacker node drops the data packets, yet before arriving at the destination node the intermediate node drops the data packet that shows in Figure 2.6. Therefore, our problem is to detect the data packet-dropping attacker and try to reduce the packet drop ratio.

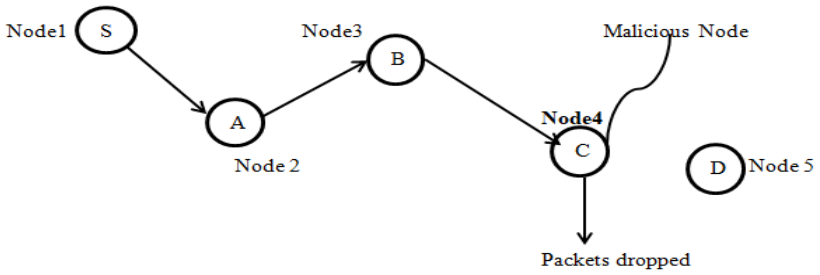


Figure 2. 6 Dropping Data Packets by Malicious Node [42]

The common attacks that perform malicious activities in data packets and are complex to detect in MANET are black and gray hole attackers. The DoS attack can be classified into a full packet drop and partial packet drop attack, which is shown in Figure 2.7. A black hole attack is a term used for a full packet drop attack and the gray hole attack is the term used for a partial packet drop attack.

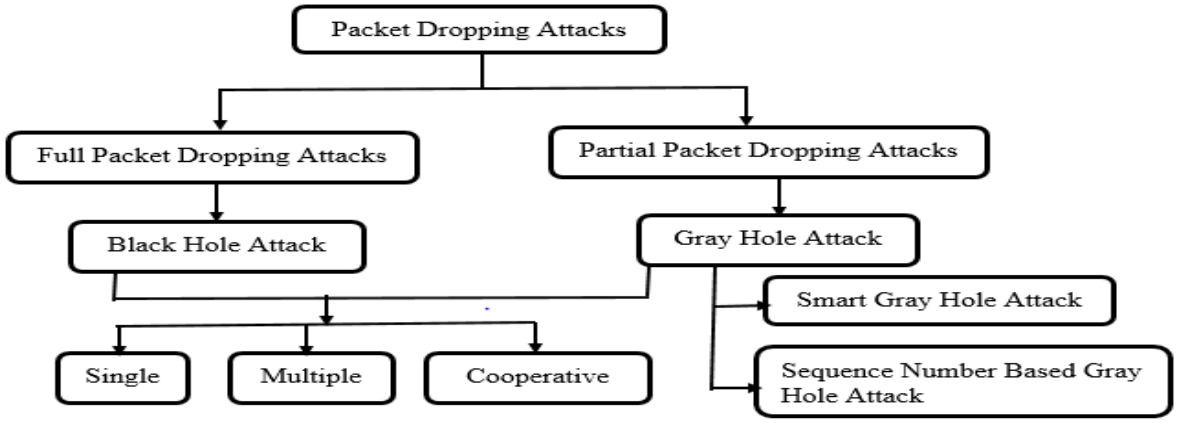


Figure 2. 7 Taxonomy of Packet Dropping Attack [17]

2.5.2.1 Black Hole Attack

In a MANET, one of the very common network layer attacks is a black hole attack [43]. It is a sort of DoS attack, where a malicious node sends false route information, asserting that it has an optimum route and makes another great node route data packets through the malicious one. It does this pose itself as a destination or as a node having a valid route to the destination [19]. For instance, in AODV, on receiving the RREQ request, a black hole node responds to false routing information in the RREP to the source node without checking its routing table to advertise itself having up to date information [14]. The information contains a fake destination sequence number [15, 26].

On receipt of the RREP packet, the malicious node will be selected as one of the intermediate nodes, then the route will be built up and the source node will send all its data packets to the black hole node thinking it has fresh enough route to the destination. In this way, all traffic will be directed through the malicious node, and along these lines, the malicious node can abuse or dispose of the traffic. The malicious node never forwards any of the data packets to the genuine destination, so the genuine destination node never gets any data packets. Therefore, the communication between the source node and the destination node did not establish. As a result, the black hole node will drop all the packets it receives from the source node. For this reason, a black hole attack is known as a packet dropping attack, which seriously decreases the performance of the network [11]. The point of the black hole attacker is to attract traffic towards it and block data packets by dropping them. Along these lines, consequently, the source and the destination nodes became unable to communicate with one another [19].

Figure 2.8, illustrates the malicious node (black hole) participation in the AODV route discovery operation. Assume source node S is trying to establish a path to destination node D. So node S sends RREQ packet to all neighboring nodes. Node A, B and C have received the RREQ. If A, B and C have a valid route to the destination D, they send RREP packet to node S, in this figure, there is no valid route, they use broadcasting to send the RREQ packet. The exchange of route information will be repeated until RREQ reaches an intermediate node that has a fresh route and node D. However, node B (assumed to be a malicious node) has not a valid route to the node D, but it sends back RREP to node S. The node G (it has a fresh route to node D) and destination node D send back RREP message to node S. After node S receives the RREP, a route is established. In case the source node may receive multiple RREPs, in this figure, the source node S receives three RREPs.

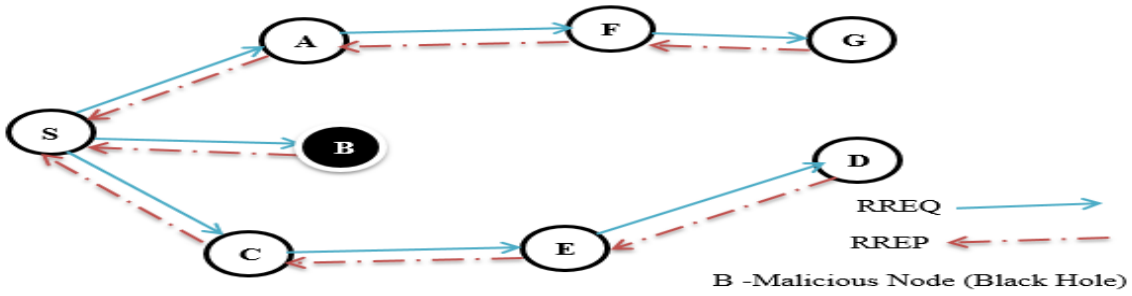


Figure 2. 8 Sending False RREP by Black Hole Node [17]

In Figure 2.9, node S gets three RREPs based on Figure 2.8. The two RREPs are correct, which are S➔A➔F➔G➔D and S➔C➔E➔D, but one is incorrect, which is S➔B➔D. The source node S will select the RREP having the highest destination sequence number. If destination sequence numbers are equal, then it will select the RREP with the minimum hop count [40]. In this figure, the source node S selects the path S➔B➔D because it has a destination sequence number and it starts sending data packets to node D through this path assuming the path is correct. However, malicious node B (black hole) randomly generates false RREP. Now malicious node B absorbs all packets forwarded from node S to node D. This is how a black hole attack is set up. The malicious node B gets the data packets and then drops all the incoming data.

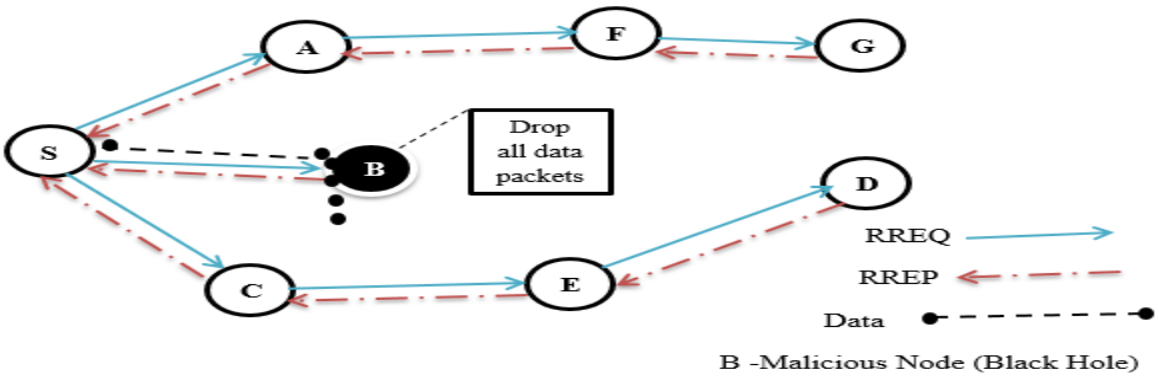


Figure 2. 9 Packets Drop by Black Hole Node [17]

2.5.2.2 Gray Hole Attack

The Gray hole attack is known as variants of the black hole attack [35, 41]. Like a black hole attack, a gray hole attack is also a network layer attack and it is a kind of DoS attack. When it gets the data packets, it drops a portion of the data packets and forwards the rest data packets to its neighbors is called a partial packet drop attack [19, 22]. Because of this explanation, the gray hole attack is viewed as a sort of black hole attack. The difference between the black hole and the gray hole attack is, in the black hole attack the traffic is redirected itself by false information and drops all data packets while in the gray hole attack the node participates as a normal node and then drops the data packets by partial forwarding. The Gray hole attack is classified as a smart gray hole attack and sequence number based gray hole attack.

A. Smart Gray Hole Attack

A smart gray hole attack is the first class of gray hole attack in which the node can participate genuinely in the route discovery process, then, after getting data packets it drops partially of them [19]. During route discovery operation, smart gray hole nodes do not send false routing information as malicious nodes. Due to sending correct destination sequence numbers during the path discovery phase, the attackers are participating as a normal node to establish a path to the destination node. However, when receiving the data packet from the source node, it turns its behavior into malicious nodes. It has a valid route to the destination node but drops some portion of data packets. The activity of smart gray hole attacks [5] in MANET happens through the accompanying stages.

- The smart gray hole node misuse routing protocol and declares itself as having a correct route to the destination node to degenerate the packets.
- The smart gray hole node drops the intruded packets with partial data packet drops.

In Figure 2.10, the route discovery operation is similar to a black hole as discussed before in Section 2.7.1. Node G (smart gray hole) is a malicious node that sends true RREP, but changes behavior in the data transmission phase. Thus, the reply packet from node G reaches node S ahead of reply packets from other neighbors of node S. Therefore, node S sending packets to node D via node G is considering that node G has a fresher route to node D. Now node G absorbs partial packets forwarded from S to D. This is how a smart gray hole attack is set up.

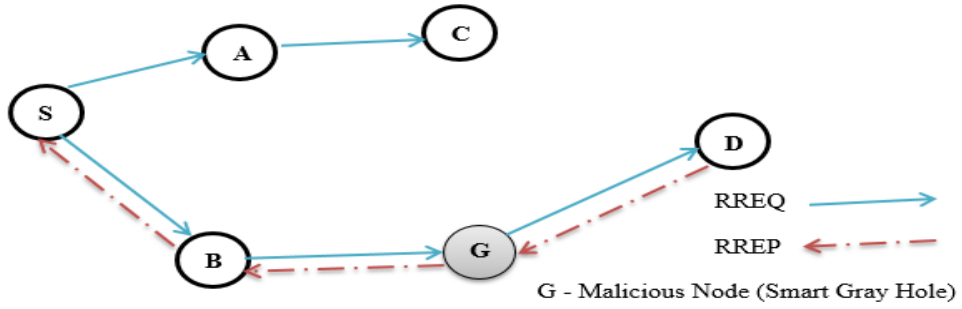


Figure 2. 10 Participation of Smart Gray Hole Node as a Normal Node during Route Discovery Phase [17]

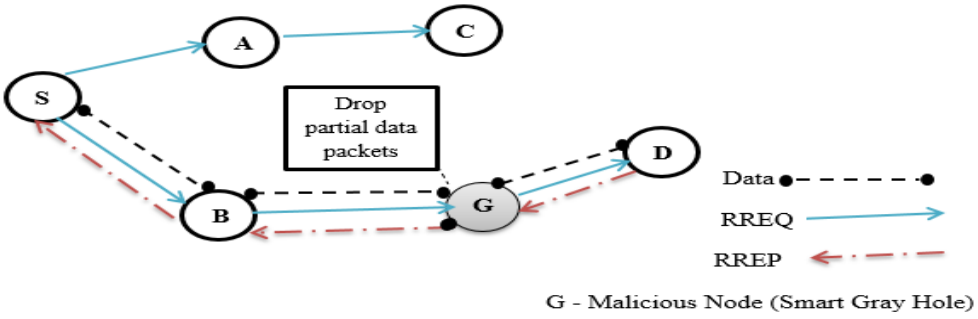


Figure 2. 11 Partial Packet Drop by Smart Gray Hole Node [17]

The malicious node G gets the data packet and then starts dropping partial data packets from the incoming data as shown in Figure 2.11.

B. Sequence Number Based Gray Hole Attack

A sequence number based gray hole attack is the second class of gray hole attack, in which the malicious node gives the false route information by sending a fake destination sequence number to the source node to attract the traffic towards it [22]. The attacker node may or may not have any valid route to the destination node. The malicious node acts as a black hole attack in the route discovery operation [44].

2.6 Related Work

In this section, we discuss the different types of MANET protocols and their works. In recent years, many researchers have proposed different predictive schemes to improve routing security in MANETs, which is reviewed in this section. Here we assess the research work by asking how they use the protocol to solve the problems and what the drawback of the protocol is. Different researchers have proposed different methods for the detection and mitigation of black hole and gray hole attacks in MANETs. Most of the researchers proposed a method in route discovery or actual data transmission separately. Therefore, we focused on the detection mechanism in the three sub-topics, i.e., Route Discovery, Actual Data Transmission and Dual Detection Mechanisms. The literature survey of these topics is presented here.

2.6.1 Detection Mechanisms in Route Discovery Operation

Many authors have proposed different algorithms based on RREQ, RREP and the source and destination sequence number of the RREQ & RREP. Among these, most of the authors used the destination sequence number of RREP for detecting black hole nodes because the source node used the destination sequence number of RREP for determining the route path. The methods are presented here:

The algorithm proposed by the authors in [16] for securing MANET from a black hole attack using the modified sequence number in the AODV routing protocol, which depends on the technique of changing the sequence number presented in control packets. In this algorithm, the authors assumed that the malicious node adds an arbitrary maximum number of 100 to the source sequence number (SSN) and then back the RREP packet to the source node. However, as the behaviors of a black hole in MANET, which is difficult to set arbitrary number because the black hole node generates a random number. Therefore this algorithm fails to detect malicious nodes when the malicious

node destination sequence number and source sequence number difference less than 100 and it cannot detect the malicious node that sends true RREP during route discovery operation and behaves maliciously during data transmission i.e., Smart gray hole attack.

In [17], the authors have proposed a dynamic threshold approach for mitigating black hole attack in MANET, the detection mechanism proceeds in the route discovery operation. In this proposed approach, two statistical features of mean and standard deviation are used for dynamic threshold calculation. The source node receives multiple RREP packets from different nodes. In this method, the destination node reply for the entire received RREQ then, after getting at least three RREPs the method formulates the average and standard deviation value using a destination sequence number of the RREP. According to the article, the standard deviation is taken as a threshold value. The method detects malicious nodes, if the threshold value greater than the average value and the destination sequence number greater than the threshold value, and the hop count is equal to one, then the node is malicious else, the hop count differs from one the node is suspected. When the node receives the RREP packet, it checks the suspected destination sequence number with the incoming destination sequence number. If the value of the destination sequence number in the RREP equals the suspected sequence number, then the packet is dropped else the reply packet accepts. This method fails in some conditions when the dispersion value of D_Seqno in RREP varies, it has high routing overhead, due to the transmission of multiple RREP by the destination node, and the method cannot detect smart gray hole attacks.

Authors in [45] have proposed a threshold-based method for the prevention of black hole attacks using multiple RREPs. In this methodology, each intermediate node updated a threshold value for sequence number progressively, based on the average of sequence numbers of each RREP creating node. At whatever point an intermediate node broadcasts the RREQ messages, it gets multiple RREPs for a similar destination from various nodes. The nodes make the duplicates of each RREP packet; it is related to the RREQ packet. Each intermediate node keeps an average sequence number table. The methodology performs operations in the intermediate node. However, the mobile nodes in MANET have limited battery power. Due to this reason, in this method the overhead and delay are high. And also it cannot detects smart gray hole attacks due to sends true RREP during route discovery operation. The authors have implemented the black hole attacks in

the network's true destination sequence number plus **40**, but the black hole node back RREP by adding random numbers.

Authors in [46] have proposed a secure and trust-based approach based on AODV (STAODV) to improve the security of the AODV routing protocol. In this methodology, a threshold value is set, by using the number of nodes, the destination sequence number of the RREP packet and the routing table sequence number in the network. If the sequence number of any RREP packet greater than the threshold value, the trust value of that node is decremented by one. A trust level is utilized for every node to detect the malicious nodes from the network. The algorithm maintains a trust table for every node so, to detect the malicious node the trust value is updated. The maintenance of an additional trust table by every node can increase the overhead.

In [47], the authors have proposed an intrusion detection system called Accurate and Cognitive Intrusion Detection System (ACIDS) for detecting the black hole attack. In this approach, the method uses the destination sequence number and route reply of a node to detect an attacker node and remove the attacker node in a routing network. The proposed ACIDS method is assessed by subtracting the previous sequence number of the node from the current sequence number and doubles the resultant value stored in a routing table that identifies the attacker node. If a node has the highest sequence value, then the node in the routing environment, which is removed from the routing network and reported as an intruder to different nodes. The drawback of the method is a high end-to-end delay and the high number of control packets leads to high routing overhead.

In [48], the authors have proposed an algorithm based on forged packets to enhance the accuracy of detection and removing a malicious node. According to the proposed algorithm, the malicious nodes are identified by sending forged RREQ and RREP routing packets, which incorporate the location of the unreal destination node. At that point, they are taken out from routing tables of nodes via sending RREP packets. The algorithm used forged RREQ to detect malicious nodes but this leads to a high number of control packets propagation. As the number of mobile nodes increases the high number of RREQ propagate. Due to this reason, the algorithm has a high routing overhead and is not appropriate for the high number of mobile nodes are exist.

2.6.2 Detection Mechanisms in Actual Data Transmission

Many authors formulated and executed several solutions in actual data packet transmission using data packets to detect and mitigate black hole and gray hole attacks, especially, smart gray hole attacks because it acts as a normal node in the route discovery process. The methods are listed here.

Authors in [49] have proposed a reliability factor based algorithm to detect the black hole attack. Initially, the reliability factor value for the entire node in the network is 0.5. Then, the algorithm calculates the reliability factor of the nodes in the path through which packets are forwarded. Therefore, the algorithm identifies the node whether malicious or normal using the calculated reliability factor value. If the value of the reliability factor is near zero, it will indicate that the node is a black hole. If the value of reliability factors greater than 0.5, then the route will establish and the packet will be forwarded. However, the algorithm used fake RREQ to detect malicious nodes but this leads to a high number of control packets propagation. As the number of mobile nodes increases the high number of RREQ propagate. Due to this reason, the algorithm has a high routing overhead and is not appropriate for the high number of mobile nodes are exist.

In [50], the authors have proposed a Path-Hop-based Secure AODV (PHS-AODV to detect and discard the malicious nodes, including black hole and gray hole nodes during the data forwarding phase of the basic AODV protocol. In this algorithm, multiple paths are used for transferring data. Furthermore, the proposed PHS-AODV algorithm is designed so that the destination node reacts to each RREQ or Enquiry packet arriving from the particular node, but not from the same node and sends RREP for the first 10 RREQ or Enquiry packets. Here Enquiry packet is sent by an intermediate node to locate the current destination sequence number of the destination node. In this proposed algorithm, when a node receives RREP with a destination sequence number less than its value, then that RREP is sent to handle malicious RREP, which is then updated at the source node. Along these lines, the source node holds only one RREP from the same next-hop that is, the one, which was received recently. The algorithm has a high routing overhead and complex to implement.

An enhanced Ant-based defense mechanism proposed by the authors in [51] for selective forwarding attack in MANET. In this mechanism, the trust model defines the trustworthiness of the node based on the number of times the packet dropped. The methods used two ant agents,

which are the forward ant agent that performs a trust mechanism and the backward agent that detects the misbehaving node in the path. The drawback of this technique is to detect malicious nodes after dropping data packets and routing overhead increased due to extra control packets.

Authors in [52] have proposed a trust-based approach to detect black hole and gray hole attack. The approach is used for creating a cluster-based network. In each cluster network has ten nodes, a maximum of two nodes are trusted having higher energy. A trusted node in each cluster sends the received packet to the destination or the next trusted node in another cluster. To find out the malicious node in the network, formulate calculations based on sent and received packets as well as route response. This paper takes a threshold value set as is 30. The algorithm used the cluster method, as the behaviors of smart gray hole node participate genuinely in route discovery operation, the gray hole node becomes the cluster head, it drops data packets.

In [53], the authors have proposed a trust value-based algorithm for identifying and defending black hole and gray hole attack. In this methodology, the threshold value initialized as 5.5 and taken as an assumption one trust value equals n packet dropped. The method divided all nodes into three clusters. It formulates the upgraded trust value. If the upgraded trust value is less than the threshold value, then the node is marked as a malicious node. The algorithm has the same problems as the article in [52] when the smart gray hole attack exist and energy consumption due to the monitoring of cluster head activities.

2.6.3 Dual Detection Mechanisms

Some authors proposed algorithms that are detecting the malicious node in both route discovery and data transmission phases.

Authors in [54] have the authors proposed a method that detects and removes both the black hole and gray hole attack in MANET. In this method, the algorithm worked in two phases i.e., route discovery and monitoring phase. The algorithm used to trap RREQ to trap the malicious node in the route discovery phase. After receiving the fake RREQ response the source node record sends back the fake RREP and adds a node to the malicious list. The drawback of the method is routing overhead due to the trap RREQ.

A security algorithm proposed by the authors in [55] to detect the gray hole attack. This algorithm provided a solution in both phases that is a route discovery phase and data transmission phase. In

the route discovery phase, the threshold value is calculated based on the number of RREQ, number of RREP and routing table sequence number. If the destination sequence number in the RREP packet is greater than the threshold value, then the node sent to the RREP is considered a malicious node. The source node ignores that RREP and hence the malicious node is prevented from getting into a route in discovery operation. If the drop ratio is greater than 97%, then the node is malicious. According to the authors, the gray hole node above 97% drops the data packet but as the behaviors of the smart gray hole node, it drops selectively. Therefore, the selection of threshold is not appropriate because the gray hole node forwards some data packets to its neighbors.

Authors in [56] have proposed a novel hybrid approach for detecting both the black and gray hole attacks in Dynamic Source Routing (DSR) protocol for MANET. The source node discovers a route across multiple networks to get the destination node. In this hybrid approach, the initialized monitor nodes received the packet flow information about the neighboring nodes. Then computed information distance metric using which two detection thresholds are determined. Then the computed information distance metric for all the nodes is compared with the first threshold. If the information distance metric of a node is greater than the first detection threshold, then the node is considered as malicious nodes. If the information distance metric of the nodes is below the second threshold, but not less than the first threshold, the nodes are marked as gray hole attackers while if they are greater than the second threshold, the nodes are marked as black hole attackers.

In [57], the authors have proposed a dual attack detection mechanism for the black and gray hole (DDBG) in MANETs. The proposed DDBG algorithm chose the intrusion detection system (IDS) node utilizing the connected dominating set method with two additional features i.e., the energy and its nonexistence in the blacklist. In the IDS, a trusted node with the highest energy will be chosen as the IDS node for broadcasting the status packet. After the determination of the broadcaster node, it sends the status packets occasionally in the IDS set to check that each node is forwarding the data packets properly or to distinguish any malicious nodes that are available. As indicated by the status packet, regardless of whether any node is sending a high sequence number. Nodes that send an average sequence number and drop all data packets are declared as black hole nodes. If any node is given an average sequence number, not considered high, alongside the dropping of selective data packets, it is declared as a gray hole node. The drawback of the proposed

DDBG is the limited battery power of the nodes, as it cannot continually monitor the nodes for a long period.

2.7 Summary of Related Work

Many authors provided various methods to improve security in MANET but there are gaps in the security of the MANET. Most of the methods are secure the network separately in route discovery or actual data transmission operation. Some methods fail to detect malicious nodes in some scenarios and additional overhead in either intermediate node or destination or both. Therefore, it is necessary to detect the malicious node in various scenarios and reduce the routing overhead from the intermediate node and the destination node, because the nodes in MANET have limited battery power. Hence, in this thesis work, we focus on both destination sequence numbers in the route discovery path and data packets in the data transmission phase based on AODV MANETs routing protocol.

Table 2. 1 Summary of Related Work

Authors, publisher & year	Methodology	Objective	Performance metrics	Simulator	Drawback
Sijan Shrestha et al. IEEE (2020) [16]	Sequence number based using the destination sequence number	Detect the black hole attack	PDR & Throughput	NS-2	Selecting an arbitrary maximum number, which is 100 and cannot detect smart gray hole attack
Shashi Gurung et al. Springer (2017) [17]	A dynamic threshold approach using a destination sequence number	Detect and prevent the black hole attack	False Positive Rate, True Positive Rate, PDR, Overhead & Throughput	NS-2	Fails in some conditions when the dispersion value of D_Seqno in RREP vary and cannot detect smart gray hole attack

Taku Noguchi et al. IEEE (2018) [45]	Threshold based using the destination sequence number	Detect the black hole attack	PDR, Throughput & Normalized routing overhead	NS-2	The extra calculations performed by each node can increase overhead and delay and cannot detect smart gray hole attack
Gupta P. et al. Springer (2019) [49]	Trust value based using reliability factor	Detect black hole attack	PDR, Throughput & End to End Delay	NS-2	Detect after the loss of data and high routing overhead due to fake RREQ
S.V. Vasantha et al. Journal of Critical Review (2020) [50]	Path hop based with data forwarding detection mechanism	Detect and discard black hole or gray hole attacks	Throughput, Packet Dropped, PDR & End to End Delay	NS-2	High routing overhead and complex to implement
Neha Sharma et al. IEEE (2016) [54]	Dual detection mechanism using the sequence number and data packets	Detect and remove black hole and gray hole attacks	PDR, Throughput, Packet Dropped & End to End Delay	NS-2	High routing overhead due to trap RREQ
Zardari A. Z et al. Future Internet (2019) [57]	Dual detection mechanism with IDS node using the sequence number and data packets	Detect black hole or gray hole attacks	Detection Rate, PDR, Throughput, Overhead & End to End Delay	NS-2	The limited battery power of the nodes, as it cannot continually monitor the nodes for a long period

Chapter 3 DS-AODV: Proposed Dual Security Based Algorithm

In this chapter, the overall proposed work process and the working mechanism of the proposed DS-AODV algorithm for detecting and mitigating the black hole and gray hole attacks are discussed. Furthermore, proposed algorithm scenarios are also discussed in this chapter.

3.1 Overview of Proposed Work

The major intention of this study is to modify the AODV protocol by employing a security mechanism against black hole and gray hole attacks. In a MANET, the AODV routing protocol has no mechanisms to separate the normal node from the malicious node information. Due to this reason, the source node receives the RREPs from the intermediate and the destination node, regardless of the responding nodes. The data packet sent to the preeminent responding node depends on the highest destination sequence number among the received RREPs. However, the black hole node responds false RREP and the smart gray hole node attempts to show up as a normal node in the route discovery operation, which answers correct RREP messages. However, it changes behaviors to the malicious node after establishing the path. Therefore, in this proposed DS-AODV algorithm thinking about these practices.

The proposed algorithm makes the following assumptions:

- The source and destination nodes are trusted. However, intermediate nodes are not.
- Malicious (black hole and gray hole) nodes are present in the network.

The proposed algorithm is designed with the following features:

- It used two statistical features, i.e., Mean and Standard Deviation for the detection of malicious nodes using the destination sequence numbers.
- The nodes need to be in promiscuous mode for calculating Data Forwarding Value.

3.2 Proposed DS-AODV Algorithm Phases

The methodology used in the proposed algorithm worked upon the detection of the black hole and gray hole attacker node during the route discovery phase as well as the data transmission phase. Hence, the proposed algorithm provides a solution that tends to detect the misbehaving malicious node for both phases. In these proposed algorithm phases, we used the following notations to formulate the calculation. The overall notations are listed in Table 3.1.

Table 3. 1 Summary of Notation

Notations	Meaning
CURRENT_TIME	The current time of the system
D_Seqno	Destination sequence number
DFV	Data Forwarding Value
Get_Time	Waiting time after getting the first RREP
N	Number of RREP packets
prestore_rrep_table	New Routing Table
Received_Packet_Count	Number of packets forwarded by the neighboring node to its neighboring node
RT.Seqno	Routing table sequence number
SD	Standard Deviation
Set_Time	The time setting by adding Get_Time and Wait_RREP_Time
Send_Packet_Count	Number of packets sent by a monitoring node to a neighboring node
Wait_RREP_Time	Waiting time for RREP packet

3.2.1 Route Discovery Phase

The proposed algorithm can be used to find the secured routes and prevent the malicious node from getting a route path in MANET. The reason behind this phase is to detect the black hole nodes in the network before actual data transmission, to avoid data loss. According to the original AODV routing protocol, when the source node gets the RREP packet, it checks the destination sequence number (D_Seqno) in the RREP packet, because the determination of a route largely depends upon the D_Seqno of the received RREP packets. If the D_Seqno is greater than the routing table sequence number, then that packet is accepted; otherwise, it is dismissed. The malicious node takes advantage of this reality and replies with the RREP packet having a false D_Seqno. It adds a random number in the D_Seqno of RREQ packets and sends RREP. In this proposed method, the mechanism in the route discovery phase is considered a random number added in the D_Seqno of RREQ because this consideration helps to detect black hole attacks in the network. Therefore, some modification happened in AODV.

In this phase, we have modified the working of the source node by adding the prestore_recvReply (Packet *P) function. This function contains routing tables, which are prestore_rrep_table and black_list_table. To wait for RREP from different nodes we use a timer i.e., Get_Time and

Set_Time. The source node after receiving the first RREP, the Get_Time value initializes to be the current time of the system and then calculates Set_Time by adding Get_Time and Wait_RREP_Time. Wait_ RREP_Time is the time for which the source node waits for the RREP before regenerating RREQ. By default, the source node waits for RREP for 2.8 seconds. If the source node does not receive RREP within 2.8 seconds, it generates another RREQ message and broadcasts it [58]. It stores the incoming RREPs in the newly created table, which is prestore_rrep_table, until the current time greater than Set_Time.

In this method, the source node first calls the prestore_recvReply () method and stores D_Seqno and ID of the incoming RREP into prestore_rrep_table. The detection mechanisms are performed by the prestore_recvReply() method, after detecting calls to the original AODV method i.e., recvReply(). Generally, the source node after receiving RREP and before selecting the route path for actual data transmission, the following tasks will be taken on it.

Average and Standard Deviation value calculation

- First, the source node receives RREP.
- Second, set a time after receiving the first RREP to store all incoming RREPs.

$$Get\_Time = get(CURRENT\_TIME).$$

$$Set\_Time = Get\_Time + (Wait\_RREP\_Time/2) \ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3.1)$$

- Third, the source node waits for RREPs until the current time greater than the Set_Time. Add the incoming RREP in the prestore_rrep_table; from the elements of RREP, we use destination sequence numbers for calculation.

$$D\_Seqno_1, D\_Seqno_2, \ldots, D\_Seqno_{N-1}, D\_Seqno_N.$$

- Fourth, using those destination sequence numbers calculates the average value. The average value is calculated as follows, which we use from authors [17].

$$Average = \frac{Sum\ of\ D\_Seqno}{Number\ of\ RREP} = \frac{1}{N} \sum_{i=1}^{N} D\_Seqno_i \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.2)$$

- Fifth, using the destination sequence number (D_Seqno_i) and the Average value, calculates a Standard Deviation value. The Standard Deviation value is calculated as follows, we use from authors [17]:

$$Standard\ Deviation(SD) = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(D\_Seqno_i - Average)^2} \ldots\ldots\ldots\ldots\ (3.3)$$

Where N is the number of the RREP, D_Seqno_i is the destination sequence number of RREP.

Detection of Malicious Node

- If $(SD < Average)$, then
  - If $(SD < (D\_Seqno_i - Average))$, then the node has D_Seqno_i is a malicious node.
  - Else, the node is normal. Therefore, the black hole node is detected. The source node performs this comparison for all D_Seqno stored in the prestore_rrep_table.
- Else
  - If($D\_Seqno_i > SD$), then the node has D_Seqno_i is a malicious node.
  - Else, the node is normal. Therefore, the black hole node is detected. The source node performs this comparison for all D_Seqno stored in the prestore_rrep_table.

After detecting malicious nodes, add its id (ID) and destination sequence number (D_Seqno) of the node into a blacklist table and then broadcast alert messages to their neighbors. The source node does not consider that RREP for the route formation and simply ignores that RREP packet. Therefore, the black hole node acting maliciously during the route discovery phase can be avoided from getting into the route path.

Mitigation of Malicious Node

- When the node receives RREP, it checks the nodes with the blacklist table.
  - If the replied node ID is found in a blacklist, then the RREP is dropped.
  - Else, forward RREP until source node.

Figure 3.1 shows that the proposed detection mechanism in the route discovery phase that detects the malicious node that sends false RREP. In this figure, the malicious node B advertised itself as a fresher node and it sends a false D_Seqno to get a route path. However, in this proposed route discovery detection mechanism, the source node S detects the malicious node B that sends false RREP. As shown in Figure 3.1, the source node S received three RREPs with the destination sequence numbers 9, 10, and 70.

$D\_Seqno = \{9, 10, 70\};$

$$Average = \frac{Sum\ of\ D\_Seqno}{Number\ of\ RREP} = \frac{1}{N}\sum_{i=1}^{N} D\_Seqno_i = \frac{9+10+70}{3} = 29.7;$$

$$SD = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(D\_Seqno_i - Average)^2} = \sqrt{\frac{(9-29.7)^2+(10-29.7)^2+(70-29.7)^2}{5}} = 28.5;$$

If $(SD < Average)$ ➔ (28.5 < 29.7) is true, $if\ (SD < (D\_Seqno_i - Average))$ then the node is malicious.

Check for each entry i from 0 to 2 with the condition ($SD < (D\_Seqno_i - Average)$).

- ✓ $i = 0$ ➔ $(28.5 < 9 - 29.7)$ ➔ $28.5 < -20.7$ is false, then the node is normal node.
- ✓ $i = 1$ ➔ $(28.5 < 10 - 29.7)$ ➔ $28.5 < -19.7$ is false, then the node is normal node.
- ✓ $i = 2$ ➔ $(28.5 < 70 - 29.7)$ ➔ $28.5 < 40.3$ is true, then the node is black hole node.

Therefore, the node has $D\_Seqno = 70$ is ignored from the routing table and does not participate in actual data packet transmission. After that select other RREP having higher D_Seqno among others and send data packets to the destination node D.

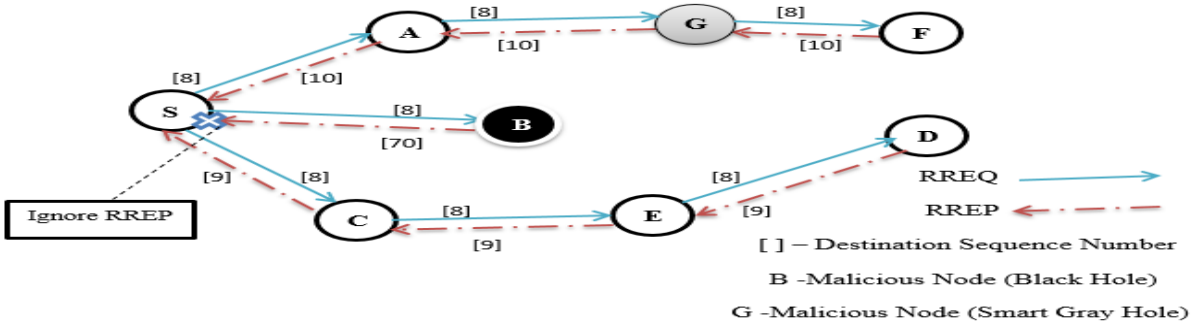


Figure 3. 1 Malicious Node Detection in Route Discovery Phase

Figure 3.2 shows that the source node S selects RREP that is S-A-G-F-D having $D\_Seqno = 10$, then sends data packets to the destination node D through the S-A-G-F-D path. However, the smart gray hole attacker exists in this path i.e., node G, behaves normally in the route discovery phase, but changes behaviors to malicious in the actual data packet transmission phase, the node G drops partial data packets.

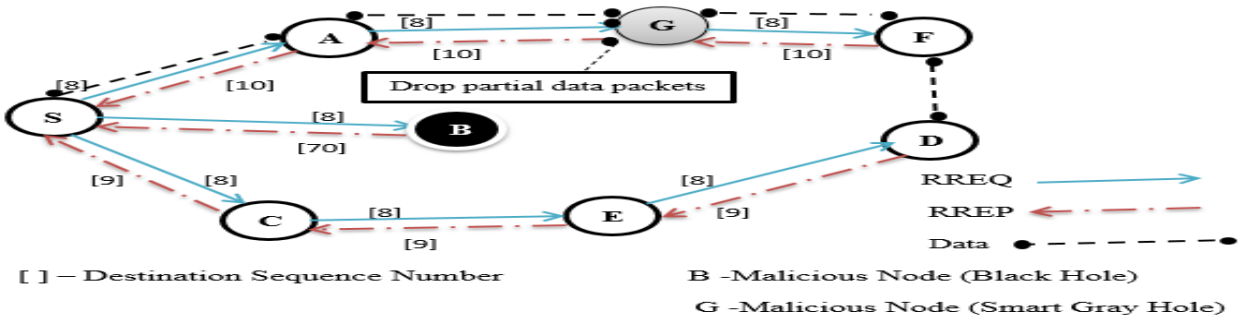


Figure 3. 2 Smart Gray Hole in Actual Data Transmission Phase

To detect this malicious node, the detection mechanism in the actual data transmission phase is proposed.

3.2.2 Actual Data Transmission Phase

The proposed method is that after the route path is established, the actual data packet transmission phase is applied. The smart gray hole attacker node acts normally during the route discovery operation. It does send the correct destination sequence number in the RREP packet. If such an attacker node becomes part of the route, then it may drop the data packets as shown in Figure 3.2. Therefore, in such circumstances, the only route discovery mechanism will not work. Hence, we need to add security mechanisms in data transmission. In our proposed method during the data transmission phase, every node will screen the neighboring node in the route in the promiscuous mode. Every node will keep the number of data packets sent to the neighboring node in the route so that it can prevent smart gray hole nodes. To check a neighboring node forward packet, a caching mechanism is performed at each node to gather the packets being sent to a neighboring node. Based on Figure 3.2, node G is a smart gray hole attacker. Therefore, node A is a monitoring node that checks node G forwards the data packet to node F or not.

Figure 3. 3 Tapping of Packets in Promiscuous Mode [59]

As shown in Figure 3.3, node A caches the packet P before it sends it to node G. Once node G forward the packet P to node F, node A captures the packet in promiscuous mode and verifies it with the one in the cache. Therefore, every node will know its neighboring nodes' behaviors. During the source node selects a route path, the proposed detection mechanism in the route discovery phase detects the malicious node. After that, it sends a data packet to the destination node through the selected path, but in the selected path it may have a malicious node (smart gray hole) is exist. It detects in the data transmission phase. The proposed detection mechanism in the actual data transmission phase performs the following tasks.

Data forwarding value calculation

- First, enter all nodes in the promiscuous mode and monitor their neighbors.
- Second, initialize *Send_Packet_Count=0 and Received_Packet_Count=0,* then incremented.
  - Send_Packet_Count is defined as data packets are sent by a monitoring node to the neighboring node. Each node will maintain the count of the number of data packets sent to the neighboring node in the route. As shown in Figure 3.3, node A maintains how many data packets send to node G by the caching mechanism. When the data packets are sent to the neighboring nodes, the Send_Packet_Count is incremented.
  - Received_Packet_Count is defined as data packets that are forwarded by the neighboring node to its neighboring node in promiscuous mode. According to Figure 3.3, node A received how many data packets forwarded from node G to node F. When the neighboring node forwarded data packets to its neighboring node, the Received_Packet_Count is incremented.
- Third, the monitoring node will compute the data forwarding value of the neighboring node using the Send_Packet_Count and Received_Packet_Count.

$$Data\ Forwarding\ Value\ (DFV) =$$

$$\left(1 - \frac{(Send\_Packet\_Count - Received\_Packet\_Count)}{Send\_Packet\_Count}\right) \ldots\ldots\ldots\ldots\ldots\ldots \quad (3.5)$$

Where *Send_Packet_Count* is the number of data packets sent to the neighboring node and *Received_Packet_Count* is the number of data packets forwarded by the neighboring node to its neighboring node.

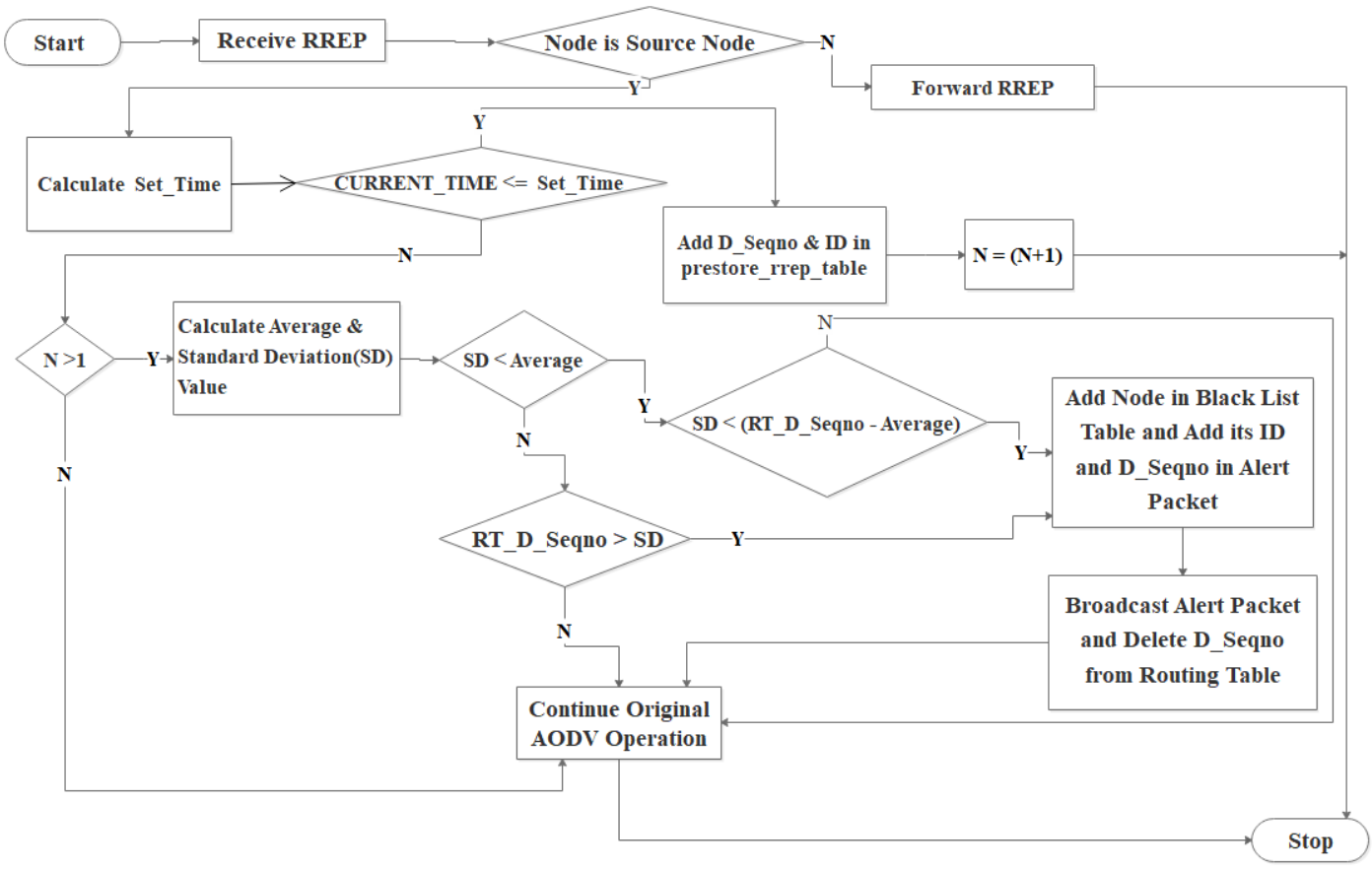
The DFV always between zero (0) and one (1), the maximum value becomes 1 when the neighbor node sends all the data packets to its neighboring node and the minimum value become 0 when the neighboring node does not send all data packets to its neighboring node or drop all the data packets received from the monitoring node.

Detection of Malicious Node

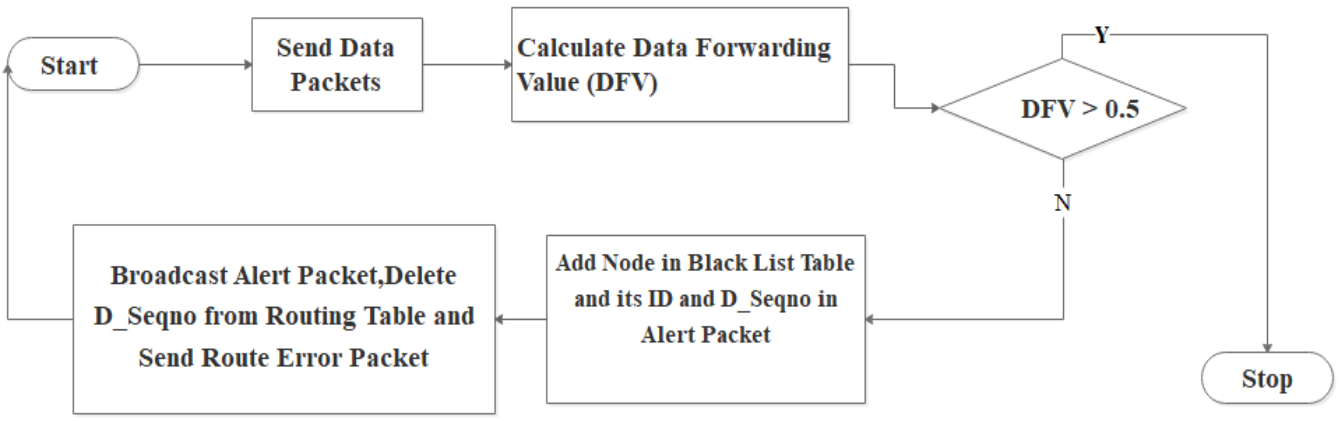
If DFV is greater than a threshold value i.e., 0.5, then the neighboring node can be determined as a normal node else, the node is determined as a malicious node. After the monitoring node detects the malicious node, then it stops transmitting the data to the neighboring node, it adds D_Seqno and ID into the blacklist table, broadcasts an alert packet, and sends a route error packet to the source node then the source node reinitiates the route discovery process.

3.3 Flow Chart and Algorithm of the Proposed DS-AODV Protocol

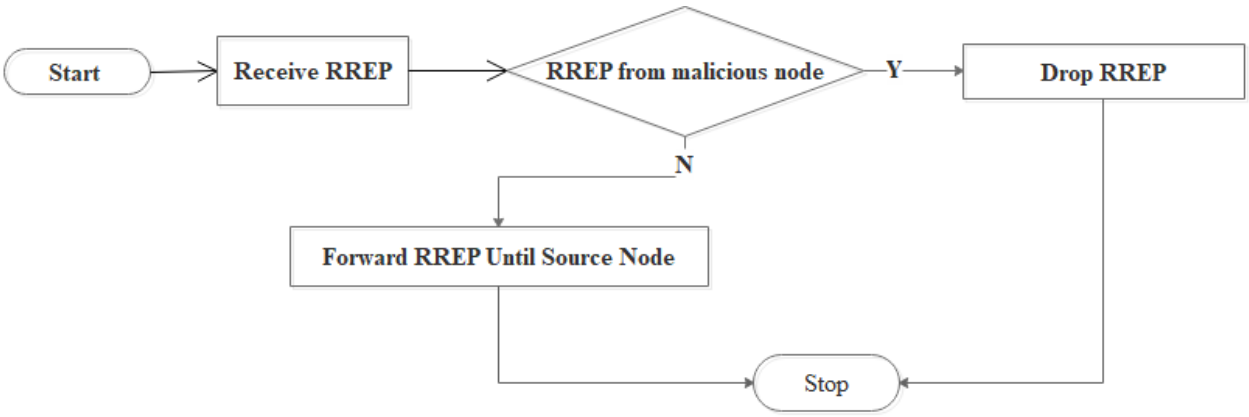
This section shows the flow chart and algorithm of the proposed DS-AODV protocol for the detection and mitigation of black hole and gray hole attacks. Figure 3.4 shows the general progression of the proposed DS-AODV protocol beginning with route discovery from the source node and the sequence that follows the assessment of true route information and burden on the nodes by the source node lastly ignoring the false route information and finding the safe way towards the destination node.



a) Black Hole Attack Detection in Route Discovery Phase



b) Gray Hole Attack Detection in Data Transmission Phase



c) Black Hole and Gray Hole Attack Mitigation in Route Discovery Phase

Figure 3. 4 Proposed DS-AODV Algorithm Flow Chart when Receiving RREP and Sending Data Packets

Proposed DS-AODV Algorithm:

Procedure 1 Action of the node when receiving reply packets

Algorithm 1: Black Hole Attack Detection on source node: prestore_recvReply () method

```
1.  Node receive RREP;
2.      If (Node ==  Source Node) then
3.          Get_Time  = get(current time value);
4.          Set_Time  =  Get_Time  + (Wait_RREP_Time/2);
5.          do
6.            Add D_Seqno and ID in prestore_rrep_table  ;
7.              N += 1;
8.          end do
9.            while ( CURRENT_TIME <= Set_Time);
10.           if (N == 1) then // N is the number of RREP
11.             Continue  Original AODV Operation ;
12.           else //  the number of RREPs greater than or equal to 2 (N >= 2)
13.                 Set Average =  1/N ∑_{i=1}^{N} D_Seqno_i  ;
```

```
14.                    Set SD = sqrt( (1/N) Σ_{i=1}^{N} (D_Seqno_i − Average)^2 );
15.                if (SD < Average ) then
16.                    for each entry in Routing Table do
17.                        if ( SD < (RT_D_Seqno − Average) ) then
18.                            Add the node as a malicious in the blacklist table;
19.                            Add its ID and D_Seqno in Alert packet;
20.                            Broadcast Alert packet;
21.                            Delete D_Seqno from the routing table;
22.                        end if
23.                    done
24.                    Continue Original AODV Operation;
25.                else // for line 15
26.                    for each entry in Routing Table do
27.                        if ( RT_D_Seqno > SD) then
28.                            Add the node as a malicious in the blacklist table;
29.                            Add its ID and D_Seqno in Alert packet;
30.                            Broadcast Alert packet;
31.                            Delete D_Seqno from the routing table;
32.                        end if
33.                    done
34.                    Continue Original AODV Operation;
35.                end if
36.            end if // for line 12
37.        else //for line 2
38.            Forward RREP packet;
39.    end if
```

Procedure 2 Action of the node when sending data packets for calculating data forwarding value.

Algorithm 2: Gray Hole Attack Detection in Actual Data Packet Transmission:

Select the route path having maximum destination sequence number among the nodes, which satisfies the condition $SD > (D\_Seqno_i - Average)$ *or* $D\_Seqno_i < SD$ *using original AODV operation;*

1. *All nodes in the route, enter in the promiscuous mode and monitor their neighbors;*
2. *Source node sends data packets;*
3. *Increments Send_Packet_Count (Send_Packet_Count++);*
4. *The node sending the data packet monitors its neighboring node*
5. ***if** the neighboring node forwarding the data packet **then***
6. *Increments Received_Packet_Count (Received_Packet_Count++)**;***
7. ***end if***
8. *Compute Data Forwarding Value (DFV);*
9. $DFV = 1 - \frac{(Send\_Packet\_Count - Received\_Packet\_Count)}{Send\_Packet\_Count}$**;**
10. ***if** (DFV <= 0.5) **then***
11. *Add the node as a malicious node in the blacklist table;*
12. *Add its* ID *and* D_Seqno *in Alert packet;*
13. *Broadcast Alert packet;*
14. *Delete* D_Seqno *from the routing table;*
15. *Send Route Error // To reinitiate route discovery operation*
16. ***end if***

Procedure 3 Action of the node when receiving RREP

Algorithm 3: Black Hole and Gray Hole Attack Mitigation: prestore_recvReply () method

1. Node receive RREP;

2. ***if*** *(the D_Seqno & ID of RREP exist in blacklist table)* ***then***

3. *Drop RREP;*

4. ***else***

5. *Forward RREP Until Source Node;*

6. end if

Chapter 4 Implementation and Performance Evaluation

In this chapter, the proposed method implementation tools and the performance metrics for analyzing the result of the proposed algorithm are discussed. Also, show the results of the proposed algorithm and the existing one. Furthermore, the implementation of the simulation setup, tools and design are explained.

4.1 Simulation Tools

In this section, we have discussed the generally utilized simulation tools for MANETs to assess the performance of the protocols. The simulator is a software program that models the network behavior, which may difficult to model the network behavior in the real world. Simulation refers to a real-word system, which is imitated via computational re-enactment of its behaviors based on rules in a mathematical format. There are various methods of experimenting with different research works, for example, utilizing an analytical model, emulation and simulation used to measure the behavior and performance of the protocol in a wireless network. The development of real simulation for any predefined situation is generally a costly or even impossible task if factors like portability, testing region. Moreover, most simulations are not repeatable and require a high effort. Subsequently, simulations are expected to these issues [60, 61]. It utilizes simulator tools to test run network design before the organization, to take out or diminish mistakes, harm, or wastage of assets [62]. There is a lot of MANETs simulation tool as of now being used of computer network and protocol development and testing reason, such as NS-2, NS-3, OMNET++, SWAN, OPNET, QUALNET, J-SIM, GLOMOSIM and so on [63]. All these simulators have different characteristics, so it must consider the MANET environment for choosing the appropriate network simulator tools to assess the proposed work is essential.

In [64], the authors have discussed various simulations and they explained different features of simulation tools with their advantages and disadvantages. Based on this article, the authors performed different simulation analyses with different available simulation tools, but they have selected the best tools, which are recently known and used in MANET such as NS-2 and OMNET++.

The author in [65] has presented a broad review of current network simulators presenting their characteristics, advantages and limitations. The author talked about well-known network simulators include NS-2, NS-3, J-SIM, OPNETT, OMNET++, and QUALNET. In this paper, the researcher introduced the advantages and limitations of the simulator tools. For instance, advantages of NS-2: it has an enormous number of accessible models, sensible portability models, powerful and adaptable scripting and simulation setup, huge user community and progressing development, it gives simple traffic and complex scenarios that can be easily tested and popular for its modularity. Limitations of NS-2: it should be recompiled every time if there is a change in the user code and the real system is too intricate to model for example complicated infrastructure. As indicated by the researcher, currently NS-2 is the alternative simulator.

The authors in [66] have presented the network simulation tools that are used to simulate new routing protocols for MANET. The authors discussed popular network simulators include NS-2, GLOMOSIM, J-SIM, OPNETT, OMNET++ and QUALNET both their strengths and weaknesses. According to the researchers, among these, the NS-2 is the best simulator for being too complex in terms of its architecture. It supports deterministic or probabilistic packet loss in queues appended to network nodes as just as it supports deterministic and stochastic modeling of traffic distribution. The simulator can customize follow trace files by permitting users to choose the parameters to trace, in this manner saves CPU resources. It offers comprehensive documentation and a regularly updated manual just as an API for C++ and OTCL classes. Therefore, the authors have selected the NS-2 tool.

The following table is a summary of the different variables as it relates to the performance of simulation tools being considered in this research.

Table 4. 1 Comparison of Network Simulators

S/N	Main stream	Network Simulator				
		NS-2	GloMoSim	OMNET++	OPNET++	JSIM
1.	License	Free, Open Source	Open Source	Open Source, Commercial	Commercial	Open Source
2.	Programming Language	C++, TCL	Parsec C	C++, NED	C	JAVA, TCL
3.	Scope of Application	Network Protocol	Network Protocol	Communication Simulation	Network	Network
4.	Popularity	88.8%	4%	1.04%	2.61%	0.45%
5.	Documentation and user support	Excellent	Poor	Medium	Good	Poor
6.	Simulation Techniques	Discrete-Event	Discrete-Event	Discrete-Event	Discrete-Event	Discrete-Event

Generally, along these lines, considering issues talked about above, rules like the scope of application, the capacity to run huge systems, accessibility of assortments of modules, popularity, and dynamic topology creation, we have chosen NS-2 for actualizing and assessing our study. NS-2 is used for two main reasons. First, the majority of the studies use it to simulate their protocols, which demonstrates its good reputation in the research community. Second, much documentation is available online, which alleviates the difficulty of the learning process and coding.

4.1.1 Network Simulator (NS-2) Overview

Network simulator 2 (NS-2) is a discrete event simulator tool targeting networking research. It uses an object-oriented language that is used to simulate different network protocols and is written in two key languages, C++ and Object-oriented Tool Command Language (OTCL). The C++ and the OTCL linked together using TclCL [65]. The front-end interpreter in NS-2 is OTCL, which links the script type language of TCL to the C++ backbone of NS-2. While the C++ defines the internal mechanism (i.e., a back end) of the simulation objects, the OTCL sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a front end) using TclCL. Together, these two different languages create a script controlled C++ environment.

The yield of NS-2 can be content-based or graphical based. There is an in-assembled apparatus in NS-2 for graphical-based simulation, to be a specific Network Animator (NAM). This device gives a pictorial perspective on the exchange of packets on the nodes and the situation of the nodes. The following is the NS-2 fundamental design.

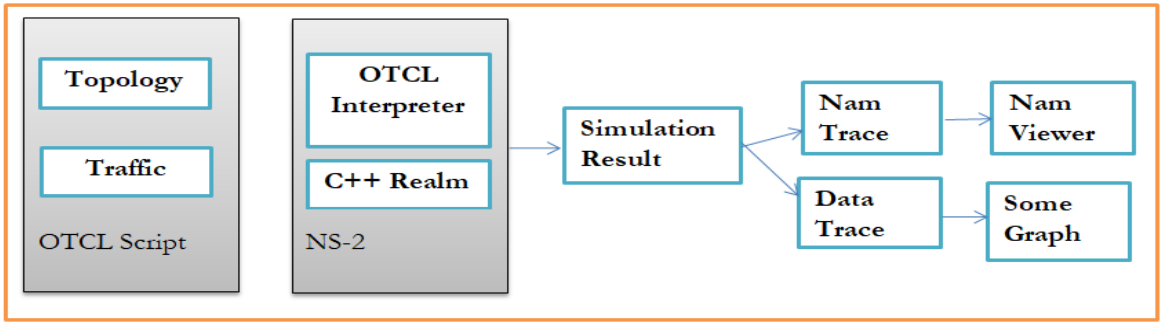


Figure 4. 1 Basic Architecture of NS-2 [62]

4.1.2 NSG2.1

NS-2 Scenarios Generator 2(NSG2) is a Java-based NS-2 scenario generator. Since NSG2 is written in JAVA language, you can run NSG on any platform.NSG2 is capable of generating both wired and wireless TCL scripts for NS-2.

4.2 Performance Evaluation

In this section, we discussed the simulation environment, the implementation of the malicious nodes and the proposed DS-AODV algorithm and the performance metrics.

4.2.1 Simulation Environment

In our simulation environment, we carried out the simulations in the NS-2 (ver. 2.35) simulator in Ubuntu 12.04. We used the existing C++ libraries of NS-2.35 with our modified AODV C++ library. The components utilized for simulating and assessing the performance of our proposed algorithm are Tool Command Language (TCL), Network Animator (NAM), and Trace chart alongside AWK programming. In this simulation, we used UDP in the transport layer and for data packet transmission of the application layer, CBR (Continuous Bit Rate) packets are used; it means the simulation bit rate is constant that supports audio and video communication. The size of the packet is 512 bytes. We use a 1000m x 1000m terrain area for all simulations. The number of nodes involved in the experiments is 30, the number of malicious nodes involved in the

experiments is varied from 1 to 6. In this simulation, random waypoint mobility is used as the mobility model i.e., 5 to 40 m/s because, most of the researchers use random waypoint, and it is commonly used for mobility model by various works in MANET [67]. In the data transmission phase, we have taken 0.5 as a threshold value because in the normal network scenario without malicious nodes the packet forward ratio is between 0.5 and 1 [68], black hole attacks drop all data packets [19], and smart gray hole attacks are dropped partial data packets [19, 57]. AODV, MBDP-AODV, DDBG-AODV and DS-AODV are used as routing protocols. The overall experimental parameters are summarized in Table 4.2.

Table 4. 2 Simulation Parameters

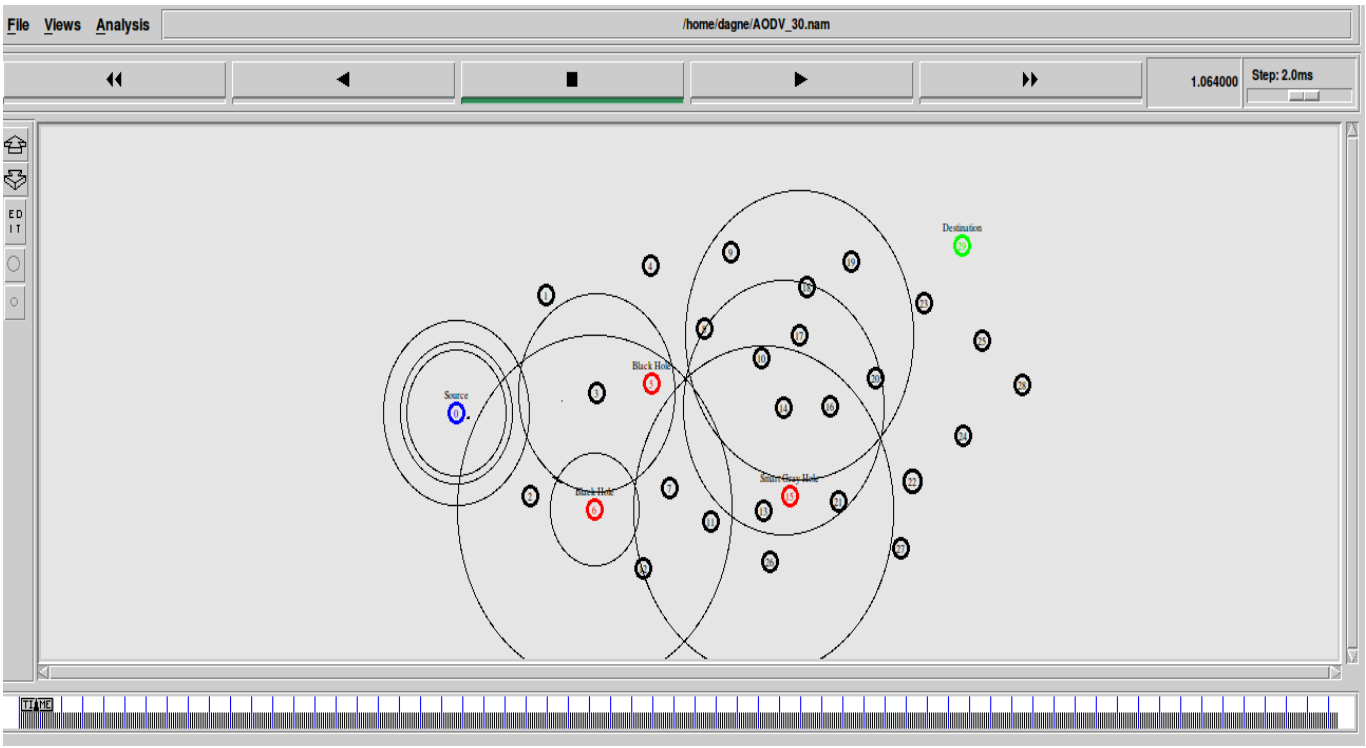
Parameter	Value
Operating System and Simulator	Ubuntu 12.0, NS-2(version 2.35)
X-dimension of Topography	1000 m
Y-dimension of Topography	1000 m
Simulation Time	80 seconds
MAC	802.11
Transport Protocol	UDP
Application Traffic	CBR
Routing Protocols	AODV, MBDP-AODV, DDBG-AODV & DS-AODV
Mobility	5 to 40 m/s
Number of Nodes	30
Number of Malicious Nodes	1 to 6
DoS attack	Black Hole & Smart Gray Hole Attack
Threshold Value in Data Transmission	0.5

In DDBG-AODV, it used the two approaches known as connected dominating set (CDS) and intrusion detection system (IDS). With the use of CDS, the small-sized groups of nodes are developed, which is called IDS sets. In this IDS set, the trusted node that contains more energy is selected for broadcasting the status of the packet. Subsequently, all the trust nodes gave the correct routing information. However, it cannot be used in all situations because most gray hole nodes are the trust nodes.

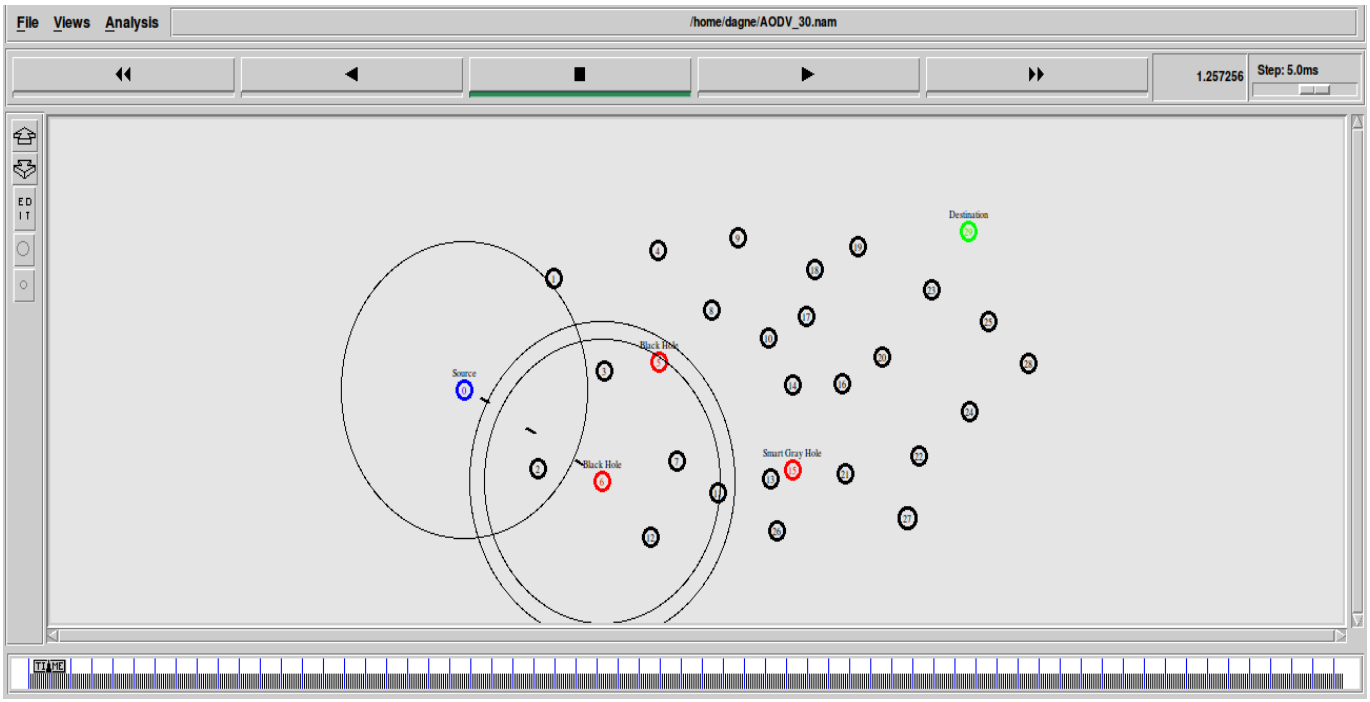
4.2.2 Implementation of Black Hole and Smart Gray Hole Attacks in MANET

We implemented the black hole and smart gray hole attacks behavior in MANET by modifying the existing C++ files of aodv in ns-2.35 and observe the effect of malicious node(s) occurrence within a MANET. Then we can analyze the result gained based on selected performance metrics. This is done by adding a malicious node that causes the black hole and smart gray hole attacks of the network. In our case, black hole and smart gray hole behavior are implemented in the AODV routing protocol by modifying files that are already present in the aodv folder such as aodv.h and aodv.cc. The behavior of black hole attackers is implemented by adding the destination sequence number (D_Seqno) of RREQ and random number using the random function (rand ()) i.e., rq->rq_dst_seqno + random number in route discovery operation. The behavior of smart gray hole attackers is implemented by dropping data packets in data transmission. Next, we implemented the proposed DS-AODV algorithm. The detailed modified codes are listed in the appendix.

Figure 4.2, shows the architecture of the AODV with two black hole nodes and one smart gray hole node introduced with 27 normal nodes, which are implemented in NS 2.35.



(a) Route Discovery Operation



b) Actual Data Transmission

Figure 4. 2 Simulation under Black Hole and Smart Gray Hole Attacks

4.2.3 Implementation of DS-AODV Algorithm

We implemented the proposed DS-AODV algorithm that detects and mitigates the occurrence of a black hole and smart gray hole attacks behavior in MANET. The proposed method has the same files as the original AODV. However, the proposed DS-AODV algorithm has modified the existing aodv C++ files in the ns-2.35 files, i.e., aodv.cc, aodv.h, aodv_rtable.cc, aodv_rtable.h. All files of aodv exist in the ns-allinone-ns-2.35 modules. In the aodv.cc file, add additional prestore_recvReply (Packet *P) function for identifying the malicious node (black hole) and formulate Data Forwarding Value (DFV) for identifying malicious node (smart gray hole). To formulate DFV, we used two data packet variables, which are Send_Packet_Count and Received_Packet_Count. Moreover, in aodv.cc file, we have modified methods such as sendRequest(), recvRequest(), sendReply(),recvReply() and forward() to consider malicious node information during route discovery and selection route path. In the aodv_rtable.h/.cc file, we have been modified to incorporate the additional tables for storing the incoming RREP request and the detected malicious nodes. The detailed modified codes are listed in the appendix.

4.2.4 Performance Metrics

This section explores the appropriate metrics used to evaluate the performance of the proposed algorithm efficiently by varying the dispersion value of the destination sequence number of RREP and varying the number of malicious nodes. Different performance metrics used in the evaluation of routing protocols, which represent different characteristics of the entire network performance [14]. We aimed to declare the effect of the black hole and smart gray hole attacks and the effectiveness of the detection mechanism by analyzing how much performance of a network has been compromised. To analyze the performance of the proposed DS-AODV algorithm, we use the following performance metrics.

Detection Rate: Detection rate is an important metric in examining the accuracy of the status packet to detect malicious nodes. It is the ratio of the number of malicious nodes detected divided by the total number of existing malicious nodes in the network multiplied by 100%. The reason for selecting this metric is to show the ability of DS-AODV to identify the malicious nodes in the network.

False Positive Rate (FPR): It is the total number of normal nodes wrongly detected as a malicious node (black or smart gray hole) divided by the total number of a normal node multiplied by 100%, which is the percentage of the normal node being wrongly detected.

False Negative Rate (FNR): It is defined as the ratio of the number of malicious node ones being detected as normal nodes to the total number of normal nodes in the network multiplied by 100%, which is the percentage of malicious nodes being incorrectly detected.

Packet Delivery Ratio (PDR): It is calculated by the total number of packets received by the destination divided by the total number of packets sent by the source multiplied by 100%. A high value of PDR indicates that most of the packets are being delivered to the higher layers and are a positive sign of performance.

Normalized Routing Overhead: It is calculated by the total number of control packets divided by the total number of data packets received at the destination.

4.3 Simulation Result and Discussion

To evaluate the proposed algorithm, a sequence of tests has been executed over the NS-2 simulator using the different simulation scenarios. As mentioned in the previous Section 4.2.4, the performance metrics are detection rate, false positive rate, false negative rate, PDR and normalized routing overhead used in our simulation analysis. We have used thirty (30) nodes in the simulation cases and all the metric values were calculated for the proposed DS-AODV and the other algorithms. Result analysis is further discussed for each of the performance metrics separately. All simulation results are taken from five different simulation runs as an average.

The performance metrics are evaluated for three types of simulation scenarios such as follows:

- Scenario 1: Varying D_Seqno dispersion value of RREP with source node sends small D_Seqno of RREQ.
- Scenario 2: Varying D_Seqno dispersion value of RREP with source node sends high D_Seqno of RREQ.
- Scenario 3: Varying the number of malicious nodes with a fixed number of normal nodes.

Scenario 1: Varying D_Seqno Dispersion Value of RREP with Source Node Sends Small D_Seqno of RREQ

This scenario aims to show the detection rate of the protocols regarding the dispersion value of D_Seqno in RREP. In this scenario, we have evaluated the detection rate of DS-AODV and MBDP-AODV protocols under 1 black hole nodes with varying the D_Seqno of RREP with the source node sends small D_Seqno of RREQ, which is 19, this value is assigned statically for D_Seqno of RREQ i.e., In sendRequest () method. The simulation was performed by varying the black hole node dispersion value of D_Seqno in RREP i.e., from 10 to 130. This dispersion value of D_Seqno in RREP is implemented for 1 black hole node with a fixed value i.e., In the sendReply() method (rq->rq_dst_seqno + dispersion value of D_Seqno in RREP i.e., 10, 50, 90, 130). All the other parameters were kept fixed listed in Table 4.2.

Table 4. 3 Detection Rate of DS-AODV with Source Node Sends Small D_Seqno of RREQ

Dispersion value of D_Seqno in RREP	Detection Rate (%)	
	MBDP-AODV	DS-AODV
10	0	100
50	0	100
90	0	100
130	100	100

As shown in Table 4. 3, the detection rate is either 100 % or 0% because the number of black hole node is one. If it detects the node, the detection rate is 100 % else 0%. Throughout all the dispersion values of D_Seqno, the proposed DS-AODV algorithm has been found that the same detection rate. It indicated that our DS-AODV algorithm worked for any dispersion value of RREP (the dispersion value of RREP may be high or small). In the case of MBDP-AODV cannot detect the black hole node until the dispersion value of D_Seqno up to 130. It indicated that until the dispersion value of D_Seqno up to 130 the algorithm assumed that there is no malicious node in the network. The reason for this result, the standard deviation value is less than the average value when the dispersion value is small. Besides, when the number of black hole nodes increases the average value increase because the central tendency becomes for the black hole D_Seqno due to the black hole nodes sends higher D_Seqno than normal nodes.

Scenario 2: Varying D_Seqno dispersion value of RREP with the source node sends high D_Seqno of RREQ

The aims of this scenario also similar to scenario 1. The only difference is the source node sends high D_Seqno of RREQ to the destination node i.e., 300. The protocols are DS-AODV and MBDP-AODV under 1 black hole node**.** As we have seen in scenario 1, the MBDP-AODV algorithm detects a black hole node when the dispersion value of D_Seqno in RREP becomes 130. However, when the source node assigns high D_Seqno in RREQ, even the dispersion value is high, the detection rate is low. The simulation was performed by varying the black hole node dispersion value of D_Seqno in RREP i.e., varying from 150 to 1950. All the other parameters were kept fixed listed in Table 4.2.

Table 4. 4 Detection Rate of DS-AODV with Source Node Sends High D_Seqno of RREQ

Dispersion value of D_Seqno in RREP	Detection Rate (%)	
	MBDP-AODV	DS-AODV
150	0	100
750	0	100
1350	0	100
1950	100	100

As shown in Table 4. 4, the detection rate is the same as scenario 1 either 100 % or 0%. In this scenario, the dispersion values of D_Seqno are high. However, the MBDP-AODV algorithm cannot detect the black hole node until the dispersion value of D_Seqno up to 1950. It indicated that the MBDP-AODV algorithm fails to detect the black hole node when the source node sends a high D_Seqno of RREQ i.e., 300. In the case of our proposed DS-AODV algorithm, it can detect the black hole node throughout all dispersion values of D_Seqno.

Scenario 3: Varying number of malicious nodes with a fixed number of normal nodes

This scenario aims to show the performance of routing protocols regarding the number of malicious nodes. In this scenario, we have evaluated the routing protocols, which are AODV, DS-AODV, MBDP-AODV and DDBG-AODV under the black hole and smart gray hole attacks. The simulation was performed by varying the number of malicious nodes (black hole and smart gray hole) from 1 to 6 nodes in the network and keeping the number of normal nodes fixed. All the other parameters were kept fixed listed in Table 4.2.

I. Detection Rate (%) of Malicious Nodes

In Figures 4.3 and 4.4, the x-axis shows the number of malicious nodes, the y-axis shows the detection rate (the finding accuracy) of DS-AODV compared to MBDP-AODV and DDBG-AODV against the black hole and smart gray hole attacks. However, the MBDP-AODV is not able to detect a smart gray hole node in the network due to the normal participation in the route discovery process and does not send any false routing information in the RREP. Therefore, the MBDP-AODV algorithm does not include smart gray hole attacks analysis.

Figure 4.3 shows that the detection rate of DS-AODV, MBDP-AODV, and DDBG-AODV under black hole attack. It has been found that the detection rate of DS-AODV is higher than MBDP-AODV and DDBG-AODV. Because it examined and judged malicious nodes by the standard deviation and average value. If the standard deviation is less than the average value then, compare the standard deviation and the difference of destination sequence number and average value. In the case of MBDP-AODV, it also examined and judged black hole nodes by the standard deviation and average value. However, if the standard deviation value less than average, the algorithm cannot detect it. In the case of DDBG-AODV, it examined and judged black hole nodes by the average value. Table 4.5, 4.6, and 4.7 describes the analysis of the proposed DS-AODV, MBDP-AODV, and DDBG-AODV algorithms detection rate that was examined in the occurrence of 1 to 6 black hole nodes respectively.

Table 4. 5 Analysis of DS-AODV Detection Rate under Black Hole Nodes

Existing Black Hole Node in the Network	Detected Black Hole Node in the Network
1	1
2	2
3	3
4	3
5	4
6	4

Table 4. 6 Analysis of MBDP-AODV Detection Rate under Black Hole Nodes

Existing Black Hole Node in the Network	Detected Black Hole Node in the Network
1	1
2	1
3	2
4	2
5	2
6	3

Table 4. 7 Analysis of DDBG-AODV Detection Rate under Black Hole Nodes

Existing Black Hole Node in the Network	Detected Black Hole Node in the Network
1	1
2	2
3	2
4	3
5	3
6	3

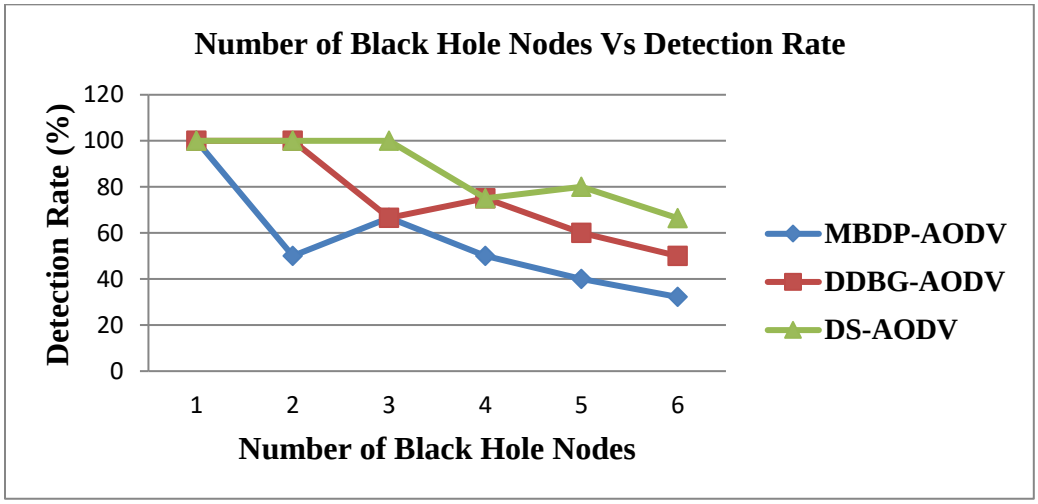


Figure 4. 3 Detection Rate under Black Hole Attacks

Figure 4.4 shows that the detection rate of DS-AODV and DDBG-AODV under smart gray hole nodes. The smart gray hole nodes reply correct RREP as a normal node. Therefore, our proposed algorithm detects smart gray hole nodes when data drop in data transmission. If the data forwarding value of the node less than or equals to the threshold value, i.e., 0.5, at that time DS-AODV algorithm can judge the node as the malicious node. Table 4.8 and 4.9 describes the analysis of the proposed DS-AODV and DDBG-AODV algorithm detection rate that was examined in the occurrence of 1 to 6 smart gray hole nodes.

Table 4. 8 Analysis of DS-AODV Detection Rate under Smart Gray Hole Nodes

Existing Smart Gray Hole Node in the Network	Detected Smart Gray Hole Node in the Network
1	1
2	2
3	2
4	3
5	4
6	4

Table 4. 9 Analysis of DDBG-AODV Detection Rate under Smart Gray Hole Nodes

Existing Smart Gray Hole Node in the Network	Detected Smart Gray Hole Node in the Network
1	1
2	2
3	2
4	2
5	3
6	3

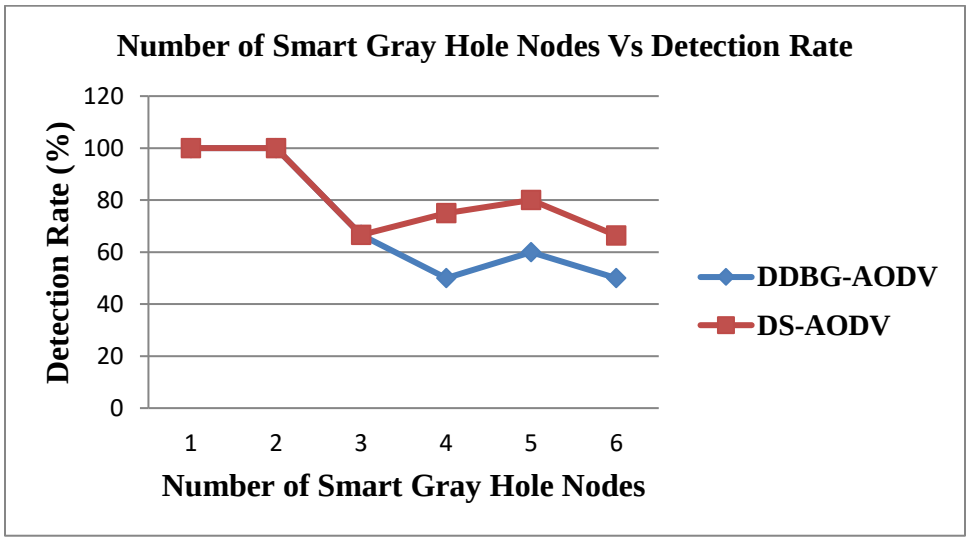


Figure 4. 4 Detection Rate under Smart Gray Hole Attacks

II. False Positive Rate (FPR)

Figure 4.5 shows that the FPR of DS-AODV, MBDP-AODV, and DDBG-AODV under black hole nodes. In the case of MBDP-AODV, the FPR is almost zero because it used the standard deviation value to judge the node is malicious or not. When the number of black hole nodes is small the average value (central tendency) to the normal node D_Seqno because the normal node D_Seqno is smaller than the black hole D_Seqno. In the case of DDBG-AODV, it used the average value to judge the node is malicious or not. As we can see in Figure 4.5 when the number of black hole nodes is one, the FPR of DDBG-AODV is 3.3 %. When the number of black hole nodes is two, the FPR of DDBG-AODV is 6.7 %. The reason behind this the variation of black hole node D_Seqno is nearest to the normal node D_Seqno i.e., the normal node D_Seqno may larger than the average value. In the case of our DS-AODV algorithm, the FPR is almost zero, due to the algorithm considered any dispersion value of D_Seqno with standard deviation and average value. In most case, the normal node D_Seqno less than the stranded deviation value.

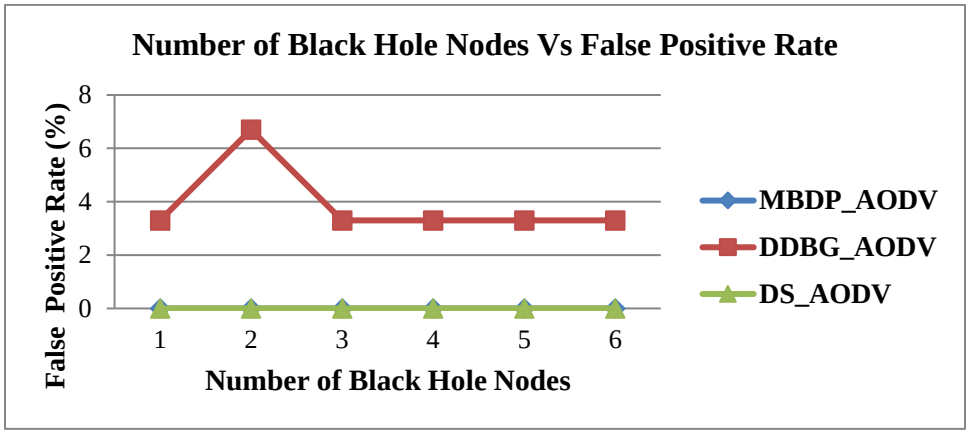


Figure 4. 5 False Positive Rate under Black Hole Attacks

Figure 4.6 shows that the FPR of DS-AODV and DDBG-AODV under smart gray hole nodes. In this metric, the normal node is considered as a malicious node when the dropped data packets greater than 0.5. Therefore, the data packets may be dropped by other cases like congestion, queue, and energy. As shown in Figure 4.6 the value of the FPR is zero, this indicates that the smart gray hole node drop greater than or equals 0.5 data packets and there is no other condition of the data packets drops. The properties of smart gray hole attacks drop data packets selectively. Therefore, the dropped data packets may less than 0.5, the algorithm jugged the node as normal. In this simulation, the DDBG-AODV and DS-AODV have the same FPR because both algorithms use

data packets to judge the node is normal or malicious. The reason behind the results, the normal node forward data packets are greater than 0.5.

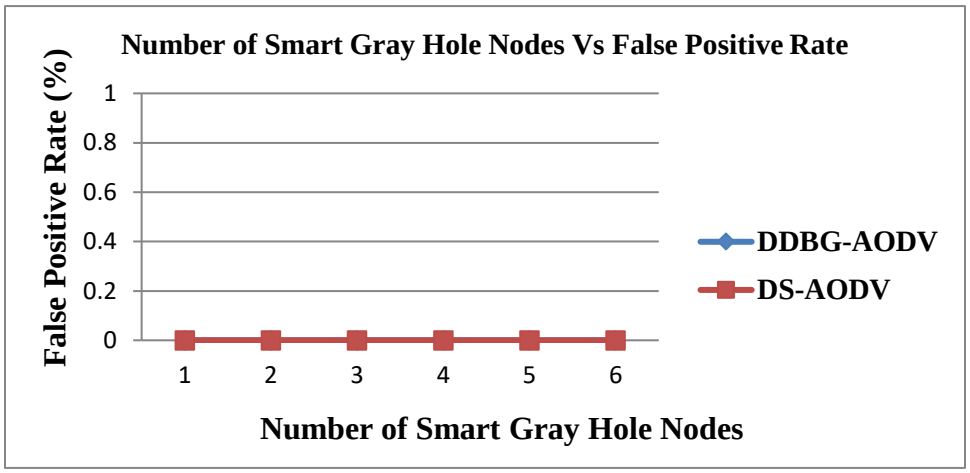


Figure 4. 6 False Positive Rate under Smart Gray Hole Attacks

III. False Negative Rate (FNR)

This metric is calculated as the number of malicious nodes minus the detected node divided by the total number of a normal node multiplied by 100%.

Figure 4.7 shows the FNR of DS-AODV, MBDP-AODV, and DDBG-AODV under black hole nodes. The FNR of our DS-AODV algorithm is small because it considers any dispersion value of D_Seqno in RREP. However, in the case of MBDP-AODV, the FNR is high because if the dispersion value of D_Seqno in RREP is small, then the standard deviation value less than the average value. Therefore, it cannot detect the black hole nodes. In the case of the DDBG-AODV algorithm, it is used average value. Therefore, if the malicious node D_Seqno is less than the average value, then the node is considered a normal node.

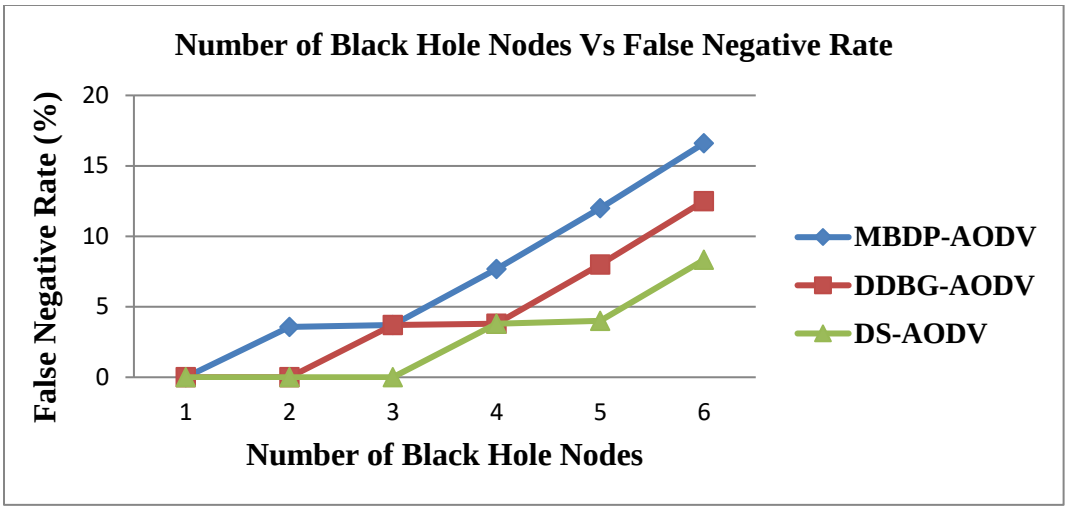


Figure 4. 7 False Negative Rate under Black Hole Attacks

Figure 4.8 shows that the FNR of DS-AODV and DDBG-AODV under smart gray hole nodes. In some conditions, the dropped data packets may be less than the threshold value i.e., 0.5, at that time the detection algorithms can judge the node as the normal node.

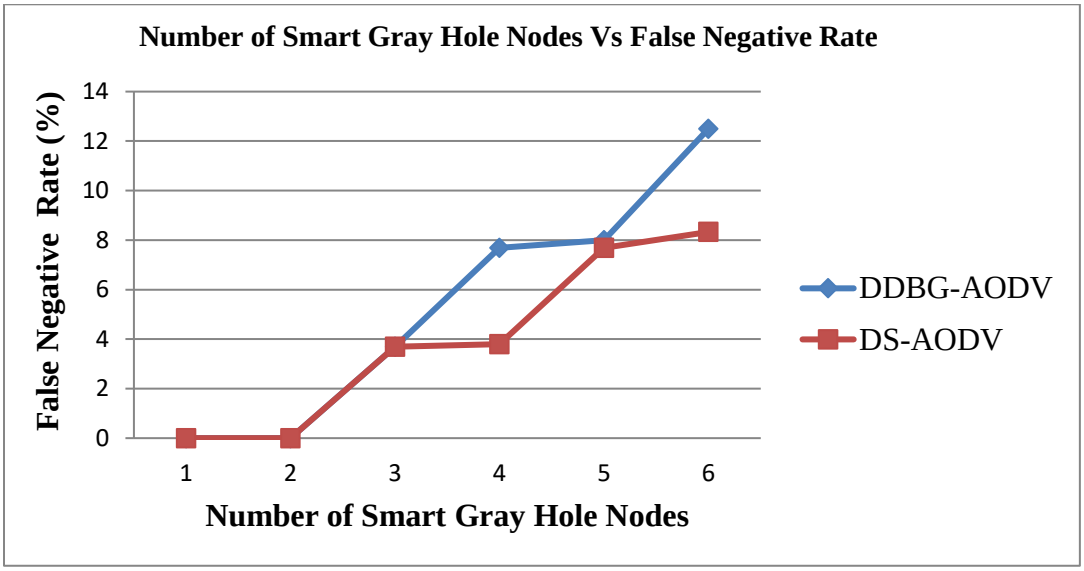


Figure 4. 8 False Negative Rate under Smart Gray Hole Attacks

IV. Packet Delivery Ratio

Figure 4.9 shows the packet delivery performance for AODV, DS-AODV, MBDP-AODV, and DDBG-AODV against the number of black hole nodes. The PDR of AODV quickly decreases to almost zero with an increase in the number of black hole nodes. The reason behind the poor results is the coverage of the network with black hole nodes, which will indeed cut any communication between the source and destination nodes. As the percentage of malicious nodes increases, the packet delivery ratio decreases. Because they will cover most of the network and will disturb the communication by sending fake replies and not delivering data packets to the destination properly. The proposed method achieves a higher packet delivery ratio than MBDP-AODV, DDBG-AODV, and AODV.

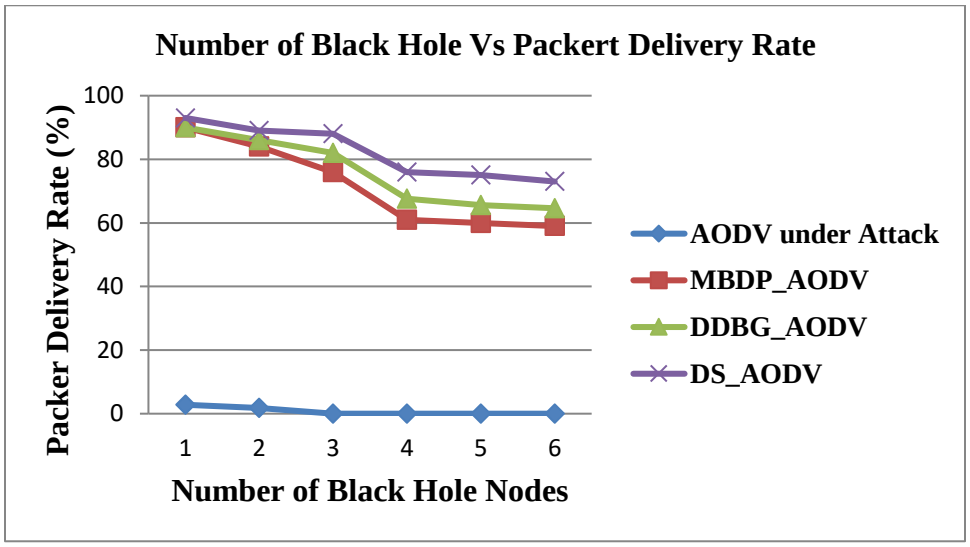


Figure 4. 9 Packet Delivery Ratio under Black Hole Attacks

Figure 4.10 shows the packet delivery performance for AODV, DS-AODV, and DDBG-AODV against the number of smart gray hole nodes. The PDR of AODV decreases to almost half and below with an increase in the number of smart gray hole nodes. This is due to true routing information in the reply packet by smart gray hole nodes. The DS-AODV and DDBG-AODV has high PDR compared to native AODV

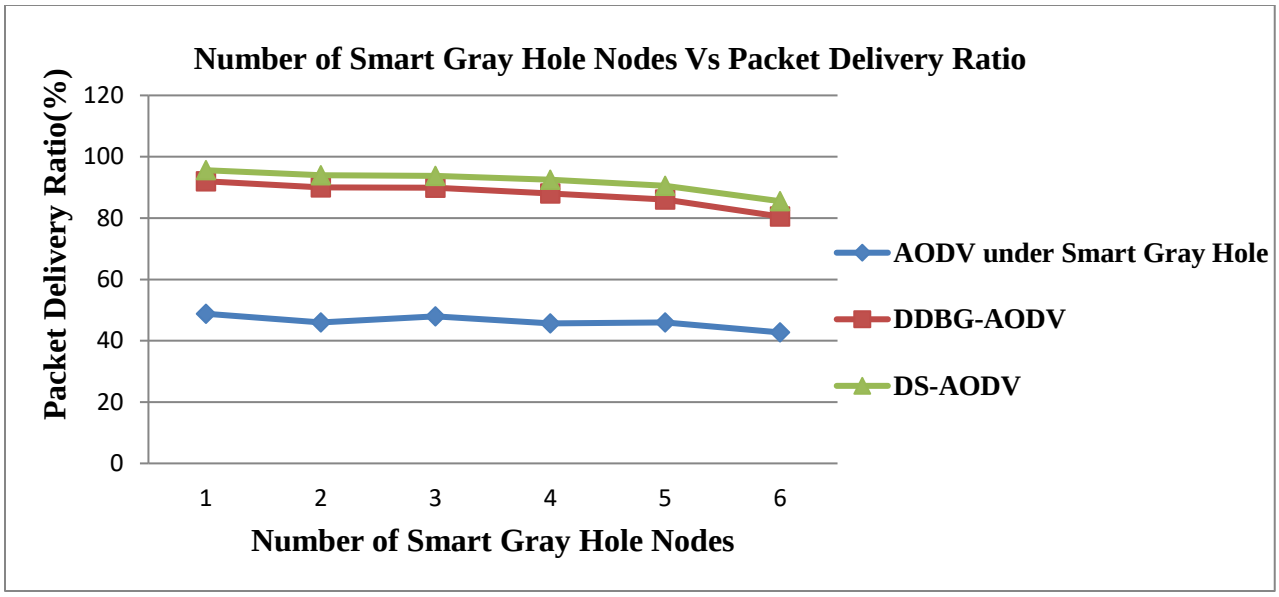


Figure 4. 10 Packet Delivery Ratio under Smart Gray Hole Attacks

V. Normalized Routing Overhead

It is calculated as the total number of control packets divided by the total number of data packets that reached the destination.

Figure 4.11 shows the normalized routing overhead of AODV, DS-AODV, MBDP-AODV, and DDBG-AODV against the number of black hole nodes. As the number of black hole nodes increases, the normalized routing overhead decreases. Due to the black hole nodes do not participate in the operation of route discovery and do not broadcast the RREQ packet in the network, so the neighboring nodes do not get the RREQ packet, which leads to generating lesser control packets in the network. The normalized routing overhead of AODV slightly decreases with an increase in the number of black hole nodes. Because the data packets dropped by black hole nodes, data packets cannot be reached to the destination node. In the MBDP-AODV algorithm, the number of RREP packets sent by the destination node is larger than AODV, DDBG-AODV, and DS-AODV due to multiple RREPs from the destination node. However, the packet delivery rate of the MBDP-AODV algorithm is much higher than AODV. Therefore, the MBDP-AODV algorithm achieves a less normalized routing overhead than AODV. In the DDBG-AODV algorithm, it sends the status packet to check the node is malicious or not. It achieves a less normalized routing overhead than AODV and MBDP-AODV. Whereas the DS-AODV algorithm

achieves a less normalized routing overhead than AODV, MBDP-AODV and DDBG-AODV. Because it does not use additional packets and the PDR is higher than others.

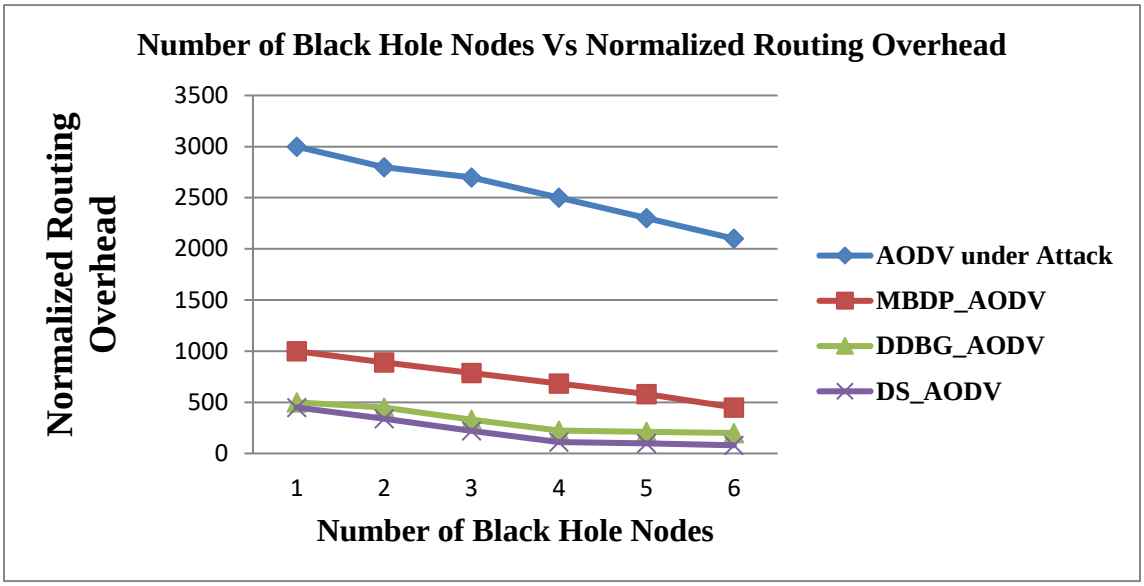


Figure 4. 11 Normalized Routing Overhead under Black Hole Attacks

Figure 4.12 shows the normalized routing overhead for AODV, DS-AODV and DDBG-AODV against the number of smart gray hole nodes. As the percentage of smart gray hole nodes increases, the normalized routing overhead increases due to the number of data packets dropped by smart gray hole nodes. Smart gray hole node participates in the route discovery operation and gives correct route information. Therefore the control packet flows are the same as the normal AODV (AODV without smart gray hole nodes). However, the data packets are partially dropped by it. As we can see in Figure 4.12, the normalized routing overhead of the AODV is higher than other algorithms due to the data packet dropped by the smart gray hole nodes. In the case of DS-AODV and DDBG-AODV, the normalized routing overhead is lesser than the AODV due to detected the smart gray hole nodes and data packets reached the destination node.

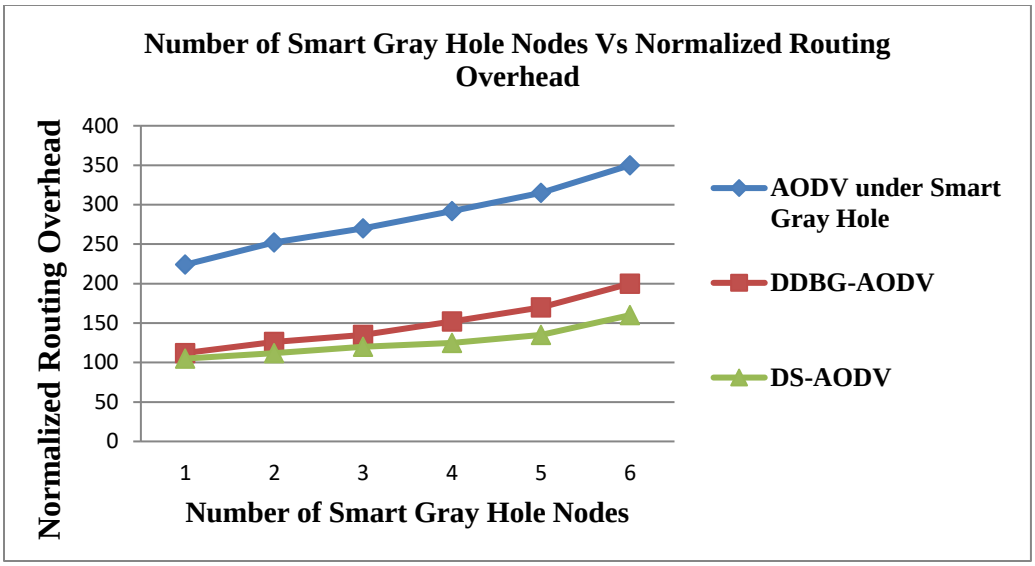


Figure 4. 12 Normalized Routing Overhead under Smart Gray Hole Attacks

Chapter 5 Conclusion and Future Work

5.1 Conclusion

In MANETs, the mobile nodes behave like routers. This includes is what leads to security challenges within the routing protocols. The black hole and gray hole attacks are one of the well-known security dangers in MANETs. The performance of MANET has been degraded by the black hole and gray hole attacks, which becomes a great issue for the research. To defend against a black hole and gray hole attack in AODV, we have proposed dual security based black hole and gray hole attack detection and mitigation algorithm, which uses the destination sequence number of RREPs and data packets. The proposed method calculates the standard deviation and the average value in the route discovery operation using the destination sequence numbers and the data forwarding value in data packet transmission. If the attacker nodes send a false RREP, the proposed algorithm detects it. Also, if the attacker nodes dropping data packets by sending true RREP, the proposed algorithm detects it. Therefore, our proposed algorithm is a dual detection algorithm. Therefore, it operates in route discovery and data transmission phases. The detection mechanism in the route discovery phase doesn't need the involvement of intermediate nodes in the detection operation. The proposed algorithm overcomes the drawbacks in the existing algorithms and this can be proved by the experimental results using the NS-2 simulation tool. The performance has been analyzed based on different scenarios, which are varying the dispersion value of D_Seqno in RREP and varying the number of malicious nodes. In all scenarios, the detection rate of our proposed algorithm is higher than the existing algorithms. From the results, it can be concluded that the proposed algorithm detects the malicious nodes more efficiently with a low packet drop rate, higher packet delivery ratio, and small normalized routing overhead than the existing detection algorithms.

5.2 Future Work

The proposed DS-AODV algorithm is done based on forwarded and dropped data packets in actual data transmission for detecting smart gray hole attacks. However, it does not consider other data packet drop reasons, i.e., congestion, queue and energy in future enhancement will be considered.

References

[1] Boulaiche M., "Survey of Secure Routing Protocols for Wireless Networks," *Wireless Personal Communication,* April 2020. http://doi.org/10.1007/s11277-020-07376-1.

[2] Zeba S. & Ahmad S., " Detection and Verification of Malicious Node in Black Hole Attack using DSA*," International Journal of Advanced Research in Computer Science*, vol. 9, April 2018.

[3] Sampoornam K P & Raaga Darshini G, "Performance Analysis of Bellman Ford, AODV, DSR, ZRP and DYMO Routing Protocol in MANET using EXATA," IEEE, 2019.

[4] Ruo Jun Cai, Xue Jun Li, & Peter Han Joo Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," IEEE, 2018.

[5] Gurung S. & Chauhan S., "A novel approach for mitigating gray hole attack in MANET," *Wireless Network*, Springer US, 2018.

[6] Singh M. M. & Mandal K. J., "Gray Hole Attack Analysis in AODV Based Mobile Adhoc Network with Reliability Metric," *4th International Conference on Computer and Communication Systems*, IEEE, 2019.

[7] Merlin R. T. & Ravi R., "Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET," *Wireless Personal Communication,* February. 2019. https://doi.org/10.1007/s11277-019-06120-8.

[8] Rahma MEDDEB, Bayrem TRIKI, Farah JEMILI & Ouajdi KORBAA, "A survey of Attacks in Mobile Ad hoc Networks," IEEE, 2017.

[9] Rutvij H. Jhaveri, Sankita J. Patel & Devesh C. Jinwala, "DoS Attacks in Mobile Ad-hoc Networks: A Survey," *Second International Conference on Advanced Computing & Communication Technologies*, IEEE, 2012.

[10] Kulwinder S., and Sharma S., "A new technique for AODV based secure routing with detection black hole in MANET," *International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI*), pp. 1528-1534. IEEE, 2017.

[11] Gurung S. & Chauhan S., "A Review of Black-Hole Attack Mitigation Techniques and its Drawbacks in Mobile Ad-hoc Network," *WiSPNET conference*, pp. 2379 – 2385, IEEE, 2017.

[12] Sandeep Kumar, Monika Goyal, Deepak Goyal & Ramesh C. Poonia, "Routing Protocols and Security Issues in MANET," *International Conference on Infocom Technologies and Unmanned Systems (ICTUS)*, IEEE, Dec.2017.

[13] Khan, Danista, and Mahzaib Jamil, "Study of detecting and overcoming black hole attacks in MANET: A review," *Wireless Systems and Networks (ISWSN*), pp. 1-4, IEEE, 2017.

[14] Muhammad Salman Pathan , Jingsha He, Nafei Zhu, Zulfiqar Ali Zardari, Muhammad Qasim Memon & Aneeka Azmat, "An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs", (*IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, 2019.

[15] Jamal T. & Butt A. S., "Malicious node analysis in MANETS," Springer, April. 2018.

[16] Sijan Shrestha , Ranjai Baidya, Bivek Giri & Anup Thapa, "Securing Black hole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol," *8th International Electrical Engineering Congress*, IEEE,2020.

[17] Gurung S. & Chauhan, S., "A dynamic threshold based approach for mitigating black-hole attack in MANET," Springer, April. 2017.

[18] Aneri Mukeshbhai Desai & Rutvij H. Jhaveri, "Secure routing in mobile Ad hoc networks: a predictive approach," *Int. j. inf. Tecnol*, Springer, April.2018. https://doi.org/10.1007/s41870-018-0188-y.

[19] Gurung S. & Chauhan S., "Performance analysis of black-hole attack mitigation protocols under gray-hole attacks in MANET," Springer Science &Business Media, December. 2017.

[20] Deepak S. & Anandakumar H., "AODV Route Discovery and Route Maintenance in MANETs," *5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, IEEE, 2019.

[21] Aparna Junnarkar & A.B. Bagwan, "Efficient Algorithm and Study of QoS-Aware Mobile Ad Hoc Network Methods," International Conference on Trends in Electronics and Informatics (ICEI) IEEE, 2017.

[22] K. U. Adhvaryu & Pariza Kamboj, "Performance Comparison between Multicast Routing Protocols in MANET," IEEE, 2017.

[23] Lee.D.C. & Lee.D.H., "Novel routing protocol scheme for real-time applications in mobile Ad Hoc networks," *Cluster Comput*, Springer, September 2017. https://doi.org/10.1007/s10586-017-1139-2.

[24] Abdel-Fattah F., AlTamimi F., Farhan A. K & Al-Tarawneh H. F., "Security Challenges and Attacks in Dynamic Mobile Ad-hoc Networks MANETs," *Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT*), IEEE, 2019.

[25] Bekti Maryuni Susanto, Agus Hariyanto, & Surateno, "Performance Comparison of Proactive and Reactive Routing Protocol in Mobile Ad Hoc Network," *Journal of Communications* vol. 13, no. 5, May 2018.

[26] Ranjan R., Singh K. N. & Singh A., "Security Issues of Black Hole Attacks in MANET," *International Conference on Computing, Communication and Automation (ICCCA*), IEEE, 2015.

[27] Liu G., Yan Z. & Pedrycz W., "Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey," *J. Netw. Comput*. Appl. 2018.

[28] Y. Harold Robinson & E. Golden Julie, "MTPKM: Multipart Trust Based Public Key Management Technique to Reduce Security Vulnerability in Mobile Ad-Hoc Networks," *Wireless Personal Communications*, 2019. https://doi.org/10.1007/s11277-019-06588-4

[29] Ravneet Kaur Sidhu & Ram Krishan, "Security Threat of MANET: A Comprehensive Architecture," *International Journal of Innovative Technology and Exploring Engineering (IJITEE),* pp. 2278-3075, vol.9, March 2020.

[30] Radha Raman Chandan & Pramod Kumar Mishra, "A Review of Security Challenges in Ad-Hoc Network," *International Journal of Applied Engineering Research,* vol. 13, pp. 16117-16126, 2018.

[31] Swati Agarwal, Rupinder Kaur & Tushar Agarwal, "MANET Expansion Security Challenges Attacks and Intriguing future Trends," *International Journal of Computer Sciences and Engineering (JCSE),* vol.6, May. 2018.

[32] Aadri A. & Idrissi N.,"An Advanced Comparative Study of MANETs Routing Protocols Under Varied Number of Nodes and Mobility Rate," *Journal of Communications,* vol. 13, no. 6, June 2018.

[33] Russell Skaggs Schellenberg, Nan Wang & Daniel Wright, "Performance Evaluation and Analysis of Proactive and Reactive MANET Protocols at Varied Speeds," IEEE,2020.

[34] Gunseerat Kaur & Poonam Thakur, "Routing Protocols in MANET: An Overview," *2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT),* IEEE, 2019.

[35] Kriti Chadha & Sushma Jain, "Impact of Black Hole and Gray Hole Attack in AODV Protocol," *International Conference on Recent Advances and Innovations in Engineering (ICRAIE),* IEEE, May. 2014.

[36] HoudaMoudni, Mohamed Er-rouidi, HichamMouncif & Benachir El Hadadi, "Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks," *2nd International Conference on Electrical and Information Technologies (ICEIT),* 2016.

[37] Houda Moudni, Mohamed Er-rouidi , Hicham Mouncif & Benachir El Hadadi , "Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack," IEEE, 2016.

[38] Gurung S. & Chauhan S., "A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability," Springer Science Business Media, LLC, 2019.

[39] Deepak Kumar Verma, Renu Jain & Ashwani Kush, "Intrusion Detection using RREP Messages of AODV Routing Protocol," *International Journal of Applied Engineering Research,* vol.12, pp.1956-1961, 2017.

[40] Seryvuth Tan & Keecheon Kim, "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs," IEEE, 2013.

[41] Parmar Roshani & Ankit Patel , “Techniques to Mitigate Grayhole Attack in MANET: A Survey,” *International Conference on Innovations in information Embedded and Communication Systems (ICIIECS),* IEEE, 2017.

[42] A.Janani & A.Sivasubramanian, “Survey of Packet Dropping attack in MANET,” *Indian Journal of Computer Science and Engineering (IJCSE),* vol. 5, no.1, Mar. 2014.

[43] Muhammad Salman Pathan, Jingsha He, Nafei Zhu, Zulfiqar Ali Zardari, Muhammad Qasim Memon & Aneeka Azmat, “An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs,” *International Journal of Advanced Computer Science and Applications(IJACSA),*vol.10, 2019.

[44] Omid Moradipour & Mohammad Fathi, “An Anti-Gray Hole Attack Scheme in Mobile Ad Hoc Network,” Springer, July. 2020.

[45] Taku Noguchi & Mayuko Hayakawa, “Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks,” *Computer Security*, IEEE, 2018.

[46] Mohammed Baquer M.Kamel, Ibrahim Alameri & Ameer N.Onaizah, “STAODV: a secure and trust based approach to mitigate blackhole attack on AODV based MANET,” IEEE, 2017.

[47] S. Sivanesh & V. R. Sarma Dhulipala, “Accurate and Cognitive Intrusion Detection System (ACIDS): a Novel Black Hole Detection Mechanism in Mobile Ad Hoc Networks,” Springer, 2020.

[48]Taher Delkesh, Mohammad Ali Jabraeil Jamali, “EAODV: detection and removal of multiple black hole attacks through sending forged packets in MANETs,” *Journal of Ambient Intelligence and Humanized Computing, Springer, March.2018*.

[49] Gupta P., Goel P., Varshney P., and Tyagi N., "Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET," *In Smart Innovations in Communication and Computational Sciences*, pp. 271-279, Springer,2019.

[50] S.V. Vasantha, A. Damodaram & S. Rama Krishna, “Path-Hop Based Secure AODV to Detect Black Hole and Gray Hole Attacks in MANET,” *Journal of Critical Reviewa*, vol.7, 2020.

[51] Kumari, S. V., & Paramasivan, B. “Ant based defense mechanism for selective forwarding attack in MANET,” *In Data engineering workshops (ICDEW), IEEE international conference on Piscataway,* April. 2015.

[52] Nilesh N.Dangare & R.S.Mangrulkar, “Design and Implementation of Trust Based Approach to Mitigate Various Attacks in Mobile Ad-hoc Network,” *International Conference on Information Security& Privacy (ICISP),* Elsevier, Dec.2016.

[53] Neelam Janak Kumar Patel & Khushboo Tripathi, “Trust Value based Algorithm to Identify and Defense GrayHole and Black-Hole attack present in MANET using Clustering Method,” *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET),* vol.4,2018.

[54] Neha Sharma & Anand Singh Bisen, “Detection As Well As Removal Of Black hole And Gray hole Attack In MANET,” *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT),* IEEE, 2016.

[55] Ankit D. Patel & Kartik Chawda, “Dual Security Against Gray hole Attack in MANETs,” Springer, 2015.

[56] P.Rathiga & S.Sathappan, “Hybrid Detection of Black hole and Gray hole attacks in MANET,” *International Conference on Computational Systems and Information Systems for Sustainable Solutions,* IEEE, 2016.

[57] Zardari A. Z., He J., Zhu N., Mohammadani H. K., Pathan S. M., Hussain I. M. & Memon Q. M.,“A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs,” *Future Internet,* March 2019.

[58] Khandelwal V. & Goyal D., “Black Hole Attack and Detection Method for AODV Routing Protocol in MANETs,” *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* pp. 1555-1559, vol.2, April 2013.

[59] Fidel Thachil & K C Shet, “A trust based approach for AODV protocol to mitigate black hole attack in MANET,” International Conference on Computing Sciences, IEEE, 2012.

[60] N. Bhatt & D. Kathiriya, “Comparison and Analysis of Simulators for Ad hoc Wireless Networks,” *Comparison Anal. Simulators Ad hoc Wirel. Networks*, vol. 3, no. 12, pp. 14–22, 2013.

[61] Ling Liu1 & Lei Zhu, “Improvement of AODV Routing Protocol with QoS Support in Wireless Mesh Networks,” *International Conference on Solid State Devices and Materials Science*, vol. 25, pp. 1133–1140, 2012.

[62] B.I. Bakare & J.D. Enoch, “A Review of Simulation Techniques for Some Wireless Communication System*,” International Journal of Electronics Communication and Computer Engineering (IJECCE),* vol.10, 2019.

[63] Amer Abu, Hebatallah Awad, “Mobile Ad-hoc Network Simulators, a Survey, and Comparisons,” *International Journal of P2P Network Trends and Technology (IJPTT*), vol. 4, pp. 22–26, 2014.

[64] S. V Mallapur, “Survey on Simulation Tools for Mobile Ad-Hoc Networks,” *IRACST – Int. J. Comput. Networks Wirel. Commun. (IJCNWC)*, vol.2, pp. 241–248, 2012.

[65] L. RAJA, “Study of Various Network Simulators,” International Research Journal of Engineering and Technology (IRJET), vol. 05, Dec 2018.

[66] Gibson Chengetanai & Grant Blaise OReilly, “Survey on Simulation Tools for Wireless Mobile Adhoc Networks,” IEEE, 2015.

[67] A Pramanik, B. Choudhury, T. S. Choudhury, W. Arif, and J. Mehedi, “Simulation Study of Random Waypoint Mobility Model for Mobile Ad hoc Networks", pp. 3– 7, 2015.

[68] S.Naveena , C.Senthilkumar & T.Manikandan , “Analysis and Countermeasures of Black-Hole Attack in MANET by Employing Trust-Based Routing,” *6th International Conference on Advanced Computing & Communication Systems (ICACCS)*, IEEE, 2020.

Appendix

==========

Appendix A: Implementing Black Hole Attack in AODV

==========

In **aodv.h**, add the following line of code in the AODV class:

In protected Scope:

```
bool blackhole;
int d_count;
```

In **aodv.cc,** add the following line of code in the AODV command function:

```
int AODV::command(int argc, const char*const* argv) {
…
//Code added by Dagne
   if(strcmp(argv[1], "malicious") == 0) {
     blackhole=true;
     return TCL_OK;
   }
}
```

In constructor scope:

```
blackhole=false;
 d_count=0;
```

```
void AODV::rt_resolve(Packet *p) {
    …
  //Code added by Dagne
 if(blackhole == true){
printf("Number of packets dropped by node %d is %d",idex, d_count)
  drop(P,DROP_RTR_ROUTE_LOOP);
}
}
void AODV::recvRequest(Packet *p) {
…
//Code added by Dagne
 else if(blackhole==true)
 {
  int R= (rand() % 51)+30;  //random value
  sendReply(rq->rq_src,
                  1,
            rq->rq_dst,
            rq->rq_dst_seqno+R,
            MY_ROUTE_TIMEOUT,
            rq->rq_timestamp);
  Packet::free(p);
```

```
 }
}
```

==========

Appendix B: Implementing Smart Gray Hole Attack in AODV

==========

In **aodv.h**, add the following line of code in the AODV class

In protected Scope:

```
        bool grayhole;
         int d_count;
```

In **aodv.cc,** add the following line of code in AODV

```
int AODV::command(int argc, const char*const* argv) {
…
//Code added by Dagne
    if(strcmp(argv[1], "malicious1") == 0) {
      grayhole=true;
      return TCL_OK;
    }
}
```

In constructor scope:

```
grayhole=false;
  d_count=0;
```

```
void AODV::forward(aodv_rt_entry *rt, Packet *p, double delay)
 {    …
            //Code added by Dagne
if(grayhole == true) {
if(ch->ptype_ == PT_CBR){
int x;
x=Random::uniform(0,10);
printf("The number randomly selected %d is", x );
if(x>3){
drop(P,DROP_RTR_ROUTE_LOOP);
d_count++; }
printf("The number of packet dropped by node %d is %d", index, d_count);
} } }
```

Appendix C: Implementing proposed DS-AODV algorithm

==========

I. Our Modification in Route Discovery Operation

==========

In aodv.h

```
#define WAIT_RREP_TIME    2.8  // sec
 void prestore_recvReply(Packet *p);
```

==========

In aodv.cc

```
void AODV::prestore_recvReply(Packet *p) {
…
mali = malitable.malitable_lookup(rp->rp_dst); // check the blacklist table
if (rp->rp_dst == index) {  //First check if the RREP is come from malicious node or not
     fprintf(stderr, "%s: discarding request\n", __FUNCTION__);
        Packet::free(p);
         return; }
else {
       if (ih->saddr() != index) { // if the node is not the source node
            recvReply(p);// calling the recvReply function for original AODV operation
           }
      else { //if the node is the source node
            Get_Time= CURRENT_TIME;
       Set_Time= Get_Time + (WAIT_RREP_TIME/2);// +WAIT_RREP_TIME=2.8 seconds
          do {
          rrep = rreptable.rreptable_insert(rp->rp_dst, rp->rp_dst_seqno);//add id and destination
sequence number in the table.
```

```
            N +=1; // count the number of RREP
} while (CURRENT_TIME <= Set_Time);
    if (N ==1) {
                recvReply (p); // calling the recvReply function for original operation
            }
    else {
          for(rrep = rreptable.head(); rrep; rrep = rtn1) {  // for each rrep entry
           rtn1 = rrep->rreptable_link.le_next; // point the next dst_seqno in the table
                    Sum =Sum + dst_seqno; // for all dst_seqno in the table
                  }
                      Average = Sum / N;
                  printf("The average value %d =",Average);
            for(rrep = rreptable.head(); rrep; rrep = rtn1) {  // for each rrep entry
                    rtn1 = rrep->rreptable_link.le_next;
                    S_devation = S_devation + pow( dst_seqno - Average,2);
                  }
                   SD = sqrt(S_devation / N);
                  printf("The standard deviation value %d =",SD);
          if(SD < Average) {
              for(rrep = rreptable.head(); rrep; rrep = rtn1) { // for each rrep entry
               rtn1 = rrep->rreptable_link.le_next;
```

```
        if(SD <  (dst_seqno – Average)) {
                mali = malitable.malitable_add(rp->rp_dst, rp->rp_dst_seqno);
                rrep = rreptable.rreptable_delete(rp->rp_dst, rp->rp_dst_seqno);
                id_insert(rp->rp_dst, rp->rp_dst_seqno);
              }}
    recvReply (p); // calling the recvReply function for original AODV operation
          }
        else {
              for(rrep = rreptable.head(); rrep; rrep = rtn1){  // for each rrep entry
                      rtn1 = rrep->rreptable_link.le_next;
           if( dst_seqno > SD){
                mali = malitable.malitable_add(rp->rp_dst, rp->rp_dst_seqno);
                rrep = rreptable.rreptable_delete(rp->rp_dst, rp->rp_dst_seqno);
                id_insert(rp->rp_dst,rp->rp_dst_seqno);
                }}
  recvReply(p); // calling the recvReply function for original AODV operation
        }}}
}}
```

==========

II. Actual data packets transmission

Our modification to formulate the Data Forwarding Value

==========

In aodv.h

```
class AODV: public Tap, public Agent {
        public:
        void  tap(const Packet *p);
              };
//=================================================================
```

In aodv.cc

```
        else if (strcmp(argv[1], "install-tap") == 0) {
            mac_ = (Mac*)TclObject::lookup(argv[2]);
           if (mac_ == 0) return TCL_ERROR;
           mac_->installTap(this);
           return TCL_OK;
             }
 //add in constructor scope
           recieved_packet_count = 0;
           send_packet_count = 0;
```

```
        void AODV::tap(const Packet *p) {
        struct hdr_cmn* hdcmn = HDR_CMN(p);
           if (index == 0){
              if (hdcmn->ptype_ == PT_CBR) {
                 received_packet_count++;
              }
           }
        }
AODV::forward(aodv_rt_entry *rt, Packet *p, double delay) {
        if (index == 0) {
              if (ch->ptype_ == PT_CBR) {
                 send_packet_count++;
              }
           }
        DFV = (1-(send_packet_count - recieved_packet_count)/send_packet_count);
                    printf("The data forwarding value is %f", DFV);
             if (DFV <= 0.5){
  mali = malitable.malitable_add(rp->rp_dst, rp->rp_dst_seqno);//add in blacklist table
  rrep = rreptable.rreptable_delete(rp->rp_dst, rp->rp_dst_seqno);//delete from routing table
id_insert(rp->rp_dst, rp->rp_dst_seqno);//broadcast alert packet
recvError(p); //send route error to reinitiate route discovery
```

```
        }
```

==========

Appendix D: Implementation of DDBG AODV Algorithm

==========

In aodv.h

```
    #include <mobilenode.h>//add mobilenode.h as header
```

In aod.cc

```
//Add the following line of code in the forward () function
void AODV::forward(aodv_rt_entry *rt, Packet *p, double delay) {

 d_node=(MobileNode*)(Node::get_node_by_address(index));

         ((MobileNode*)d_node)->getLoc(&xpos,&ypos,&zpos);

            fprintf(fp,"usage_energy");

           usage_energy=d_node->energy_model()->energy();

          current_energy=initial_energy - usage_energy;

   // To formulate Connected Dominate Set

        node.resize(n);

         memset(dual,0,sizeof(dual));

         for(i=0;i<e;i++){

            x=xpos;   y=ypos;

                 x--; y--;

                 node[x].push_back(y);

                 node[y].push_back(x); }
```

```
for(i=0;i<n;i++){
        if(!dual[i]){
                BG.push_back(i);
                dual[i]=true;
                for(j=0;j< node[i].size();j++){
                        if(!dual[node[i][j]]){
                                dual[node[i][j]]=true;
                                break;
                        }}}}
printf("The required Dominant Set is as follows:\n");
for(i=0;i<(int)BG.size();i++){
 printf("%d",BG[i]+1);}
            a = new int[n];
          for (int i = 0; i < n; i++) {
      if (max_energy < *(a+i))    {
                Max_energy = *(a+i);
               }   }
```