Arab American University

Faculty of Graduate Studies

Enhancing MANET Security by eliminating Flooding and black hole attacks

By

Mahmoud Abu-Zant

Supervisor

Prof.Adwan Yasin

This thesis was submitted in partial fulfillment of the requirements for the masters' degree in Computer Science

April/ 2019

Enhancing MANET Security by eliminating Flooding and black hole attacks

By

Mahmoud Abu-Zant

This thesis was defended successfully on 29/4/2019 and approved by:

Committee Members	Signature
1. Supervisor:	
Prf. Adwan Yasin	……
2. Internal Examiner:	
Dr. Mohammad Hamarsheh	……
3. External Examiner:	
Dr. Saeed Salah	……

Declaration

I declare that this thesis has been written by me under the regulations, instructions, decisions and laws of the Arab American University. I take full responsibility for its content if it is objecting the guidelines. This thesis is a presentation of my original research work. Wherever contributions of others are involved, it is indicated clearly. With the exception of these quotations, this thesis is entirely my own work.

Acknowledgment

At the beginning I would like to thank god for everything he gave me, also I thank my family who supported me through my learning life especially my mother and my father. I would like to express the deepest appreciation to my supervisor Professor Adwan Yasin, who has the attitude and the substance of a genius: he continually and convincingly conveyed a spirit of adventure in regards to research and scholarship and excitement in regard to teaching. Without his guidance and persistent help, this dissertation would not have been possible. And I would like also to thanks all the doctors and Professors who taught and gave me the knowledge that enabled me to complete the master program in Arab American University Jenin.

Abstract

Mobile Ad-hoc Network (MANET) is an infrastructure-less network with no central unit that controls and coordinates the communication between nodes in the network. The topology of the network keeps changing due to the randomized movement of the nodes in the network. Different types of routing protocols are used to adapt to the changes in the topology of the network and to connect nodes with each other in order to exchange data and information between them. Ad Hoc On-Demand Distance Vector (AODV) is a reactive routing protocol type where nodes exchange information about other nodes only when a route is needed by flooding the network with requests to the desired nodes. AODV is vulnerable to different types of attacks that affect its performance and functionality in the network such as Black-hole and Flooding attack. AODV should be enhanced with different algorithms in order to resist different types of attacks. In this thesis, different types of attacks especially Black-hole and Flooding attack were presented which affect the functionality and performance of AODV routing protocol. The effects of Black-hole and Flooding attacks on the performance of AODV under different performance metrics were shown, such as Packet Delivery Ratio, End to End Delay and Throughput, by simulating these attacks in different scenarios like nodes density and mobility. The results show that these attacks have a huge impact on the performance of AODV under different performance metrics, which leads us to the importance of enhancing and improving AODV with different algorithms to resist these attacks. AODV was enhanced with two different algorithms to resist Black-hole and Flooding attack. two new models were proposed that detect and isolate the Black-hole and flooding attacker nodes in the network.

A simulation for these models was carried out in different scenarios and compared them with other proposed models to prove their efficiency. The simulations results

show the effectiveness of the proposed models in resisting Black-hole and flooding attack under different performance metrics. We discuss the results of the proposed models in the last two chapters.

To resist Black-hole attack a new model called Timer Based Baited Technique (TBBT) was proposed that consist of a bait-timer that whenever this timer reaches its determined time it broadcast a fake request to bait the Black-hole nodes. Whenever a node in the network receives a reply for any fake request it simply adds the ID reply sending node in the blacklist to avoid interacting with this node. To resist RREQ flooding attack a new model called Avoiding and Isolating Flooding attack (AIF) was proposed that depends on tables that record the number of the requests received by a node in the network. Whenever a node sends a number of requests higher than a determined limit value, the ID of the requesting node is added a suspicious list. Any node in the suspicious list has a limited amount of request that could be processed which is half of the determined limit. Based on our assumption there is no node in the network wants to communicate with a large number of nodes in the same second. So, if the requester node sends requests for many nodes ID which is higher than the determined ID_limit value then the node is moved to the blacklist to avoid processing requests for it.

The comparison between TBBT and the other proposed models show that TBBT has a better performance in terms of Throughput but not in terms of End-to-End Delay. AIF also shows a better performance in terms of Throughput but not in terms of End-to-End Delay compared to other proposed models.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

MANET: Mobile Ad-hoc Network

WANET: Wireless Ad-hoc Network

AODV: Ad-hoc on-Demand Distance Vector

DSR: Dynamic Source Routing

DSDV: Destination-Sequenced Distance Vector

PRNET: Packet Radio Network

SURAN: Survivable Adaptive Radio Network

VANET: Vehicular Ad-hoc Network

FANET: Flying Ad-hoc Network

PAN: Personal Area Network

WLAN: Wireless Local Area Network

DSN: Destination Sequence Number

SSN: Source Sequence Number

TTL: Time-To-Live

RREQ: Route Request Packet

RREP: Route Reply Packet

PDR: Packet Delivery Ratio

Avg ETE: Average End-To-End delay

ARE: Average Residual Energy

NRL: Normalized Route Load

NS: Network Simulation

TBBT: Timer Based Bating Technique

AIF: Avoiding and Isolating Flooding attack

Chapter 1 : Introduction

1.1 Mobile Ad-hoc Network (MANET):

1.1.1 Background

The wireless network is classified into two classes' infrastructure network and infrastructure-less network. In infrastructure network nodes depend on a central unit to coordinate and control the communication between nodes in the network. But in infrastructure-less networks, nodes depend on themselves to coordinate the communication between them instead of depending on a central unit. Mobile Ad-Hoc Network (MANET) is an infrastructure-less network that connects mobile nodes via wireless links like radio and microwave signals while they are moving randomly [1] [2]. Mobile nodes have a limited coverage that allows them to only communicate with other nodes that are located within that coverage. In single-hop communication, nodes communicate with each other directly because they are located in the same coverage. But in multi-hop communication, in which nodes are not in the same coverage, they ask for the help of the other nodes that are located between them to work as a bridge and forward data between them [3]. Figure 1.1 describes the difference between direct communication (single-hop) and indirect communication (multi-hop).

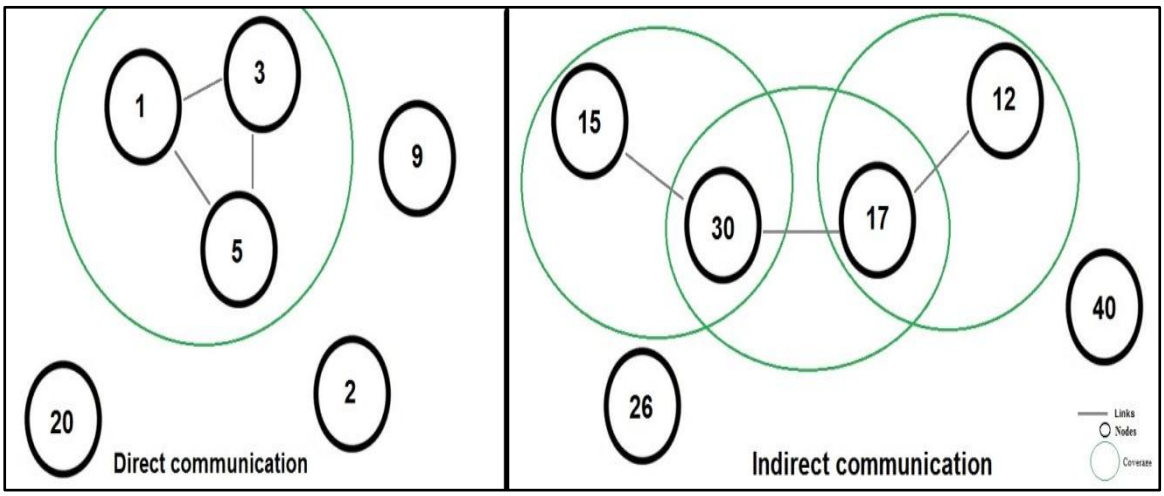

Figure 1.1 Direct and indirect communication

As shown in Figure 1.1, in direct communication node 1, 3, and 5 can communicate directly without the need of other nodes help in the network because they are in the same coverage of each other. But in indirect communication node, 15 asks for the help of node 30 and 17 by forwarding its data to node 12 because node 12 is out of the coverage of node 15 so node 30 and 17 worked as a bridge between node 15 and 12.

The originality of MANET's idea was military. Back in 1970, there was a military research called Packet Radio Network (PRNET) which considers the transmission of packets over a radio network. In 1980, there was a program called Survivable Adaptive Radio Networks (SURAN) and a part of it provided an infrastructure-less network that was based on packet switching for a battlefield environment. SURAN showed the ability to create an infrastructure-less network based on radio signals to transmit packets over it. In the 1990s the Ad-hoc Network developed and started to connect different types of devices. After creating the standers of mobile Ad-hoc network in the 1950s, there were two types of mobile networks: infrastructure network called WLAN (Wireless Local Area Network) and infrastructure-less network called MANET [4] [5]. Figure 1.2 describes the difference between WLAN and MANET.

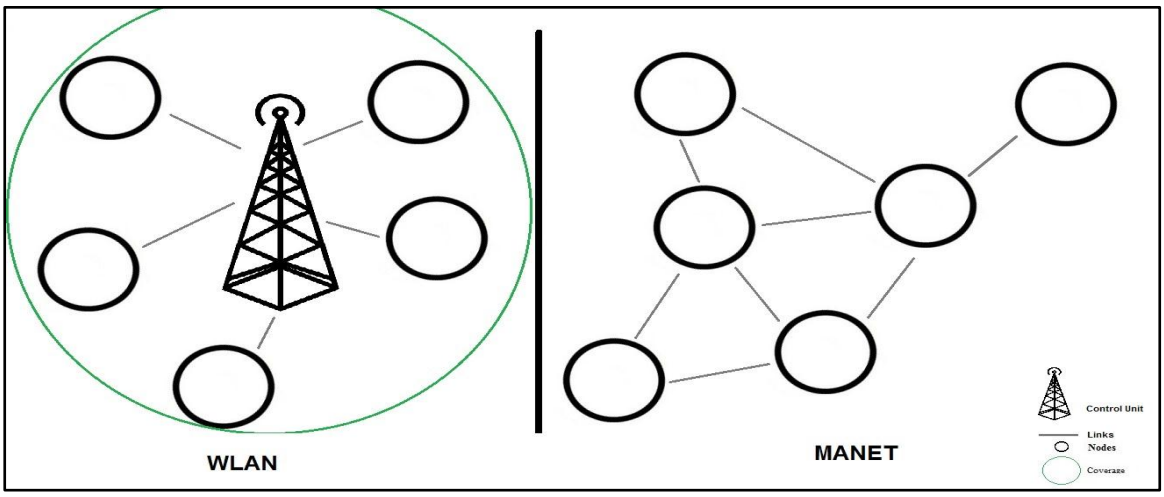

Figure 1.2 WLAN vs. MANET.

Nodes in WLAN depend on a central unit like a base station to connect and coordinate the connection between them. Nodes in WLAN can't communicate directly with each other. Unlike in MANET nodes communicate directly or indirectly without depending on a central unit to connect and coordinate the connection between them. Because of the fact that nodes in MANET can communicate directly and can move randomly, the topology of MANET frequently keeps changing which makes it harder to control and to maintain the connection between any two nodes. Protocols in MANET are designed to overcome and adapt the changes in the topology.

1.1.2 MANET properties

MANET has different properties and features such as autonomous behavior, inferior link capacity, dynamic topology, multi-hop routing, lightweight, infrastructure absence, heterogeneous, and partitioned operation.

The autonomous behavior of nodes in the network property means that nodes in the network can be both client and host. A node can be a client and use the network to forward its own packets to any desired node in the network. Nodes can be the host and work as a bridge that forwards other nodes packets to their destinations. Inferior link capacity property describes how links in wireless communication are inferior to those in wired links.

Links in wireless communication are vulnerable to noise, fading, and interference from other links in the same network. So, the bandwidth of wireless links is lower than wired links.

Dynamic topology property means that the topology of the network keeps changing due to different reasons like the randomized movement of nodes, the death of nodes in the network because of energy absences and the contiguous leaving and participating of nodes to the network.

Multi-hop routing property means that packets and data travel through multiple nodes until they reaches their destinations. When nodes are not in the same coverage of each other, they depend on other nodes to forward their packets.

Lightweight property implicates that most of the mobile nodes have a low power storage and small resource capacity.

Infrastructure absence property means that there is no central unit in MANET that controls and coordinates the communication between nodes. Nodes in MANET can be different devices such as laptops, vehicles, and robots, which lead to difficulties to deal with this heterogeneity of mobile nodes in the network. Partitioned operations because of the absences of central unit nodes should work and cooperate with each other to deliver packets between themselves [6] [7]. The control of MANET is difficult because it has different properties and the developing of routing protocol should take into consideration these properties and features.

1.1.3 MANET applications

The flexibility of MANET made it popular so there are several applications for MANET in real life like Military, Emergency, Vehicular, Commercial, Personal Area Network, Smart Cities, Wireless Sensor Networks, Education, Internet of Things, Flying, and Entertainment [8].

- Military:
- This type of network application called Tactical networks connects soldiers to each other and also connects them with their headquarters or military vehicles.
- Emergency: The flexibility of MANET and the absence of depending on a central unit made it suitable to be used for emergency and distracter management because most central units in distracters are disabled or destroyed. Emergency teams can

communicate with each other directly without the need of any central unit that could be disabled or destroyed.

- Vehicular: MANET is used to connect mobile nodes such as Vehicular. This type of network application is called VANET. Nowadays, Vehicles are equipped with wireless communication units, which allow them to communicate with each other. This communication also allows them to coordinate themselves on the roads and in the environment. The main goal of VANET is to avoid vehicles accident and save human lives.
- Commercial: The popularity of MANET allows it to be used in commercial areas like e-commerce and electronic payment.
- Personal Area Network: This type of network application is called PAN and connects different devices such as cameras, mobile phones or televisions on a local network in order to share and exchange information between them.
- Smart Cities: Building smart cities is a new trend that depends on connecting all objects and devices with each other to control them remotely.
- Wireless Sensor Networks: This type of network application called WSN connects the different sensors to each other in order to exchange sensed information between them and to send out this information to a central unit so it can be analyzed later.
- Education: MANET can be applied in education in a variety of forms, for example in virtual classes and communication during meetings.
- Internet of Things: This type of network application called IoT connects objects to each other using a wireless network. Connecting objects allows them to exchange information which can be very useful in life such as building surveillance cameras and home appliances systems.

- Flying: This type of network application is called FANET and connects flying vehicles like drones, helicopters, and balloons. This type of network may need a base station to coordinate the movement of these vehicles and to exchange information between them.
- Entertainment: MANET can be used in multiplayer games, robot bets, and peer to peer network.

1.1.4 Challenges that MANET faces

MANET faces a lot of challenges that should be solved when creating and developing any protocol such as energy, security, dynamic topology, node resources and heterogeneity [9].

- Limited energy: Mobile nodes' energy is limited because mobile nodes usually have a low power capacity, which indeed needs to be conserved. When developing a protocol one of the main issues that should be taken into consideration is the energy consumption of the protocol.
- Security: MANET is prone to the different types of attacks that aim to affect its functionality or to consume the nodes' recourses. The security of protocols is essential and important to prevent the attacks harm on nodes or data.
- Dynamic topology: the topology of the network changes dynamically because of the mobility and the limited energy of nodes. These changes should be adapted by any routing protocol.
- Nodes resources and heterogeneity: Mobile nodes usually have low resources like low memory and low capability of CPU processing. Also there could be different types of mobile devices such as vehicles, phones, and laptops. Any routing protocol should be aware of the heterogeneity of the nodes and therefore it should take into consideration the low capability of these nodes.

1.1.5 Attacks in MANET

Before we talk about attacks in MANET, we should mention the security goals of the network that should be accomplished. According to [10] there are five different security goals: Availability, Confidentiality, Integrity, Authentication, and Non-Repudiation.

1. Availability: All data and nodes should be reachable whenever an authorized node wants to reach them. This is considered a big problem in MANET since the topology of MANET is dynamic. Access time to data is also important as nodes should be able to receive their desired data from the network in the smallest amount of time. Security levels that are implemented in data and nodes communication by the secure protocol may affect the access time of the data.
2. Confidentiality: Authorized nodes in the network can only access sensitive and protected data. The process of confidentiality is usually accomplished by using encrypt and decrypt techniques that depend on distributing a secret key between authorized nodes. In MANET there is no central unit that helps in distributing the secret key. Key distribution in MANET is a big problem that, in some scenarios could sometimes be impossible to solve in some scenarios.
3. Integrity: Authorized nodes can create and modify data in the network. Some attacks in MANET edit the forwarded packets like Man in the middle attack. In this attack, the attacker node modifies the packets or may delete some of them.
4. Authentication: Nodes should be trusted in order to communicate with them in the network. One of the ways to ensure the authentication is by using certifications but the absence of the central unit which is responsible for the distribution of certification and key management creates a big problem in ensuring this goal.

5. Non-Repudiation: Sender and receiver node can repudiate their packets or behavior in the network. For example, if node 1 received a packet from node 3 and node 1 sent a reply to node 3, node 3 then can't deny that it sent the packet to node 1.

There are two types of attacks in MANET: Passive and Active attacks. In Passive attacks, the attacker node aims only to gather information from nodes in the network without affecting the protocol operations like Eavesdropping and Traffic Analysis attack. But in Active attacks, the attacker node aims to affect the protocol operation by dropping, editing, and delaying packets, or by altering the path of the packets. Sybil Attack, Wormhole Attack, Jellyfish Attack, Jamming Attack, Byzantine Attack, Black-holes and Gray-holes Attack, Man in the Middle Attack, and Flooding Attack are examples on Active attacks in MANET [10-13].

- Eavesdropping and Traffic Analysis attack: In this attack, the attacker nodes keep sniffing other nodes communication in order to gain some information out of these communications, in order to analyze them later and use them in another type of attacks.
- Sybil Attack: In this attack, the attacker nodes claim to have multiple fake identities in order to affect the network operation. The attacker nodes gain the confidence of other nodes by establishing a connection with them or forward packets to them. This attack has a huge impact on the network, especially on network resources [14].
- Wormhole Attack: In this attack, the attacker nodes store the forwarded packets to them and then tunnel these packets to other attacker nodes in the network in different locations.

- Jellyfish Attack: In this attack, the attacker nodes should be a part of the path between two communicating nodes; the attacker node works to delay the forwarded packets to it, before forwarding them to the destination node [15].
- Jamming Attack: in this attack, the attacker nodes work on interfering with the wireless communication between any two nodes that are communicating. The attacker nodes may prevent the source node from sending packets or prevent the destination node from receiving packets.
- Byzantine Attack: In this attack, the attacker nodes create a packet looping by injecting false route information in the network. The attacker nodes control the network by sending fake requests or by modifying and dropping requests. This will indeed harm the delivering process of packets between nodes in the network.
- Man in the Middle Attack: In this attack, the attacker nodes are part of the path between the source and the destination node and the attacker node modifies and edits packets that they have been received from the source node. This attack affects the correctness of the received packets at the destination node.
- Black-holes and Gray-holes Attack: In this attack, the attacker nodes claim to have the shortest path to any desired node in the network even if they don't have any route to it. Normal nodes will trust the reply of the attacker node and start to forward packets to it hoping to deliver them to the desired node. The attacker node then drops these packets. The main difference between a Gray-hole attack and the Black-hole attack is that in the Gray-hole attack the attacker node drops the packets based on different probabilities, unlike the Black-hole attack in which the attacker node drops all the incoming packets. The Gray-hole attack is harder to detect than the Black-hole because it sometimes behaves as a normal node. The Black-hole attacks can be classified into two types: Single and cooperative Black-

hole attacks where the classification is based on the number of attacker nodes. In a Single Black-hole attack, only one attacking node is active, whilst in a cooperative Black-hole attack, a group of attacking nodes works together in order to degrade the network reliability [16].

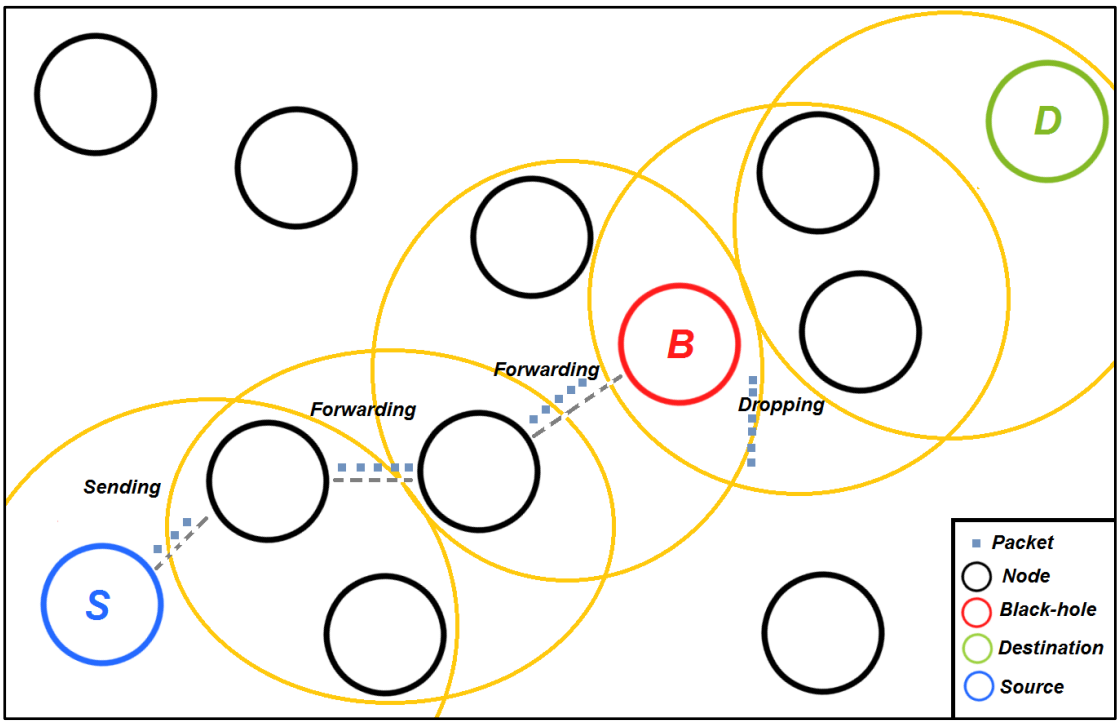

Figure 1.3 Example of Black-hole attack in MANET.

Figure 1.3 shows an example of how an attacker node drops all the packets that were forwarded to it, in the Black-hole attack. The source node forwards packets hoping that the intermediate nodes deliver them to the destination node. Node B claims to have the shortest path to D but when it receives the forwarded packets from node S it starts to drop them.

- Flooding attack: In this attack, the attacker nodes flood the network with the protocol main messages in order to affect the network operation and to consume its resources such as energy and bandwidth. There are several forms of Flooding Attack Hello Flooding, RREQ Flooding, Data Flooding, Error Flooding, and SYN Flooding [17].

- Hello Flooding: In this form, the attacker node has a powerful transmitter that has a higher range than the normal nodes. The attacker keeps broadcasting Hello messages convincing other nodes that he is adjacent and a neighbor to them. Normal nodes keep forwarding packets to the attacker node hoping to deliver it to the destination node because it has a higher power than any other normal node in the network.
- RREQ Flooding: In this form, the attacker node keeps flooding the network with requests (RREQs) for a random node IDs that do not exist in the network. Normal nodes keep forwarding these RREQs hoping to find a path of fake nodes.

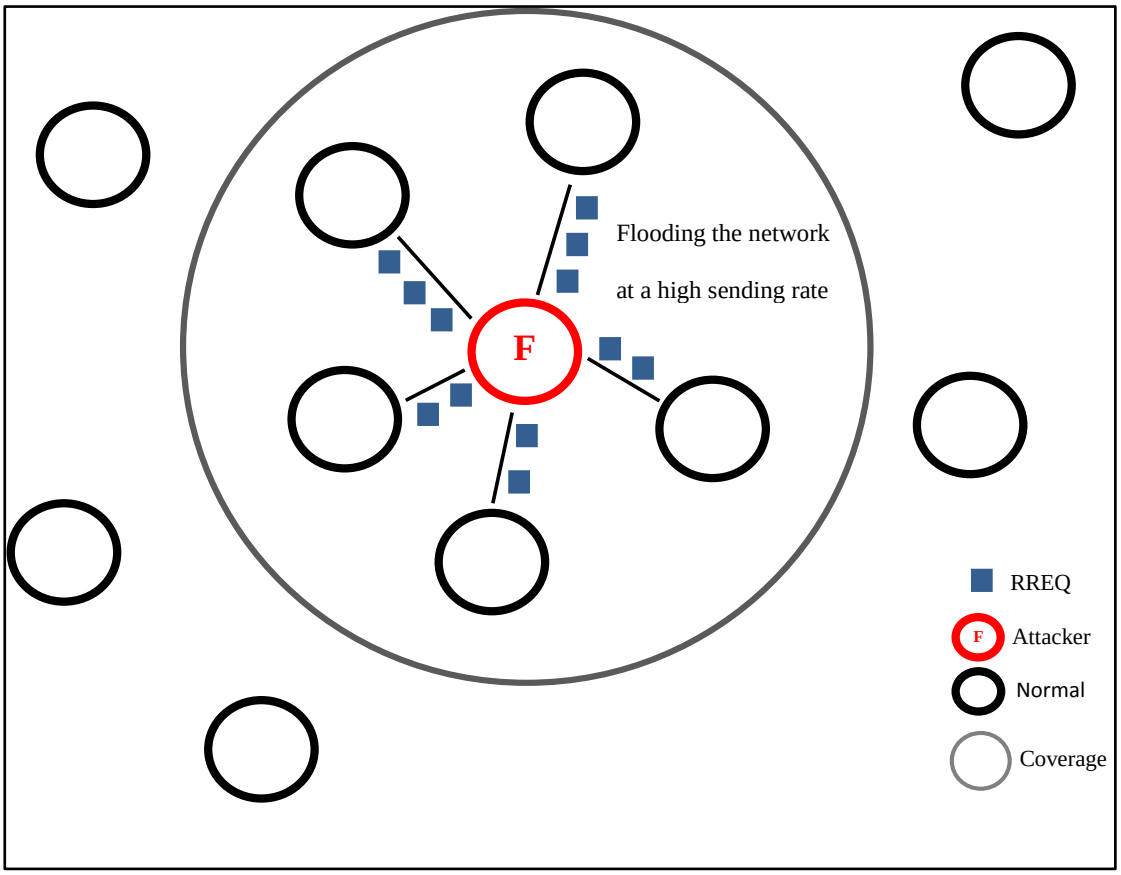

Figure 1.4 Example of RREQ attack in MANET.

As shown in Figure 1.4 the attacker node keeps broadcasting RREQ for fake nodes and normal nodes rebroadcast these RREQ hoping to find a path to the fake

node. Attacks in MANET may target different layers in the network [18]. Different security solutions should be implemented in each and every layer to avoid the attacks [19]. The following table shows examples of attacks in each layer and the security solution that should be implemented for each layer.

- Data Flooding: also called Sleep Deprivation Attack. In this form, two attacker nodes in the network start to transmit an enormous amount of fake data to each other in a high sending rate in order to consume the energy of each normal node that is a part of the path between those two nodes.
- SYN Flooding: In this form, the attacker node consumes normal nodes memory by continuously sending a huge amount of synchronization packets to the victim node.
- Error Flooding: In this form, the attacker node should be a part of the path between any two nodes transmitting data to each other or near them. The attacker node keeps flooding error messages (RERRs) to randomly selected nodes within its range. This will lead to interruptions of the transmission process between those nodes because they think that one of the nodes that forwards their packet is unreadable so they start the discovery phase again.

Table 1.1 Examples of attacks in different Network layers [19].

Network Layer	Example of different attacks	Security Solution should be implemented
Application Layer	Different virus, worms, & malicious codes.	Prevent and Detect viruses, worms, malicious codes, and application abuses.
Transport Layer	Session Hijacking & Jelly Fish Attack	Provide authentication and secure end-to-end communications using encryption techniques.
Network Layer	Black-hole Attack Gray-hole Attack Wormhole attack	Protect Ad hoc routing protocols.

Data Link Layer	WEP targeted Attack Stealth Attack	Provide Link-layer security support and protect the wireless MAC protocol.
Physical layer	Jamming Attack	Prevent signal jamming.

As shown in Table 1.1 there are different types of attacks that target different layers and there should be a technique to prevent these attacks. In this thesis, the main focus is to work against Black-hole and RREQ flooding attacks.

1.1.6 Classifications of MANET routing protocols

There are three main classes in MANET routing protocols that are classified based on the cast techniques used between nodes: Unicast, Multicast, and Broadcast. Unicast protocols are classified into three main classes: ID-based Flat, ID-based Hierarchal and Geographical based. ID based Flat routing protocols aim to distribute information about nodes in order to find a path between nodes without organizing the network or traffic. ID based Hierarchal aim to organize the network in a hierarchy way in order to control the communication between nodes. Some protocols depend on forming clusters in the network to control the communication between nodes in the network. Geographical based routing protocols depend on GPS or a reference point to determine the actual physical location of nodes in the network to help nodes to communicate with each other. This class of protocol reduces the overhead used to find a path between nodes because each node knows the exact physical location of other nodes in the network [20]. Figure 1.5 shows MANET routing protocols.

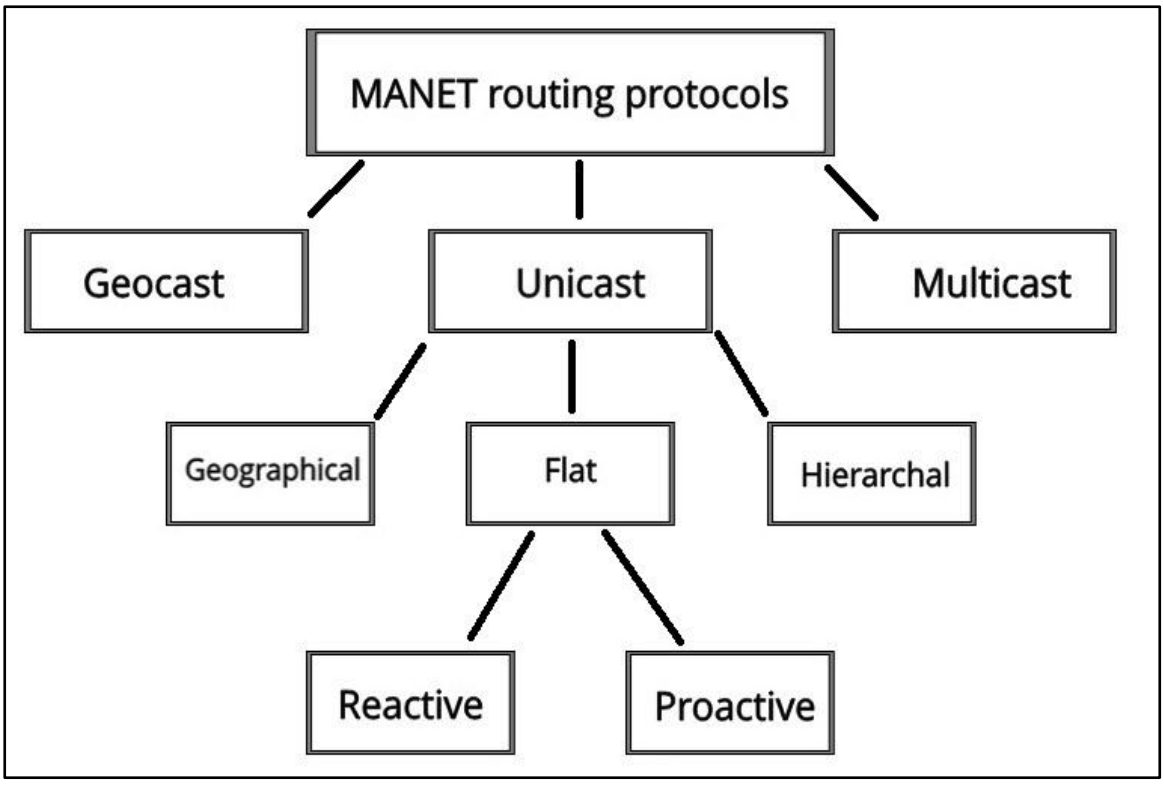

Figure 1.5 Classification MANET routing protocols.

The flat class has two main types of protocols: reactive and proactive. In proactive routing protocols, nodes have a table that consists of information about other nodes in the network. Tables are continuously updated by messages that are sent between nodes in the network. Nodes use the information stored in their tables to communicate with other nodes. Destination Sequenced Distance Vector (DSDV) is considered as one of the most popular proactive routing protocols. In reactive routing protocols, nodes obtain information about other nodes when a route is needed in order to find the shortest path to any desired node in the network. Reactive routing protocols avoid continues updates for the nodes' tables unlike in reactive protocols which reduce the resources already used. Reactive routing protocols depend on flooding the network with request packets to find a path to a desired node in the network, which create a route overhead. Ad Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols are considered as the most popular reactive routing

protocols [21] [22]. The following table 1.2 shows the comparison between flat class routing protocols in terms of Routing overhead, Scalability, Periodic updates, Latency, Storage requirement, and Routing scheme [23].

Table 1.2: Comparison between Flat routing protocols [23].

Parameters	Reactive	Proactive
Routing overhead	Low.	High.
Scalability	Not suitable for large networks.	Low.
Periodic updates	Not needed as the route is available.	Yes, every time that the topology of the network changes.
Latency	High because of the flooding process.	Low because it uses routing tables.
Routing scheme	On-demand.	Table-driven.
Storage requirement	Generally, low based on the number of paths.	High, due to the routing tables.

In this thesis, the main focus was on reactive routing protocol, especially AODV routing protocol.

1.2 Problem statement:

Security of MANET is important and essential to prevent the harm that could be caused by an attacker node on the data and nodes in the network. Since MANET uses wireless links to connect nodes together, data may be viewed or modified by an unauthorized user which is called eavesdropping threat. Also, in MANET, there is no central infrastructure that controls the communication between nodes, so nodes rely on themselves to deliver data to the destination node. Thus, a malicious attacker node may alter the connection link or drop the forwarded data. Denial of Service (DoS) attack is considered one of the most serious threats to MANET, in which a malicious attacker node drains the battery and the resources of other nodes by requesting them to forward a huge amount of data. The Flooding attack, for example, is considered to be one of the Denial of Service (DoS) attacks that threatens the network operations and aims to congest the network with false packets in order to affect the

communication between nodes in the network. The Black-hole attack, as another example, aims to prevent the connection between any two nodes in the network. The native AODV is an on-demand routing protocol, which finds the shortest possible path between nodes in the network, but it lacks mechanisms that detect and prevent Black-hole and Flooding attack. Many algorithms and techniques are proposed and developed to detect and isolate different types of attacks in MANET. The main differences between these algorithms are the methods that are used to detect the attacker node in the network, isolation of the attacker node and the avoidance of the attack's effects. This thesis discusses different types of attacks that threat MANET, especially Black-hole and Flooding attack, and also presents the developed models and techniques to resist a Black-hole and Flooding attack in MANET.

In addition to that, it includes a presentation of our enhancement on AODV routing protocol to detect both Black-hole and Flooding attack in the network. Our proposed models are simulated and compared with other proposed models and techniques in different performance metrics to prove their efficiency.

1.3 Thesis goals:

The first goal in this thesis is to gather information about the proposed models that detect both Black-hole and Flooding attacks in MANET.

The second goal is to study the collected models, and to find the weaknesses in these models.

The third goal is to propose new models to resist both Black-hole and Flooding attack and to design them well in order to outperform the other proposed models in different performance metrics.

The fourth goal is to simulate the proposed models using the NS-2.35 simulator in different scenarios and evaluate it under different performance metrics. And the final

goal is to compare our proposed models with other developed models to prove that our models can outperform other models in different performance metrics.

1.4 Research methodology:

In order to achieve these goals, the effects of both Black-hole and Flooding attack on AODV routing protocol are studied by simulating these attacks and by comparing the performance metrics before and after the attack. Some of the proposed models in the literature, that can resist Black-hole and Flooding attack, are studied, and the advantages and the limitations of these models are discussed. New models are proposed considering the limitation of the existing models. Proposed models are simulated in order to evaluate them. The simulation was performed using NS-2.35 simulator, which can create different scenarios and compare AODV performance in all these scenarios. The creation of scenarios was done using CMU tool, which is a NS-2.35 tool that creates files containing a random placement and movement of nodes during a fixed period of time. We used two different network sizes 1000x1000m and 850x850m, the nodes' placement was random. Nodes move with a maximum speed of 15 mps. At the initial stage, the source and the destination node were set at the edges of the network, and the attacker node was set in the middle of the network. The number of nodes was varying between 25 to 150 in 1000x1000m scenarios and 20 to 80 in 850x850m scenarios. Finally, an AWK script is used to analyze the trace file that is generated from running NS-2.35.

1.5 Thesis outline:

This section describes the content of each chapter:

Chapter 2 AODV and Literature review: this chapter discusses AODV routing protocol, AODV phases, AODV routing table structure, Route Discovery and AODV advantages and disadvantages. Also, this chapter provides a literature review of

security mechanisms that are used against attacks in MANET, especially Black-hole and Flooding attack.

Chapter 3 Black-hole and Flooding Attack effects on MANET: This chapter studies the simulation results of AODV under Black-hole and Flooding attack in different scenarios under different performance metrics.

Chapter 4 Timer Based Detection Technique (TBBT): This chapter introduces the newly developed model against Black-hole attack, which is called TBBT and studies the results of simulating it in different scenarios under different performance metrics. Also, this chapter shows the overall performance comparison between TBBT with other proposed models.

Chapter 5 Avoiding and Isolating Flooding attack (AIF): This chapter introduces the newly developed model against RREQ Flooding attack, which is called AIF and studies the results of simulating it in different scenarios under different performance metrics. Also, this chapter shows the overall performance comparison between AIF with other proposed models.

1.6 Contributions

The security of MANET is important to ensure the safe delivery of packets between nodes in the network. MANET is prone to different types of attacks that threaten the safety of packet delivery between nodes. The Black-hole attack works to prevent the successful connection between any two nodes that want to communicate. The Black-hole node keeps replying to have the shortest path to any received request. There are different developed mechanisms to mitigate the effect of the Black-hole node and to detect it. Most of the developed mechanisms have a high overhead because of using extra tables and a new special type of packets to detect the attacker node in the network. Batting technique is a lightweight technique that does not have high

overheads like other mechanisms. a new technique was proposed that is based on a batting mechanism to detect a Black-hole attack in the network. The developed technique is an integration of both timer and batting requests to detect the attacker node. The developed technique also has the ability to counter Smart Black-hole attack and prevent it from countering the proposed model.

Flooding attack is a type of Dos attack that aims to affect the performance of the protocol by continuously using the protocol's main messages in order to flood the network and to create congestion in it. a new model was proposed that is based on two algorithms to detect the attacker node in the network. The first algorithm avoids the effect of the flooding node and the second algorithm detects the attacker node in the network.

Chapter 2 : AODV and Literature review

This chapter first gives a quick overview of AODV, and then about the developed techniques and models against Black-hole and Flooding attack. Also, it describes the limitation of the proposed models against the so-called Smart Black-hole attack. Smart Black-hole attack is an integration between Black-hole and Blackmail attack. In Blackmail attack, the attacker node is able to use the protocol mechanism and the protocol control messages against itself. Some protocols keep the ID of the attacker saved in the Blacklist and use an alarm to notify other nodes about the attacker node. The Blackmail node keeps using these alarms to tell other nodes to add normal nodes to their blacklist [28] .The Smart Black-hole node keeps replying to any request and also tries to counter the protocol security mechanism. This chapter is divided into two sections Black-hole and Flooding attack section.

2.1 Ad Hoc On-Demand Distance Vector (AODV)

AODV is a reactive (On-Demand) routing protocol. Nodes that use AODV protocol receive information about how to reach other nodes in the network only when a route is needed. AODV uses Distance Vector algorithm to compute the shortest distances based on the number of hops between any two nodes that want to communicate. AODV has a better performance than other reactive routing protocol according to [24] [25], especially in terms of Throughput and End to End Delay. Nodes that use AODV have routing tables and these tables only get updated when nodes receive control messages. Entries of routing tables get deleted after a period of time if no control messages are received within this period. AODV depends on timers to remove any old routing information in the routing tables. AODV uses network flooding process in order to find a path between any two nodes that want to communicate with each other,

which increase the overhead. AODV uses four types of control messages: Hello message, Route Request message, Route Reply message and Route Error message. Hello message is used to notify other adjacent nodes about the node existence in their coverage. Route Request and Route Reply are used to establish a connection between nodes in the network. Finally, Route Error message is used to maintain routes between nodes. The reason why AODV performs better than other reactive routing protocols is that AODV uses the concept of a sequence number that is used in DSDV (Destination-Sequenced Distance Vector is a proactive routing protocol), which indicates the freshness of the route. Also, AODV uses the concept of request flooding as in DSR (Dynamic Source Routing) in order to find a route between nodes. AODV, unlike DSR, uses routing tables to maintain information about routes in the network [26].

2.1.1 AODV Phases

AODV has two phases: Route Discovery phase and Route Maintenance phase. These phases are responsible of finding a path between any two nodes that want to communicate in the network and then to maintain that path [27].

2.1.2 Route Discovery

When two nodes in the network want to communicate with each other, the source node first checks if the destination node is within its coverage and can communicate with it directly. Afterwards, it sends the packet directly to the destination node. Else source node checks its table to see if it has a route to the destination node and then starts communicating with the destination node using that route. Otherwise, the source node starts route discovery by broadcasting a route request message (RREQ) to all its neighbor nodes, hoping to find a path to the destination node. RREQ contains the ID of the source and the destination node, destination sequence number, source sequence

number, RREQ ID, TTL (Time to Live, which indicates the maximum number of hops that RREQ can travel) and a set of flags that are received for multicast. Figure 2.1 shows the structure of RREQ in AODV.

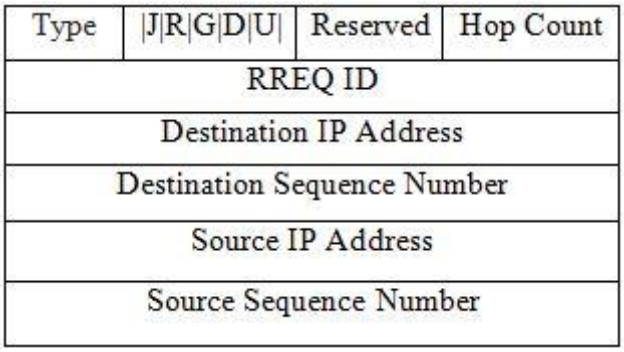

Figure 2.1 RREQ structure.

In the set of flags, that is shown in Figure 2.1, J is a Join flag that is received for multicast, R is a Repair flag that is also received for multicast, G is a Gratuitous RREP flag indicating that any gratuitous RREP should be unicast to the destination node, D is a Destination only flag and indicates that the destination node only can send a reply for this request and U is an Unknown flag which indicates that the sequence number is unknown. Any node receives RREQ first checks if it is the destination node or has a path to the destination node and then unicasts a Route Reply message (RREP) to the source node. Otherwise, the intermediate node rebroadcasts the RREQ and increments the hop count field in RREQ by one in order to find a path to the destination node. Any node that receives RREQ creates a reserved path, containing the broadcast ID, source node ID, the previous hop node ID and destination sequence number. Reserved path information is used to unicast the RREP back to the source node when a path to the destination node is found. RREP contains the ID of the source and the destination node, destination sequence number, TTL, a set of flags that are received for multicast and a 5 bits prefix size. Figure 2.2 shows the structure of RREP in AODV.

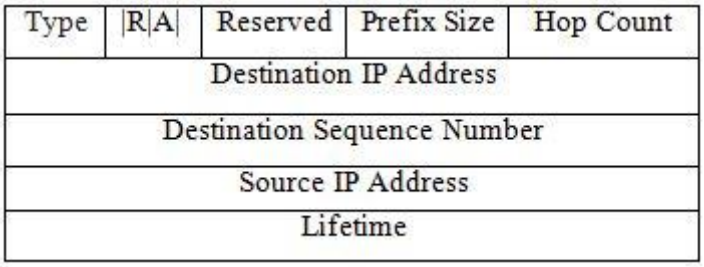

Figure 2.2 RREP structure.

When the source node receives multiple RREP, it selects the path with the least number of hops. Then, the source node starts forwarding packets to the destination node using the selected path.

2.1.3 Route Maintenance

The Mobility of nodes in MANET creates a big problem, especially after creating routes between nodes because the topology of the network keeps changing and links between nodes get broken. When an intermediate node finds a route failure with other nodes that forward packets to the destination node, it first stops forwarding packets to the failure node, removes its entry for the route table and finally, broadcasts a Route Error message (RERR). Any node receives RERR stops forwarding packets to failure node and rebroadcasts the RERR. The rebroadcasting process stops when the source node receives RERR. Then the source node starts the Route Discovery phase again in order to find another path to the destination node. RERR contains the ID of the unreachable destination node, the unreachable destination sequence number, additional unreachable nodes and additional unreachable destination sequence numbers. No delete flag indicates that there is no need to remove the entry because the node has performed a local repair of a link and the number of the unreachable nodes. Figure 2.3 shows the structure of RERR in AODV.

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

Figure 2.3 RERR structure.

2.1.4 AODV routing table structure

As we mentioned above, AODV depends on routing tables to maintain information about routes between nodes in the network. Each entry in the routing table has the following information: the destination node's ID, the Destination Sequence Number (DSN), Hop Count which indicates the number of hops needed to reach the destination node, Next Hop indecates the ID of the neighbor node that will forward packets to the destination node, List of Precursors, Lifetime which indicates the expiration time of the route, Network Interface and a set of flags like valid, invalid and repairable. Figure 2.4 shows the structure of the routing table in AODV.

Destination ID
DSN
Hop Count
Next Hop
Network Interface
List of Precursors
Set of flags
Lifetime

Figure 2.4 Routing table in AODV protocol.

2.1.5 AODV advantages and disadvantages

As known, AODV is an on-demand routing protocol which means that the routes and information about them are created only when they are needed. This reduces the overhead of storing the full topology of the network in routing tables as in the

proactive routing protocols. AODV uses a sequence number that indicates the freshness of the route and also helps in avoiding route loops problems that are found in distance vector algorithms. AODV stores route information in routing tables. Stored routing information in the nodes' tables can be used for different paths which may reduce the routing overhead in some scenarios. AODV avoids storing the route information in the packet header as in DSR. Sending Hello messages periodically consumes bandwidth, especially in high dense scenarios. A single RREQ may have a multiple RREP, which is considered as a high control overhead.

2.2 Black-hole attack

In this section, we are going to focus on the developed technique against Black-hole attacks, especially bating technique, because it is a lightweight technique that does not require any extra overhead to detect the attacker node, unlike other techniques. Some of the developed techniques depend on the value of the Destination sequence number (DSN), that is used in AODV to determine the freshness of the route. Because the Black-hole node always replies to any request with a high DSN [29]. Some of them depend on neighbor nodes to determine the behavior of other nodes which is called Watchdog technique and in which nodes are in a promiscuous mode, starting to listen and ensuring that the other nodes are forwarding packets. In this way, nodes can determine if there is a Black-hole node that does not forward packets to other neighbors [30]. Some of them use a trust-based algorithm, in which each node in the network has a trust value that is determined by the behavior of the node in the network. If the value of the node is too low, it is then considered a Black-hole node [31]. And finally, some of them use a fake packet as a bait to detect Black-hole nodes in the network. In baiting techniques, nodes send a request for a non-existing node in the network and wait for a reply, since a Black-hole node always replies to any

request. Then, the Black-hole node replies to the fake node's request [32]. As mentioned above, we focused on baiting techniques to detect the attacker node in the network. We concluded three different baiting techniques:

A) Baiting using its own ID, where any node wants to bait a Black-hole node and broadcasts a request containing its own ID. When it receives a reply, it checks if any of the replies has a higher DSN than its own Source Sequence Number (SSN) then it's considered as a Black-hole node, since it always replies to any request with a high DSN.

B) Baiting using one of its neighbor nodes' IDs, where any node wants to bait a Black-hole node and selects one of the neighbor nodes' IDs and broadcasts a bait request containing the neighbor's ID. Any node sending a reply to that bait request may indicate that there is a Black-hole node in the network. The source node keeps track of the suspicious node and it gets identified as a normal node or a Black-hole node.

C) Baiting using a fake ID, where any node wants to bait a Black-hole node and broadcasts a request containing a fake ID that does not exist in the network. Any node replies to that bait request it is immediately considered as a Black-hole.

P. TSOU et al. [32] developed a scheme that depends on using a fake ID to bait a Black-hole node. The Source node starts by broadcasting a bait request containing an ID that does not exist in the network. The black-hole node will reply to that bait RREQ due to its normal behavior which is replying to any RREQ in the network, claiming that it has the best path. The developed scheme is implemented in DSR so they modified the RREQ and RREP header in order to determine the Black-hole node within the path. An alert is broadcasted to neighbor nodes when a Black-hole node is

detected. The Source node keeps checking if there is a decrease below the determined threshold, and it then starts the baiting again.

The limitation of this scheme is that it increases the size of the control packets (RREQ and RREP) which leads to an increase in the overhead. Also, the Black-hole alert can be used by a Smart Black-hole to isolate nodes in the network.

B. Singh et al. [33] proposed a model that starts by flooding a fake request in the network. Any node replying is considered a suspicious node. With the help of the neighbor nodes, a Black-hole node can be detected by checking if the suspicious node is forwarding packets to the destination node. The proposed model has a localization system that gets the position of the Black-hole node since the model has been developed to be used in the military.

The limitation of this model is that it floods the network with a fake request which may lead to congestion in the network.

A. R. Rajeswari et al. [34] proposed a system that depends on a special type of nodes called Guard nodes. These nodes help in detecting Black-hole nodes in the network. Guard nodes are nodes that are in the promiscuous mode, checking the behavior of other nodes in the network. Guard nodes contain tables that record the behavior of the nodes in the network. Each node has a trust value which is determined according to its behavior in the network, and it decreases when the node only sends RREP and does not send RREQ. If the trust value of a node decreases below the determined threshold, then it is blocked or isolated. Guard nodes broadcast an alarm to all adjacent nodes when a Black-hole node is detected.

The limitation of this system is that it needs a special type of nodes (guard nodes) and a huge number of guard nodes to cover the entire network. Also, this system has a high overhead because of having many tables.

N. Kalia et al. [35] developed a baiting technique which depends on the own node's ID. The detection of a Black-hole node starts by broadcasting a bait request to all adjacent nodes. The bait request contains source sequence number (SSN) and the source ID. When the source node receives replies it checks if there is a reply that has a higher DSN than its own SSN and this indicates that the reply came from a Black-hole since there is no node in the network that should have a higher DSN than the SSN of the source node. After the detection of the Black-hole node in the network, the source node broadcasts a Black-hole alarm to all adjacent nodes to notify them.

The limitations of this technique are that a smart Black-hole node can check if the received RREQ asks for a route to the same source of the RREQ, and then it simply does not reply to that request. Also, a smart Black-hole node can use the Black-hole alarm and start broadcasting false Black-hole alarms to isolate selective nodes in the network.

P. L. Chelani et al. [36] developed a technique which depends on using Cooperative Bait Detection method Scheme (CBDS). In CBDS, the detection of a Black-hole is divided into three phases: Bait phase, Reverse Trace, and Reactive Defense.

In Bait phase, the source node selects one of its neighbors randomly and sends a bait request using its ID. In Reverse Trace phase a list of the suspicious node is created from the RREP of the bait's RREQ. Afterwards, the neighbor nodes enter in promiscuous mode to detect if there is an attacker node in the path. For each Black-hole node detected in the network, a Black-hole alarm is broadcasted to neighbor nodes. In Reactive Defense phase, the source node checks if the PDR is lower than a determined threshold, and then runs Bait phase again.

The limitation of this technique is that the nodes enter a promiscuous mode which is not acceptable to all nodes. Since some nodes do not want any unauthorized user to

listen to their own transmissions, also being in promiscuous mode will facilitate passive attacks. A Smart Black-hole node can use the Black-hole alarm feature and start broadcasting false Black-hole alarms to isolate network nodes.

S. R. Deshmukh et al. [37] proposed a model that depends only on a validity bit that is set in RREP. In this model it is assumed that the attacker node is unaware of the validity bit that should be sent upon sending the RREP. When the source node receives RREP it checks the validity bit. If it is set to one, it then uses that path and if not, then it considers the RREP came from a Black-hole node and discards it.

The limitation of this model is the unrealistic assumption since the attacker node, that wants to attack the network, will use the same protocol, and it will analyze it before the attack, so any Smart Black-hole node will notice this validity bit and send an RREP to any request with a set validity bit.

S. Dhende et al. [38] proposed a model called SAODV which detects Black-hole and Gray-hole nodes by depending on the neighbor nodes opinion. All nodes in SAODV contain two tables Neighbor list (NL) which records IDs of neighbor nodes and Opinion list (OL) which is used to judge nodes by depending on their activity in the network. When the source node receives a reply for a route request, it broadcasts an opinion message to neighbor nodes to ask them about their opinion on the node that claims to have the shortest path. If all nodes respond with a NO message, this node is a Black-hole node, if some nodes respond with a YES message and the rest with NO messages, then this node is a Gray-hole node. Otherwise, it is a normal node. If any attacker node is detected, an alarm is broadcasted to the network to notify them about the attacker.

The limitation of this model is high overhead because nodes store the information about other nodes in the OL table. Also, there is a risk in asking neighbor nodes about

their opinion as the node that it claims to have the shortest path could also be a Smart Black-hole node that sends a false opinion when they are asked about other nodes. In addition, using the alarm in a false way will eventually isolate other nodes in the network.

Sathish M. et al. [39] proposed a model depends that on using fabricated requests to detect Black-hole nodes in the network. The Source starts by broadcasting a fabricated request in the network, and any node replying to the fabricated request is considered a Black-hole node. The Source node stores the average DSN received from every reply coming for the fabricated request. Then, the source node broadcasts a request to the desired node. When the source node receives a reply for the request, it checks the DSN of the reply and if it is close to the stored average DSN, the node is then considered the node a Black-hole node. Otherwise, the node sending a reply is a normal node. The proposed model is also provided with a prevention technique that depends on digital signatures and trust value to reduce the effect of Black-hole nodes in the network.

A. Koujalagi [54] proposed a technique called bdsAODV to detect the Black-hole attack in the network. In bdsAODV, when the requesting node receives multiple replies for a request, it simply drops the first reply that it received because the first reply is more likely to come from a Black-hole node as the Black-hole node sends a reply for any request without checking its table. And the source node then chooses the second node that sent the reply to it and starts to forward packets to that node. The results of bdsAODV in terms of Throughput and PDR is higher than native AODV Black-hole attack.

Z. Zardari et al [55] proposed a technique called dual attack detection for black and gray hole attacks (DDBG). DDBG combines two algorithms a connected dominating

set (CDS) and intrusion detection system (IDS). CDS is a set of lowest number of nodes that cover the network. IDS is a set of nodes from CDS nodes that has high energy. DDBG starts by selecting nodes that cover the network based on the energy level along with trust level. Nodes can check the behavior of neighbor nodes by entering the promiscuous mode. Then nodes can determine the trust level. After that, a subgroup of the CDS nodes is selected based on the energy level. Then the node with the highest energy level from IDS is selected to coordinate the communication between nodes, which is called IDS node. The IDS node broadcasts a status packet to detect any misbehaving node. If a misbehaving node is detected, the IDS node broadcast a Black message to inform other nodes about it so they block it. The results of the proposed technique showed a low End to End delay and a high Throughput and detection ratio.

2.3 Flooding attack

In this section, we will discuss anti DoS attack techniques and the most known anti Flooding attack techniques, especially RREQ Flooding as it is considered the most popular form and has the highest impact on the network. Also, we will discuss some limitations for some of the techniques.

T. Pandikumar et al. [40] proposed a model that prevents the RREQ Flooding attack in MANET. The proposed model employs a Dynamic Profile Based Detection Scheme (DPDS) to detect the attacker node. Each node records the number of sent requests and the number of received requests in order to compute the average of RREQ which is used to compute RATE_LIMIT. The value of RATE_LIMIT is then used to determine the threshold value, and any node sending a number of RREQ exceeding this threshold is isolated and considered as an attacker node. This model

decreases the Packet Loss Ratio (PLR) for two different scenarios compared to the native AODV under attack.

O. Singh et al. [41] developed a new model called SAODV to detect and isolate the RREQ Flooding attack in MANET. SAODV uses a statistical threshold to detect the attacker node, which depends on two parameters: the mean number of RREQ (MRREQ) made by different nodes in the network, and the mean deviation from the mean of all RREQ (MDRREQ). After computing these two parameters, the value of the threshold is set. Any node that sends a number of RREQ higher than the threshold is considered as an attacker node and an alarm will be broadcasted to isolate this node. The results of SAODV showed a high Throughput that is near to the native AODV, and a low delay that is also near to the native AODV.

S. Gurung et al. [42] proposed a novel approach to mitigate RREQ Flooding attack in MANET. The proposed approach is called F-IDS. It is divided into three phases dynamic threshold calculation, confirmation, and resetting phase. In F-IDS, nodes are in the promiscuous mode to observe the nodes' behavior in the network. In the first phase, after a period of time, each node calculates the threshold value based on the standard deviation of the received requests number. In the second phase, if nodes detect a misbehaving node that broadcasts a fake request greater than the threshold, an alarm is broadcasted to all normal nodes to block this node and add it to the blacklist. In the third phase, nodes reset blocked nodes in the blacklist after a period of time, and only if a node has been blocked for three times, then this node will be blocked forever. The results showed a high average throughput that is near to the native AODV but a higher normalized routing load than the native AODV.

N. S. Chouhan et al. [43] proposed a model to prevent RREQ flooding attack. The proposed model categorizes nodes into three main types stranger, acquaintance, and

friend type. Each node has a table that categorizes each node in it to acquaintance or friend based on the trust level. Any node that does not exist in the table is considered as a stranger node. Each type also has a threshold value that varies from other types as the friend type has the highest threshold value and the stranger type has the lowest value. Whenever a node receives an RREQ, it first checks the type of the sender node and counts the number of RREQ received. If the number exceeds the threshold value, the sender node is then considered as a malicious node and the receiver node drops any RREQ coming from that node. The results showed higher Throughput values comparing to the native AODV under attack.

M. Rmayti et al. [44] developed a detection system for RREQ flooding attack in MANET. The developed system has two components Anomaly notification procedure and Malicious flooding detection mechanism. In Anomaly notification procedure, each node in the network exchanges information about generated and received requests. This information can be exchanged by a Hello message, which has an extra field that is designed to carry this information. The exchange process is important to periodically keep track of the network's state as each node keeps track of average requests of other nodes in its table, and whenever it receives information about an average request that exceeds the threshold, it triggers the second component. The threshold value is determined by computing Exponentially Weighted Moving Average (EWMA). In the Malicious flooding detection mechanism, each node searches its neighbor node's list to find the source of the Flooding attack by comparing the number of received RREQ with RREQ RATELIMIT. After the detection of the attacker node, an RRER message is broadcasted to cut any communication with the attacking node. They simulated the system and found that the system is capable of detecting a Flooding attack node when α equal 0.25 in EWMA.

S. Kumar et al. [45] developed an algorithm to prevent RREQ attack in MANET. Each node has three lists whitelist, graylist, and blacklist. Whenever a node receives a request, it searches the sender in these three lists. If the sender is from the blacklist, the request is dropped, and if the packet is from a graylist, then it is checked if there is a black alarm broadcasted about the sender node. If such an alarm exists, it drops the request else serves the request. Finally, if the sender is from the whitelist, then serves the request. The judgment on nodes depends on the request number received from the node. If it is higher than the major threshold, then it is in the blacklist and a black alarm is broadcasted. If it is higher than the minor threshold, then it is in the graylist and a gray alarm is broadcasted. Otherwise, it is in the whitelist. Four different scenarios were used to test the performance of the algorithm. The results of all scenarios show an almost equal Threshold but a varying in Energy Consumption.

S. Bhalodiya et al. [46] proposed a schema to detect the RREQ flooding attack in MANET. The proposed schema uses a filtering technique to check the RREQ_RATELIMIT for every node. Therefore, whenever a node sends RREQ more than the RREQ_RATELIMIT, then it immediately gets blocked and is considered as a flooder node. The value of RREQ_RATELIMIT is static and equals 10 according to RFC 3561. The results showed an increase in Packet Delivery Ratio (PDR), decrease in End to End Delay, and increase in Throughput comparing to the native AODV under attack.

D. S. Rao et al. [47] proposed a technique to avoid the RREQ flooding attack in MANET. The proposed technique depends on dividing the network into clusters to avoid any RREQ flooding because only cluster head nodes are allowed to broadcast RREQ in the network. Any RREQ that comes from a normal node is dropped. The proposed technique is divided into three phases Join Network, Cluster head election,

and Path cutoff. When a node joins a network in the Join Network phase, it identifies itself and joins the nearest cluster, and then it gets a Unique Identifier (UID). In the second phase, nodes are elected to be a cluster head to control communication between nodes. And in the third phase, when a node receives an RREQ not from a cluster head, then the request is then dropped. The results showed a high Packet Delivery Ratio (PDR) that is almost the same as the native AODV but it also showed a higher Overhead than the native AODV.

V. Vimal et al. [48] developed a technique used to detect and prevent RREQ flooding attack in MANET. The developed technique has a Detection and Prevention mechanisms. In Detection mechanism, the number of neighbor nodes is used to determine the value of the threshold, which is used to detect the malicious node. Any node that sends a number of RREQ more than the threshold is considered as a malicious node and is added to the Blacklist to avoid communicating with it. In Prevention mechanism, neighbor nodes are notified about the malicious node by an alarm packet. To continue the communication normally, routes are modified by replacing any malicious node that forwards packets to destination nodes, with the nearest normal node. The results showed an increase in Packet Delivery Ratio (PDR) up to 95% compared to native AODV under attack and a high Detection Rate of the malicious nodes up to 90%.

S. Jatthap et al. [49] proposed a technique to detect and isolate RREQ Flooding attacker nodes based on their energy. The proposed technique analyzes a node's energy consumption in the network without an attack and then analyzes a node's energy consumption after an attack. The analysis process is performed to determine max and min energy threshold. If the node's energy is equal to or less than the min energy threshold, then the node is dead. And if the sender node has a higher energy

than the max threshold, it is considered as an attacker node and is then added to the Blacklist in order to isolate it and to avoid communication with it. The results showed a lower protocol power consumption, and a lower node power consumption compared to the native AODV under attack.

A. Katal et al. [50] proposed a novel technique to detect and prevent the datagram chunk dropping attack in the network. In datagram chunk attack, the attacker node randomly drops a chunk of datagrams, which has been sent by nodes in the network, and that in turn affects the throughput of the communication between any two nodes in the network. The proposed technique, which is called Cluster Based Datagram Chunk Dropping Detection and Prevention Technique (CBDCDDPT), is based on clustering the network. In each cluster, a head node is elected by the nodes based on the highest energy, and each cluster head node is responsible for finding the optimal path between any nodes that want to communicate in the network. Each intermediate node including the cluster head has a buffer that consists of two fields' chunk_no and chunk_data. After finding the optimal path between nodes, the source node sends the buffer filled with its corresponding values to the cluster head node, which checks the values of each buffer. If the values are different, then this means that the intermediate node has dropped some chunk of the datagrams which in turn means that this intermediate node is an attacker node. After the detection and removal of the attacker node, the discovery process between the source and the destination node starts again. The result of the technique shows an enhancement in terms of throughput.

M. Wazid et al. [51] proposed two techniques that detect the Jellyfish Reorder attack in the network. In Jellyfish Reorder attack, the attacker node reorders the packets sent between the source and the destination node which in turn affects the goodput of the communication between nodes. Both of the following proposed techniques are based

on clustering the network. Generally, all nodes can have the chance to become a cluster head, and the cluster head node is elected based on its effectiveness for example if it has high energy. The first proposed technique is called Cluster Based Intrusion Detection and Prevention Technique (CBIDPT). In this technique, each node has a FIFO buffer that stores each sent packet with its corresponding sequence number. An optimal path between the source and the destination node is found by the cluster node. The source node shares the buffer of each packet with the cluster head, and the cluster head compares the sequence number of each packet with all the intermediate nodes in the path. If any of these nodes has a different sequence number (reordered), then this means that there is an attacker node in the path. Following, the cluster head removes the attacker node from the path and searches for a new path. But this technique fails if the attacker node is a cluster head. The second technique is called Super Cluster Based Intrusion Detection and Prevention Technique (SCBIDPT), in which a super cluster is the group of all clusters in the network and a super cluster node is a node that supervises all the cluster head nodes in the network. When the source node sends packets to the destination node, it then shares its buffer with the super cluster node. The aim of the super cluster node is to check the sequence number of each packet in the cluster head nodes and if there is a different value (reordered), which means that the cluster head node is an attacker node. The super cluster node then removes the attacker node. The results of these two techniques showed a slight increase in term of End to End Delay but it showed an increase in goodput.

The limitation in [41] and [46] is that they depend on a static value as a threshold to detect the attacker node in the network, which should be a dynamic value. The

limitation in [41], [48], [45] and [42] is that an alarm message is broadcasted to normal nodes after the detection of an attacker node in the network, which makes the network vulnerable to a blackmail attack because a blackmail attacker node can broadcast false alarm messages containing normal nodes ids to isolate them from other normal nodes in the network. The limitation in [44] is that the detection of an attacker node depends on the exchange of information about other nodes, which makes the network vulnerable to false information exchange by cooperative attacker nodes. The limitation in [47] is that the proposed model depends on clustering the network to detect the attacker node and it is known that clustering has a high overhead in MANET. That is why some network environments avoid clustering. To avoid false information and blackmailing, the detection of the attacker node should be a self-decision, which we were able to achieve in our proposed model.

Chapter 3 : Black-hole and Flooding Attack effects on MANET

This chapter describes the main parameters that affect the creation of a network scenario and the performance metrics we used to simulate both of the attacks to show how they have a bad effect on MANET. Also, it describes the effects of both Black-hole attack and Flooding attack.

3.1 Experimental Setup

3.1.1 Effect of network size on the network scenario

One of the factors that affect network scenarios is the network size in different terms. Network size means that the actual area of the network along with the number of nodes inside that area. In sparse networks, the number of nodes is few which creates a problem called unreachable destinations especially if the area of the network is big. In sparse networks, nodes are distributed along the network and the chance that all these nodes are connected to each other and all nodes can be reached by other nodes are very low. In some cases, nodes in the sparse network are isolated. Also, if the mobility of nodes is zero (static position), the isolated nodes will never be reached by any other node in the network. In dense networks, nodes are distributed along the network, and almost all nodes can reach other nodes in the network because the number of nodes is big and may cover the whole network area. The chance to have an isolated node in the dense network is very low due to the huge number of nodes that are distributed along the network area. In case that the number of nodes in a dense network, is very big and the area of the network is small, this may create a problem as nodes use wireless links to communicate with each other, and when the number of nodes is big, the chance of interfering between signals gets higher. In addition, some

nodes may not participate in any network activity simply because they are extra nodes, which is a waste of energy. That is why we need to choose a network size that is big in terms of area and has the least number of nodes to cover the whole network. Figure 3.1 shows an example of both sparse and dense networks.

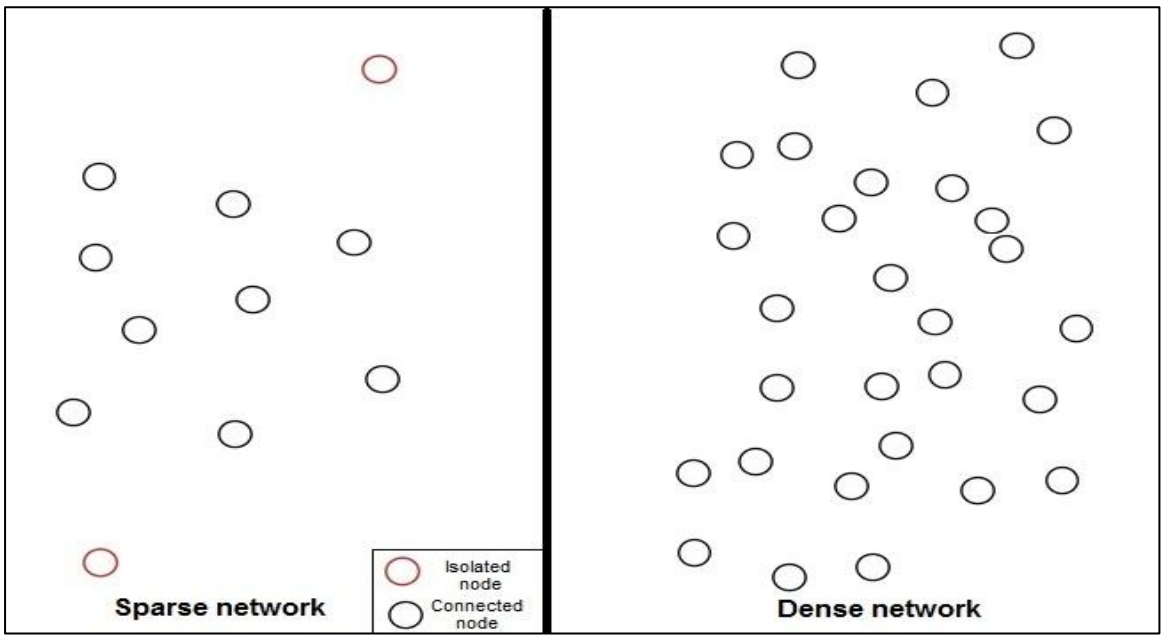

Figure 3.1 Example of Dense and Sparse network.

As shown in Figure 3.1, in sparse network, some nodes may be isolated as the two nodes at the edges of the network. If the mobility of this network is zero (static network), these two nodes will never communicate with any other node in the network. Unlike in the dense network, where the chance of an isolated node is very low. In our experiments, two network sizes 850x850m and 1000x1000m have been selected and the number of nodes in them varies between 20-100 and 25-150 nodes. The reason for choosing these numbers is to show the effect of the attacker node and how the proposed models can overcome these attacks. When the number of nodes is low, the Black-hole attack will have the highest impact because it can almost cut every connection between any two nodes that want to communicate with each other.

When the number of nodes is high, RREQ flooding attack will have the highest impact because all nodes in the network will participate in route discovery for fake nodes and will try to find a path to a node that does not exist in the network.

3.1.2 Effect of nodes mobility on the network scenario

In MANET, nodes are mobile which means that they move in different directions at different speeds. Nodes mobility has a huge impact on network scenarios. There are two types of network in terms of mobility: high mobility and low mobility networks. In high mobility network, nodes in the network are moving very fast which affects the connectivity between nodes because the topology keeps changing in a small period of time. VANET is considered an example of high mobility networks. In low mobility networks, nodes are moving so slow or in an average speed. The topology of low mobility networks is more stable than in high mobility networks. WSN is considered as an example of low mobility network. In our experiment, the random waypoint model was used to simulate the movement of nodes at different speeds. NS-2.35 provides a tool called CMU to create the mobility scenario of nodes. A CMU tool was used to create a random movement of nodes in a closed terrain for a specified simulation time. In order to use CMU tool, “setdest” command is used in the terminal and is provided with the node number, node maximum speed, pause time, simulation time, and network coordination as parameters to create the random scenario file. In CMU tool, the maximum speed parameters need to be defined which means that nodes in the scenario can move at different speeds between zero and the maximum value. For example, if the maximum speed is set to 25 m/s, then nodes will move in different directions at different speeds ranging between 0 to 25. In our experiments, we set the maximum speed to 15 m/s, which is between human and vehicle movement speeds.

Pause time describes the time that the node is supposed to sit in its position before it can moves to another position. For example, if the pause time is set to 5 sec, it means that each node in the scenario will wait 5 sec before moving to another position. In our experiments, we set the pause time to 5 sec.

3.1.3 Performance metrics

There are different performance metrics that can be used to measure the behavior of the protocols in MANET. These metrics can be used to distinguish the difference between protocols and to compare them. We mainly focused on five performance metrics that we considered the most affected metrics when the network is under attack.

Packet Delivery Ratio (PDR): It indicates the ratio of packets successfully received by the destination node to the total number of packets sent from the source node. PDR can be computed using the following formula (1):

$$PDR = \frac{R_{packets}}{S_{packets}} \qquad (1)$$

Where Rpackets is the number of received packets, and Spackets is the number of sent packets.

Throughput: It indicates the rate at which packets are received from the source node over a period of time. Throughput can be computed using the following formula (2):

$$\text{Throughput} = \frac{R_{packets}}{C_{time}} * \frac{8}{1024} \qquad (2)$$

Where $R_{packets}$ is the number of received packets, and C_{time} is the connection time between nodes.

Average End to End Delay: It indicates the average time needed for a packet to be transmitted across the network from the source node to the destination node. End to End Delay can be computed using the following formula (3):

$$Avg_{EtE} = \frac{\sum_{i-1}^{N} Rt_i - St_i}{N} \quad (3)$$

Where N is the number of nodes in the network, R_t is receiving time of packet i and S_t is Send time of packet i.

Average Residual Energy (ARE): It indicates the average of remaining energy in every node in the network. ARE can be computed using the following formula (4):

$$ARE = \frac{R_E}{N} \quad (4)$$

Where R_E is the residual energy, and N is the number of nodes in the network.

Normalized Routing Load (NRL): It indicates the number of routing packets received over the number of packets received at the destination node. NRL can be computed using the following formula (5):

$$NRL = \frac{Rt_{packets}}{R_{packets}} \quad (5)$$

Where $Rt_{packets}$ is the number of routing packets and $R_{packets}$ is is the number of received packets at the destination node.

In our experimental study, we a used NS-2.35 simulator that is installed on Ubuntu operating system version 14 over VMware Workstation 10.0.2 build-1744117, CPU i5-2450 2.50 GHz, 4GB RAM. We used the NS2 visual trace analyzer version 0.2.72, AWK script, and perl script, to analyze the trace file that is generated after the execution of the NS-2.35 program.

3.2 Attacks effects

This section shows the effects of each attack on the performance metrics. In order to study the attack's effect on the network, we varied the number of nodes in the network at a constant speed of 15 m/s and a constant pause time of 5 sec. For Black-hole attack, the number of nodes varies between 25-150 nodes in 1000x1000m network area size. For RREQ flooding attack, the number of nodes varies between 20-80 nodes in 850x850m network area size. In order to obtain the highest impact on the network the initial position of the attacker node was in the middle of the network. There is one CBR connection between the source and the destination node. The initial position of the source and the destination nodes was at the edges of the network in order to hold as many nodes as possible to forward packets between the source and destination nodes. The creation of network scenarios was done using CMU tool. The scenario's time was set to 200 sec which we believe was fair enough to study the protocols.

3.2.1 Effects of a single Black-hole attack on some performance metrics

We compared the performance of native AODV under Black-hole attack using three performance metrics End to End Delay, Throughput, and PDR, which are considered the most affected parameters under Black-hole attack in AODV according to [52]. In this experiment, there is only a single attacker node in the network. The parameters of the environment are summarized in Table 3.1.

Table 3.1: Simulation environment parameters for a single Black-hole node.

Simulation Environment Parameters for a single Black-hole node	
Speed	Maximum 15 m/s
Pause Time	5s
Simulation Time	200s

Coordination	1000*1000 m
Connection	CBR (Constant Bit Rate) Item size 512(Byte)
Radio type	802.11b Radio
Data rate	0.5 Mbps
MAC Protocol	802.11
Routing Protocol	AODV
Transport Protocol	UDP
Node Number	25,50,100, and 150
Node Placement	Random
Transmission range	150 m

3.2.1.A Throughput

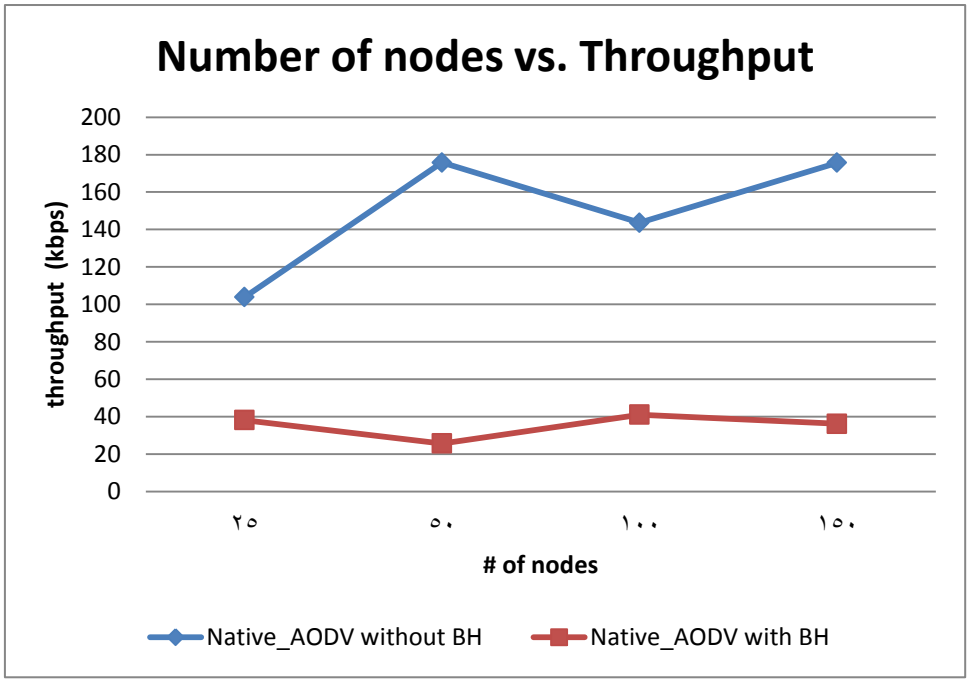

Figure 3.2 Number of nodes vs. throughput for the single Black-hole node.

As shown in Figure 3.2, throughput in native AODV showed a very low result under Black-hole attack because the Black-hole node aims to cut every connection in the

network and tries to absorb all packets. The Black-hole node keeps replying to all requests that come to it, and keeps pretending to have the shortest and freshest path to the desired node. As we can see from the figure, the results look almost the same and the lowest throughput value was when the number of nodes equals 50. The position of the Black-hole node plays a big role if the Black-hole node was in the center of the network and two nodes on opposite edges want to communicate the Black-hole node will then indeed cut this connection. Referring to section 3.1.3, we knew that throughput depends on the number of the received packets at the destination node in the network. Since the Black-hole node does not forward packets to the destination node and it keeps dropping the forwarded packets to it, throughput is one of the most affected performance metrics by the Black-hole attack.

3.2.1.B End to End Delay

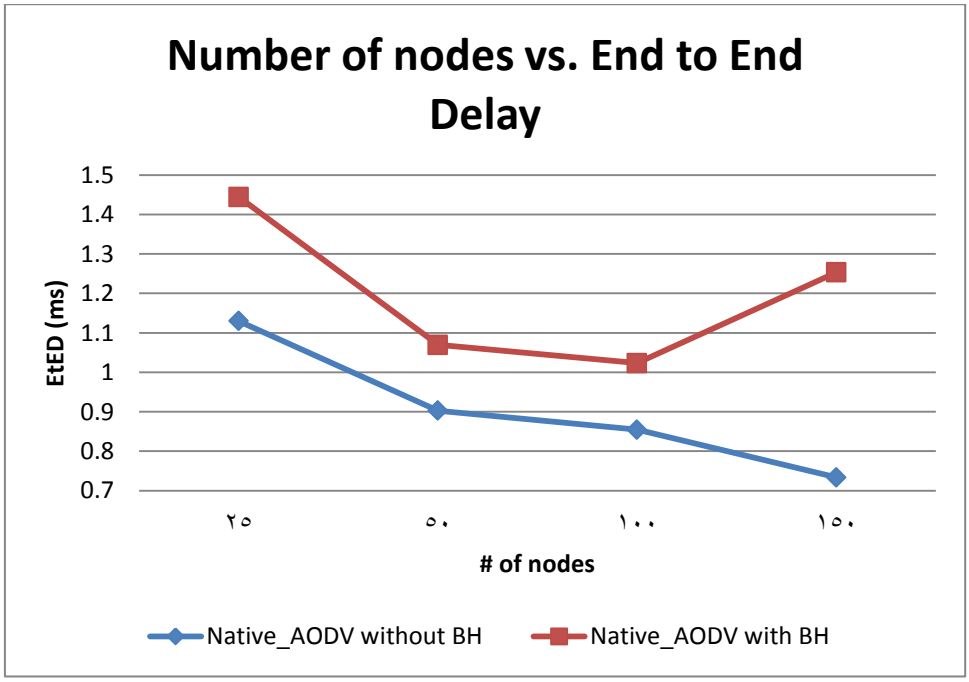

Figure 3.3 Number of nodes vs. end to end delay for the single Black-hole node.

As shown in Figure 3.3, the result of end to end delay was very high when Native AODV is under the attack of a Black-hole node. As known, Native AODV always try

to find the shortest path to any desired node in the network by depending on the least number of hops to reach the desired node. The Black-hole node keeps preventing the communication between nodes in the network and the only way that these nodes can communicate is by taking a longer path than the shortest one. The distance (number of hops) affects End to End delay value as the least number of hops means lower End to End delay values. As shown in the above figure, the result of end to end delay when Native AODV is under the attack was highest when the number of nodes equals 25 because the network is sparse and there are a few paths to the destination node.

4.2.1.C Packet Delivery Ratio (PDR)

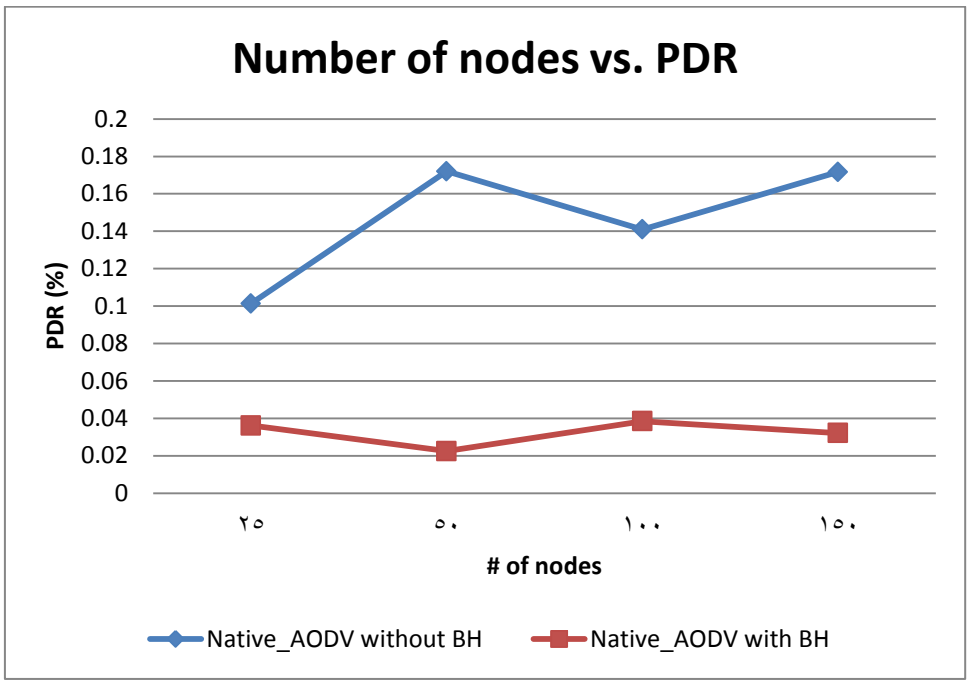

Figure 3.4 Number of nodes vs. PDR for the single Black-hole node.

As shown in Figure 3.4, the result of PDR was very close to zero when Native AODV is under the attack of a Black-hole node. The reason behind this is that the Black-hole node always aims to cut the connection between any two nodes that tries to communicate in the network and try to absorb all packets between them. The Black-hole node keeps replying to all requests, telling nodes that it has the freshest and shortest path to the desired node. As we can see in the figure the results look almost

the same and the lowest PDR value was when the number of nodes equaled 50. The Black-hole node keeps absorbing packets in the network and drops them. That is the reason why PDR is also one of the most affected performance metrics by the Black-hole attack. Table 3.2 shows the numeric results of a single Black-hole attack on native AODV in terms of Throughput, End to End Delay, and PDF.

Table 3.2: Numeric results of a single Black-hole node attack.

Number of nodes	Native_AODV Without BH	Native_AODV With BH
Throughput (kbps)		
25	103.835	38.162
50	175.736	25.644
100	143.648	41.051
150	175.689	36.148
Avg of End to End Delay (ms)		
25	1.130	1.444
50	0.902	1.069
100	0.854	1.023
150	0.733	1.253
Packet Delivery Ratio (%)		
25	0.101352	0.036153
50	0.172043	0.022453
100	0.140977	0.038482
150	0.171634	0.032198

This section showed the huge impact of a single Black-hole node in the network. The attack showed a significant decrease in the throughput and PDR values and an increase in End to End Delay values.

3.2.2 Effects of cooperative Black-hole attack on some performance metrics

We compared the performance of native AODV under cooperative Black-hole attack in three performance metrics: End to End Delay, Throughput, and PDR. In this experiment, there are multiple attacker nodes in the network, the parameters of the environment are summarized in Table 3.3.

Table 3.3: Simulation environment parameters for Cooperative Black-hole nodes.

Simulation Environment Parameters for Cooperative Black-hole nodes	
Speed	Maximum 15 m/s
Pause Time	5s
Simulation Time	200s
Coordination	1000*1000 m
Connection	CBR (Constant Bit Rate) Item size 512(byte)
Radio type	802.11b Radio
Data rate	0.5 Mbps
MAC Protocol	802.11
Routing Protocol	AODV
Transport Protocol	UDP
Node Number	50
Node Placement	Random
Transmission range	150 m
Black Hole Nodes	2,4,8 & 10

3.2.2.A Throughput

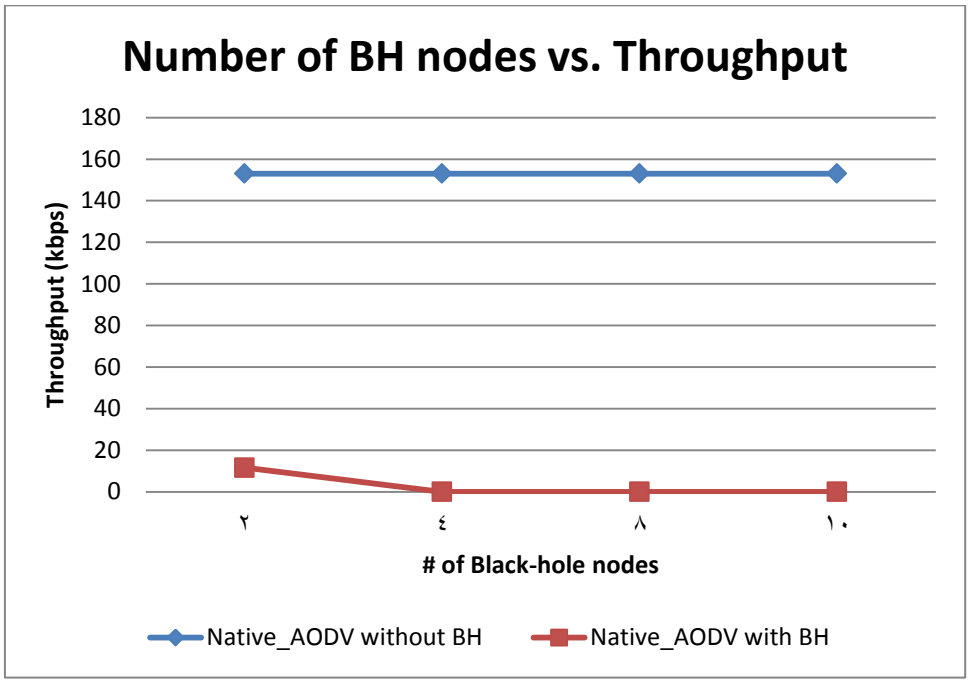

Figure 3.5 Number of BH nodes vs. Throughput.

As shown in Figure 3.5, throughput values reached zero when there were 4 to 10 Black-hole nodes in the network because Black-hole nodes work together to cut any communication in the network. The positions of Black-hole nodes play a big rule because each node can cut any connection within its coverage, and if these Black-hole nodes are distributed along the network and each one of them covers a sector of the network, then there will be zero connection between any two nodes in the network that want to communicate. This figure shows the danger of the Cooperative Black-hole node attack on the network and how they can kill the network and prevent any connection to happen. Also, Cooperative Black-hole nodes can work together to avoid being revealed as attacker nodes to the network. A large number of techniques depend on neighbor nodes decision to detect the Black-hole node in the network and in this case, a Cooperative Black-hole node may work together to isolate a normal node or to

avoid being revealed. In our proposed model, we depend on self-decision instead of neighbor-decision in judging any node in the network.

3.2.2.B End to End Delay

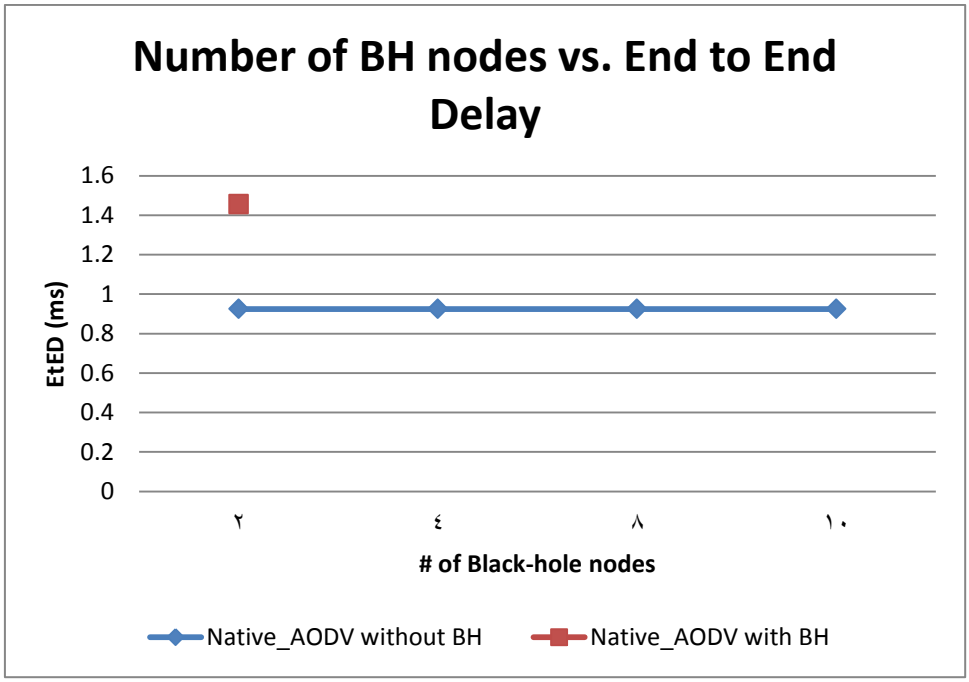

Figure 3.6 Number of BH nodes vs. End to End Delay.

As shown in Figure 3.6, end to end delay values reached infinity when there were 4 to 10 Black-hole nodes in the network because Black-hole nodes work together to cut any communication in the network, and when there is no connection between nodes, it means the time between these connections is infinite. And since there is no connection between the source and destination nodes, then the time is infinite. This figure also shows the danger of the Cooperative Black-hole node attack on the network and how it can kill the network and prevent any connection to happen. Some QoS in networks aim to obtain the lowest End to End Delay which so far has been impossible in the present of Cooperative Black-hole but this shows the need to create a method to detect the attacker nodes in the network and isolate them.

3.4.2.C Packet Delivery Ratio (PDR)

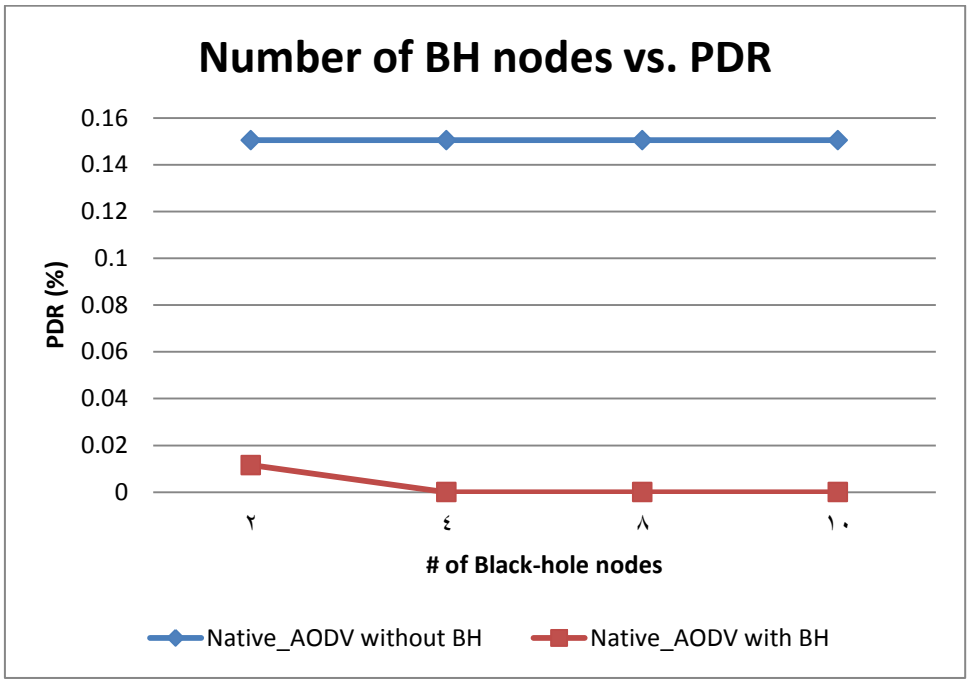

Figure 3.7 Number of BH nodes vs. PDR.

As shown in Figure 3.7, PDR values reached zero when there were 4 to 10 Black-hole nodes in the network because of the cut in the connection between any two nodes in the network which is caused by the Cooperative Black-hole nodes. As in throughput, the positions of Black-hole nodes play a big role, and if Black-hole nodes are distributed to cover the entire network, then there will be no connection between any two nodes that want to communicate. This figure also shows the dangers of the Cooperative Black-hole node attack on the network and how they can kill the network and prevent any connection to happen.

Cooperative Black-hole attack has a higher impact comparing to a single Black-hole node because in a single Black-hole attack the source and the destination node may communicate, but in Cooperative Black-hole they cannot communicate at all. In Cooperative Black-hole attack, nodes coverage the entire network so there will be zero connection between any two nodes in the network. Table 3.4 shows the numeric

results of Cooperative Black-hole attack on native AODV in terms of Throughput, End to End Delay, and PDF.

Table 3.4: Numeric results for Cooperative Black-hole attack.

Number BH nodes	Native_AODV Without BH	Native_AODV With BH
Throughput (kbps)		
2	153.044	11.651
4	153.044	0
8	153.044	0
10	153.044	0
Avg of End to End Delay (ms)		
2	0.925	1.455
4	0.925	∞
8	0.925	∞
10	0.925	∞
Packet Delivery Ratio (PDR)		
2	0.150456	0.011572
4	0.150456	0
8	0.150456	0
10	0.150456	0

In section 3.2.1 and 3.2.2, we showed the effects of the Black-hole attack on the network and we showed the effects of the attack on some of the performance metrics. This leads us to the need of developing a model that can detect the Black-hole nodes in the network and isolate them.

3.2.3 Effects of RREQ flooding attack on some performance metrics

Flooding attack is a type of Denial of Service (DoS) attack that floods the network with the protocol main messages in order to affect the network operation and to consume the nodes' energy. In this experiment, we implemented RREQ flooding attack. According to [53] , any normal node in the network can send up to 10 RREQ in a sec. So, the attacker node in the network is going to send more than 10 RREQ per second for different nodes ID that does not exist in the network. We compared the performance of native AODV under RREQ flooding attack in five performance

metrics End to End Delay, Throughput, Packet Delivery Ratio, Normalized Route Loading (NRL) and Average Residual Energy (ARE), at two different intervals 0.1 and 0.02. The parameters of the environment are summarized in Table 3.5.

Table 3.5: Simulation Environment Parameters for RREQ flooding attack.

Simulation Environment Parameters for RREQ flooding attack	
Speed	Maximum 15 m/s
Pause Time	5s
Simulation Time	200s
Coordination	850*850 m
Connection	CBR (Constant Bit Rate) Item size 512(byte)
Radio type	802.11b Radio
Data rate	0.5 Mbps
MAC Protocol	802.11
Routing Protocol	AODV
Transport Protocol	UDP
Node Number	20,40,60, and 80
Node Placement	Random
Transmission range	150 m
Sending interval	0.1 and 0.02

3.2.3.A Throughput

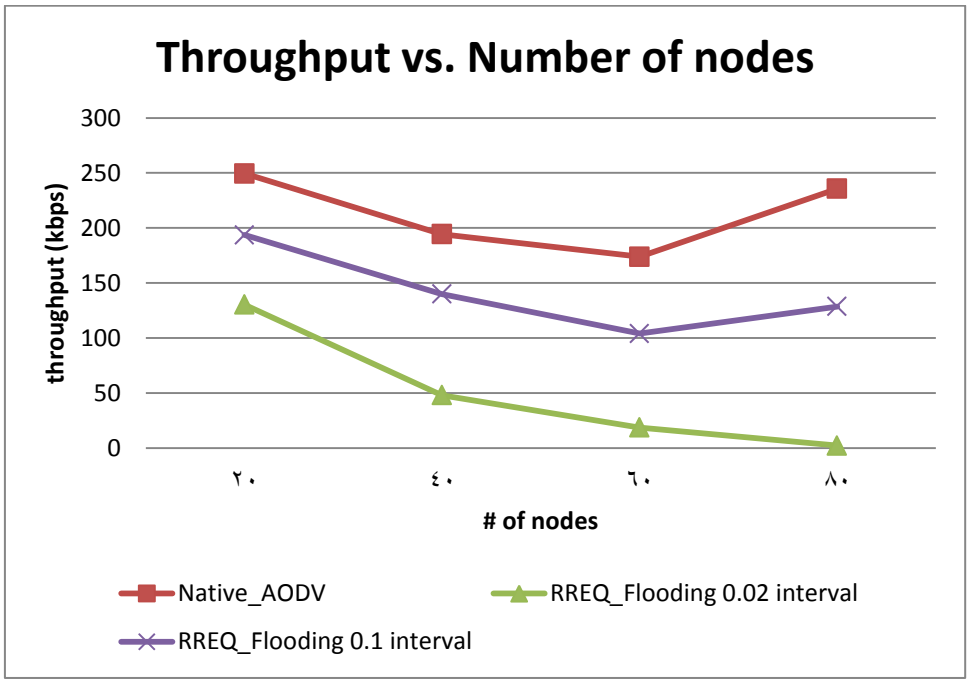

Figure 3.8 Throughput vs. Number of nodes in RREQ flooding attack.

As shown in Figure 3.8, throughput values decrease when the native AODV is under RREQ flooding attack. Throughput values keep decreasing while the number of nodes is increasing because there will be more normal nodes in the network that rebroadcast the fake requests hoping to find paths to nodes that do not exist in the network. When the interval was 0.1, which means that the attacker node sends 10 fake requests per second for different fake nodes' IDs in the network, the effect of the attack was less than when the interval was 0.02, which means that the attacker node sends 20 fake requests per second. The reason is obvious because the normal node will rebroadcast more fake requests which will lead to congesting the network with the fake request. Throughput value was the lowest when the number of nodes equaled 80 and the sending interval was equal to 0.02. But since the network is congested with the fake request, the number of the received packets at the destination node will be decreased, which will lead to a decrease in the throughput.

3.2.3.B End to End Delay

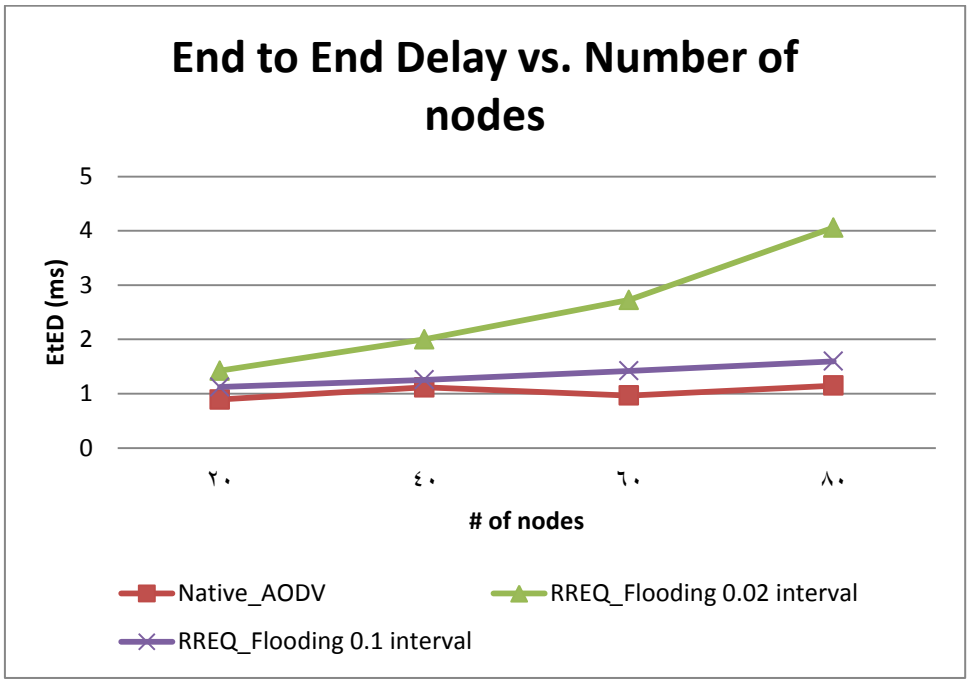

Figure 3.9 End to End Delay vs. Number of nodes in RREQ flooding attack.

As shown in Figure 3.9, the values of end to end delay were higher when the native AODV is under attack especially when the sending interval was 0.02. The RREQ flooding attacker node keeps broadcasting requests for fake IDs that do not exist in the network and normal nodes keep rebroadcasting these requests. Because of the rebroadcasting process by the normal nodes, the network will get congested which will indeed delay the arrival of normal packets. And since the network is congested, the end to end delay will increase because there is a delay in delivering packets to the destination node. The End to End Delay value was the lowest when the number of nodes equaled 80 and the sending interval was 0.02. This experiment shows that the huge effect of the RREQ flooding attack on the network and on the end to end delay parameter especially when the sending interval was 0.02.

3.2.3.C Packet Delivery Ratio (PDR)

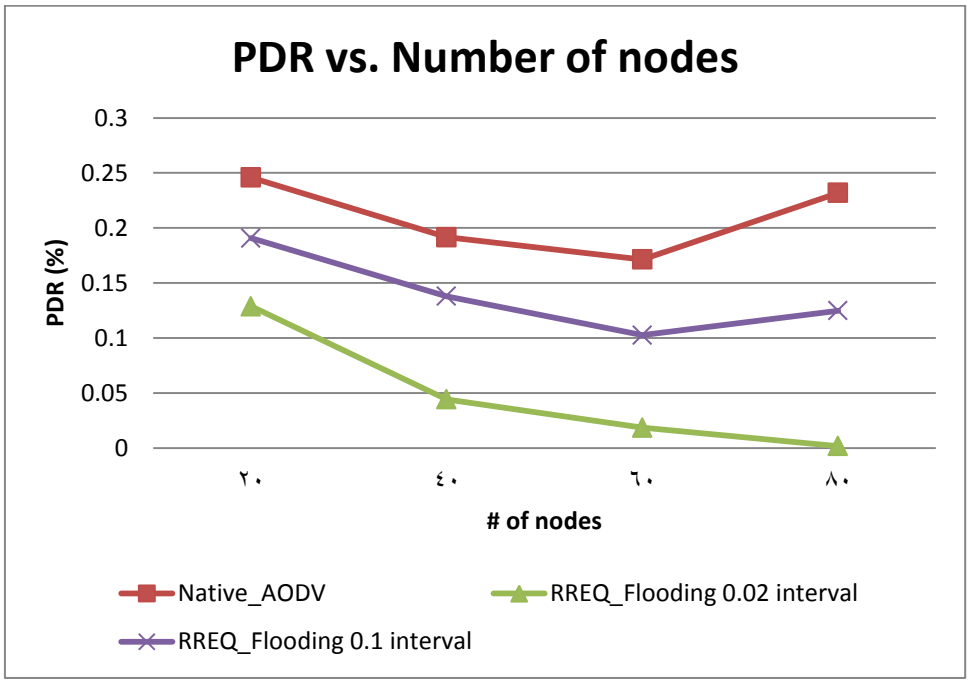

Figure 3.10 PDR vs. Number of nodes in RREQ flooding attack.

As shown in Figure 3.10, the values of PDR decrease while the number of nodes increases when the native AODV is under RREQ flooding attack because there will be more nodes involved in the retroacting process of fake requests in the network which indeed is going to congest the network. And because the network is congested with fake requests and nodes are busy in processing requests packets the number of packets received at the destination will decrease. As shown in the figure the lowest PDR which almost reached zero was when the number of nodes was equal 80 and the sending interval equal 0.02. This figure also shows the huge impact of RREQ flooding attack on the network.

3.2.3.D Average Residual Energy (ARE)

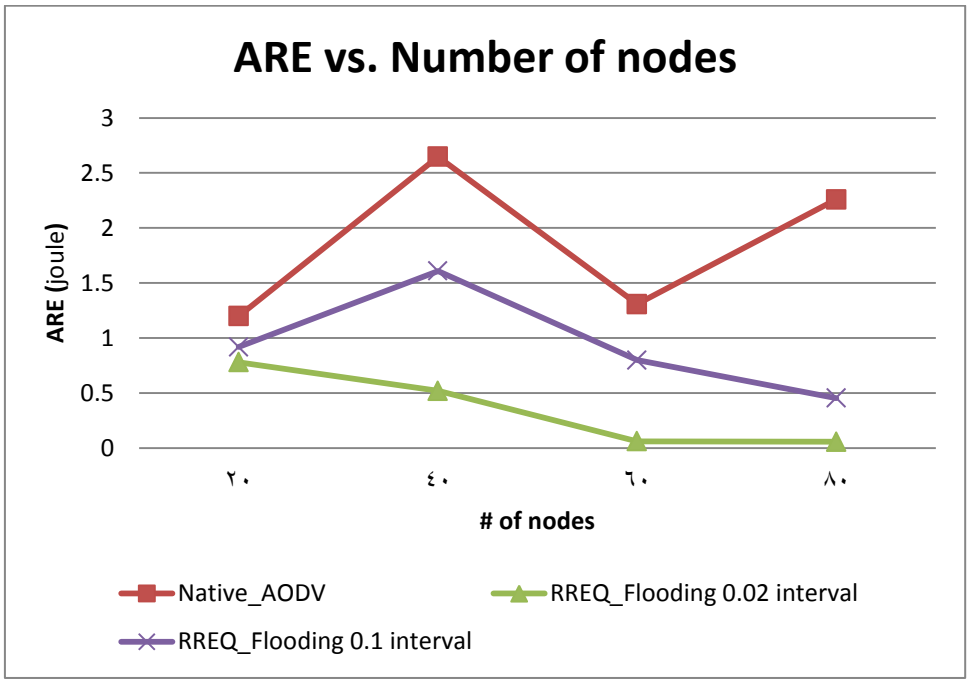

Figure 3.11 ARE vs. Number of nodes in RREQ flooding attack.

As shown in Figure 3.11, the values of ARE decreases while the number of nodes increases when the native AODV is under RREQ flooding attack. As we know, the flooding attack aims to consume the nodes' resources in the network, especially their energy. When nodes are busy in rebroadcasting fake request all the time then nodes will consume more energy, which will kill the nodes after a period of time. Referring to section 3.1.3, we knew that ARE depends on the left energy in nodes and because nodes are busy all the time in the rebroadcasting process this will lead to reducing the energy left in the nodes. As shown in the figure the lowest ARE was when the number of nodes equaled 80 and the sending interval 0.02. ARE almost reached zero (dead nodes) at that point. RREQ flooding attack has a huge impact on the network resources and it indeed consumes a lot of the nodes energy, which leads us to the need of developing a model to resist this type of attack that may kill the network after a small period of time.

3.2.3.E Normalized Route Loading (NRL)

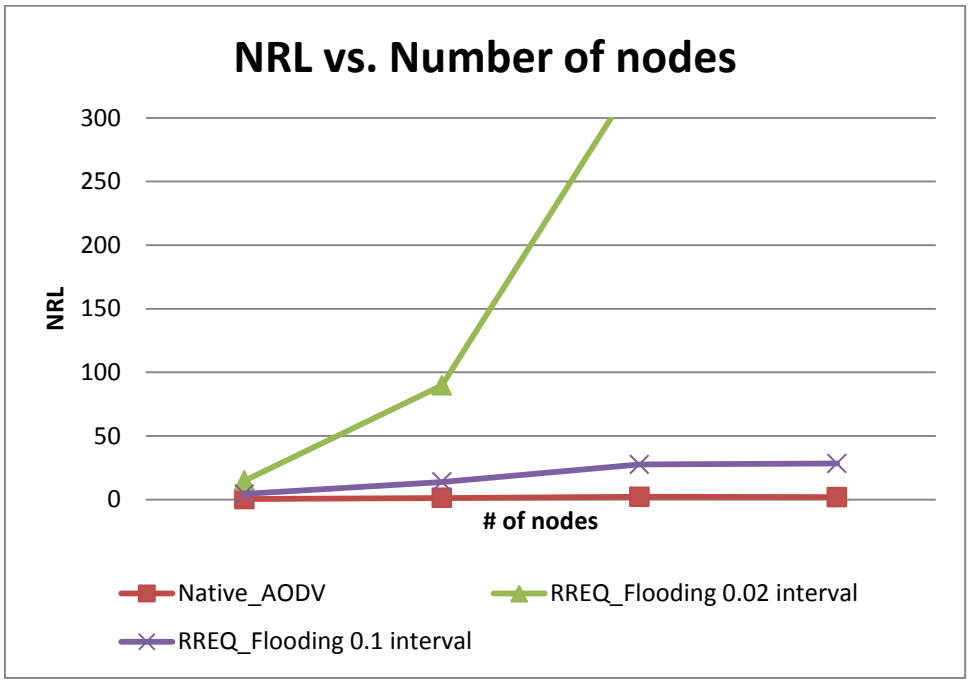

Figure 3.12 NRL vs. Number of nodes in RREQ flooding attack.

As shown in Figure 3.12, the results of NRL were increasing when the number of nodes increased when native AODV is under RREQ flooding attack. And NRL depends on the number of routing packets. In RREQ flooding attack, the attacker nodes keep flooding the network with a fake request, which is going to increase NRL. Normal nodes in the network will rebroadcast fake requests, which are also going to increase NRL. Indeed, when the sending interval was 0.02 the NRL showed higher values because the attacker node sends up to 50 requests per second. As shown, the highest value of NRL was when the number of nodes equaled 80 and the sending interval equaled 0.02. NRL is a good indicator that gives information about the number of nodes that need to create a connection between nodes in the network, and the number of packets needs to control the network. RREQ flooding attack has the highest impact on this parameter because it uses protocol main messages to congest the network. after considering this study of the RREQ flooding attack and how its affect five different performance metrics, it leads us to the importance of developing a

model that is capable of detecting an attacker node in the network and to isolate it and stop the communication with it. Table 3.6 shows the numeric results of RREQ flooding attack on native AODV in terms of Throughput, End to End Delay, PDF, ARE, and NRL.

Table 3.6 numeric results for RREQ flooding attack.

Number of nodes	Native_AODV Without RREQ flooding	Native_AODV With RREQ flooding 0.1	Native_AODV With RREQ flooding 0.02
Throughput (kbps)			
20	249.471	193.570	130.320
40	194.311	139.928	47.9578
60	173.781	103.954	18.6164
80	235.645	128.526	2.18280
Avg of End to End Delay (ms)			
20	0.891	1.120	1.422
40	1.117	1.256	2.001
60	0.965	1.418	2.726
80	1.149	1.598	4.059
Packet Delivery Ratio (%)			
20	0.245858	0.190766	0.128768
40	0.191497	0.137901	0.044203
60	0.171276	0.102445	0.018344
80	0.231931	0.124770	0.001631
Average Residual Energy (Joule)			
20	1.19772	0.917236	0.779448
40	2.64692	1.608950	0.518297
60	1.30768	0.798406	0.060380
80	2.25959	0.453798	0.055810
Normalized Route Loading (NRL)			
20	0.42	4.43	14.9
40	1.26	13.83	89.7
60	2.19	27.56	335.69
80	1.9	28.27	486.66

3.3 Conclusions

In this chapter, we simulated both Black-hole and RREQ flooding attacks and showed their effects on the network. The Black-hole attack has two forms: single and cooperative. In single Black-hole attack, there is only a single attacker node in the network. In cooperative Black-hole attack, there are multiple attacker nodes in the

network that aim to kill the network. In our experiments, we showed how both of these attacks can kill the network and prevent any connection in it, especially in the cooperative Black-hole attack when the number of nodes was between 4 and 10, the result became obvious as there was no connection between the source and the destination nodes. Our experiments showed that the reason behind the need for a model that is capable of detecting the Black-hole attacker node in the network and to isolate it. We said in previous chapters that we are going to deal with a Smart Black-hole node, which is capable of countering some of the developed model, and in the new chapter, we will present our model that is capable of detecting single and cooperative Smart Black-hole attack in the network. In this chapter, we also showed that the effect of RREQ flooding attack in two different sending intervals. When the sending interval was 0.02 the attacker node had a huge impact on the network, especially when the network was dense. In our experiment, we showed how RREQ flooding attack affects the network in five different performances metrics and how this attack consumes nodes resources. Also, our experiment showed that the reason behind the need for creating a model that is capable of detecting the attacker node and isolating it. Next, we will introduce two models one for resisting Black-hole attack and the second one to resist RREQ flooding attack in the network.

Chapter 4 : Timer Based Detection Technique (TBBT)

The previous chapter showed how both Black-hole and RREQ flooding attack have a huge impact on the network performance and how, in some scenarios, they may prevent the connection between any two nodes in the network as in cooperative Black-hole attack. This chapter presents a new algorithm that is developed to resist Smart Black-hole attack in two forms: single attacker node and cooperative attack nodes. The chapter also shows how our model can handle the Smart Black-hole attack and includes a comparison of the overall performance of the proposed model with other proposed models in order to prove its efficiency.

4.1 TBBT model description

In the proposed model, a fake ID baiting technique was used to bait Black-hole nodes in the network. Fake node ID technique is hard to counter by the Black-hole node because the Black-hole node does not know all the IDs of nodes in the network. The Black-hole node response to any request which makes this technique harder to counter. The proposed technique is developed to resist Smart Black-hole attacks by employing timers and baiting messages. The proposed technique consists of two phases: Baiting and Non-Neighbor Reply. In Baiting phase, each node has a bait-timer, and the value of the timer is set randomly to B seconds. When the timer reaches B, it creates and broadcasts a bait request with a randomly generated fake ID. When the Black-hole receives the baited request, it sends a reply to the source node, claiming to have a route. When the source node receives the reply, it immediately considers the node which responded as a Black-hole and adds it to the Black list. In the bait request, the value of TTL (Time-To-live) is set to one in order to avoid congesting the network with fake requests. As in a native AODV when any node

wants to communicate with another in the network, it broadcasts RREQ to the destination node. In Non-Neighbor Reply phase, each node knows its adjacent nodes because of the Hello message broadcasting process. When the source node receives a reply, it checks the ID of the Node With the Shortest Path (NWSP), and if it is in the Black-hole list, it then discards the reply. Otherwise if the ID exists in the neighbor's list by comparing the ID with those ones in the neighbor's list. If NWSP is not a neighbor node, then the source node discards that reply to avoid any communication with unknown nodes. The proposed technique provides a self-detection and isolation for any Black-hole node which enables the connectivity between MANET nodes. The suggested technique does not use the Black-hole alarm in order to prevent any Smart Black-hole node from using this feature by broadcasting false alarms. We set the TTL of the bait request to one to avoid congesting the network by a bait requests and responds. The randomness in both fake ID and Bait-timer will prevent the Black-hole node from identifying any pattern to counter this technique. No overhead or special packets are used which makes it a light-weight technique.

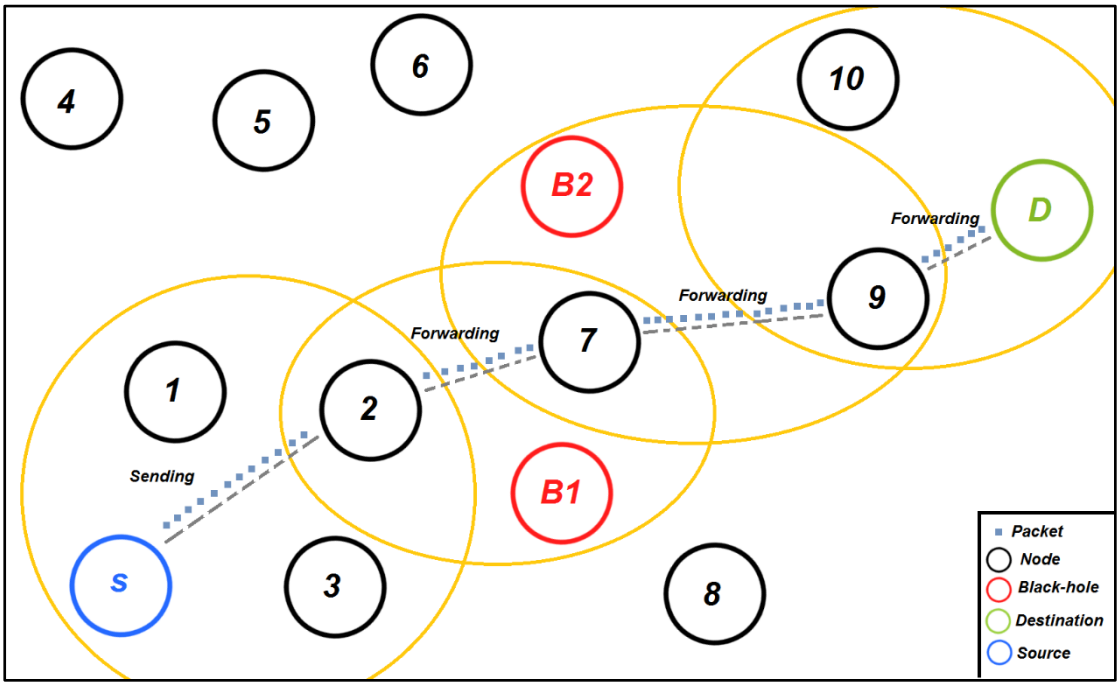

Figure 4.1 Sketch of Black- holes and baiting request

As shown in Figure 4.1, each node broadcasts hello messages to identify itself to adjacent nodes. In Baiting phase, each node creates a bait request with a random fake ID and with a TTL equal to 1 and then broadcasts the bait requests to all its adjacent nodes. Both Black-hole nodes B1 and B2 will reply to the bait request. Nodes 2, 7 and 8 will add node B1 to their Black-hole list because node B1 replied to each bait coming from 2, 7 and 8 based on the natural behavior of the Black-hole node, replying to each request even if it does not have an existing route for the desired node. Node 6, 7, 9 and 10 will add B2 to their Black-hole list because node B2 also replied for each bait request that came from 6, 7, 9 and 10. Each node resets a Bait-timer with random B sec. When S wants to communicate with node D, it broadcasts RREQ and node 2 sends RREP, claiming it has the best path. Node S then checks if node 2 exits in its neighbor list or not and since node 2 is in the coverage of node S, node 2 is in the neighbor list and node S starts to transmit data through 2 to D. The algorithms of the proposed model, which we call it TBBT_AODV, are described using a pseudo code.

Algorithm 1: Baiting phase

```
Begin
If (CurrentTime == Bait_Time) Then
    Create Bait request;
    Generate a random ID and  Set it in Bait request;
    Set TTL of Bait request to 1;  // TTL (Time-To-Live)
    Broadcast Bait request;
    Reset Bait-time;
 End if
  Foreach (received Reply to the Bait request) Do
   Store node ID in the Black-hole list; End for
End
```

Algorithm 2: Non-Neighbor Reply phase

```
Begin
Broadcast request to the Destination node as native  AODV;
  Foreach (received Reply to the Destination node request) Do
     If (NWSP in the Black-hole list) Then // NWSP (Node With the
Shortest Path)
```

```
    Discard reply;
  End if
  If  (NWSP not in neighbor list && Not from Destination node) Then
    Discard reply;
 End if
 Else
  Continue as native AODV and start transmitting   packets to the
Destination node;
 End else
End for
End
```

The Figure 4.2 shows the diagram of the proposed system model and how each algorithm works in order to detect the Black-hole attack in the network.

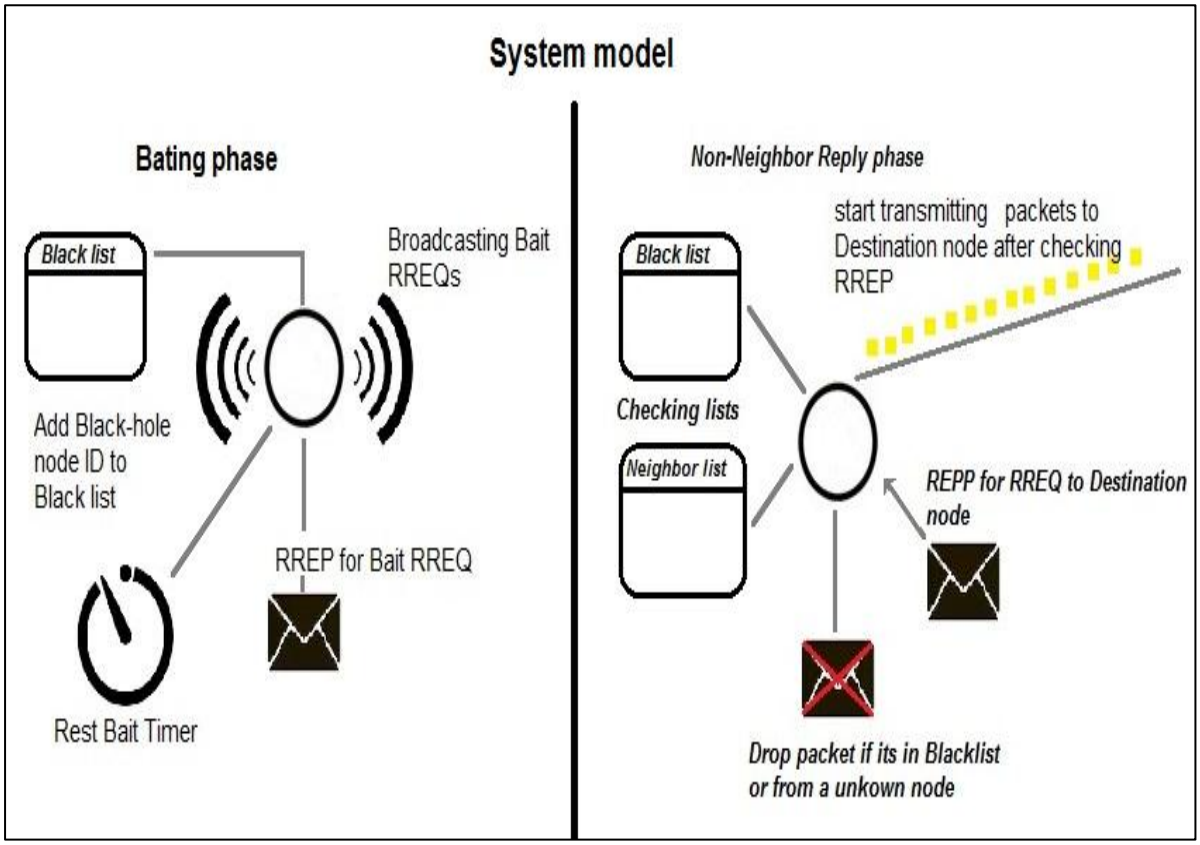

Figure 4.2 TBBT_AODV system model.

4.2 TBBT simulation and results

This section tests the new proposed model against Black-hole attack (TBBT_AODV). The simulation parameter are the same as in Table 3.1 for a single Black-hole attack

and as in Table 3.3 for the cooperative Black-hole attack. TBBT is tested under three different performance metrics: Throughput, End-to-End Delay, and Packet Delivery Ratio.

4.2.1 Single Black-hole attack

4.2.1.A Throughput of TBBT_AODV under a single Black-hole attack

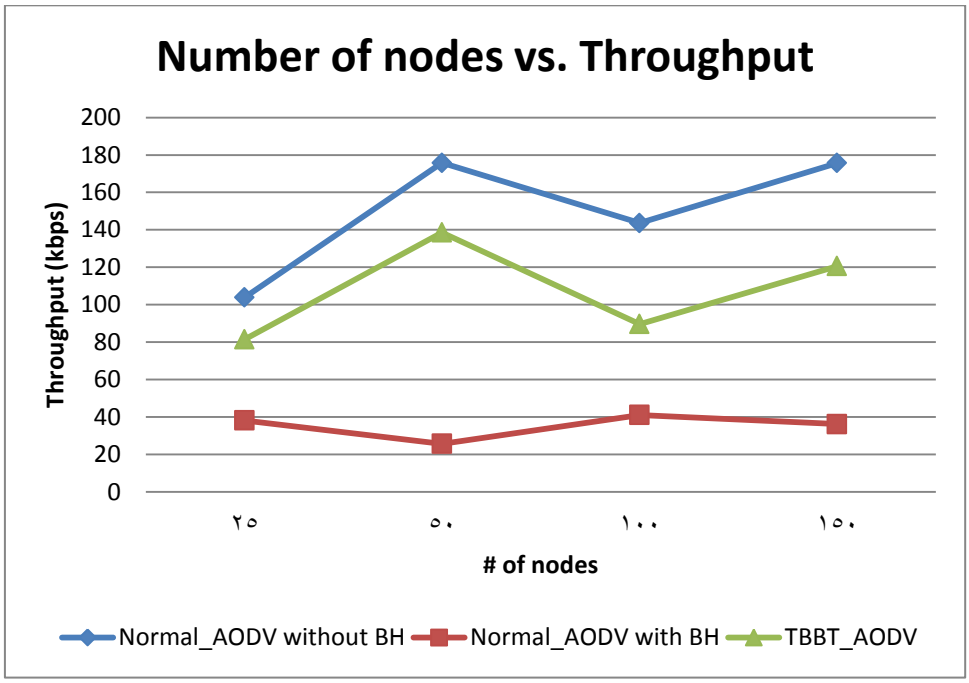

Figure 4.3 TBBT results in terms of Throughput vs. the number of nodes under a single Black-hole attack.

As shown in figure 4.3, the result of Throughput in native AODV when there is a Black-hole node in the network was the lowest because of the packet dropping caused by the Black-hole node. The result of Throughput in native AODV when there is no Black-hole node in the network was the highest. Looking at the results of TBBT, a higher throughput than native AODV when there is a Black-hole node can be seen, but it is lower than native AODV when there is no Black-hole node in the network. The throughput enhancement of suggested TBBT is due to the dropping of any replies from unknown nodes that claim to have a shorter path than any other nodes to the destination node, which leads to decreasing the throughput. In addition, the position

of the Black-hole node plays an important role as it may be located in the shortest path between the source and destination.

4.2.1.B End to End Delay of TBBT_AODV under a single Black-hole attack

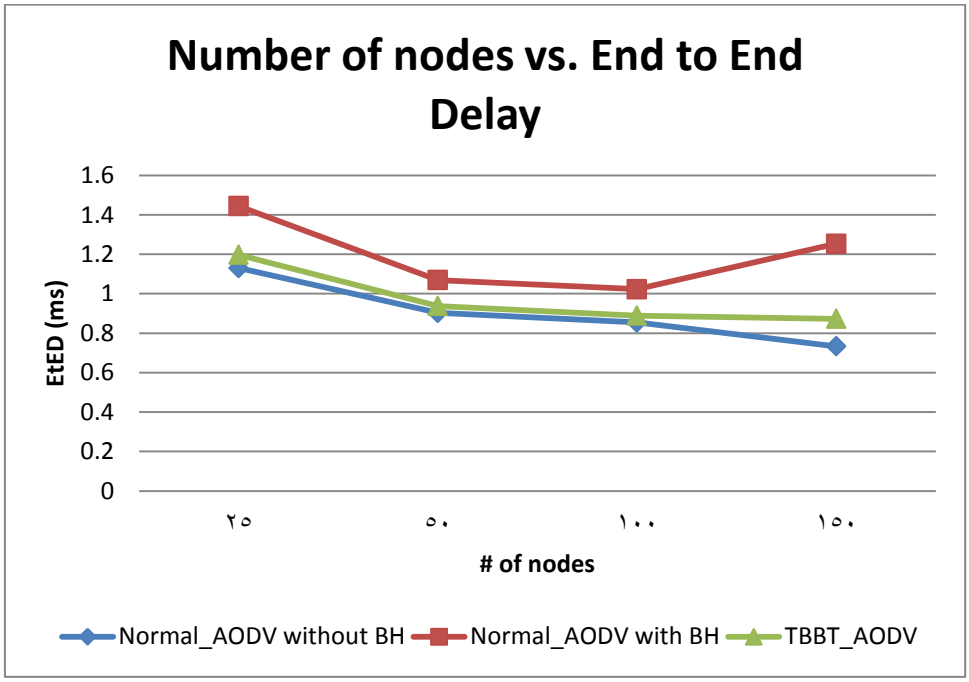

Figure 4.4 TBBT results in terms of End to End Delay vs. the number of nodes under a single Black-hole attack.

As shown in figure 4.4, the result of End to End Delay in native AODV was the highest when there is a Black-hole node in the network. The result of End to End Delay in native AODV was the lowest when there is no Black-hole node in the network because of the AODV mechanism in selecting the shortest path. The results of TBBT showed a slight difference in End to End Delay results compared with native AODV when there is no Black-hole node, and this is because of the path selection mechanism in TBBT which remains the same as in native AODV.

4.2.1.C Packet Delivery Ratio of TBBT_AODV under a single Black-hole attack

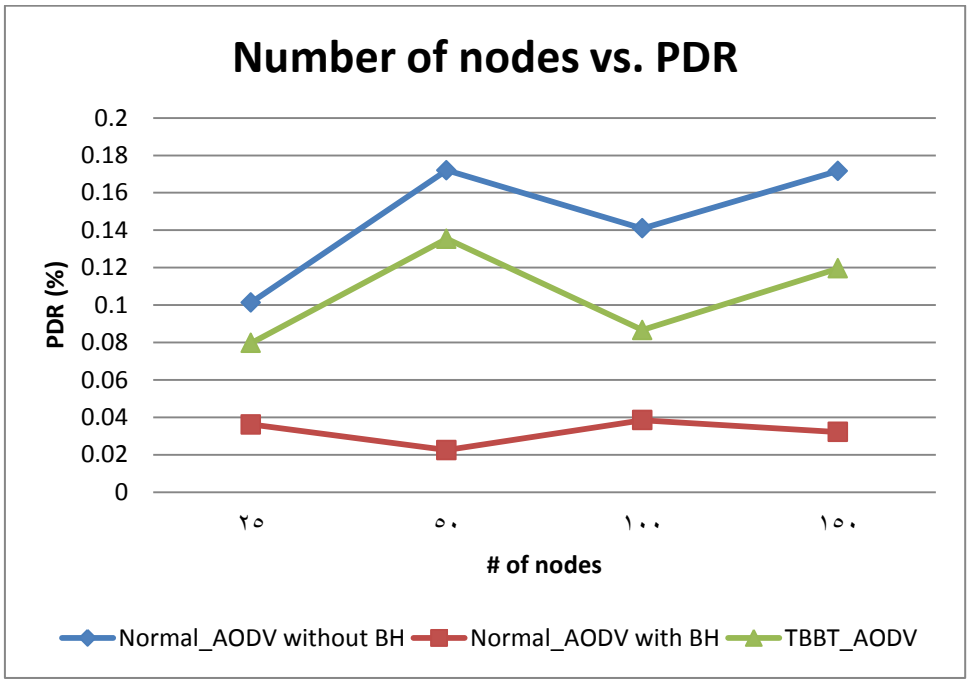

Figure 4.5 TBBT results in terms of PDR vs. the number of nodes under a single Black-hole attack.

As shown in figure 4.5, the result of PDR in native AODV was very low (near zero) when there was a Black-hole node in the network because a Black-hole node always aims to cut the connection between any two nodes that try to communicate in the network and tries to absorb all packets between them. The result of PDR in native AODV was the highest when there is no Black-hole node in the network. Looking at the results of TBBT, it can be seen that the PDR is higher than native AODV when there is a Black-hole node but lower than native AODV when there is no Black-hole node in the network. The PDR enhancement of suggested TBBT is because of the dropping of any reply that is from an unknown node which decreases PDR. Table 4.1 shows the numeric results of TBBT in terms of Throughput, the average of End to End Delay and Packet Delivery Ratio while the numbers of nodes increases.

Table 4.1 Numeric results of TBBT for a single Black-hole node

Number of nodes	Native_AODV Without BH	Native_AODV With BH	TBBT_AODV
	Throughput (kbps)		
25	103.835	38.162	81.388
50	175.736	25.644	138.527
100	143.648	41.051	89.642
150	175.689	36.148	120.600
	Avg of End to End Delay (ms)		
25	1.130	1.444	1.197
50	0.902	1.069	0.938
100	0.854	1.023	0.889
150	0.733	1.253	0.873
	Packet Delivery Ratio (PDR)		
25	0.101352	0.036153	0.07967
50	0.172043	0.022453	0.13542
100	0.140977	0.038482	0.08663
150	0.171634	0.032198	0.11960

4.2.2 Cooperative Black-hole attack

4.2.2.A Throughput of TBBT_AODV under cooperative Black-hole attack

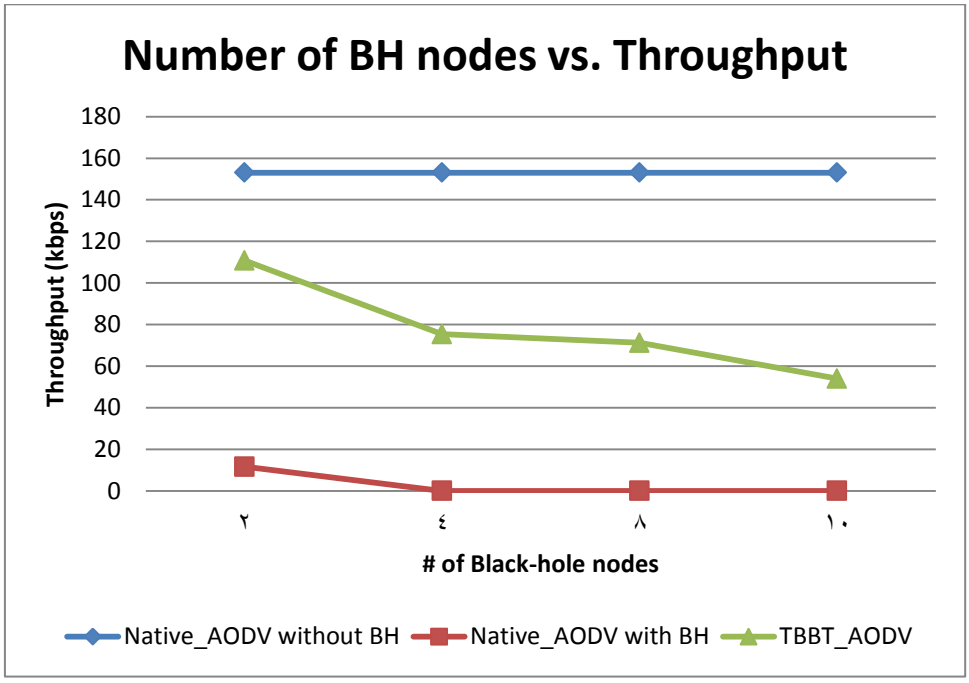

Figure 4.6 TBBT results in terms of Throughput vs. the number of BH nodes under cooperative Black-hole attack

As shown in figure 4.6, the result of native AODV against 2 to 10 Black-hole nodes showed zero Throughput due to fact that the increasing number of Black-hole nodes in the network will indeed prevent the connection between the source node and the destination node. The result of Throughput in TBBT_AODV decreased by the increasing number of Black-hole nodes in the network. The drop in Throughput is because of the position of the Black-hole nodes, which may be located in the path between the source node and the destination node, in addition to the fact that TBBT drops any reply from unknown nodes.

4.2.2.B End to End Delay of TBBT_AODV under cooperative Black-hole attack

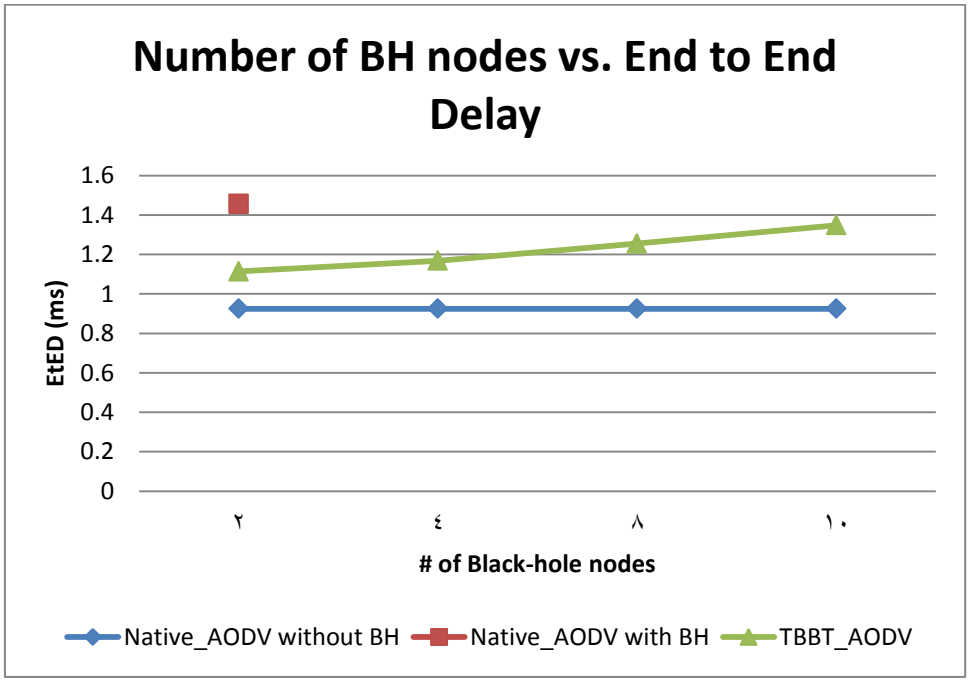

Figure 4.7 TBBT results in terms of End to End Delay vs. the number of BH nodes under cooperative Black-hole attack

As shown in figure 4.7, the result of End to End Delay in native AODV was highest when there were only two Black-hole nodes in the network. Also, when the number of Black-hole nodes increased, the connection between the source node and the destination node was prevented so the End to End Delay reached infinity. TBBT_AODV showed slightly different End to End Delay results with native AODV

when the number of Black-hole nodes increased because the mechanism in selecting the path stays the same as in native AODV.

4.2.2.C PDR of TBBT_AODV under cooperative Black-hole attack

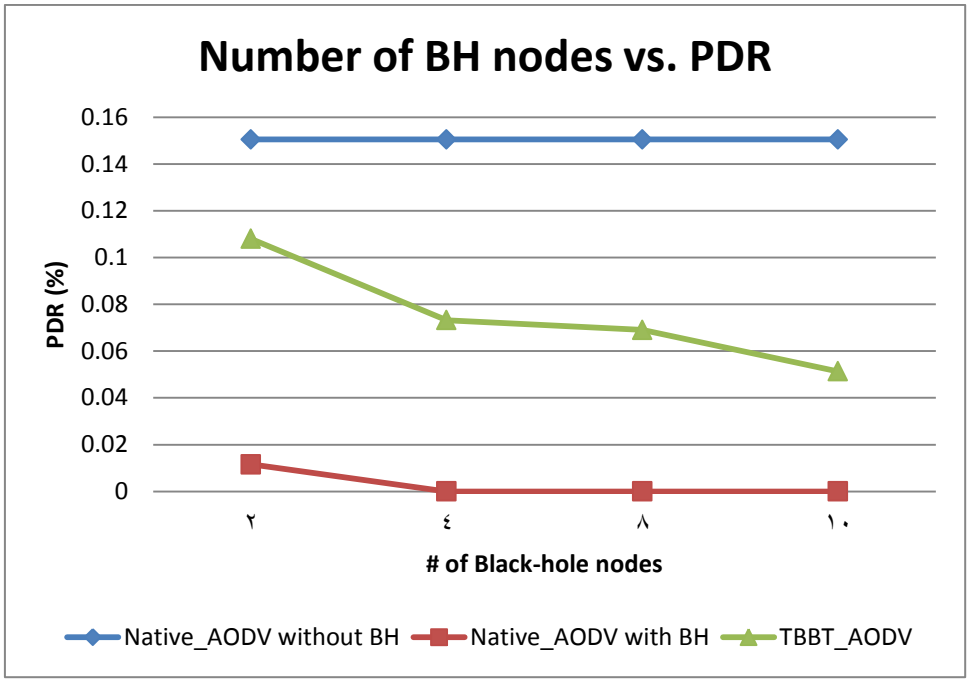

Figure 4.8 TBBT results in terms of PDR vs. the number of BH nodes under cooperative Black-hole attack

As shown in figure 4.8, the result of native AODV against cooperative Black-hole nodes showed a zero PDR because when the number of Black-hole increases, they will cover the whole network which will indeed cut any communication between any two nodes in the network. The result of PDR in TBBT_AODV is decreased while the number of Black-hole nodes in the network was increasing. Table 4.2 shows the numeric results of TBBT in terms of Throughput, the average of End to End Delay and Packet Delivery Ratio while the numbers of nodes increases.

Table 4.2 Numeric results of TBBT for cooperative Black-hole attack

Number BH nodes	Native_AODV Without BH	Native_AODV With BH	TBBT_AODV
	Throughput (kbps)		
2	153.044	11.651	110.794

4	153.044	0	75.368
8	153.044	0	71.167
10	153.044	0	53.987
Avg of End to End Delay (ms)			
2	0.925	1.455	1.113
4	0.925	∞	1.168
8	0.925	∞	1.254
10	0.925	∞	1.348
Packet Delivery Ratio (PDR)			
2	0.150456	0.011572	0.10795
4	0.150456	0	0.07318
8	0.150456	0	0.06901
10	0.150456	0	0.05128

4.3 Comparison between TBBT model and other proposed models

TBBT model was implemented in two different scenarios in order to compare the overall performance of our model with other models [39] and [35] described in it Black-hole related work section. the proposed model in [39] is called PAODV. It can't be countered by a Smart Black-hole node unlike other proposed techniques which are previously discussed in section Black-hole related work section. TBBT is simulated in the same metric as in PAODV where the number of nodes was varying from 25 to 50. TBBT obtained a 22.1 % decrease in End to End Delay unlike PAODV, which obtained a 70 % decrease in End to End Delay according to [39]. TBBT obtained a 373.00 % increase in Throughput unlike PAODV, which obtained only a 12 % increase in Throughput according to [39]. By comparing the two results it is clear that TBBT is better than PAODV in terms of Throughput but not in terms of End to End Delay.

Table 4.3 Numeric results of implementing TBBT_AODV in the same PAODV scenario environment parameters.

Type/# of nodes	25	30	35	40	45	50
End to End Delay						

Native_AODV without BH	1.130202	0.98398	0.884242	0.696609	0.906069	0.733763
Native_AODV with BH	1.44435	1.149403	1.511515	0.964757	0.985247	1.253405
TBBT_AODV	1.197252	0.989631	0.893448	0.719212	0.924569	0.873268
End to End Delay Enhancement	17.11%	13.90%	40.89%	25.45%	6.16%	30.33%
Overall Enhancement : 22.31%						
Type/# of nodes	25	30	35	40	45	50
Throughput						
Native_AODV without BH	103.8352	159.1672	140.5471	191.9087	187.8213	175.7361
Native_AODV with BH	38.16213	43.06742	32.76251	37.42086	11.06373	25.64439
TBBT_AODV	81.38836	93.44741	80.96708	146.0653	136.0915	138.528
Throughput Enhancement	113.27%	116.98%	147.13%	290.33%	1130.07%	440.19%
Overall Enhancement : 373.00%						

Table 4.4 Comparison results between TBBT and PAODV.

Metric	TBBT	PAODV
End to End Delay	22.31%(decrease)	70%(decrease)
Throughput	373.0% (increase)	12%(increase)

The second comparison is done with the proposed model in [35] which is called DAODV. TBBT is simulated using the same metrics as in DAODV where the mobility of nodes varied from 0 to 10. TBBT obtained a 3.78% increase in End to End Delay and a 15.60% decrease in Throughput comparing to the native AODV without Black-hole attack, a 9.04% decrease in End to End Delay and 542.85% increase in Throughput comparing to the native AODV with a Black-hole attack.

Table 4.5 Numeric results of implementing TBBT_AODV in same DAODV scenario environment parameters.

Type/Mobility	0	2.5	5	7.5	10
End to End Delay					
Native_AODV without BH	1.219503	0.964685	1.069389	1.028826	0.954835
Native_AODV with BH	1.297908	1.091389	1.336241	1.119104	1.132747
TBBT_AODV	1.243647	0.982131	1.133413	1.064437	1.008979
End to End Delay (Native AODV without Black-hole attack) Enhancement	1.98%	1.81%	5.99%	3.46%	5.67%
End to End Delay (Native AODV with Black-hole attack) Enhancement	4.18%	10.01%	15.18%	4.88%	10.93%
Overall End to End Delay When Native AODV without Black-hole attack Enhancement : 3.78%					
Overall End to End Delay When Native AODV with Black-hole attack Enhancement : 9.04%					
Type/Mobility	0	2.5	5	7.5	10
Throughput					
Native_AODV without BH	151.5296	157.9711	181.4354	154.594	160.8762
Native_AODV with BH	14.34616	16.67587	20.13112	47.6565	32.3409
TBBT_AODV	143.4762	137.9907	142.9755	111.9081	142.8319
Throughput (Native AODV without Black-hole attack) Enhancement	5.31%	12.65%	21.20%	27.61%	11.22%
Throughput (Native AODV with Black-hole attack) Enhancement	900.10%	727.49%	610.22%	134.82%	341.64%
Overall Throughput When Native AODV without Black-hole attack Enhancement : 15.60%					
Overall Throughput When Native AODV with Black-hole attack Enhancement : 542.85%					

Table 4.6 Numeric results of DAODV while mobility of nodes increases.

Type/Mobility	0	2.5	5	7.5	10
End to End Delay					
Native_AODV without BH	35	42	42	51	62
Native_AODV with BH	29	44	75	81	270
DAODV	29	42	40	49	62
End to End Delay (Native AODV without Black-hole attack) Enhancement	17.14%	0%	- 4.76%	-3.92%	0.00%
End to End Delay (Native AODV with Black-hole attack) Enhancement	0.00%	4.55%	46.67%	39.51%	76.67%
Overall End to End Delay When Native AODV without Black-hole attack Enhancement : 1.69%					
Overall End to End Delay When Native AODV with Black-hole attack Enhancement : 33.48%					
Type/Mobility	0	2.5	5	7.5	10
Throughput					
Native_AODV without BH	180	179	174	173	171
Native_AODV with BH	70	108	45	71	40
TBBT_AODV	143	118	121	117	118
Throughput (Native AODV without Black-hole attack) Enhancement	20.56%	34.08%	30.46%	32.37%	30.99%
Throughput (Native AODV with Black-hole attack) Enhancement	104.29%	9.26%	168.89%	64.79%	195%
Overall Throughput When Native AODV without Black-hole attack Enhancement : 29.69%					

Overall Throughput **When Native AODV with Black-hole attack Enhancement : 108.45%**

It should be noted that results in Table 4.6 are approximated. It is clear that our proposed model overcomes DAODV in terms of Throughput but not in terms of End to End Delay.

Table 4.7 Comparison results between TBBT and DAODV.

Metric	TBBT	DAODV
End to End Delay (Native AODV without Black-hole attack)	3.78% (increase)	1.69% (decrease)
Throughput (Native AODV without Black-hole attack)	15.60% (decrease)	29.69% (decrease)
End to End Delay (Native AODV with Black-hole attack)	9.04% (decrease)	33.48% (decrease)
Throughput (Native AODV with Black-hole attack)	542.85% (increase)	108.45% (increase)

It should mention that when there is no mobility of nodes, native AODV throughput is 151.529 in case if there is no Black-hole node in the network, otherwise the Throughput is 14.346. TBBT's throughput is 143.476 in case of black-hole existence which is very close to the native AODV because the changing in the topology is very low and TBBT will not drop any packet from a known node within its range so there are no replies from unknown nodes. The Black-hole attack is considered to be one of the most serious attacks affecting the operation of MANET. The detection and isolation of any Black-hole node in the network are considered an essential task to prevent network collapse. In this research, we introduced a Smart Black-hole detection and isolation technique that should be considered in constructing and

developing any black-hole fighting protocols or techniques. The proposed TBBT integrates both timers and baiting techniques in order to enhance black-hole detection capability whilst preserving Throughput, End to End Delay and Packet Delivery Ratio. The simulation results of the proposed technique showed that the End to End Delay, Throughput and Packet Delivery Ratio are very close to the native AODV. As a future work, we aim to enhance the proposed model in order to increase the Throughput and Packet Delivery Ratio and also to decrease the End to End Delay.

Chapter 5 : Avoiding and Isolating Flooding attack (AIF)

This chapter presents a new proposed model that has been developed to resist RREQ flooding attack and to avoid its effects on the network. It also shows how the proposed model can handle the RREQ flooding attack. Also, we present a comparison of the overall performance of the proposed model with other proposed models in order to prove its efficiency.

5.1 AIF model description

The proposed model AIF_AODV is developed to avoid the effects of the Flooding attack, identify the attacker, and to isolate it (see figure 5.1). AIF_AODV consists of two algorithms Flooding Avoidance and Attacker Isolation algorithm. In Flooding Avoidance algorithm, each node in the network has a table called Request_Counter that records the source of the request and the number of requests received from the same source. Whenever a node receives a request, it first checks if the source of the request is in the Request_Counter table, then it increases the request counter of that node, else it adds a new entry for that node in the table. After checking the source of the requesting node, it checks the number of the received requests and if it is higher than the limit, it adds the node to the suspicious list, else processes the request normally. According to AODV RFC [53] , any normal node should send up to 10 requests per second. The default value of the limit is set to 10. The limit value varies between half of the limit value to one and half of the limit value depending on the number of neighbor nodes (closed interval [limit/2, limit*1.5]).

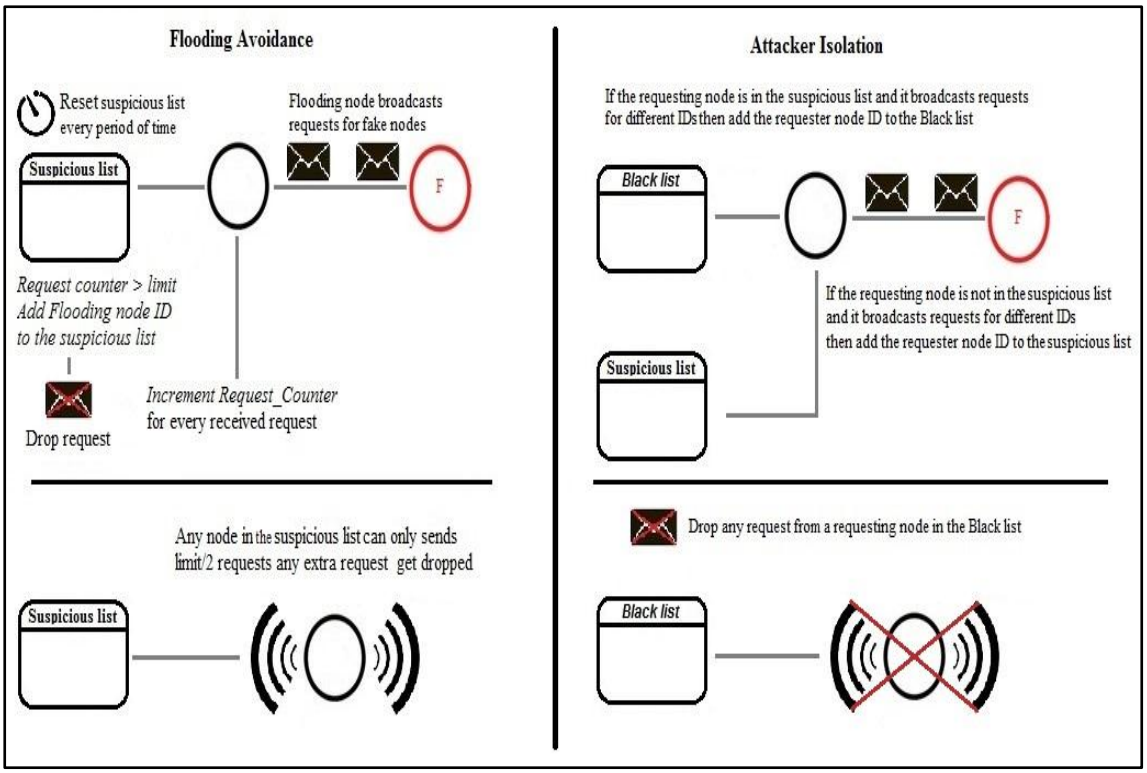

Figure 5.1 AIF_AODV system model.

If the number of neighbor nodes is less than half of the limit, then set the limit to limit/2, if it is higher than one and half of the limit, then set the limit to limit*1.5, otherwise set the limit to an equal number of neighbor nodes. When the AODV protocol receives hello message, it stores the ID of the sending neighbor node along with its Destination Sequence Number (DSN) in a table called Neighbors_Table. AODV keeps updating the table by inserting new entries when it receives new hello messages and by removing old entries when the entry lifetime expires. The Number of Neighbor nodes (NoN), which is also called connectivity, equals the number of entities in the Neighbors_Table. To avoid the effects of the Flooding attack, any node in the suspicious list can only send requests up to half of the limit, and nodes only process that number of requests. Any extra request is simply dropped. The avoidance of the attack's effects is achieved by enforcing the nodes to only process a specified number of requests, and hence we prevent flooding the network by attacker requests.

The suspicious list gets reset every period of time to avoid false judgment on normal nodes. Algorithm 1 describes the Flooding Avoidance.

In Attacker Isolation algorithm, each node has a table called Request_Destination_ID that records the source of the request along with the destination of the request (desired node's ID). We assume that there is no such node in the network that wants to communicate with a large number of nodes at the same time. Whenever a node receives a request, it first checks if the source of the request along with its destination are not in the Request_Destination_ID table, then it adds a new entry for that request. If the number of destinations of a single node is higher than ID_limit, then check if the node is in the suspicious list, and if so, add the node to the Black list, otherwise add it to the suspicious list. We assumed that ID_limit value is equal to half of the request limit. This algorithm blocks and isolates any node that wants to flood the network with fake requests for different random IDs that do not exist in the network. Algorithm 2 describes the Attacker Isolation. Both mentioned algorithms work together to detect and isolate the Flooding attack in the network.

Algorithm 1: Flooding Avoidance

```
Begin
 Foreach (received request) Do
  If (source_ID of the request in Request_Counter table)  Then
         Increment request_counter of that node;
 End if
 Else  Add a new entry  for the source of the request to
           Request_Counter  table;
 End else
  If  (source_ID of the request in the suspicious list) Then
      limit = limit/2;
  End if
  If   (request counter > limit) Then
       Add source ID to the suspicious list;
       Drop request;
  End if
  Else  Process request;
  End else
 End for
End
```

Algorithm 2: Attacker Isolation

```
Begin
 Foreach (received request) Do
 If  (source_ID of the request and destination not in
        Request_Destination_ID table)  Then
    Add a new entry  for the source of the request and
    destination to Request_Destination_ID  table;
 End if
 If  (source_ID of the request in the Black list) Then
       Drop request;
 End if
  If   (ID_request_count > ID_limit) Then
      If ( source_ID in the suspicious list) Then
           Add source ID to the Black list;
           Drop request;
      End if
      Else  Add source ID to the suspicious list;
            Drop request;
      End else
  End if
 End for
End
```

5.2 AIF simulation and results

this section tests the new proposed model against RREQ flooding attack (AIF_AODV). The simulation parameter is the same as in Table 3.5 but the sending interval is set to 0.06 (16 request per second). TBBT is tested under five different performance metrics Throughput, End-to-End Delay, Packet Delivery Ratio, Normalized Route Loading, and Average residual energy.

5.2.1 Throughput of AIF_AODV under RREQ flooding attack.

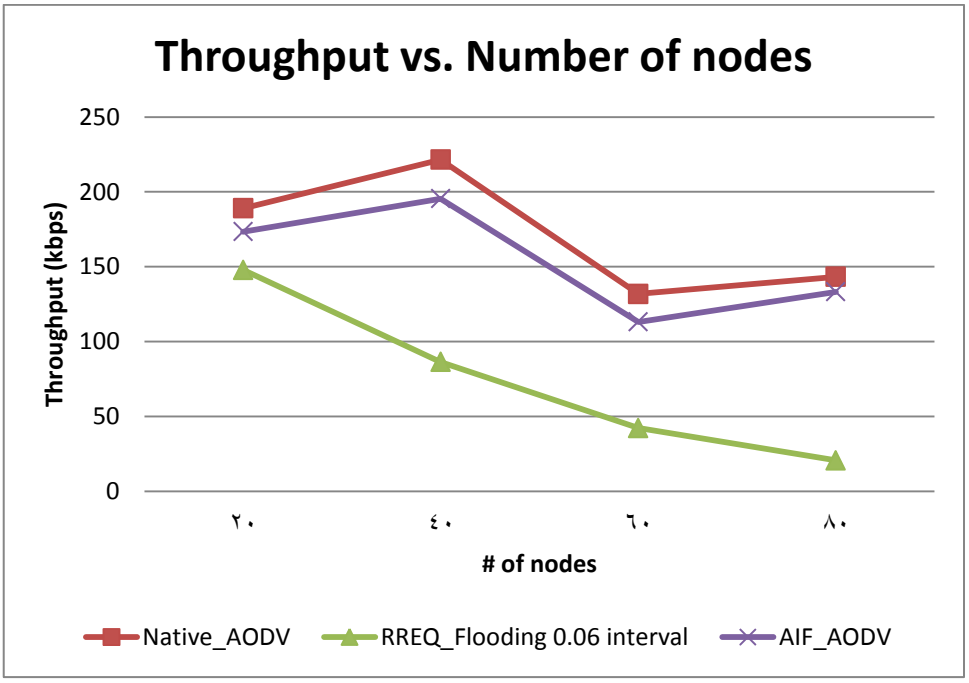

Figure 5.2 AIF_AODV results in terms of Throughput vs. the number of nodes under a RREQ flooding attack.

As shown in Figure 5.2 the result of Throughput in native AODV when there is a Flooding attack is decreasing while the number of nodes increases as a result of the rebroadcasting of fake requests. The Flooding attack will lead to congestion in the network which also leads to dropping and delaying normal packets which in turn will affect the Throughput and PDR. The result of PDR in native AODV is the highest when there is no Flooding attack in the network. The result of AIF_AODV shows a higher Throughput than native AODV under Flooding attack and a slightly lower Throughput than native AODV without Flooding attack.

5.2.2 End to End Delay of AIF_AODV under RREQ flooding attack.

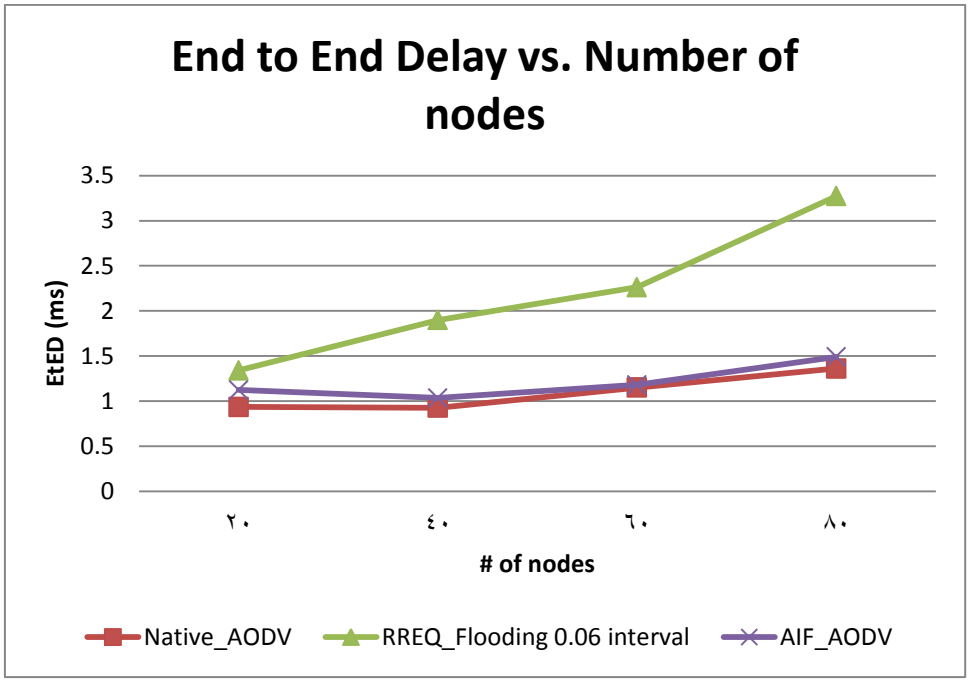

Figure 5.3 AIF_AODV results in terms of End to End Delay vs. the number of nodes under a RREQ flooding attack.

As shown in Figure 5.3, the result of End to End Delay in native AODV when there is a Flooding attack is increasing while the number of nodes increases because of the congestion generated by the flooding node. Normal packets will get dropped or delayed which will increase the End to End Delay. The result of End to End Delay in native AODV when there is no Flooding attack in the network is the lowest. The result of AIF_AODV shows a lower End to End Delay than native AODV under Flooding attack because AIF_AODV detects and isolates the attack node in the network. AIF_AODV shows a slightly higher End to End Delay than native AODV without Flooding attack, because AIF_AODV uses the same mechanism of native AODV in finding the shortest path between nodes that want to communicate.

5.2.3 PDR of AIF_AODV under RREQ flooding attack.

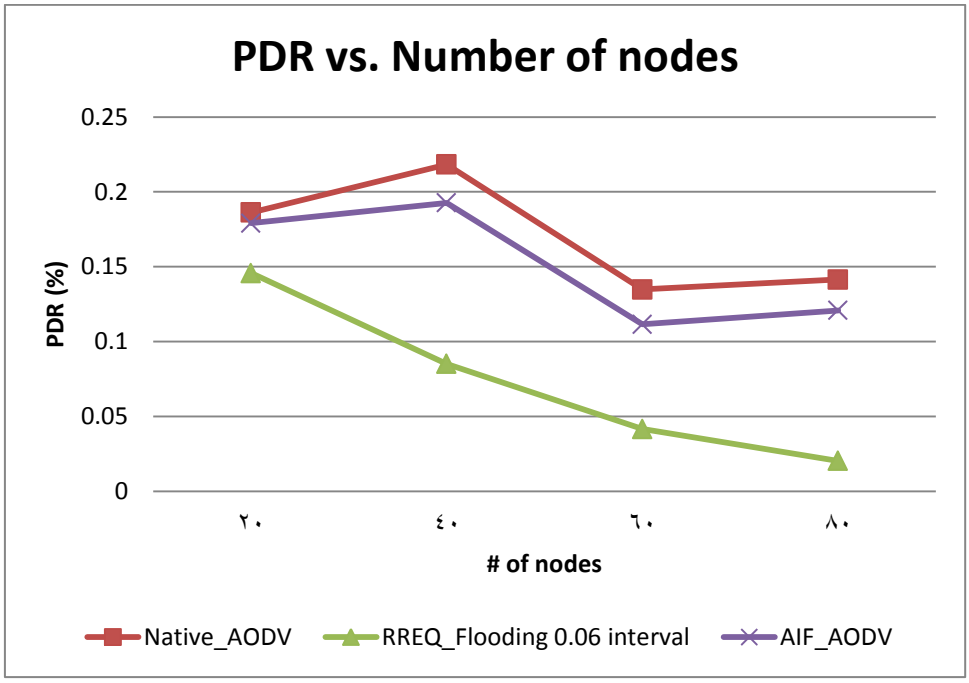

Figure 5.4 AIF_AODV results in terms of PDR vs. the number of nodes under a RREQ flooding attack.

As shown in Figure 5.4, the result of PDR in native AODV is the lowest when there is a Flooding attack especially when the number of nodes increased. It is clear that the effect of the attack increases when the number of nodes increases because of the rebroadcasting of fake requests and the overhead of finding the fake nodes in the network. The result of PDR in native AODV is highest when there is no Flooding attack in the network. The result of AIF_AODV simulation shows a higher PDR than native AODV under Flooding attack whilst a slightly lower PDR than native AODV without Flooding attack.

5.2.4 ARE of AIF_AODV under RREQ flooding attack.

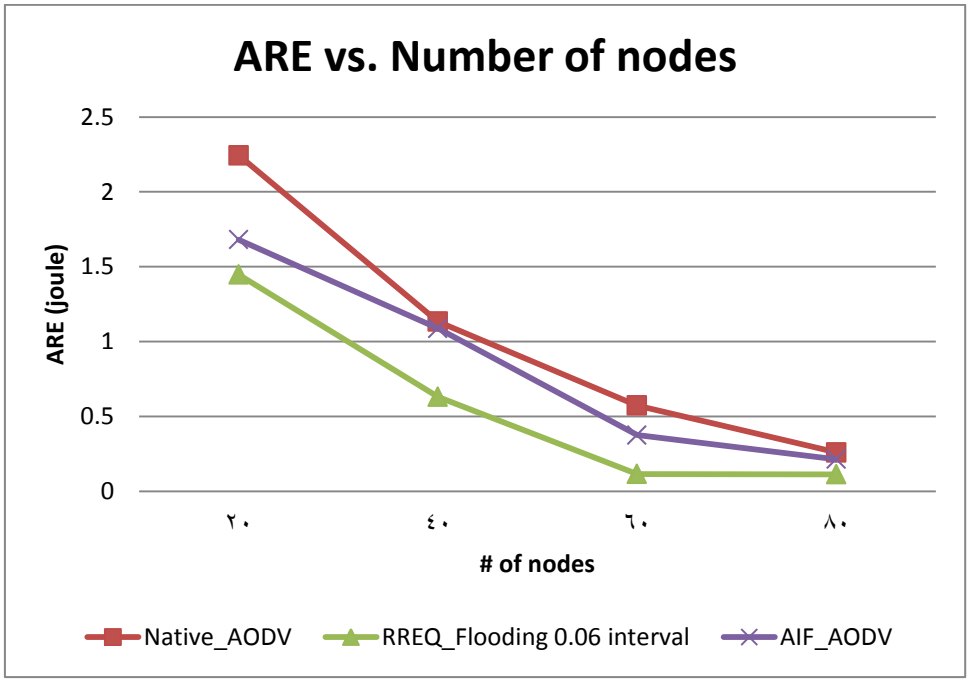

Figure 5.5 AIF_AODV results in terms of ARE vs. the number of nodes under a RREQ flooding attack.

As shown in Figure 5.5, the result of ARE in native AODV when there is a Flooding attack is the lowest especially when the number of nodes increases as the Flooding attack consumes the energy of nodes by keeping them busy in rebroadcasting fake requests in the network. The result of ARE in native AODV when there is no Flooding attack in the network is the highest. The result of AIF_AODV shows a higher ARE than native AODV under Flooding attack because AIF_AODV prevents the Flooding attack in the network. AIF_AODV shows a slightly lower ARE than native AODV without Flooding attack because AIF_AODV has a higher overhead than native AODV because it uses extra tables that store information about nodes.

5.2.5 NRL of AIF_AODV under RREQ flooding attack.

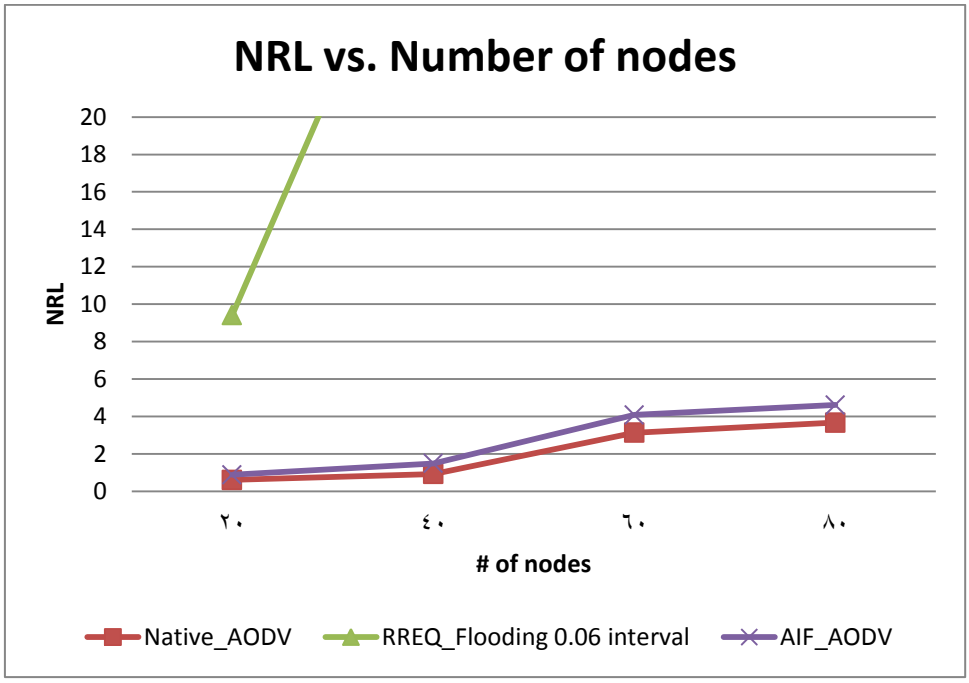

Figure 5.6 AIF_AODV results in terms of NRL vs. the number of nodes under a RREQ flooding attack.

As shown in Figure 5.6, the result of NRL in native AODV when there is a Flooding attack is increasing when the number of nodes increases because the flooding node keeps broadcasting fake requests, and the nodes will continue to rebroadcast these fake requests which will increase the number of routing packets. When the number of nodes increases, the rebroadcasting of fake requests will also increase. The result of NRL in native AODV is lowest when there is no Flooding attack in the network. The result of AIF_AODV shows a lower NRL than native AODV under Flooding attack and a slightly higher NRL than native AODV without Flooding attack.

Table 5.1 Numeric results of AIF_AODV for RREQ flooding attack

Number of Nodes	Native_AODV Without RREQ_Flooding	AIF_AODV	Native_AODV With RREQ_Flooding
Packet Delivery Ratio (PDR) (%)			
20	0.186	0.179	0.145
40	0.218	0.192	0.085
60	0.134	0.111	0.041
80	0.141	0.120	0.020
Throughput (kbps)			
20	189.0	173.4	147.8
40	221.5	195.4	86.35
60	131.8	113.1	42.21
80	143.2	133.2	20.64
Avg of End to End Delay (ms)			
20	0.934	1.124	1.339
40	0.926	1.034	1.899
60	1.149	1.180	2.262
80	1.360	1.490	3.272
Avg Residual Energy (ARE) (joule)			
20	2.244	1.680	1.447
40	1.133	1.087	0.630
60	0.572	0.375	0.115
80	0.259	0.214	0.113
Normalized Routing Load (NRL)			
20	0.610	0.880	9.420
40	0.920	1.490	34.14
60	3.130	4.080	104.2
80	3.670	4.610	281.9

5.3 Comparison between AIF model and other proposed models

AIF_AODV was implemented in different scenarios in order to compare it with the two other proposed models [40] and [46] from the related work section. A comparison of the overall performance between AIF_AODV with the proposed model in [46] , which we called EDR (Enhanced Detection and Recovery), in terms of Throughput and PDR. The number of nodes increases from 25 to 100 nodes, the terrain coordinates 500x500 m, and the speed of nodes is 3 mps (low mobility scenario). In EDR, they obtained a 114.33% increase in Throughput and a 111.13% increase in PDR. In AIF_AODV, we obtained a 389.85% increase in Throughput and a 386.54%

increase in PDR. By comparing the two results, AIF_AODV proved that it is better than EDR in terms of Throughput and PDR. Table 5.4 shows the results of the AIF_AODV and EDR comparison in terms of Throughput and PDR while the number of the nodes changes. Note that AIF_AODV works better in low mobility scenarios than high mobility scenarios.

Table 5.2 Numeric results of EDR while number of nodes increases.

Type/#of nodes	25	50	75	100
Throughput				
Native_AODV	38	39	58	58
EDR	58	100	140	120
Throughput enhancement	52.63%	156.41%	141.38%	106.90%
Overall Enhancement: 114.33%				
Type/#of nodes	25	50	75	100
PDR				
Native_AODV	42	28	31	30
EDR	72	73	71	55
PDR enhancement	71.43%	160.71%	129.03%	83.33%
Overall Enhancement: 111.13%				

Table 5.3 Numeric results of implementing AIF_AODV in same EDR scenario environment parameters.

Type/#of nodes	25	50	75	100
Throughput				
Native_AODV	143	65	28	17
AIF_AODV	211	190	157	163
Throughput enhancement	47.55%	192.31%	460.71%	858.82%

Overall Enhancement: 389.85%				
Type/#of nodes	25	50	75	100
PDR				
Native_AODV	0.140	0.063	0.027	0.015
AIF_AODV	0.208	0.187	0.155	0.139
PDR enhancement	48.57%	196.83%	474.07%	826.67%
Overall Enhancement: 386.54%				

It should be noted that the results in Table 5.2 and 5.3 are approximate. It is clear that our proposed model overcome EDR in terms of Throughput and PDR.

Table 5.4 Comparison results between AIF_AODV and EDR.

Metric	AIF_AODV	EDR
Throughput	389.85% (increase)	114.33%(increase)
PDR	386.54%(increase)	111.13%(increase)

A comparison of overall performance between AIF_AODV with the proposed model in [40], which we called DPDS (Dynamic Profile Based Detection Scheme), in terms of Throughput and End to End Delay. The number of attacker nodes increases from 1 to 6, the terrain coordinates 1700x700, and the number of normal nodes varies between 24 to 29. In DPDS, they obtained a 236.22% increase in Throughput and a 96.23% decrease in End to End Delay. In AIF_AODV, we obtained a 311.32% increase in Throughput and a 40.10% decrease in End to End Delay. By comparing the two results, AIF_AODV proved that it is better than DPDS in terms of Throughput but not in term of End to End Delay. Table 5.7 shows the results of comparing both AIF_AODV and DPDS in terms of Throughput and End to End Delay by varying the number of attacking nodes. Out of this comparison, we can see

the ability of AIF_AODV to resist multiple flooding attacker nodes in the same network.

Table 5.5 Numeric results of DPDS while number of nodes increases.

Type/# of attacker nodes	1	2	3	4	5	6
End to End Delay						
Native_AODV	937.52	1450.17	979.16	1837.35	588.22	588.2
DPDS	32.85	31.44	38.61	32.31	33.68	32.48
End to End Delay enhancement	96.50%	97.83%	96.06%	98.24%	94.27%	94.48%
Overall Enhancement : 96.23%						
Type/# of attacker nodes	1	2	3	4	5	6
Throughput						
Native_AODV	13.71	8.96	3.76	1.83	3.29	3.29
DPDS	16.16	13.92	14.51	12.29	8.77	13.82
Throughput enhancement	17.87%	55.36%	285.90%	571.58%	166.57%	320.06%
Overall Enhancement : 236.22%						

Table 5.6 Numeric results of implementing AIF_AODV in same DPDS scenario environment parameters.

Type/# of attacker nodes	1	2	3	4	5	6
End to End Delay						
Native_AODV	0.9597	1.267986	0.829078	1.902203	1.27577	1.757696
AIF_AODV	0.85633	0.706124	0.755449	0.498475	0.755044	0.667353
End to End Delay enhancement	10.77%	44.31%	8.88%	73.79%	40.82%	62.03%
Overall Enhancement : 40.10%						

Type/# of attacker nodes	1	2	3	4	5	6
Throughput						
Native_AODV	59.63175	28.38446	19.32683	18.1451	12.15179	10.51789
AIF_AODV	88.13347	90.73028	64.71879	91.252	62.49785	103.3032
Throughput enhancement	47.80%	219.65%	234.86%	402.90%	80.56%	882.17%
Overall Enhancement : 311.32%						

Table 5.7 Comparison results between AIF_AODV and DPDS.

Metric	AIF_AODV	DPDS
Throughput	311.32% (increase)	236.22%(increase)
End to End Delay	40.10% (decrease)	96.23% (decrease)

It should be noted that the results in table 5.5 and 5.6 are approximate. It is clear that our proposed model overcame DPDS in terms of Throughput but not in term of End to End Delay. From these comparisons, we can see that AIF_AODV showed better performances than other proposed models in term of Throughput. Flooding attack is considered one of Denial of service (Dos) attacks that consumes the network resources. Flooding attack affects the network in different performance metrics. Prevention and detection of flooding node in the network is important to avoid its effect on the network. AIF_AODV depends on two algorithms to avoid the effects of a flooding attack in the network and to isolate the attacker node. The simulation results of AIF_AODV showed that PDF, Throughput, End to End Delay, ARE, and NRL are very close to the native AODV. AIF_AODV proved its efficiency in avoiding the effects of a flooding attack. As a future work, we aim to find an algorithm to detect Error flooding and Sleep Deprivation attack in MANET.

References

[1] Sadiya Mirza, and Sana Zeba Bakshi, "Introduction to MANET," *International Research Journal of Engineering and Technology (IRJET),* vol. 5, no. 1, pp. 17-20, 2018.

[2] K. Sri Varsha and S. Naga Mallik Raj, "Applications, Challenges and Protocols of MANETs: A Review," *Asia-pacific Journal of Convergent Research Interchange,* vol. 4, no. 1, pp. 21-29, 2018.

[3] Aditya Gupta, Prabal Verma, and Rakesh Singh Sambyal, "An Overview of MANET:Features, Challenges and Applications," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT),* vol. 4, no. 1, pp. 122-126, 2018.

[4] Vikas Goyal and Geeta Arora, "Review Paper on Security Issues in Mobile Adhoc Networks," *International Research Journal of Advanced Engineering and Science (IRJAES),* vol. 2, no. 1, pp. 203-207, 2017.

[5] Ankur O. Bang and Prabhakar L.Ramteke, "MANET : History,Challenges And Applications," *International Journal of Application or Innovation in Engineering & Management (IJAIEM),* vol. 2, no. 9, pp. 249-251, 2013.

[6] Saurbh Sharma and Kanchan Bala Jaswak, "MANET Review: Characteristics, Routing Protocols, Attacks and Performance Metrics," *International Journal of Advance Research, Ideas and Innovations in Technology (IJARIIT),* vol. 3, no. 6, pp. 392-399, 2017.

[7] Mahima Chitkara and Mohd. Waseem Ahmad, "Review on MANET: Characteristics, Challenges,Imperatives and Routing Protocols," *International Journal of Computer Science and Mobile Computing (IJCSMC),* vol. 3, no. 2, p. 432–437, 2014.

[8] Diaa Eldein Mustafa Ahmed and Othman O.Khalifa, "An Overview of MANETs: Applications, Characteristics, Challenges and Recent Issues," *International Journal of Engineering and Advanced Technology (IJEAT),* vol. 6, no. 4, pp. 128-133, 2017.

[9] Abdalftah Kaid Said Ali and . U. V. Kulkarni, "Characteristics, Applications and Challenges in Mobile Ad-Hoc Networks (MANET): Overview," *International Journal of Electronics & Communication (IIJEC),* vol. 3, no. 12, pp. 6-12, 2015.

[10] Ali Dorri, Seyed Reza Kamel, and Esmaeil Kheirkhah, "Security challenges in mobile ad hoc networks:a survey," *International Journal of Computer Science & Engineering Survey (IJCSES),* vol. 6, no. 1, pp. 15-29, 2015.

[11] Sheikh Abdul Wajid and KiranGupta, "A Review of Secure Routing Protocols in Manets," *International Journal of Engineering Science and Computing (IJESC),* vol. 6, no. 10, pp. 2552-2556, 2016.

[12] Neha Sharma and Harpal Singh, "ATTACKS AND ROUTING PROTOCOLS IN MANET: A REVIEW," *International Research Journal of Engineering and Technology (IRJET),* vol. 4, no. 12, pp. 735-739, 2017.

[13] Anuj Mehta and Ravina Saini, "A REVIEW PAPER ON SECURITY IN MOBILE ADHOC NETWORK," *International Journal of Advanced Research in Science and Engineering (IJARSE),* vol. 4, no. 8, pp. 120-131, 2015.

[14] Ankit Gupta, P. G Scholar, Deepak Sukheja, and Amrita Tiwari, "Impact of Sybil Attack and Security Threat in Mobile Adhoc Network," *International Journal of Computer Applications (IJCA),* vol. 124, no. 9, pp. 5-12, 2015.

[15] Simranpreet Kaur, Rupinderdeep kaur, and A.K. Verma, "Jellyfish attack in MANETs: A Review," in *International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, 2015.

[16] Aanchal Joshi, "A Review Paper on Black Hole Attack in MANET," *International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS),* vol. 4, no. 5, pp. 16-21, 2016.

[17] C.M. Nalayini, Dr. Jeevaa Katiravan and Arvind Prasad. V, "Flooding Attack on MANET – A Survey," *International Journal of Trend in Research and Development*

(IJTRD), pp. 25-27, 2017.

[18] Ram Kishore Singh and Parma Nand, "Literature Review of Routing Attacks in MANET," in *International Conference on Computing, Communication and Automation (ICCCA2016)*, 2016.

[19] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang, "SECURITY IN MOBILE AD HOC NETWORKS:CHALLENGES AND SOLUTIONS," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38-47, 2004.

[20] Petteri Kuosmanen, "Classification of Ad Hoc Routing Protocols," in *Finnish Defence Forces, Naval Academy*, Finland, 2002.

[21] J. Kaur and G.Singh, "MANET Routing Protocols: A Review," *International Journal of Computer Sciences and Engineering (IJCSE)*, vol. 5, no. 3, pp. 60-64, 2017.

[22] Lubdha M. Bendale, Roshani. L. Jain, and Gayatri D. Patil, "Study of Various Routing Protocols in Mobile Ad-Hoc Networks," *International Journal of Scientific Research in Network Security and Communication (IJSRNSC)*, vol. 6, no. 1, pp. 1-5, 2018.

[23] Pragati Jain and Akash Sanghi, "Review of Various Routing Protocols in Mobile Ad-Hoc Networks (MANETs)," *International Journal of Innovations & Advancement in Computer Science (IJIACS)*, vol. 7, no. 4, pp. 45-54, 2018.

[24] Yuxia Bai, Yefa Mai, and Nan Wang, "Performance Comparison and Evaluation of the Proactive and Reactive Routing Protocols for MANETs," in *Wireless Telecommunications Symposium (WTS)*, Chicago, IL, USA, 2017.

[25] Abdalftah Kaid Said Ali and U.V. Kulkarni, "Comparing and Analyzing Reactive Routing Protocols (AODV, DSR and TORA) in QoS of MANET," in *IEEE 7th International Advance Computing Conference*, 2017.

[26] Rutvij H. Jhaveri and Narendra M.Patel, "Mobile Ad-hoc Networking with AODV: A Review," *International Journal of Next-Generation Computing (IJNGC)*, vol. 6, no. 3, pp. 1-27, 2015.

[27] Daxesh N. Patel, Sejal B. Patel, Hemangi R.Kothadiya, Pinakin D. Jethwa, and Rutvij H. Jhaveri, "A Survey of Reactive Routing Protocols in MANET," in *International Conference on Information Communication & Embedded Systems (ICICES)*, 2014.

[28] J. Godwin Ponsam and R.Srinivasan, "A Survey on MANET Security Challenges,Attacks and its Countermeasures," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),* vol. 3, no. 1, pp. 274-279, 2014.

[29] Sandeep Kumar Arora, Shivani Vijan , and Gurjot Singh Gaba, "Detection and Analysis of Black Hole Attack using IDS," *Indian Journal of Science and Technology,* vol. 9, no. 20, pp. 1-5, 2016.

[30] Tarun Varshney, Tushar Sharmaa, and Pankaj Sharma, "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network," in *Fourth International Conference on Communication Systems and Network Technologies IEEE*, Bangalore, 2014.

[31] Apurva Jain, Urmila Prajapati, and Piyush Chouhan, "Trust Based Mechanism with AODV Protocol for Prevention of Black-Hole Attack in MANET Scenario," in *Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, India, 2016.

[32] Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han-Chieh CHAO, and Jiann-Liang CHEN, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs," in *Advanced Communication Technology (ICACT),13th International Conference on.IEEE*, 2011.

[33] Bikramjeet Singh, Dasari Srikanth, and C.R. Suthikshn Kumar, "Mitigating effects of Black hole Attack in Mobile Ad-hoc Networks: Military Perspective," in *2nd IEEE International Conference on Engineering and Technology (ICETECH)*, 2016.

[34] A Raja Rajeswari, Kanagasabai Kulothungan, and Ashwin Kannan, "GNB-AODV: Guard Node Based –AODV to Mitigate Black Hole Attack in MANET," *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET),* vol. 2, no. 6, pp. 671-677, 2016.

[35] Nishu Kalia and Harpreet Sharma, "Detection of Multiple Black hole nodes attack in MANET by modifying AODV protocol," *International Journal on Computer Science and Engineering (IJCSE),* vol. 8, no. 5, pp. 160-174, 2016.

[36] Pooja L. Chelan and Sudhir T. Bagde, "Detecting Collaborative Attacks by Malicious Nodes in MANET : An Improved Bait Detection Scheme," in *Communication and Electronics Systems (ICCES), International Conference on*, 2016.

[37] Sagar R Deshmukh, P N Chatur, and Nikhil B Bhople, "AODV-Based Secure Routing Against Blackhole Attack in MANET," in *IEEE International Conference On Recent Trends In Electronics Information Communication Technology*, 2016.

[38] Sandeep Dhende, Sandeep Musale, Suresh Shirbahadurkar and Anand Najan, "SAODV: Black Hole and Gray Hole Attack Detection Protocol in MANETs," in *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017.

[39] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Single and Collaborative Black Hole Attack in MANET," in *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2016.

[40] D. &. H. Desta, "RREQ Flooding Attack Mitigation in MANET Using Dynamic Profile Based Technique," *International Journal of Engineering Science and Computing (IJESC),* vol. 7, no. 6, pp. 12700-12705, 2017.

[41] Opinder Singh, Jatinder Singh, and Ravinder Singh, "SAODV: Statistical Ad hoc On-Demand Distance Vector Routing Protocol for Preventing Mobile Adhoc Network against Flooding Attack," *Advances in Computational Sciences and Technology,* vol. 10, no. 8, pp. 2457-2470, 2017.

[42] Shashi Gurung and Siddhartha Chauhan, "A novel approach for mitigating route request flooding attack in MANET," *Wireless Networks,* vol. 23, no. 4, pp. 1-16, 2017.

[43] M. N. S. C. &. M. S. Yadav, "Flooding Attacks Prevention in MANET," *International Journal of Computer Technology and Electronics Engineering (IJCTEE),* vol. 1, no. 3, pp. 68-72, 2011.

[44] M. Rmayti, Y. Begriche, R. Khatoun, L. Khoukhi, and D. Gaiti, "Flooding Attacks Detection in MANETs," in *International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC)*, 2015.

[45] Surendra Kumar, Satish Alaria and Vijay Kumar, "Prevention in Sleep Deprivation Attack in MANET," *International Journal of Latest Technology in Engineering (IJLTEMAS)*, vol. 4, no. 2, pp. 139-144, 2015.

[46] Shruti Bhalodiya and Krunal Vaghela, "Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol," *International Journal of Computer Applications (IJCA)*, vol. 125, no. 4, pp. 10-15, 2015.

[47] D. Srinivasa Rao and P.V. Nageswara Rao, "An Efficient RREQ Flooding Attack Avoidance Technique for Adaptive Wireless Network," *International Journal of Applied Engineering Research (IJAER),* vol. 11, no. 5, pp. 3696-3702, 2016.

[48] Vrince Vimal and Madhav J.Nigam, "Plummeting Flood Based Distributed-DoS Attack to Upsurge Networks Performance in Ad-Hoc networks Using Neighborhood Table Technique," in *TENCON, IEEE Region 10 International*, Malaysia, 2017.

[49] Sheetal Jatthap and Pankaj Dashore, "Battery Capacity Based Detection and Prevention of Flooding Attack on MANET," *International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS)*, vol. 4, no. 9, pp. 89-99, 2016.

[50] Avita Katal, Mohammad Wazid ,R H Goudar and D P Singh , "A Cluster Based Detection and Prevention Mechanism against Novel Datagram Chunk Dropping Attack in MANET Multimedia Transmission," in *IEEE Conference on Information and Communication Technologies (ICT 2013)*, 2013.

[51] Mohammad Wazid,Avita Katal ,and RHGoudar, "Cluster and Super Cluster Based

Intrusion Detection and Prevention Techniques for JellyFish Reorder Attack," in *2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, 2012.

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

[53] C. Perkins, E. Belding-Royer and S. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing (RFC 3561)," 2003.

[54] Ashok Koujalagi, "Considerable Detection of Black Hole Attack and Analyzing its Performance on AODV Routing Protocol in MANET (Mobile Ad Hoc Network)," American Journal of Computer Science and Information Technology (AJCSIT), vol. 6, no. 2:25,2018.

[55] Zulfiqar Ali Zardari, Jingsha He, Nafei Zhu, Khalid Hussain Mohammadani, Muhammad Salman Pathan, Muhammad Iftikhar Hussain and Muhammad Qasim Memon "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, vol. 11,2019.

[56] Adwan Yasin and Mahmoud AbuZant " Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique " Hindawi-Wireless Communications and Mobile Computing (WCMC), 2018.

[57] Mahmoud AbuZant and Adwan Yasin "Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV)" Hindawi-Security and Communication Networks (SCN), 2019.

لمقاومة هجوم الثقب الأسود ، تم اقتراح نموذج جديد يسمى TBBT والذي يتكون من مؤقت طعم حيث أنه عندما يصل هذا المؤقت إلى الوقت المحدد له ، فإنه يبث طلبًا مزيفًا لخداع عقد الثقب الأسود. عندما تتلقى عقدة المرسلة في الشبكة ردًا على أي طلب مزيف ، فإنها تضيف العقدة التي قامت برد الى القائمة السوداء لتجنب التعامل مع هذه العقدة. لمقاومة هجوم فيضان RREQ ، تم اقتراح نموذج جديد يسمى AIF يعتمد على الجداول التي تسجل عدد الطلبات التي تلقتها عقدة في الشبكة. كلما أرسلت عقدة عددًا من الطلبات أعلى من قيمة الحد المحددة (Limit)، تتم إضافة هذه العقدة الطالبة الى القائمة المشبوهة. أي عقدة في القائمة المشبوهة لها كمية محدودة من الطلب يمكن معالجتها وهي نصف الحد المحدد (Limit) . افترضنا انه لا توجد عقدة في الشبكة تريد التواصل مع عدد كبير من العقد في نفس الثانية. لذلك ، إذا أرسلت عقدة الطالب طلبات عديدة لعقد مختلفة والتي يزيد عددها عن قيمة ID_limit المحددة ، يتم نقل العقدة المرسلة إلى القائمة السوداء لتجنب معالجة طلباتها.

توضح المقارنة بين TBBT والنماذج الأخرى المقترحة أداء أفضل من حيث الإنتاجية ولكن ليس من حيث التأخير في ايصال المعلومات . يُظهر AIF أيضًا أداء أفضل من حيث الإنتاجية ولكن ليس من حيث التأخير في ايصال المعلومات مقارنةً بالنماذج المقترحة الأخرى.

ملخص

شبكة المحمول المخصصة (المانيت) هي عبارة عن شبكة ولا يوجد فيها وحدة تحكم مركزية كي تتحكم وتنسق الاتصال بين الأجهزة الموجودة فيها وذلك بسبب أن طوبولوجيا الشبكة تتغير باستمرار بسبب الحركة العشوائية الموجودة في الشبكة. هناك أنواع مختلفة من خوارزميات البحث عن المسار الافضل صممت للتكيف و التأقلم مع التغيرات التي تحدث في طوبولوجيا الشبكة من اجل ربط الاجهزة مع بعضها البعض وذلك لضمان تبادل البيانات و المعلومات فيما بينها. ان خوارزمية (AODV) هو نوع من خوارزميات البحث عن المسار الافضل التوجيهية التفاعلية التي تقوم بتبادل المعلومات حول المسار الافضل للأجهزة الأخرى في الشبكة فقط عند الحاجة إلى ارسال بيانات عن طريق إغراق الشبكة بطلبات تحديد مسار الهدف المطلوب التراسل معه. ان خوارزمية AODVمعرضة لأنواع مختلفة من الهجمات التي تؤثر في أدائها و وظيفتها في الشبكة مثل هجوم الثقب الاسود و هجوم الفيضان وبناء علية هناك حاجة الى تحسين و تدعيم هذه الخوارزمية لإعطائه القدرة على مقاومة انواع مختلفة من الهجمات .

في هذه الأطروحة ، عرضنا أنواعا مختلفة من الهجمات على المانيت بالأخص هجوم الثقب الأسود و هجوم الفيضان والتي بدورها تأثر بشكل كبير على اداء خوارزمية AODV. لقد أظهرنا تأثير هجوم الثقب الأسود و هجوم الفيضان على أداء خوارزمية AODV في الشبكة تحت مقاييس أداء مختلفة ، مثل نسبة تسليم الحزم ، والتأخير في ايصال المعلومات والإنتاجية ، من خلال محاكاة هذه الهجمات في سيناريوهات مختلفة مثل كثافة الاجهزة وحركتها في الشبكة. وقد أظهرت النتائج أن هذه الهجمات لها تأثير كبير على أداء AODV تحت مقاييس الأداء المختلفة ، الأمر الذي يقودنا إلى أهمية تحسين AODV بخوارزميات مختلفة لمقاومة هذه الهجمات. لقد قمنا باقتراح تعزيز ال AODV بخوارزميتين مختلفتين لمقاومة كل من هجوم الثقب الأسود وهجوم الفيضان. قمنا بمحاكاة هذه الخوارزميات المقترحة في سيناريوهات مختلفة ومقارنتها مع خوارزميات أخرى مقترحة لإثبات كفاءتها. أظهرت نتائج المحاكاة فعالية الخوارزميات التي اقترحناها في مقاومة هجوم الثقب الأسود وهجوم الفيضان تحت مقاييس أداء مختلفة. وتمت مناقشة هذه النتائج في الفصول الأخيرة من هذه الأطروحة.