



**ON PERFORMANCE EVALUATION OF BLACK HOLE ATTACK IN AD-  
HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL USING  
NETWORK SIMULATOR 2**

**SAIF AL-HUSSEINI**

**APRIL 2015**

**ON PERFORMANCE EVALUATION OF BLACK HOLE ATTACK IN AD-  
HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL USING  
NETWORK SIMULATOR 2**

**A THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF NATURAL AND APPLIED  
SCIENCES OF  
ÇANKAYA UNIVERSITY**

**BY**

**SAIF AL-HUSSEINI**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE  
DEGREE OF  
MASTER OF SCIENCE  
IN  
THE DEPARTMENT OF  
MATHEMATICS AND COMPUTER SCIENCE\ INFORMATION  
TECHNOLOGY PROGRAM**

**APRIL 2015**

Title of the Thesis: **On Performance Evaluation of Black Hole Attack in Ad-Hoc on Demand Distance Vector Routing Protocol Using Network Simulator 2**

Submitted by **Saif AL-HUSSEINI**


Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

  
Prof. Dr. Taner ALTUNOK  
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

  
Prof. Dr. Billur KAYMAKÇALAN  
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

  
Assist. Prof. Dr. Yuriy ALYEKSYEYENKOV  
Supervisor

**Examination Date: 16.04.2015**

**Examining Committee Members:**

Assoc. Prof. Dr. Hadi Hakan MARAŞ (Çankaya Univ.)  
Assoc. Prof. Dr. Fahd JARAD (THK Univ.)  
Assist. Prof. Dr. Yuriy ALYEKSYEYENKOV (Çankaya Univ.)


**STATEMENT OF NON-PLAGIARISM PAGE**

I wish to declare that it has been getting the information in this document is in accordance with the rules, academic and moral behavior. I would also like to announce that the conduct and rules that are not original have labeled to sites and sources.

Name, Last Name: Saif, AL-HUSSEINI

Signature :

Date

: 16.04.2015

## **ABSTRACT**

### **ON PERFORMANCE EVALUATION OF BLACK HOLE ATTACK IN AD-HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL USING NETWORK SIMULATOR 2**

AL-HUSSEINI, Saif

M.Sc., Department of Mathematics and Computer Science  
Information Technology Program

Supervisor: Assist. Prof. Dr. Yuriy ALYEKSYEYENKOV

April 2015, 47 pages

A Wireless ad-hoc network is a network that consists of wireless nodes like (Mobile, Laptop...) moving random in the area that have no network infrastructure. The nodes communicate with each other; they work together by forwarding data packets to other nodes in the network. Thus the nodes need a routing protocol to find a path to destination node. Nevertheless, due to safety vulnerabilities of the routing protocols, wireless ad-hoc networks are open to attack of the malicious nodes. Black Hole is one of these attacks, which Attack against network integrity engrossing all data packets in the network. Where the data packets are do not reach the destination node on account of this attack, data loss will occur. So to solve this problem of detection and defense mechanisms to remove the intruder that carries out the black hole attack. In this research, we will simulate the black hole attack in wireless ad-hoc network for different scenarios. And then we will propose a detection system for Black Hole.

**Keywords:** Black Hole, Ad Hoc Network, Network Simulator.

## ÖZ

### AĞ SIMÜLATÖRÜ 2 KULLANARAK AD-HOC TALEBE BAĞLI UZAKLIK VEKTÖRÜ YÖNLENDİRME PROTOKOLÜNDEKİ KARA DELİK SALDIRISININ PERFORMANS DEĞERLENDİRMESİ

AL-HUSSEINI, Saif

Yüksek Lisans, Matematik-Bilgisayar Anabilim Dalı\

Bilgi Teknolojileri Bölümü

Tez Yöneticisi: Yrd. Doç. Dr. Yuriy ALYEKSYEYENKOV

Nisan 2015, 47 sayfa

Kablosuz ad-hoc ağı, ağ altyapısı olmayan alandaki gelişigüzel hareket eden kablosuz ağlardan ( cep telefonu, laptop) oluşmaktadır. Bu ağlar birbirlerine bağlanırlar; ağdaki diğer ağlara bilgi paketi göndermek için birlikte çalışırlar. Bu sebepten dolayı, ağların bir varış ağına için bir yol bulması amacıyla bir iletim protokolüne ihtiyaç duymaktadır. Buna rağmen, yönlendirme protokolünün güvenlik zayıflığı nedeniyle, kablosuz ad-hoc ağlar zararlı ağlara açıktır. Kara delik, ağdaki tüm veri paketlerini işgal eden ağ bütünlüğüne karşı saldıran bu saldırılardan biridir. Bu saldırı sebebiyle veri paketlerinin varış ağına ulaşmaması sebebiyle, veri kaybı olacaktır. Kara delik saldırısını yürüten işgalciyi kaldırmak için tespit ve savunma mekanizmaları kullanılmalıdır. Bu çalışmada, Kablosuz ad-hoc ağındaki kara delik saldırısını farklı bir tabloda canlandıracağız ve sonrasında kara delik için bir tespit sistemi önereceğiz.

**Anahtar Kelimeler:** Kara Delik, Ad Hoc Ağı, Ağ Simülatörü.

## **ACKNOWLEDGEMENTS**

Thanks to God the most compassionate and the most merciful. My Allah's mercy and peace be upon our leader Mohammed, who invites us to science and wisdom, and members of his family and his followers.

I would to express my deep gratitude after God almighty in the completion of this research to my supervisor Dr. Yuriy ALYEKSYEYENKOV who gave me a lot of his time. I am indebted for her suggestions and valuable remarks.

Finally, my thanks go to the members of my family for their help and encouragement, and to everyone who helped in one way or another in bringing out this work.

My God bestow health and happiness to all of them.

## TABLE OF CONTENTS

STATEMENT OF NON PLAGIARISM.....	iii
ABSTRACT.....	iv
ÖZ.....	v
ACKNOWLEDGEMENTS.....	vi
TABLE OF CONTENTS.....	vii
LIST OF FIGURES.....	ix
LIST OF TABLES.....	xi
LIST OF ABBREVIATIONS.....	xii

### CHAPTERS:

<b>1. INTRODUCTION.....</b>	<b>1</b>
<b>1.1 Research Motivation.....</b>	<b>3</b>
<b>1.2 Research Aim and Objectives.....</b>	<b>3</b>
<b>1.3 Research Strategy.....</b>	<b>4</b>
<b>2. BACKGROUND.....</b>	<b>5</b>
<b>2.1 Introduction.....</b>	<b>5</b>
<b>2.2 Mobile Ad-Hoc Network (MANET).....</b>	<b>5</b>
<b>2.2.1 Current challenges of Mobile Ad-Hoc Network.....</b>	<b>7</b>
<b>2.3 Routing protocols in Ad-Hoc Network.....</b>	<b>8</b>
<b>2.3.1 Table-Driven/Proactive Routing Protocols.....</b>	<b>8</b>
<b>2.3.1.1 Destination Sequenced Distance Vector (DSDV) Routing             Protocol.....</b>	<b>9</b>
<b>2.3.1.2 Wireless Routing Protocol (WRP).....</b>	<b>11</b>
<b>2.3.2 On-Demand/Reactive Routing Protocols.....</b>	<b>12</b>
<b>2.3.2.1 Dynamic Source Routing (DSR) Protocol.....</b>	<b>12</b>
<b>2.3.2.2 Ad hoc On-demand Distance Vector (AODV) Routing</b>	<b>15</b>



Protocol .....	
<b>2.3.2.3</b> Comparison of DSR and AODV.....	18
<b>2.3.3</b> Hybrid Routing Protocols.....	19
<b>2.4</b> Security Issues in Mobile Ad Hoc Networks.....	19
<b>2.5</b> Summary of Chapter.....	27
<b>3. RESEARCH METHODOLOGY.....</b>	<b>28</b>
<b>3.1</b> Introduction.....	28
<b>3.2</b> NS2 Simulator.....	28
<b>3.3</b> Network Simulation Topology .....	31
<b>3.4</b> Research Performance Metrics.....	31
<b>3.5</b> Summary of Chapter.....	33
<b>4. PERFORMANCE EVALUATION OF BLACK HOLE ATTACK</b>	<b>34</b>
<b>4.1</b> Introduction.....	34
<b>4.2</b> Evaluation of the Black Hole Attack.....	35
<b>4.2.1</b> Experiment 1 Design.....	35
<b>4.2.1.1</b> The Traffic Pattern.....	35
<b>4.2.1.2</b> Metrics.....	35
<b>4.2.2</b> Experiment Results and Discussion.....	37
<b>4.3</b> Implementation of Detected AODV Protocol.....	42
<b>4.3.1</b> Experiment 2 Design.....	42
<b>4.3.2</b> Experiment Results and Discussion.....	42
<b>4.4</b> Summary of Chapter.....	45
<b>5. CONCLUSION AND FUTURE WORKS.....</b>	<b>46</b>
<b>5.1</b> Introduction .....	46
<b>5.2</b> Research Conclusion.....	46
<b>5.3</b> Future Works.....	47
REFERENCES.....	R1
APPENDICES.....	A1
A. CURRICULUM VITAE.....	A1

## LIST OF FIGURES

### FIGURES

<b>Figure 1</b>	Overview of Mobile Ad-Hoc Network.....	1
<b>Figure 2</b>	An Ad Hoc Network .....	6
<b>Figure 3</b>	Classification of MANET Routing Protocols .....	9
<b>Figure 4</b>	Topology Graph of the Network.....	10
<b>Figure 5</b>	Route Discovery in DSR.....	14
<b>Figure 6</b>	Route Maintenance in DSR.....	15
<b>Figure 7</b>	Route Discovery in AODV .....	16
<b>Figure 8</b>	Route Maintenance in AODV .....	17
<b>Figure 9</b>	Classification of Attacks on MANET.....	21
<b>Figure 10</b>	An Example of Route Modification Attack.....	23
<b>Figure 11</b>	An Example of Impersonation Attack.....	23
<b>Figure 12</b>	An Example of Fabrication Attack.....	24
<b>Figure 13</b>	An Example of Wormhole Attack.....	25
<b>Figure 14</b>	Black Hole Problem.....	26
<b>Figure 15</b>	C++/OtcI.....	29
<b>Figure 16</b>	Simplified View of NS.....	30

## FIGURES

<b>Figure 17</b>	Directory Structure of N.....	30
<b>Figure 18</b>	Simulation Topology.....	32
<b>Figure 19</b>	Simulation Scenario.....	36
<b>Figure 20</b>	Packet Loss Versus Simulation Run Number.....	40
<b>Figure 21</b>	PDR Versus Simulation Run Number.....	40
<b>Figure 22</b>	Throughput Versus Simulation Run Number.....	41
<b>Figure 23</b>	End-To-End Delay Versus Simulation Run Number.....	41
<b>Figure 24</b>	Packet Loss Versus Simulation Run Number.....	43
<b>Figure 25</b>	PDR Versus Simulation Run Number.....	44
<b>Figure 26</b>	Throughput Versus Simulation Run Number.....	44
<b>Figure 27</b>	Shows the End-to-End Delay.....	45

## LIST OF TABLES

### TABLES

<b>Table 1</b>	Routing Table or Node 1.....	11
<b>Table 2</b>	Comparison of the Features of DSR and AODV.....	18
<b>Table 3</b>	Research Tools.....	33
<b>Table 4</b>	Traffic Pattern .....	36
<b>Table 5</b>	AODV without Black Hole.....	38
<b>Table 6</b>	AODV with Black Hole.....	39
<b>Table 7</b>	DETAODV .....	43

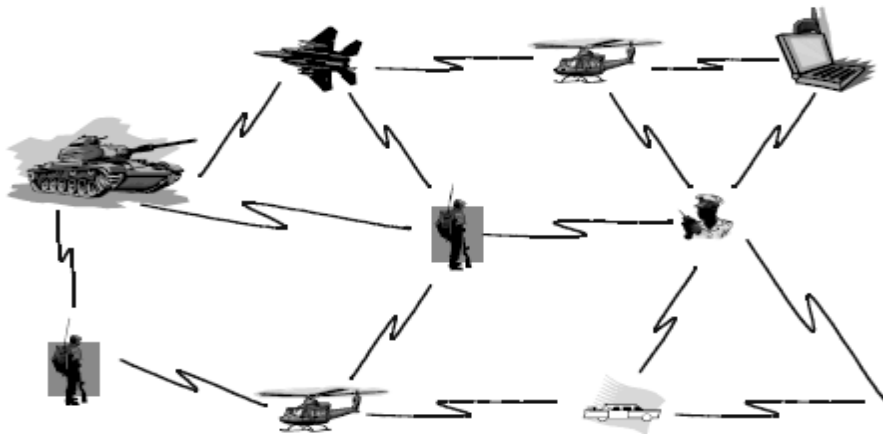
## LIST OF ABBREVIATIONS

ACM	Association for Computer Machinery
AODV	Ad-Hoc on-Demand Distance Vector
CGSR	Cluster Switch Gateway Routing Protocol
DoS	Denial-of-Service
DSDV	Destination-Sequenced Distance-Vector
DSR	Dynamic Source Routing
E2E	End-to-End
MANET	Mobile Ad-Hoc Network
NAM	Network Animator
NPDU	Network Packet Data Unit
NS2	Network Simulator 2
PDA	Personal Digital Assistants
RIP	Routing Internet Protocol
RREP	Route Reverse
RREQ	Route Request
WRP	Wireless Routing Protocol

## CHAPTER 1

### 1. INTRODUCTION

MANET is a collection of wireless equipment named wireless nodes or mobile nodes that dynamically link and transmit information. Wireless nodes or Mobile devices can be laptop, Pocket PCs, cellular phones, etc., presently inexpensive, and are becoming more public in our life according [1]. As well as Mobile devices entirely are contacting means that required an infrastructure to do their part. The infrastructures for Mobile devices might be utilize be wired, wireless cellular or wireless LAN. Nevertheless, such structure are not exist in every states. Thus, a requirement for structure less contacts. Figure 1 illustrates what MANET is.



**Figure 1** Overview of Mobile Ad-Hoc Network

Affording to [2] A network of mobile devices without an infrastructure called an Ad-hoc network as well. According to [1], a (MANET) is describe as follows:

"An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services

regularly available on the wide-area network to which the hosts may normally be connected."

In MANET, a wireless node is able to play as a resource, destination, or a middle data broadcast node. When a wireless node plays as middle node, it plays as a router which able to receive and sending packets of data to closer neighbor to the destination node. Because of an ad-hoc network nature, wireless nodes continue movement rather than remain stable. Consequently the network topology for Ad-hoc networks changes every time.

MANET are appropriate with fields where it is impossible to establish a permanent structure. Then the wireless nodes contacts between each other without a structure, wireless nodes supplied linking across sending packets between each other. In order to carry this linking, wireless nodes make utilize many of routing protocols like AODV [3, 4], DSR [5] and DSDV [6]. Moreover working as a resource, each node also perform like router to explore pathway and sending packets to exact node in network.

Wireless MANET it has a weakness an infrastructure so, they are uncovered to a bunch of invasion. Black Hole invasion [7] is one of the attacks. In the Black Hole invasion, malignant node realizes entire data packets by itself. In this way, all network packets are lost. A malignant node falling whole movement makes the network utilize of the sensitivity of the route detection packets of request protocols, like (AODV). In route explorer procedure from AODV protocol, role for middle nodes to discover new pathway to the destination, forwarding detection packets to closer nodes. This procedure do not utilize with malignant nodes, they directly react to the source node with untrue notification so however it has new sufficient pathway to destination. So resource node directs its packets of data by way malignant node to the destination guessing its correct path.

Black Hole invasion mainly occurs because of a malignant node which is destroyed node interface. Any How, network nodes will continuously attempt to discover a road for the destination that lead the node to use more power of its battery in addition to dropping packets.

## **1.1 Research Motivation**

Wireless ad-hoc networks increased significant distinguish in wireless connections. Wireless connections created by nodes playing as transferring and routers packets from one mobile node to another in MANET. As Wireless MANET come to be broadly utilize, the safety case has come to be one of the important deals for the whole times. The Black Hole invasion consider one of the most famous attack that is the public in the on-demand routing protocols like AODV. In case of AODV protocol Black hole attack regards active attack. Due to AODV protocol lack to devices, a malignant node can achieve several attacks in the network only by acting according to AODV rules [8].

## **1.2 Research Aim and Objectives**

The work presented in this thesis is aimed at the studying Performance Evaluation of Black Hole Attack on (AODV) Protocol Routing by examine AODV Protocol with and without Black Hole Attack, then we will propose an Intrusion Detection System IDS to reduce the Black Hole effects in the AODV network. In order to achieve these research aims, the following research objectives were formulated:

1. To investigate the effect of Black Hole Attack on (AODV) Routing Protocol based on the following evaluation criteria (bandwidth, delay, throughput, and packet loss).
2. To design and implement new AODV with Intrusion Detection System based in simulated network environment, where the aim of the new AODV protocol is to reduce number of dropping packets.
3. To evaluate the new AODV protocol, by a performance evaluation comparison between the new AODV protocols against the existing AODV protocol with and without attack.



### **1.3 Research Strategy**

This thesis has been arranged as follows:

**Chapter 2:** presents the overview of the background material and establishes the concepts and issues covered in this thesis. The concepts and issues covered in this chapter are. Wireless Ad-hoc networks security vulnerabilities and black hole attacks

**Chapter 3:** introduces the related work to our proposed AODV protocol.

**Chapter 4** highlights the design of the proposed AODV protocol, goals of design and steps of coding the proposed AODV protocol using NS2.

**Chapter 5** Discuss results

**Chapter6** Summarizes the research work, highlights research contributions and recommends future work related to this research.

## **CHAPTER 2**

### **BACKGROUND**

#### **2.1 Introduction**

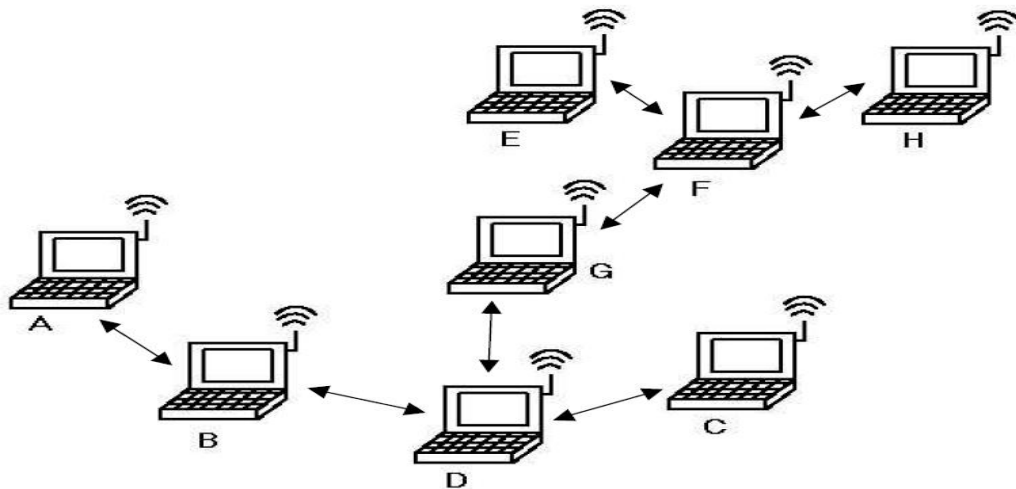
This research focuses on Performance Evaluation of Black Hole invasion on AODV Routing Protocol Using NS2. This chapter supplies the background information of the subjects to be debate in the thesis and research works that have been done on Black Hole Attack in AODV Routing Protocol. Unit 2.1 describes the overview of the MANET, while Unit 2.2 elaborates Routing protocols in MANET. Meanwhile, Section 2.3 explains the Security Issues in MANET. And finally, Section 2.4 summaries this chapter.

#### **2.2 Mobile Ad-Hoc Network (MANET)**

MANET set of nodes of wireless mobile created impermanent network short of help any stand-apart structure and compacted management [10]. Every node has wireless interface to form link and data switching with further nodes. Samples of probable MANET nodes are (PDA) and individual computer. Figure 2 displays a modest MANE that includes of mobile means modeling network short of structure.

MANET, every node of wireless possess broadcast extent. In case of all nodes in the MANET are in the same extent. So it is not necessary to use routing protocol to switching data. Nevertheless, if several of the ad hoc nodes are not inside each other's extent then a middle routers involved to contribute in sending the data between nodes. In the lack of structure in the MANET, the route would work as one of the network nodes in, hence each network node might perform as router and swarm. As a router, the node

must be capable to send data and operate routing protocol. The node performs as a swarm with an IP address in a classical sense.



**Figure 2** An Ad Hoc Network

The wireless MANET are frequently mobile. Might be dual node together in the same extent at any time. Nevertheless because their movement the two nodes probably outdoor its complement extent. Alteration in topology deals with node movement might destroy the links between nodes and consequently other links must formed. The paths in the middle of two nodes might include several links transient above several nodes in the middle: It named “multi hop routing”.

In MANET, a wireless node can be the basis, the destination, or a middle node of data transport. When a wireless node acting intermediate node role, it contributes as a router which able to receive and sending of packets data to the closer neighbor to the destination node. Because of MANET nature, wireless nodes incline to retain moving rather than remain stable. Consequently the network topology alterations from time to time. Wireless MANET have several benefits:

- a) Low cost of deployment: Ad hoc networks can be deployed on the fly; hence no expensive infrastructure such as copper wires or data cables is required.
- b) Fast deployment: Ad hoc networks are very convenient and easy to deploy since there are no cables involved. Deployment time is shortened.

- c) **Dynamic Configuration:** Ad hoc network configuration can change dynamically over time. When compared to configurability of LANs, it is very easy to change the network topology of a wireless network.

MANET has numerous likely applications. Some characteristic samples consists spare operations of search-rescue talks, debates actions and battleground traffic contacts trucks and fighters. With the facilities to face the fresh request of mobile calculation, the MANET has an actual optimistic future.

### **2.2.1 Current Challenges of Mobile Ad-Hoc Network**

In MANT whole nodes contributes with each other in purpose of send the network packet and therefore every node is successfully a router. So routing regards as one of the most distinguished issues. This thesis concerns essentially on Security topics in ad hoc networks. In this chapter, some of the other issues in ad hoc networks are termed:

- a) **Network Distribution:** A MANET is a dispersed wireless network without any stable structure. That indicates that there is no central server is involved to preserve the clients state.
- b) **Dynamic topology:** nodes are movable so therefore the network is self-order. Due to network topology maintain altering over time. Thus, the routing protocols formed to these networks have to also adaptive to the topology alterations.
- c) **Awareness of Power:** Meanwhile in an MANET nodes naturally work on batteries and are positioned in unfriendly grounds, they have harsh power wants. This suggests that the essential protocols should be formed to maintain life of battery.
- d) **Addressing scheme:** The topology of network retains altering dynamically and therefore the addressing scheme utilize is fairly important. A dynamic network topology needs a universal addressing scheme that evades any matching addresses. In wireless WAN natures, Mobile IP [11] has been

utilize. As still home clients and strange clients are wants, therefore, this answer unsuitable for MANET.

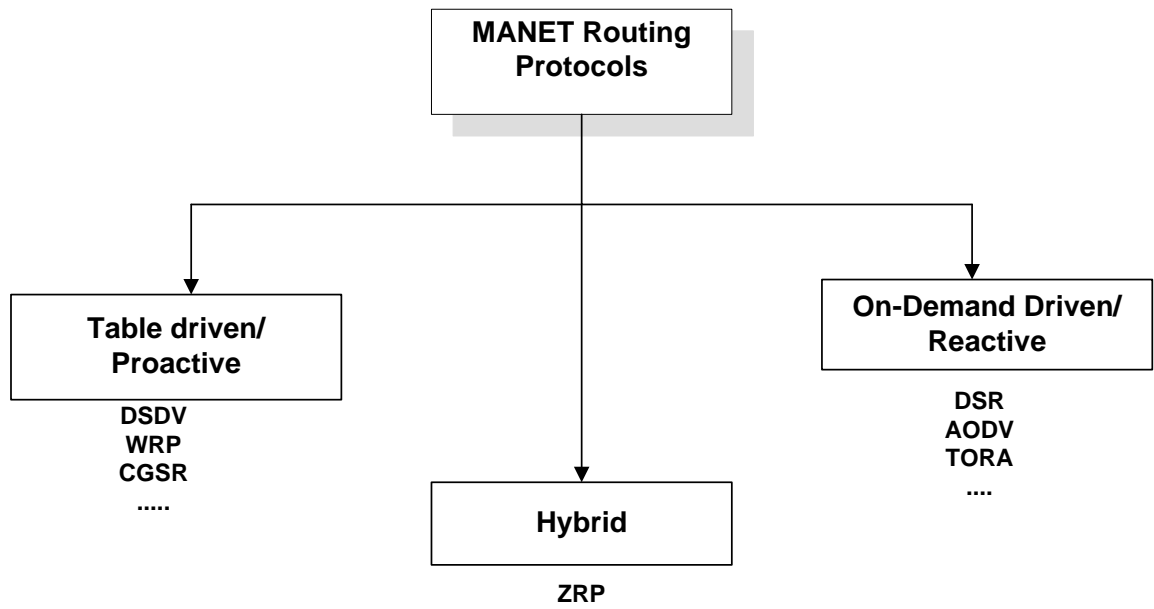
- e) Proportions of network: The capability of allow profitable tenders such like audio transport in meeting galleries, summits is a gorgeous property of MANET. Though, postponement intricate in the essential protocols positions a harsh higher relativity the network size.
- f) Security: Security in an MANET is exceedingly significant in scene such as a battleground. The security objects confidentiality, readiness, non-repudiation and integrity authenticity - are hard to accomplish in MANET, chiefly due to each node in the network contributes equally in packets of routing.

### **2.3 Routing Protocols in Ad-Hoc Network**

Routing protocols Number has suggested for ad hoc networks. In this section a broad classification of these routing protocols is given. Only the unicast routing protocols are considered and an in-depth classification of all available protocols is beyond the scope of this thesis. Figure 3 shows the classification of the routing protocols for MANETs. At one end are the table-driven or proactive routing protocols such as the (DSDV) routing protocol, (WRP), etc. At the other end, are the on-demand or reactive protocols such as (DSR) protocol and the (AODV) routing protocols. Each of these types of protocols is discussed in more detail.

#### **2.3.1 Table-Driven/Proactive Routing Protocols**

In table-driven or practical protocols, nodes preserve effectively routes list to all node in the network in routing table. Tables from time to time updated throughout spreading information to networks nodes. Thus, they are an extension to the wired network routing protocols such as the (RIP).



**Figure 3** Classification of MANET Routing Protocols

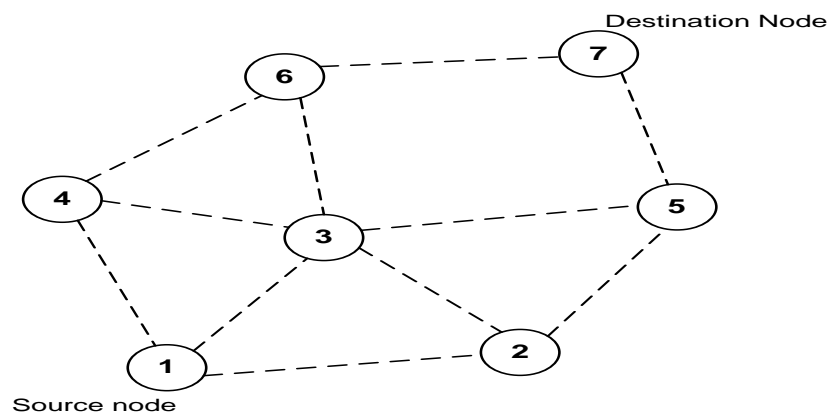
Any node wishing to communicate with another node has to obtain the next hop neighbor on the route to the destination from its table of routing. Some examples of table-driven routing protocols are (DSDV) [13], (WRP) [14], (CGSR) [15], etc. In the following sections, working of DSDV and WRP are explained, and the general pros and cons of table-driven routing protocols are enumerated.

### **2.3.1.1 Destination Sequenced Distance Vector (DSDV) Routing Protocol**

The (DSDV) [16-17] protocol is a proactive routing protocol. In this routing protocol, each mobile host preserves a table containing of the next-hop neighbor and the expanse to the destination in terms of number of hops. It utilize numbers of sequence for the destination nodes to define “freshness” of a particular route, in purpose of, to evade any little or long-lived routing iterations. If double router possess same number order, one with lesser distance metric is promoted. The sequence number increased above each update directed by the host. All the hosts from time to time transmission their tables to their neighboring nodes in order to preserve an updated the network view. The tables could be updated in two techniques – either increase or during complete discharge. Increase update is accomplished when the node doesn’t detect any chief alterations in

the topology of network. Complete discharge has achieved when network topology alterations meaningfully or in case of increment update wants more than one NPDU.

Let us consider an example to understand the routing mechanism better. Consider the network topology shown in figure 4. The routing table for this network is shown in table 1. As shown in the table, each node preserves a direction to each other node in the network during the route establishment phase. Whenever there is a link break in the network, the end node of the broken link propagates a routing table update letter with the wrecked link's weight consigned to endlessness. This message is broadcasted by every node to its neighbors. A destroyed link is denoted by an odd sequence number and an ordinary link by an even sequence number. When node 1 wants to forward data to node 7, it checks the next hop neighbor for node 7, which is 2 and passes the data packet to it.



**Figure 4** Topology Graph of the Network

Destination	Next hop	Metric	Sequence number
1	-	0	S40_1
2	2	1	S340_2
3	3	1	S22_3
4	4	1	S334_4
5	2	2	S76_5
6	3	2	S84_6
7	2	3	S94_7

**Table 1** Routing Table for Node 1

### 2.3.1.2 Wireless Routing Protocol (WRP)

The (WRP) [14] is a table-driven protocol based upon the distributed Bellman Ford algorithm and is similar to DSDV [16]. The difference between DSDV and WRP is the number of tables maintained at each node. In WRP, the following tables maintained at each node-

- a. Routing table (RT): It is used for maintaining an up to time view of the network for whole destinations. It consists of the destination node, the precursor node (penultimate node), the inheritor node (the next hop neighbor) and a flag to indicate status of the path.
- b. Link Cost Table (LCT): This table stores the cost (no. of hops to arrive the destination) of spreading messages through every link. a destroyed link cost is taken as endlessness. It also saves the update number periods conceded meanwhile the latter fruitful update was get from that link. This is achieved to distinguish link destroys.



- c. Distance Table (DT): This table stores the number of hops between a node and its destination.
- d. Message Retransmission List (MRL): The MRL consist an entrance for each update message retransmitted and has a counter for each entry which is retransmitted after the message is sent. Other fields are an acknowledgement flag and a list of messages in each update.

Every node periodically sends an update message to its neighbors, which contains a list of updates and a list of responses indicating which node must acknowledge the update. When a node detects a link break, it sends an update message to its neighbors with the link cost of the broken link set to infinity. All the nodes which had an active route to the nodes affected by the link break then update their corresponding entries to them. By storing the predecessor node information and forcing every node to check if the information is correct, WRP avoids the count to infinity problem.

### **2.3.2 On-Demand/Reactive Routing Protocols**

In difference to stand driven routing protocols, on-demand routing protocols discovery route to a destination just when it is necessary. The on-demand protocols have double stages in public – route explorer and route preservation. In route detection technique, a node desiring to connect with another node recruits a finding instrument if cannot have the route previously in its store. The destination node retorts with a legal route. The route preservation stage requires inspection for damaged links in the network and updating the boards of routing. Working of a rare responsive routing protocols is now defined.

#### **2.3.2.1 Dynamic Source Routing (DSR) Protocol**

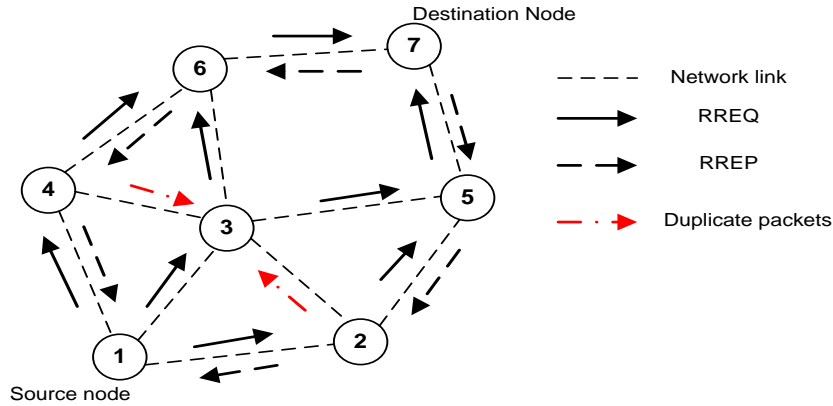
The DSR Protocol [18-19] is an on-demand routing protocol which is based on the concept of source routing. In source routing, a sender node specifies in the packet

header, the complete list of nodes that the packet must traverse to reach the destination node. This essentially means that every node just needs to forward the packet to its next hop specified in the header and need not check its routing table as in table-driven routing protocols. Furthermore, the nodes don't have to periodically broadcast their routing tables to neighboring nodes. The DSR protocol works in two phases as described below:

#### **a) Route Discovery**

Route stage of explorer, the resource node creates route through transmitting route demand (RREQ) packets to the closer neighbors. Every neighboring node, doing retransmission the packets to its neighbors if it does not previously accomplished then, if does not the destination node, affirm that TTL (Time to Live) counter is larger than zero. Additional, request ids are utilize to limit if a specific route demand has been earlier delivered by the node. Each node preserves a received list recently <initiator, request id> pairs. If double route requests with the same <initiator, request id> are received by a sending node, it transmissions just one of them and drops the other. This also avoids creation of routing iteration in the network. When the packet arrives the destination node, it unicasts a reply packet (RREP) on the reverse path return to transmitter. This reply packet includes the route to that destination. Figure 5 displays a sample of the route explorer instrument. When node 1 wishes to connect with node 7, it recruits a route explorer instrument and transmissions demand packet RREQ to the closer neighbors' nodes 2, 3 and 4 as exposed. Nevertheless, node 3 also gets the broadcast packets from 4 and 2 nodes with the same <initiator, request id> couple. It fall the two and transmissions the other packet to closer neighbor. The further nodes track same process. When the packet arrives node 7, it add its address and contraries the route in record and mono-broadcast it return on the opposite path of destination.

The destination node unicasts the best route (received first) and caches the other routes for future. A route cache is maintained at every node so that, whenever a node receives a route request and finds a route for the destination node in its own cache, it sends a RREP packet itself without broadcasting it further.

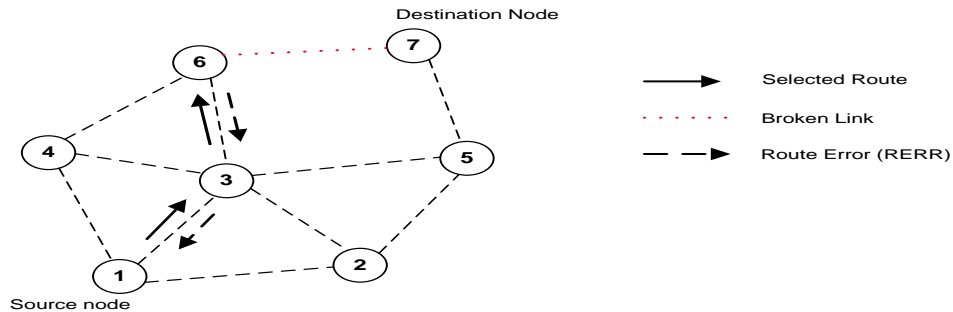


**Figure 5** Route Discovery in DSR

**b) Route Maintenance**

The maintenance route stage has accomplished when destroyed link occurred in the middle of two nodes. An unsuccessful link could determine through a node by whichever inactively watching in illegal manner or keenly watching the link. As presented in Figure 6, when a middle node in the track traffics afar. Affecting a wireless link to destroy (6-7), a route mistake packet explore process to discover a fresh route to the destination. It eliminates some route accesses it might have its in store to the destination node.

DSR profits of resource routing then the middle nodes requirement does not preserve up-to-date information of routing in purpose of route the packets which they sent. There is not want to any sporadic messages of routing advertisement. Nevertheless, the network size increases, the routing above growths since all packet must endure the whole route to the destination with it. The utilizing of route stories are a decent device to decrease the transmission postponement but overdoing of the store might conduct in weak acting. DSR disadvantage is that when there is a link breakdown, the RERR packet transmits to the creative resource, which in its role start up a process of new route explorer.



**Figure 6** Route Maintenance in DSR

Hence the link is not fixed nearby. More than a few enhancements to DSR are probable like non-transmitting route needs (when forward RREQ, nodes establish the hop border to one avoiding them from re-transmitting), complimentary route responses (when a node over hears a packet with her address itemized in the header, it forwards a RREP to the making node through fleeting the earlier hops). A comprehensive elucidation of DSR enhancement can exist in.

### 2.3.2.2 Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol

The AODV [19] become heir to the moral characteristics of dual DSDV and DSR. The AODV routing protocol utilizes responsive method to discovery routes and a proactive tactic to recognizing new path. Additionally, it discovers routes utilizing the route explorer procedure akin to DSR and utilize numbers of destination arrangement to calculate new routes. The two stages are debate in more detail-

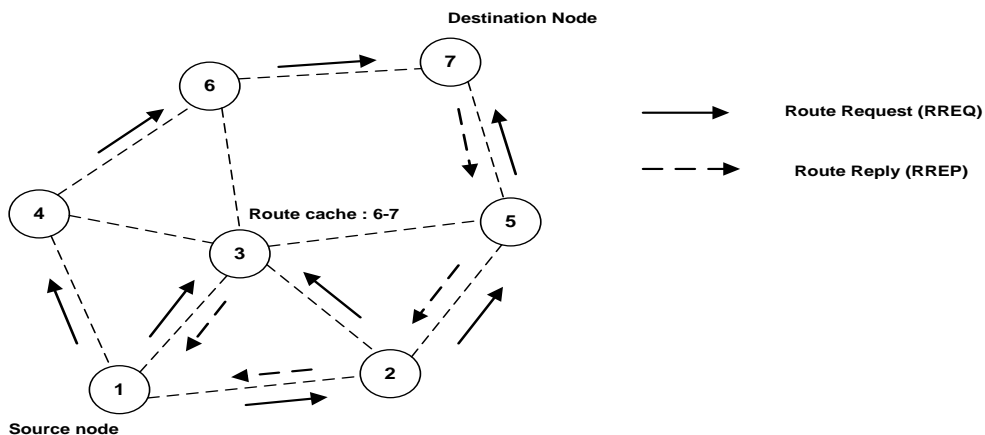
#### a) Route Discovery

Throughout process of route explorer, the resource node transmissions RREQ packets like to DSR. The RREQ packet includes the resource determiner (SId), the destination determiner (DId), and resource order number (SSeq), the destination order number (DSeq), the transmission determiner (BId) and TTL areas. When a middle node gets a RREQ packet, it either sending it or get ready a Route Reply (RREP) packet if it possess a legal route to the destination in its store. The (SId, BId) couple is utilize to define if a particular RREQ has previously been received in in purpose of remove duplicates. Every

middle node come into the former node's address and its BId while forwarding a RREQ packet. The node also maintains a timer associated with every entry in order to erase a RREQ packet if the reply is not arrived before its ending time.

Every time a RREP packet is conventional through a node, it keeps former node data in purpose of send the packet to the next hop to the destination. This performs as a "forward pointer" to the destination node. Therefore every node preserves just information of the next hop different source routing in that entire middle nodes on the route in the direction of the destination are kept.

Figure 7 displays a sample of route explorer instrument in AODV. Let us assume that node 1 wish to forward a data packet to node 7 but it does not possess in route store. Therefore it inductees a process of route explorer by transmission a RREQ packet to entire to the closer neighboring nodes.



**Figure 7** Route Discovery in AODV

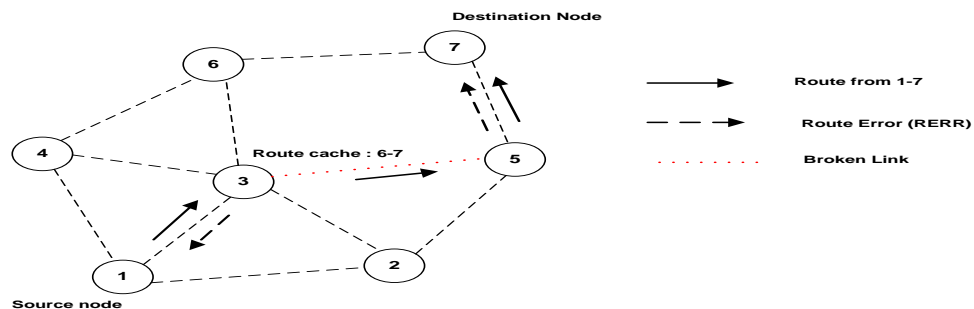
It inserts the SId, DId, SSeq, DSeq, BId, and TTL fields in the RREQ packet. When nodes 4, 3 and 2 receive this, they check their route caches to see if they already have a route. If they don't have a route, they forward it to their neighbors, else the destination sequence number DSeq in the RREQ packet is compared with the DSeq in its agreeing access in route store. If the DSeq in RREQ packet is superior, then it responses to the resource node with a RREP packet consists the route to the destination. In figure 2.6, node 3 has a route to 7 in its store and its DSeq is upper associated to that in RREQ

packet. So, it forward a RREP back to the resource node 1. Therefore the path 1,3,6,7 is kept in node 1. The destination node likewise forwards a RREP back to the resource. For model, one likely route is 1,2,5,7. The middle nodes on track of resource to destination update them list of routing with the modern DSeq in packet of RREP.

### b) Route Maintenance

The route maintenance mechanism works as follows Whenever a node detects a link break by link layer acknowledgements or HELLO beacons [20], the source and end nodes are notified by propagating an RERR packet similar to DSR. This is display in Figure 8. If the link between nodes 3 and 5 breaks on the path 1-3-5-7, then both 5 and 3 will send RERR packets to notify the source and destination nodes.

One optimization possible in AODV route maintenance is to use an expanding ring search to control the flood of RREQ and discover routes to unknown destinations [21]. The main advantage of AODV is that it avoids source routing thereby reducing the routing overload in large networks. Further, it also provides destination sequence numbers which allows the nodes to have more up-to-date routes. However, AODV requires bidirectional links and periodic link layer acknowledgements to detect broken links. Further, it has to maintain routing tables for route maintenance unlike DSR.



**Figure 8** Route Maintenance in AODV

### 2.2.2.3 Comparison of DSR and AODV

Table 2 provides a comparison of the features of DSR and AODV:

Protocol Feature	DSR	AODV
Destination Sequence Numbers	Not used	Used
Link Layer Acknowledgements	Not Required	Required (using HELLO beacons) for link breakage detection
Routing Mechanism	Source routing – Multiple route caches for each destination	Table driven – one entry per destination. Sequence numbers used for
Route Storage Mechanism	Using route caches	Using routing tables
Timers	Not Used	Used
Multiple Route Caches	Yes	No
Optimizations	Salvaging, Gratuitous route replies (RREP) and Route Error (RERR), non-propagating route requests [21]	Expanding ring search [22]

**Table 2** Comparison of the Features of DSR and AODV

The main difference is the source routing employed by DSR in contrast to table-driven routing used by AODV. Due to this, DSR has a higher routing load when the size of the network increases since each packet header has typically more information when compared to AODV. Another important difference is that AODV requires link layer acknowledgements or HELLO beacons at periodic intervals in order to detect link breaks. However, DSR avoids this feature and hence more efficient. Further, DSR stores multiple route caches for a destination whereas AODV does not. It has been found that this has an impact on the end-to-end delay and the delivery fraction as the size of the network increases [22]. DSR has been found to perform well in lightly loaded networks, whereas AODV performs well in more stressful networks (with higher density of nodes). AODV also benefits from its timer mechanisms by maintaining fresher route entries as compared to DSR, which doesn't implement any timers. Besides, in DSR all requests reaching a destination node are replied to, whereas in AODV the destination replies only once to the request arriving first and ignores others.

### **2.3.3 Hybrid Routing Protocols**

Protocols of Hybrid routing be left features of both on-demand and table-driven routing protocols. Like protocols are modeled to reduce the governor above of each reactive and practical routing protocols.

## **2.4 Security Issues in Mobile Ad Hoc Networks**

MANET have certain unique characteristics that make them vulnerable to several types of attacks. Since they are deployed in an open environment where all nodes cooperate in forwarding the packets in the network, malicious nodes are difficult to detect. Hence, it is relatively difficult to design a secure protocol for MANET, when compared to wired or infrastructure-based wireless networks. This section discusses the security goals for an ad hoc network.



To secure the routing protocols in MANETs, researchers have considered the following security services: availability, confidentiality, integrity, authentication and non-repudiation [13-14-15-16].

**Availability** guarantees the survivability of the network services despite attacks. A (DoS) is a potential threat at any layer of an ad hoc network. On the media access control layer, an adversary could jam the physical communication channels. On the network layer disruption of the routing operation may result in a partition of the network, rendering certain nodes inaccessible. On higher levels, an attacker could bring down high-level services like key management service.

**Confidentiality** ensures that certain information be never disclosed to unauthorized entities. It is of paramount importance to strategic or tactical military communications. Routing information must also remain confidential in some cases, because the information might be valuable for enemies to locate their targets in a battlefield.

**Integrity** ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.

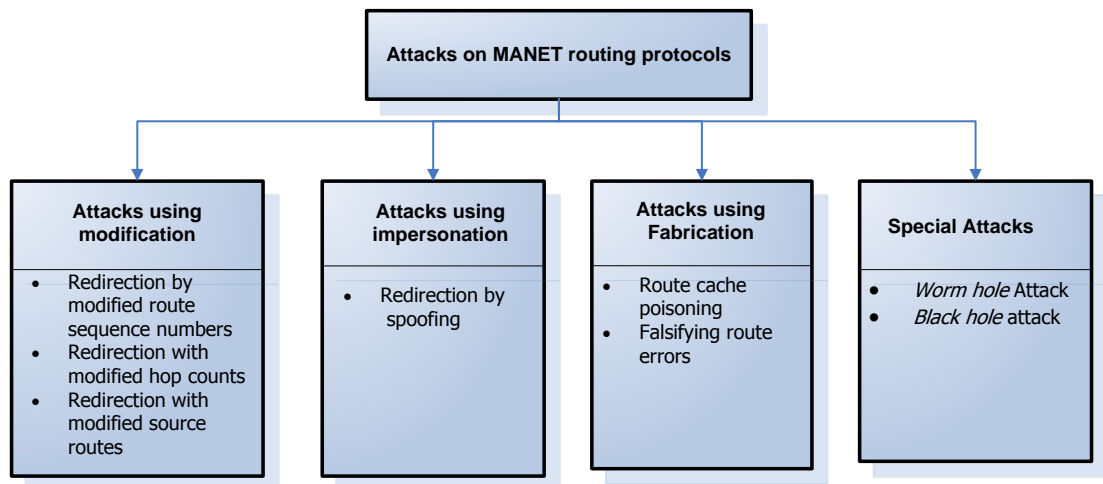
**Authentication** enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information.

**Non-repudiation** ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

The networking surroundings in wireless outlines makes the routing protocols defenseless to attacks extending from passive overhearing to on the go attacks such as sendup, message replay, network partitioning, message littering. Nose round is a risk to active and confidentiality invasion are dangers to disposal, verification, truthfulness and non-repudiation. Nodes drifting in an ad hoc surroundings with poor external protection are fairly defenseless and they might been cooperated. Once the

nodes are compromised, they could be utilize as star refer to launch invasion against the routing protocols.

In general, the attacks on routing protocols can generally be classified as routing disruption attacks and resource consumption attacks [27-28-29-30]. In routing disruption attacks, the attacker tries to disrupt the routing mechanism by routing packets in wrong paths; in resource consumption attacks, some non-cooperative or selfish nodes may try to inject false packets in order to consume network bandwidth. Both of these attacks are examples of DoS attacks. Figure 9 depicts a broader classification of the possible attacks in MANETs.



**Figure 9** Classification of Attacks on MANET [31]

**a) Attacks using Modification**

this kind of attacks, nearly of the protocol areas the letters passed across nodes are modified, thus subsequent in movement rebellion, redirection or DoS invasion. We argues these invasion in details.

✓ **Modification of route sequence numbers:**

This attack is possible against the AODV protocol. The malicious node can change the sequence number in the route request packets or route reply packets in order to make the route fresh. In Figure 2.9, malicious node M receives a route request RREQ from node B that originates from node S and is destined for node X. M unicasts a RREP to B with a higher destination sequence number for X than the value last advertised by X. The node S accepts the RREP and then sends the data to X through M. When the legitimate RREP from X gets to S, if the destination number is less than the one advertised by M, then it will be discarded as a stale route. The situation will not be corrected until a valid RREP with higher sequence number than that of M gets to S.

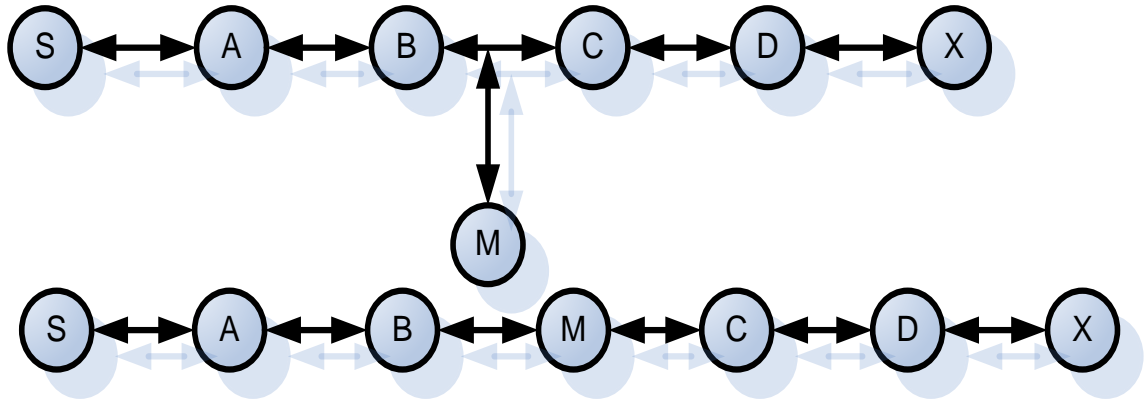
✓ **Modification of hop count:**

This attack is possible against DSR which uses source routes and works as follows. In Figure 2.9, it is assumed that the shortest path exists from S to X. It is also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to X with the source route S-A-B-C-D-X. If M intercepts this packet, it removes D from the list and forwards it to C. C will attempt to forward this packet to X which is not possible since C cannot hear X. Thus M has successfully launched a DoS attack on X.

✓ **Modification of source route:**

This attack is possible against DSR which uses source routes and works as follows. In Figure 10, it is assumed that the shortest path exists from S to X. It is also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to X with the source route S-A-B-C-D-X. If M intercepts this packet, it removes D from the

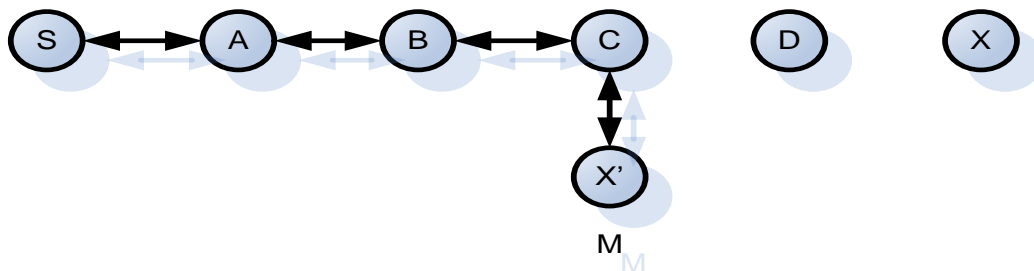
list and forwards it to C. C will attempt to forward this packet to X which is not possible since C cannot hear X. Thus M has successfully launched a DoS attack on X.



**Figure 10** An Example of Route Modification Attack [31]

**b) Attacks using Impersonation**

This type of invasion violates confidentiality and authenticity in network. A malignant node able to imitate or skit the address of different node in our pose of change the image of the network topology as observed by another node. Such attacks can be described as follows in Figure 11.

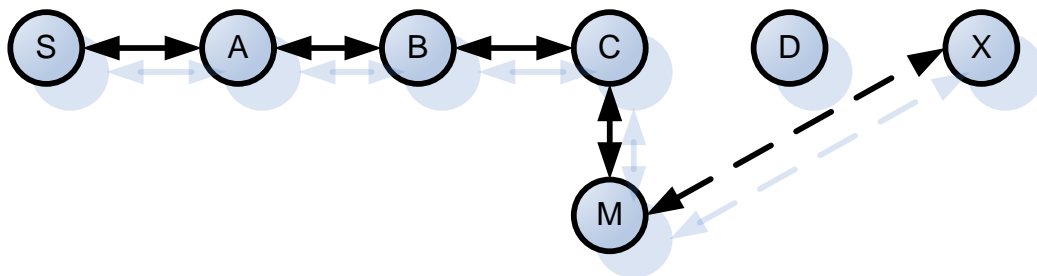


**Figure 11** An Example of Impersonation Attack [32]

Node S wish to forward information to node X and initiates process of Route explorer. The malignant node M, nearest to node S than node X, impersonates node X as X'. It sends a route reply (RREP) to node S. Shorn of inspection the RREP validity, node S receives the route in the RREP and begin to forward information to the malignant node. This kind of invasion could be reason behind loop of routing inside the network.

### c) Attacks Using Fabrication

In this type of attacks, a malicious node tries to inject fake messages or routing packets to disrupt the routing mechanism. These attacks are difficult to detect in a MANET since the routing packets appear to be legitimate packets to the nodes processing them. Attacks by fabrication are discussed in [33] [32] [34]. Figure 12 is an example of fabrication attacks. Node S wants to send data to node X, so it broadcasts a route request in order to find the oute to node X. Malicious node M pretends to have a cached route to the destination X, and returns route reply to the source node (S). The source node, without checking the validity of the RREP, accepts the RREP and starts to send data through M. Furthermore, malicious nodes can fabricate RERR to advertise a link break to a certain node in a MANET with AODV or DSR protocols.



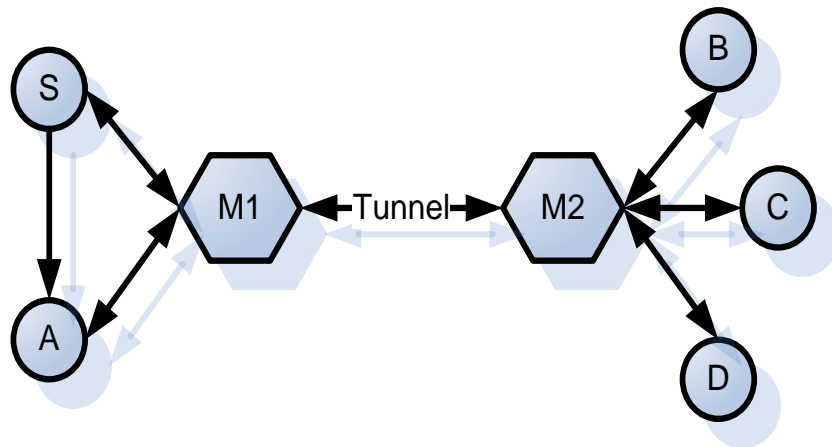
**Figure 12** An Example of Fabrication Attack [32]

### d) Special Attacks

attack of wormhole [35] [36] is a severe invasion kind that two malignant nodes able to sending packets across a special “channel” in the network as displayed in Figure 2.12.

✓ **Wormhole Attack**

Attacks of wormhole [35] [36] is a severe invasion kind that two malignant nodes able to sending packets a special “channel” in the network as displayed in figure 13. Here, M1 and M2 are two malicious nodes which connect during a special link. Every packet that M1 gets of network is advanced throughout “wormhole” to node M2, and vice versa. This invasion interrupts routing protocols by little circuiting the routing packets normal flow. Such a type of invasion is hard to determine in a network, and might destroys connections amongst the nodes. Like invasion could be avoided by utilize packet chains [36], that validate the timing data in the packets to determine fraud packets in the network.



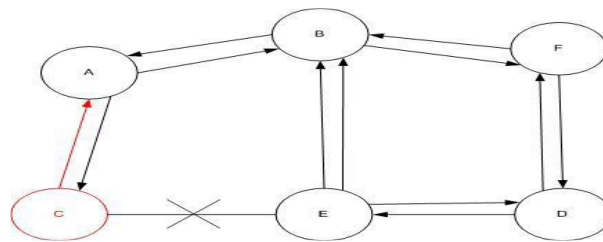
**Figure 13** An Example of Wormhole Attack [36]

✓ **Black Hole attack**

Black hole attack is that attack type that happens in (MANET). In invasion of black hole, a malignant node utilize its routing protocol in purpose of announce possess the nearest track to the destination node or to the packet it needs to interrupt. This inimical node announces its existence of fresh routes regardless of inspection its routing board. In this method invader node would constantly possess existence in responding to route demand and hence seize the data packet and preserve it. When this route is create, now it's up to the node whether to drop all the packets or sends it to the unidentified address.

The theory of malignant node fit in differs of data route. Figure 14. Displays how black hole difficult rises, now node “A” need to forward data packets to node “D” and inductee process of route mining. Then if node “C” is a malignant node at that time it is going to assertion that it possess inactive route to the definite destination as soon as possible it arrives packets of RREQ. Then It is going to forward the reply to node “A” afore any node. In this method node “A” is going to thought that this is the effective route and hence effective route explore is achieve. Node “A” would disregard all answers and are begin sowing data packets to node “C”. In this method ever packet data would waste spent.

The AODV protocol is vulnerable to such an attack which has two types of black hole invasion can be described in AODV in order to distinguish the kind of black hole attack.



**Figure 14** Black Hole Problem

**a) Internal Black Hole attack**

The black hole invasion type possess an inner malignant node that suitable in among the routes assumed resource and destination. As soon as it have opportunities malignant node make itself a lively data route component. In this phase it is currently skilled of conducting invasion during the beginning of data broadcast. This is an inner invasion due to node itself returns to data route. Inner invasion is further defenseless to protect against due to troubles in determine the inner disobedient node.

**b) Outside Black Hole Attack**

Outside invasion bodily remain outdoor of the network and reject admittance to network movement or forming crowding in network or throughout upsetting the whole network.

Outside invasion could be inner invasion type once it take place governor of inner malignant node and control it to invasion in the left nodes in MANET.

## **2.5 Summary of Chapter**

This chapter supplies the background on the subjects that are covered in this thesis. Firstly, the mobile Ad-Hoc network was presented, followed by an outline of Routing protocols in Ad-Hoc network is explained. Next, explanation of Security Issues in MANET. In the next chapter, the methodology used in this thesis effort will be explained in detail.



## CHAPTER 3

### RESEARCH METHODOLOGY

#### 3.1 Introduction

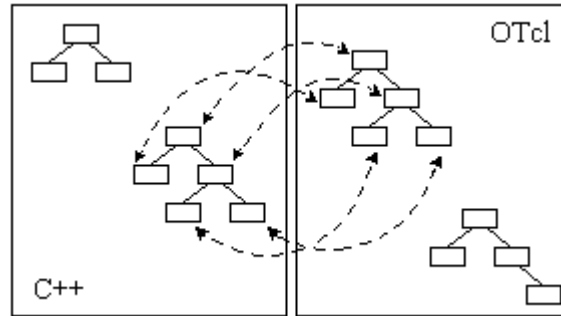
This research aims to evaluate the AODV protocol with black hole attack, designing, implementing and testing a proposed DETAODV protocol. This chapter explains a research methodology that has been chosen for performance evaluation of AODV protocol and DETAODV protocol using NS2. Section 3.1 discusses the NS2 network simulator. Section 3.2 elaborates on network simulation topology research. Section 3.3 discusses the research performance metrics, and finally, Section 3.4 summarizes the chapter.

#### 3.2 NS2 Simulator

NS2 is a program planned to make the networking simulation scene without possess the real hardware. It could be utilize to examine several phases of a networking surrounding containing the new protocols improvements.

NS2 is a discrete event simulator printed in C++, with an OTcl interpreter as a front-end. The simulator backings a class hierarchy in C++, and alike class hierarchy within the OTcl interprete. The dual hierarchies are very associated from one to another. To the operator's point of view, there is a one-to-one harmony among a class in the understood hierarchy and one in the accumulated hierarchy. Class TclObject is origin of the complied. Operator invented new simulator goals during the interpreter; these goals are instantiated inside the interpreter, and are carefully alike through a harmony goal in the compiled hierarchy. The understood session hierarchy is mechanically set up during ways determine in the layer TclClass. Goals of operator instantiated are reflected

through techniques described in the class TclObject. Figure 15 shows how an OTcl script representing a given network configuration is written. NS2 is simply composed of an OTcl script and OTcl explainer that can translate the code related to NS2 using the NS2 simulation library.

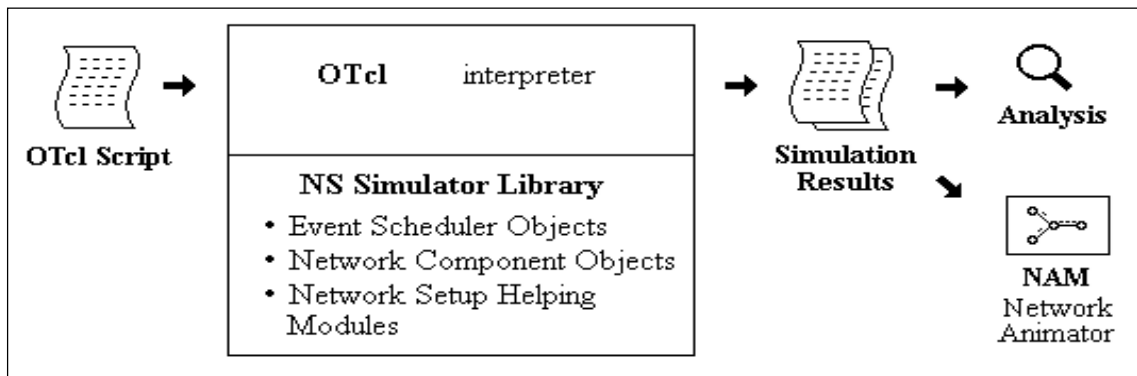


**Figure 15** C++/OTcl

NS2 uses two languages because the simulator has two different kinds of things it needs to do. On the one hand, detailed simulations of protocols require a systems programming language which can efficiently manipulate bytes, packet headers, and implement algorithms that run over large data sets. For these tasks, the run-time speed is important and the turn-around time is less important. On the other hand, a large part of network research involves slightly varying parameters or configurations, or quickly exploring a number of scenarios. In these cases, the iteration time is more important. Since configuration runs once, the run-time of this part of the task is less important. C++ is fast to run but slower to change, making it suitable for detailed protocol implementation. OTcl runs much slower but can be changed very quickly, making it ideal for simulation configuration.

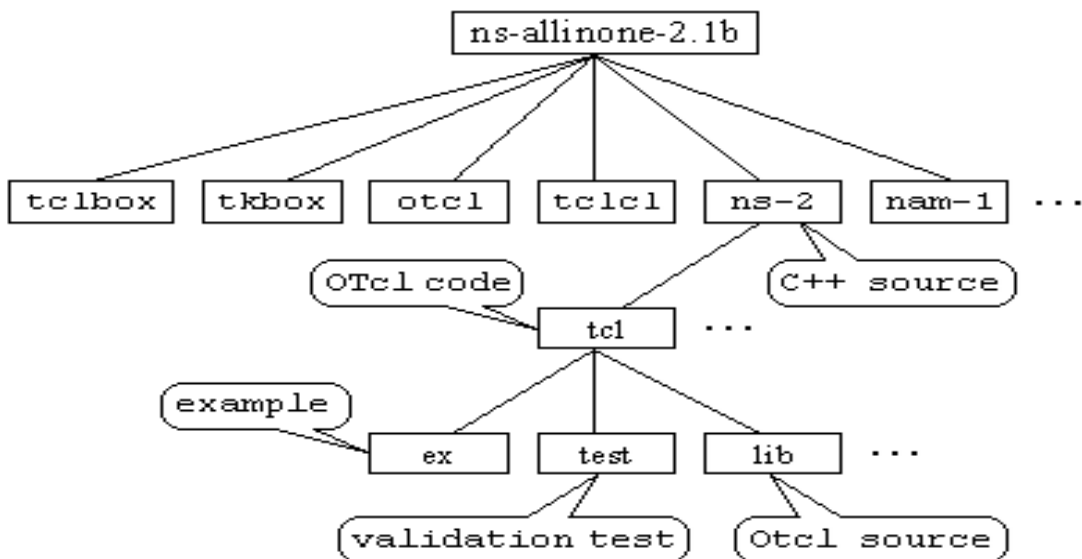
While a simulation is achieved, NS2 yields one or more text-based production records which includes clarified imitation information, if definite to do hence in the insert OTcl script. The information might utilize for imitation investigation or like an input to a graphical imitation exhibition instrument named NAM Network Animator . NAM has an enjoyable graphical operator interface which can expose information graphically alike amount and number of packet droplets in every link, though the graphical data

impossible to utilize for exact simulation examination. The overall simulation procedure in NS2 is shown in Figure 16.



**Figure 16** Simplified View of NS

The sub-directories of ns-allinone are shown in Figure 17, where NS2 has all of the imitator carrying out in C++ or in OTcl, validation of OTcl scripts and sample OTcl scripts inside the validation test directory, all OTcl codes and test/example scripts placed below the sub-directory named tcl, as well as most of the C++ code.



**Figure 17** Directory Structure of NS

NS2 is supplied with a huge collection of explained authentication scripts. Through utilizing the scripts, it makes self- authentication as sort of the form process. Via the self- authentication form process, the imitator is run utilizing a definite group of input values with common productions. Since, the productions from the self- authentication are in contrast with the famous production to authenticate the results. At last, the operator is informed if NS2 fails to authenticate one of its parts throughout the form process.

The main advantage of the NS2 simulator is that it is an open-source software and hence freely available. Further, it is also easily extensible; any addition or modification to existing routing protocols is relatively easy. However, the flip side is the complexity of coding – An understanding of two languages, C++ and Tcl is needed to develop any new protocols due to the split-programming approach. Besides, the user interface is also not attractive and the learning curve is steep.

### **3.3 Network Simulation Topology**

Selection of appropriate network topologies in simulating communication network systems is very important. The right network topology ensures that it is representing the problems under investigation, and the simulation results are as general as possible. Figure 18 show topology used in the thesis.

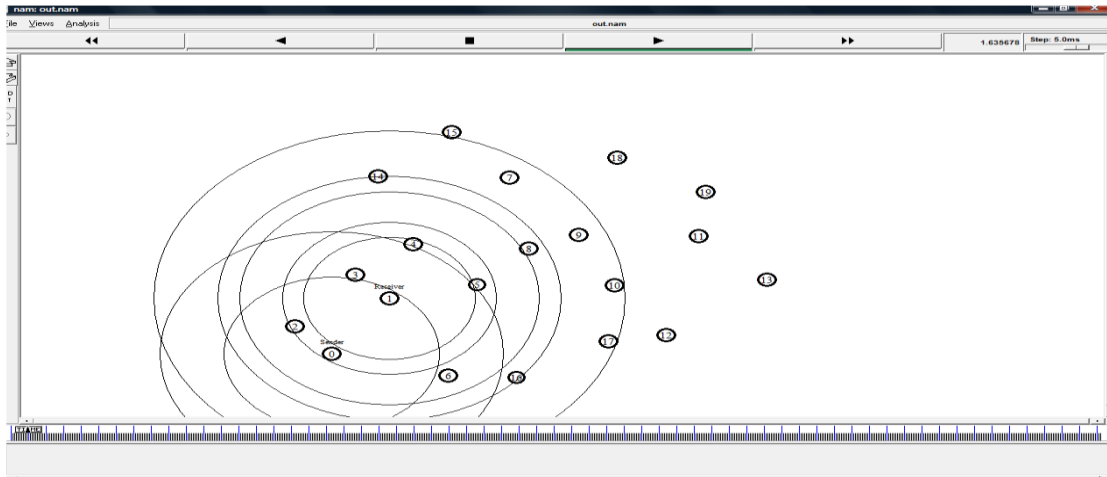
### **3.4 Research Performance Metrics**

#### **✓ End-to-End Delay**

E2E delay indicates to the consumed time for a packet in order to convey through a network from the resource to the destination. To calculate the E2E postponement, we used the following formula.

$$D = Td - Ts \tag{3.1}$$

Where  $Td$  is the time of packet arrival at the destination and  $Ts$  is the packet forward time at the resource node.



**Figure 18** Simulation Topology

✓ **Packet Loss**

Packet loss is the inability of one or more conveyed packets to reach to its destination. This incident could be obvious influence in all digital communications kinds. To calculate the packet loss, we used the formula.

$$Pd = Ps - Pa \quad (3.2)$$

Where  $Ps$  is the sum of packets forward and  $Pa$  the sum of packets arrived

✓ **Throughput**

Throughput is the degree that a network forward and receives information. It is better tunnel network contacts capability and rated in principles of bits per second (bit/s). To calculate the throughput, we used the formula.

$$Tp = \frac{Pa}{Pf} \quad (3.3)$$

So  $Pa$  is the packets arrived and  $Pf$  is the forwarded packets amount above specific time conclusive.

✓ **Packet delivery ratio**

The amount of delivered data packet ratio to the destination. This refer the delivered data level to the destination.

$$\frac{\sum \text{Number of packet receive}}{\sum \text{Number of packet send}} \quad (3.4)$$

### 3.4 Summary of Chapter

In this chapter, we have elaborated the NS2 by giving more details since the NS2 has been chosen as the network simulator for this research. We describe the network simulation topology and performance evaluation metrics used to assess the AODV protocol with and without attacked. The important tools for this research can be found in Table 3.

In this chapter, we have elaborated on the methodology for this research, and in the next chapter. We will show simulation result and effect of black hole attack in AODV protocol and the proposed protocol to solve black hole attack problem.

Item	Technique Used
Evaluation Technique	Simulation Technique
Simulator	Network Simulator 2 (NS2 )
Queuing Management	Drop Tail
Nodes Number	20
Traffic Source	CBR
Performance Metrics	packet loss, throughput, end-to-end delay, PDR,
MAC type	Mac/802_11
Routing Protocol	AODV
Packet Size	512
Area Size	678X541
Simulation Length	100 second
Channel Type	Wireless Channel

**Table 3** Research Tools

## CHAPTER 4

### PERFORMANCE EVALUATION OF BLACK HOLE ATTACK

#### 4.1 Introduction

Over the past few years there has been a growing interest in the research community for simulation study of performance evaluations of black hole attack and its effect MANET, since there is a lack of necessary infrastructure for MANET to be deployed in a realistic scenario. A simulation study gives us an idea of how a protocol performs when it is practically employed. However, the main contest in the simulation study of MANET is the dynamic behaviors of the network topology and the physical environment in which the nodes operate. In order to gain an insight of how a protocol performs when deployed in a realistic scenario, it is imperative that the simulation capture the exact nature of the physical environment and the movement of the nodes in the network, which might not be possible in all cases. For example consider a scenario where a set of nodes are deployed in a rescue operation. Even though the mobility of the nodes can be captured with certain realistic mobility models, the node doesn't capture the exact physical environment in which the nodes operate.

This chapter we will elaborate the simulation study of performance in Ad-Hoc networks using the network simulator ns-2 and certain realistic mobility models used to model the movement of the nodes. The experiments group carried out to study the behavior of AODV with and without black hole.

## 4.2 Evaluation of the Black Hole Attack

The main purpose of this experiment was to investigate and evaluate the AODV with and without Black Hole Attack to identify the needed for new AODV protocol that can detect the Black Hole Attack node. In order to investigate and evaluate the effects of the Black Hole Attack in AODV we conducted simulation experiment. The first experiment studied the AODV with and without Black Hole Attack in relation to the Drop Tail queue policy with d queue size of 30 packet. We chose, Drop Tail because Internet routers employ Drop Tail as queue management.

### 4.2.1 Experiment 1 Design

The ns-2 simulator was utilize for the tests. Right now the traffic will explained, the scene explanation and the metrics that were utilize for the tests.

#### 4.2.1.1 The traffic pattern

The traffic pattern file was generated using the “Saif1.tcl” script. The parameters used were as follows:

#### 4.2.1.2 Metrics

##### ✓ End-to-End Delay

E2E delay indicates to the time consumed for a packet to be transport through a network of the resource to the destination. To calculate the E2E delay, we used the following formula.

$$D = Td - Ts \tag{4.1}$$

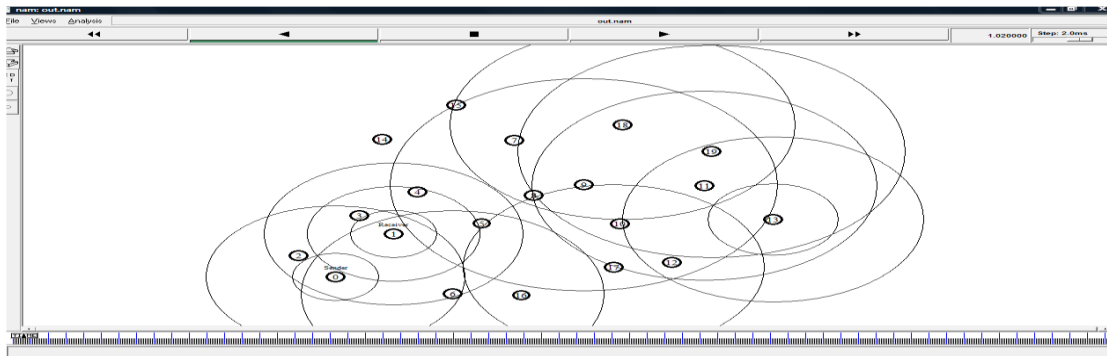


Where  $Td$  is the packet reached period at the destination and  $Ts$  is the packet forward period at the resource node.

Type of Traffic	CBR
Packet Size	1500bytes
Packet Rate	0.1Mb
Maximum Number Of Connections	30

**Table 4** Traffic Pattern

The scenario was generated using TCL as in Figure 19.



**Figure 19** Simulation Scenario

✓ **Packet Loss**

Loss of Packet is the inability of one or more transmitted packets to reaches to the destination. This incident could reason of obvious influence in all digital communications kinds. To calculate the packet waste, we used the formula.

$$Pd = Ps - Pa \quad (4.2)$$

So  $Ps$  is the packets sent amount and  $Pa$  the packets received amount.

✓ **Throughput**

Throughput is the ratio at that a network forward and reached information. It is a best tunnel capability of network contacts and rated in principles of bits per second (bit/s). To calculate the throughput, we used the formula.

$$Tp = \frac{Pa}{Pf} \quad (4.3)$$

So *Pa* is the packets received and *Pf* is the forwarded packets sum above specific time conclusive.

✓ **Packet delivery ratio**

The number of delivered data packet ratio to the destination. This explain delivered data level to its destination.

$$\frac{\sum \text{Number of packet receive}}{\sum \text{Number of packet send}} \quad (4.4)$$

#### **4.2.2 Experiment Results and Discussion**

Now, let us go on with a discussion of the simulation results experiment, which was based on the simulation trace file analysis. Tables and graphs will be used as we explain discuss its results. We present the results of the simulation experiments in Tables 4 and 5. Table 4 displays the results of an AODV without black Hole and Table 5 shows the results of an AODV without black hole.

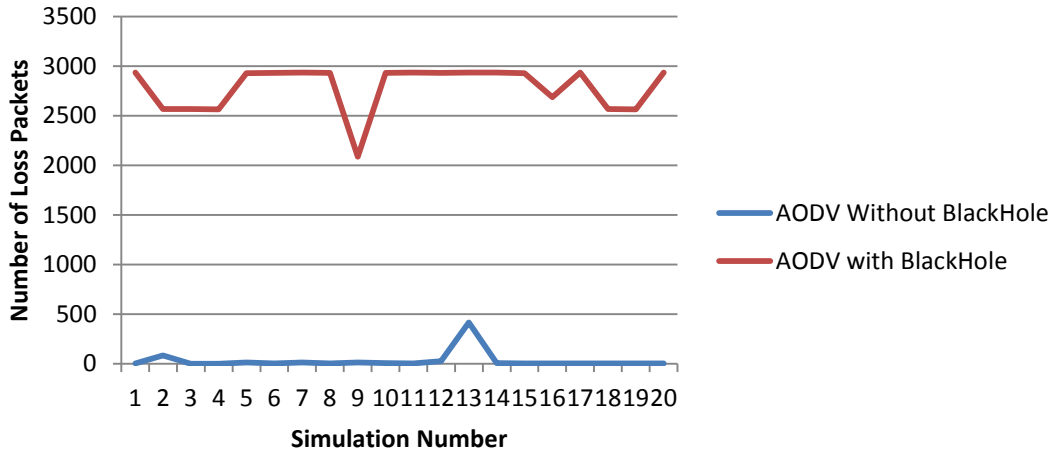
<b>E2E Delay Ms</b>	<b>Throughout kbps</b>	<b>PDR</b>	<b>Dropped</b>	<b>Received</b>	<b>Send</b>
3.0532	220.41	99.9	3	5327	5330
2.9532	217.06	98.4	84	5246	5330
2.9532	220.49	99.9	1	5329	5330
3.2532	220.49	99.9	1	5329	5330
3.5532	220.06	99.7	13	5317	5330
3.6532	220.5	99.9	2	5328	5330
2.9532	219.9	99.7	14	5316	5330
3.2532	220.41	99.9	3	5327	5330
3.1532	220.02	99.7	14	5316	5330
2.9532	220.25	99.8	7	5323	5330
3.2532	220.44	99.9	2	5328	5330
3.4532	219.46	99.5	26	5304	5330
3.7532	203.28	92.1	417	4913	5330
3.1532	220.31	99.8	7	5323	5330
3.1532	220.45	99.9	2	5328	5330
3.1532	220.52	99.9	2	5328	5330
3.1532	220.52	99.9	2	5328	5330
3.1532	220.45	99.9	2	5328	5330
3.1532	220.52	99.9	2	5328	5330
3.1532	220.52	99.9	2	5328	5330

**Table 5** AODV without Black Hole

<b>E2E delay ms</b>	<b>Throughput kpbs</b>	<b>PDR</b>	<b>Dropped</b>	<b>Received</b>	<b>Send</b>
5.0431	113.8	42.2	2936	2149	5085
4.0431	210.2	49.4	2568	2517	5085
4.6431	210.2	49.4	2568	2517	5085
4.3431	130.5	49.5	2565	2520	5085
4.8431	111.55	42.35	2931	2154	5085
4.0431	225.52	42.3	2934	2151	5085
4.0431	111.28	42.2	2935	2150	5085
4.3431	179.6	42.3	2934	2151	5085
4.0431	124.1	58.9	2086	2999	5085
4.0431	149.1	42.3	2932	2153	5085
4.7431	225.6	42.2	2935	2150	5085
6.0431	255.6	42.3	2934	2151	5085
4.5431	111.43	42.2	2935	2150	5085
4.4431	225.6	42.2	2935	2150	5085
5.0431	111.7	42.3	2930	2155	5085
4.0431	223.1	47.1	2688	2397	5085
4.0431	149.2	42.2	2935	2150	5085
5.0431	174.6	49.4	2568	2517	5085
5.0431	174.9	49.5	2565	2520	5085
4.6431	179.4	42.2	2935	2150	5085

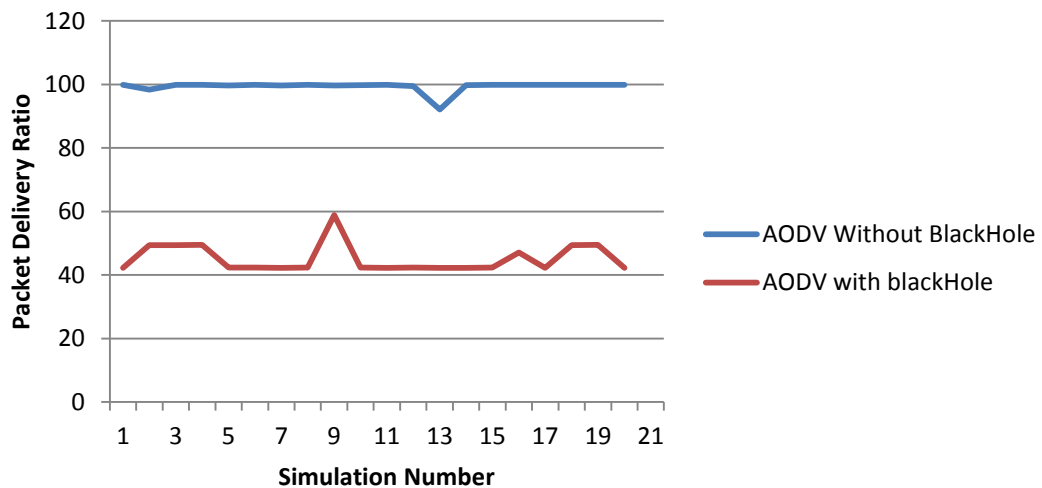
**Table 6** AODV With Black Hole

Figure 20 shows the amount of packet loss for various run number of simulation with and without using black hole.



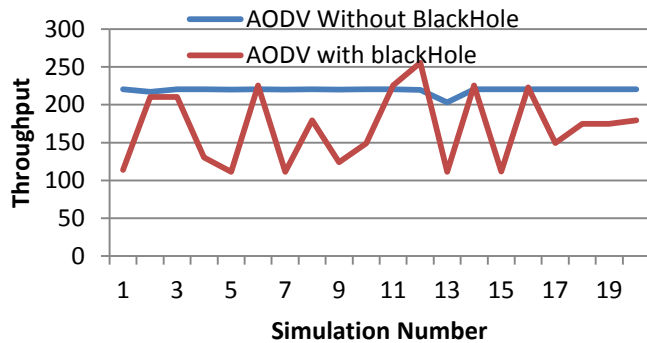
**Figure 20** Packet Loss Versus Simulation Run Number

From the figure, we can note that the packet waste amount with black hole is further than without black hole; the causer is that with black hole, the sender sends packets but black hole node drop all in coming packets. Figure 21 shows the packet Delivery ratio, for various run number of simulation with and without utilizing black hole. From the figure, we could detect that PDR amount with black hole is less than without black hole; the reason is that with black hole has more packets loss than without black hole.



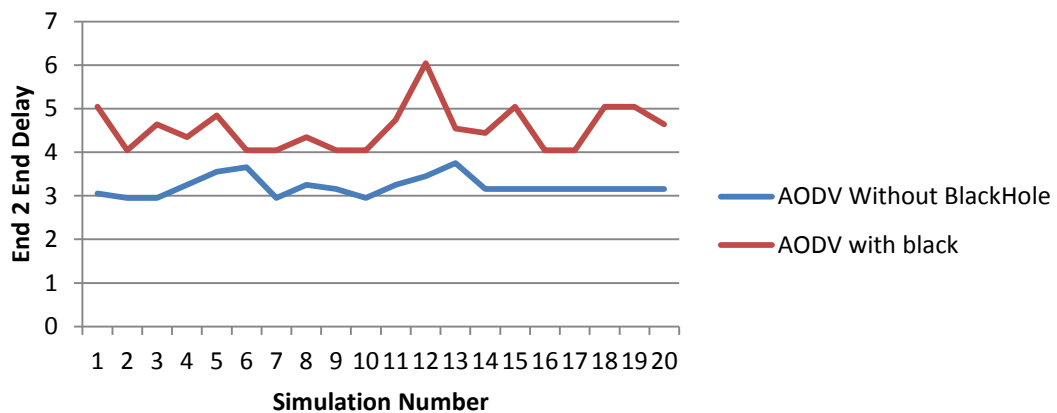
**Figure 21** PDR Versus Simulation Run Number

Figure 22 shows the Throughput, for various run number of simulation with and without using black hole.



**Figure 22** Throughput Versus Simulation Run Number

From the figure, we can observe that the amount of Throughput with black hole is not stable due to large number of packets loss, while Throughput without black hole is mostly stable due to less number of loss packets. Figure 23 shows the end-to-end delay, for various run number of simulation with and without using black hole. From the figure, we can observe that the amount of delay with black hole is more than without black hole that is because number malicious node.



**Figure 23** End-To-End Delay Versus Simulation Run Number

Finally we conclude that black hole does effect on the performance of AODV protocol, so in next section we will developed new AODV protocol that can detect the black hole and stop sending packets.

### **4.3 Implementation of Detected AODV Protocol**

The Detected AODV protocol does not exist in the NS2. Therefore, we will present the implementation of Detected AODV protocol in this following subsection.

Before we discuss further the implementation of the Detected AODV protocol, we have to declare the data structure for the new Detected AODV protocol header which is going to carry the relevant data and to declare as well that the class Detected AODV protocol Agent is considered as a subclass of the class Agent.

Implementing new objects or modifying the existing objects in NS2 requires C++ code to be used. Therefore, implementing the Detected AODV protocol requires C++ code to be added to the Detected AODV protocol agent.

After the data structure and subclass were declared we defined the linkage between the C++ code and Tcl code for Detected AODV protocol.

#### **4.3.1 Experiment 2 Design**

In order to evaluate the new Detected AODV protocol, we conducted comparative performance evaluation experiments between AODV with black hole, AODV without black hole and Detected AODV protocol. We used same configuration in experiment 1 but here we user DETADOV protocol instant of AODV.

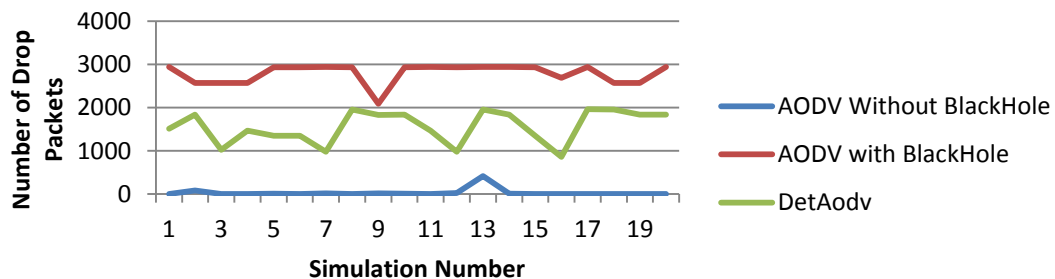
#### **4.3.2 Experiment Results and Discussion**

Now, let us go on with a discussion of the simulation results experiment, which was based on the simulation trace file analysis. Tables and graphs will be used as we explain discuss its results. We present the results of the simulation experiments in Tables 7 Table 7 shows the results of a DETAODV.

Figure 24 shows the amount of packet loss for various run number of simulation with and without using black hole and DETAODV. From the figure, we can notice that the packet waste amount have been decreased when DETADOV used as compare to AODV with black Hole. Reason when DETAODV detected the attack node it will stop send packets.

E2E delay ms	Throughput kbps	PDR	Dropped	Received	Send
4.01	358.1	70.2	1513	3572	5085
4.02	344.9	63.9	1834	3251	5085
4.1	378.3	79.8	1025	4060	5085
4.2	360.1	71.1	1467	3618	5085
4.3	365.1	73.1	1348	3737	5085
4.08	365.1	73.53	1346	3739	5085
4.01	380.2	80.7	981	4104	5085
4.02	339.8	61.5	1956	3129	5085
4.1	345	63.9	1831	3254	5085
4.2	344.9	63.9	1833	3252	5085
4.3	360	71.1	1469	3616	5085
4.08	380.2	80.7	981	4104	5085
4.01	339.9	61.5	1955	3130	5085
4.02	344.1	63.9	1834	3251	5085
4.1	365	73.5	1347	3738	5085
4.2	385.1	83	860	4225	5085
4.3	339.7	61.4	1959	3126	5085
4.2	339.8	61.5	1956	3129	5085
4.3	344.9	63.9	1834	3251	5085
4.08	344.9	63.9	1833	3252	5085

**Table 7 DETAODV**

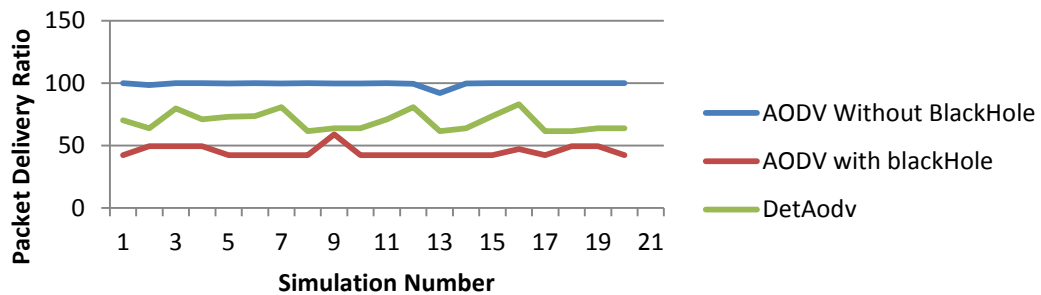


**Figure 24 Packet Loss Versus Simulation Run Number**

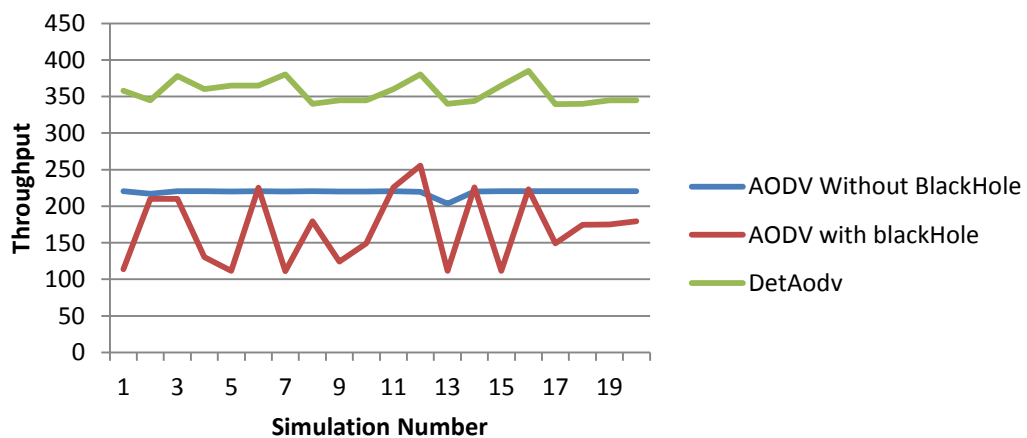


Figure 25 shows the packet Delivery ratio, for various run number of simulation with and without using black hole and DETAODV. From the figure, we can observe that the amount of PDR with black hole is less than without black hole and DETADOV; the reason is that with black hole has more packets loss than without black hole and DETADOV.

Figure 26 shows the Throughput, for various run number of simulation with and without using black hole and DETAODV. From the figure, we can observe that the amount of Throughput with black hole is not stable due to large number of packets loss, while Throughput without black hole is mostly stable due to less number of loss packets. DETAODV has more throughput as compare to AODV with and without using black hole due the Detecting mechanism.

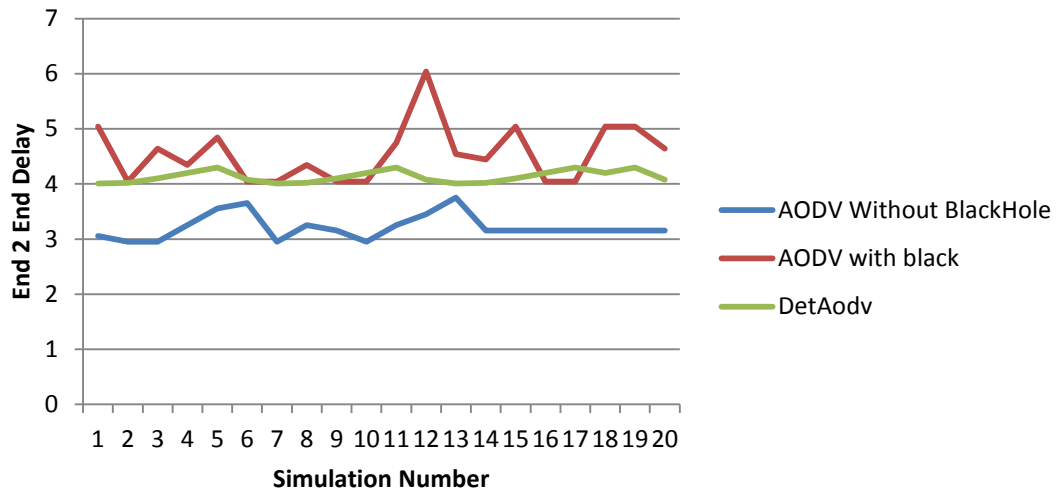


**Figure 25** PDR Versus Simulation Run Number



**Figure 26** Throughput Versus Simulation Run Number

Figure 27 shows the end-to-end delay, for various run number of simulation with and without using black hole and DETAODV. From the figure, we can observe that the amount of delay with black hole is more than without black hole and DETAODV that is because number malicious node.



**Figure 27** the End-To-End Delay, For Various Run Number of Simulation

#### 4.4 Summary of Chapter

In this chapter, we presented the results of our simulation experiment using AODV with and without using black hole and DETAODV. In the simulation experiment, several number of run to compare using AODV with and without using black hole and DETAODV. The simulation results showed that among this different number of run, DETADOV outperformed AODV with black hole in all the performance evaluations. The results showed that DETADOV is friendlier than AODV with black hole with regard to network performance.

## **CHAPTER 5**

### **CONCLUSION AND FUTURE WORKS**

#### **5.1 Introduction**

This thesis studied Performance Evaluation of Black Hole Attack. In particular, we studied the AODV Routing Protocol Using NS2 and implement new ADOV protocol called DETAODV. In this chapter, we will conclude the research findings and we will discuss the future works research.

#### **5.2 Research Conclusion**

Wireless ad-hoc networks have increased significant importance in wireless communications. Wireless communication is created by nodes playing as routers and transferring packets from one mobile node to another in ad-hoc networks. As Wireless Ad-hoc networks become widely used, the security issue has become one of the important concerns for all the times. One of the well-known attack is the Black Hole attack which is most common in the on-demand routing protocols such as AODV. Black hole attack is an active attack in case of AODV protocol. Because AODV protocol has no security mechanisms, a malignant node can perform many attacks in the network just by behaving according to AODV rules.

The work presented in this thesis is aimed at the studying Performance Evaluation of Black Hole Attack on (AODV) Protocol by examine AODV Protocol with and without Black Hole Attack, then we proposed an Intrusion Detection System (IDS) to reduce the Black Hole effects in the AODV network.

**Chapter One**, we introduced the motivation of the study as well as the problem statement. We also discussed the research aims, objectives, and framework of how to embark on the research throughout the study. "

**Chapter Two** presents the overview of the background material and establishes the concepts and issues covered in this thesis. The concepts and issues covered in this chapter are. Wireless Ad-hoc networks security vulnerabilities and black hole attacks

**Chapter Three:** introduces the related work to our proposed AODV protocol.

**Chapter Four** highlights the design of the proposed AODV protocol, goals of design and steps of coding the proposed AODV protocol using NS2 and results discussion.

**Chapter Five** Summarizes the research work, highlights research contributions and recommends future work related to this research.

### **5.3 Future Works**

Future work can be furthered in a number of directions: first, we would like to simulate other routing protocol like DSDV, DSR ... etc. different routing protocols are estimated to expose various results. So, we can determine the greatest routing protocol for decreasing the Attack of Black Hole. Second, we can improve our detection way by applying some interfacial intelligence algorithm like Fuzzy logic or genetic algorithm.

## REFERENCES

1. **Broch D. A., Maltz D. B., (2009)**, "*Routing in Ad Hoc Networks of Mobile Hosts*", Presented at Mobile Computing Systems and Applications, New York, pp. 12-23
2. **Perkins C., Belding E., and Das S., (2003)**, "*RFC 3561-Ad Hoc On-Demand Distance Vector (AODV) Routing*", Internet RFCs, USA, pp. 1-38.
3. **Perkins C. E. and Royer E. M., (2001)**, "*The Ad Hoc On-Demand Distance-Vector Protocol*", Presented at Ad Hoc Networking, Germany, pp. 45-60.
4. **Johnson D. B. and Maltz D. A., (1996)**, "*Dynamic Source Routing in Ad Hoc Wireless Networks*", in Mobile Computing, Springer, pp. 153-181.
5. **He G., (2002)**, "*Networking Laboratory*", Destination-Sequenced Distance Vector (DSDV), Protocol Helsinki University of Technology, USA, pp. 153-181.
6. **Al-Shurman M., Yoo S., (2004)**, "*Black Hole Attack in Mobile Ad Hoc Networks*", Presented at Proceedings of the 42nd Annual Southeast Regional Conference, Jordan, vol. 212, pp. 299-337.
7. **Tamilselvan L. and Sankaran V., (2007)**, "*Prevention of Black-Hole Attack in MANET*", Presented at the 2nd International Conference at Wireless Broadband and Ultra Wideband Communications, Munich, Germany, pp. 5-8.

8. **Pawlikowski K., Jeong H. D., and Lee J., (2002),** *"On Credibility of Simulation Studies of Telecommunication Networks"*, Communications Magazine, IEEE, vol. 40, pp. 132-139.
9. **Johnson D. B., (1994),** *"Routing in Ad Hoc Networks of Mobile Hosts"*, Presented on First Workshop at Mobile Computing Systems and Applications, USA, pp. 53-58.
10. **Maltz D. B. and Broch J., (2001),** *"DSR: The Dynamic Source Routing Protocol For Multi-Hop Wireless Ad Hoc Networks"*, Computer Science Department Carnegie Mellon University, Pittsburgh, pp. 15213-3891.
11. **Deng H., Li W., and Agrawal D. P., (2002),** *"Routing Security in Wireless Ad Hoc Networks"*, Communications Magazine, IEEE, vol. 40, pp. 70-75.
12. **Perkins C. E. and Bhagwat P., (1994),** *"Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers"*, Presented at ACM SIGCOMM Computer Communication Review, vol. 35, pp. 50-65.
13. **Murthy S. and Garcia J., (1995),** *"A Routing Protocol for Packet Radio Networks"*, Presented at Proceedings of the 1st Annual International Conference on Mobile Computing and Networking, pp. 5-9.
14. **Chiang C., Wu K., Liu W., and Gerla M., (1997),** *"Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel"*, Presented at Proceedings of IEEE SICON, vol. 60, pp. 60-65.

15. **He G., (2002)**, "*Destination-Sequenced Distance Vector (DSDV) Protocol*", Networking Laboratory, Helsinki University of Technology, USA, vol.12, no. 20, pp. 59–61.
16. **Divecha B., Abraham A., Grosan C., and Sanyal S., (2007)**, "*Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility Models*", Presented at Modelling & Simulation. First Asia International Conference, pp. 1-8.
17. **Broch J., Johnson D. B., and Maltz D. A., (1998)**, "*The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks*", London, vol.12, no. 20, pp. 4959–4972.
18. **Perkins C. E., (2008)**, "*Ad Hoc Networking*", Addison-Wesley Professional, London, pp. 42-50.
19. **Toh C. K., (2001)**, "*Ad Hoc Mobile Wireless Networks: Protocols and Systems*", Pearson Education, India, vol.10, no. 15, pp.49–53.
20. **Johnson D. B. and Maltz D. A., (1996)**, "*Dynamic Source Routing in Ad Hoc Wireless Networks*", in Mobile computing: Springer, USA, pp. 153-181.
21. **Perkins C. E., Royer E. M., Das S. R., and Marina M. K., (2001)**, "*Performance comparison of two on-demand routing protocols for Ad Hoc Networks*", Personal Communications, IEEE, vol. 8, pp. 16-28.
22. **Mishra A., Nadkarni K. M., and Ilyas M., (2003)**, "*Security in Wireless Ad-Hoc Networks, The Handbook of Ad Hoc Wireless Network*", CRC PRESS Publisher, India, pp. 42-50.

23. **Murthy C. and Manoj B., (2004)**, "*Ad Hoc Wireless Networks: Architectures and Protocols*", Pearson Education, India, pp.15–19.
24. **Stallings W., (2007)**, "*Network Security Essentials: Applications and Standards*", Pearson Education, India, pp. 53-61.
25. **Shah V. and Modi N. K., (2012)**, "*A Comparative Analysis of Network Layer Threats & Defense Mechanisms of Manets*", International Journal of Advanced Research in Computer Science, USA, vol. 3, pp. 35-41.
26. **Viswanatham V. M. and Chari A., (2008)**, "*An Approach for Detecting Attacks in Mobile Ad Hoc Networks*", Journal of Computer Science, USA, vol. 4, pp. 245.
27. **Xing F. and Wang W., (2006)**, "*Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks*", Presented at Military Communications Conference, London, vol. 6, pp. 25.
28. **Hu Y. and Perrig A., (2004)**, "*A survey of Secure Wireless Ad Hoc Routing*" , IEEE Security & Privacy, vol. 2, pp. 28-39.
29. **Jain A. K. and Tokekar V., (2011)**, "*Classification of Denial of Service Attacks in Mobile Ad Hoc Networks*", Presented at Computational Intelligence and Communication Networks (CICN), pp. 2-9.
30. **Sanzgiri K., Dahill B., Levine B. N., Shields C., and Belding E. M., (2002)**, "*A Secure Routing Protocol for Ad Hoc Networks*", Presented at Network Protocols Proceedings, vol.3, pp.76-81.



31. **Huang Y. and Lee W., (2004)**, "*Attack Analysis and Detection for Ad Hoc Routing Protocols*", Presented at Recent Advances in Intrusion Detection, India, pp 90-101.
32. **Shanthi N., Ganesan L., and Ramar K., (2009)**, "*Study Of Different Attacks On Multicast Mobile Ad Hoc Network* ", Journal of Theoretical & Applied Information Technology, USA, vol. 6, pp. 5-21.
33. **Jhaveri R. H., Patel A. D., Parmar J. D., and Shah B. I., (2010)**, "*MANET Routing Protocols and Wormhole Attack Against AODV*", International Journal of Computer Science and Network Security, USA, vol. 10, pp. 12-18.
34. **Choi S., Kim D., Lee D., and Jung J., (2008)**, "*WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks*," Presented At Sensor Networks, Ubiquitous and Trustworthy Computing. IEEE International Conference, pp. 13-24.
35. **Hu Y., Perrig A., and Johnson D. B., (2003)**, "*Packet Leashes: A Defense Against Wormhole Attacks In Wireless Networks*," Presented At INFOCOM. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, vol. 2, pp. 90-101.

## APPENDICES A

### CURRICULUM VITAE

#### PERSONAL INFORMATION

**Surname, Name:** AL-HUSSEINI, Saif

**Date and Place of Birth:** 23 June 1976,  
Mousel

**Marital Status:** Married

**Phone:** +90 5385558859

**Email:** [alhasani\\_saif@yahoo.com](mailto:alhasani_saif@yahoo.com)



Degree	Institution	Year of Graduation
M.Sc.	Çankaya University, Information Technology	2015
B.Sc.	Mansour University College, Computer Science	2001

#### FOREIN LANGUAGES

English, Beginner Turkish.

#### HOBBIES

Football , Reading, Travel, Swimming.