A PERFORMANCE COMPARISON OF MOBILE AD-HOC NETWORKS REACTIVE ROUTING PROTOCOLS UNDER BLACK-HOLE ATTACK

by

LINEO FLORINA MEJAELE

submitted in accordance with the requirements
for the degree of

MASTER OF SCIENCE

in the subject

COMPUTER SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: MR E O OCHOLA

DECEMBER 2015

Student number: **48082236**

I declare that

A Performance Comparison of Mobile Ad-hoc Networks Reactive Routing Protocols under Black Hole Attack

is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

_____ _____

SIGNATURE DATE

(Ms)

Acknowledgements

Firstly I would like to thank my supervisor, Mr Elisha Ochola for guiding and supporting me throughout this study. Without him, this research would have not been possible. I am also thankful to UNISA for giving me the opportunity to learn and providing necessary resources that supported this study. Most importantly, I am sincerely grateful to UNISA bursary section for financially supporting my study.

I would also like to appreciate my parents, family and friends for their unceasing support, encouraging words and prayers. I specially give my heartfelt gratitude to my husband and friend Mpho Mosehle, for the sleepless nights he spent with me while I studied, helping me with house chores and taking care of our daughter. Thank you very much for your love and support. I also express my warm thanks to my little daughter for understanding when I had to leave her for long hours.

I am also grateful to NS-2 users for responding to my queries regarding simulations and to my colleague Mr Lebajoa Mphatsi for giving me the basics of using NS-2.

Above all, I give thanks to my most high God for strengthening me till the end of this study. I cannot do anything without Him by my side.

Publications

The following peer-reviewed conference papers emanated from this research:

- **Lineo Mejaele** and Elisha Oketch Ochola, ñAODV vs. DSR: Simulation Based Comparison of Ad-hoc Network Reactive Protocols under Black Hole Attackò, proceedings of second International Conference on Advances in Computing, Electronics and Electrical Technology - CEET 2014, Kuala Lumpur, Malaysia, 20-21 December, 2014.
    - The same paper ñAODV vs. DSR: Simulation Based Comparison of Ad-hoc Network Reactive Protocols under Black Hole Attackò was also published in the International Journal of Advances in Computer Networks and Its Securityï IJCNS Volume 5: Issue 1 [ISSN: 2250-3757]. Publication date: 30 April 2015.

- **Lineo Mejaele** and Elisha Oketch Ochola, ñAnalysing the Impact of Black Hole Attack on DSR-based MANET: The Hidden Network Destructorò, proceedings of second International Conference on Information Security and Cyber Forensics ï InforSec 2015, Cape Town, South Africa, 15-17 November, 2015.

Acronyms

Abbreviation	Phrase or Word
ACK	Acknowledgement
AODV	Ad-hoc on-demand Distance Vector
CBR	Constant Bit Rate
DDOS	Distributed Denial of Service
DOS	Denial of Service
DPRAODV	Detection, Prevention and Reactive AODV
DSR	Dynamic Source Routing
EAODV	Enhanced AODV
IDSAODV	Intrusion Detection System AODV
MANET	Mobile Ad-hoc Network
MPRs	Multi Point Relays
NAM	Network Animator
NS	Network Simulator
OLSR	Optimized Link State Routing Protocol
OTCL	Object-Oriented Tool Command Language
PDA	Personal Digital Assistant
RREP	Route Reply
RREQ	Route Request
RERR	Route Error
SANET	Static Ad-hoc Network
SAODV	Secure AODV
SYN	Synchronization
TCL	Tool Command Language
TCP	Transmission Control Protocol
TORA	Temporally Ordered Routing Algorithm
UDP	User Datagram Protocol
WPAN	Wireless Personal Area Network
ZRP	Zone Routing Protocol

Abstract

Mobile Ad-hoc Network (MANET) is a group of mobile devices that can form a network, interconnect and share resources without the use of any fixed network infrastructure or centralised management. MANET is exposed to security attacks because of its fundamental characteristics such as open medium, dynamic topology and lack of central monitoring. The black hole attack is one example of the attacks MANET is exposed to. In black hole attack, a malicious node misleadingly claims to have an updated route to the destination node, absorbs and drops the packets that are supposed to be forwarded to the destination node.

The common MANET reactive routing protocols are Ad-hoc on-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). These protocols are easily attacked by the black hole during the route discovery process. This research therefore studies black hole attack in detail and assesses the performance of AODV and DSR under black hole attack. The work is achieved by simulating the two protocols under regular operation and under black hole attack using Network Simulator 2 (NS-2). The protocols are analysed using packet delivery ratio, throughput and end-to-end delay as performance metrics. The research further compares the black hole attack solutions that have been previously proposed and determines the solution that performs better than others.

The simulation results show that MANET under normal operating environment out performs MANET attacked by black hole, and that AODV is more vulnerable to black hole attack than DSR. The comparison study of the existing black hole attack solutions show that SAODV is the best effective black hole attack removal technique. But when considering the solution that brings no negative impact to the normal operation of the network, IDSAODV is the best solution.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Background

The growing number of light-weight and low-cost mobile devices and advances in computer networking has led to increased popularity of Mobile Ad-hoc Networks (MANETs). A MANET is a group of mobile devices that can form a network, interconnect and share resources without the use of any fixed network infrastructure or centralised management (Jhaveri et al., 2010). In a MANET, nodes that are in the transmission range of each other can forward messages to each other directly. On the other hand, nodes that are not in each others range have to depend on intermediate nodes to communicate. The cooperation of the nodes is important for successful communication because each node has to take the role of a router and forward packets to neighbouring nodes (Osathanunkul & Zhang, 2011).

A MANET is suitable to provide communications in many applications, particularly in cases where it is not possible to setup a network infrastructure. For instance, in a military operation, where there may be geographical barriers between participants, a MANET can be set up to facilitate communication. Also because it is easy to set up, it may be of assistance to replace the damaged network infrastructure in disaster recovery operations where temporary network infrastructure is immediately needed (Mishra et al., 2010; Sharma & Sharma, 2012).

The features of MANET such as limited battery power, open and bandwidth constraint channels, changing network topology, dissimilar devices, lack of infrastructure and central monitoring cause MANET routing to be challenging (Osathanunkul & Zhang, 2011). In order to overcome routing challenges in MANETs and attain effective routing, a number of routing protocols are defined specifically for MANETs. Examples of these protocols are Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Destination-Sequenced Distance-Vector (DSDV). Most of these protocols have been defined with an assumption that all nodes in the network can be trusted and are cooperative. However, if some of the nodes become malicious, MANETS become exposed to different kinds of attacks.

The routing attacks are more severe because they interrupt routing which is an important network service. Black hole attack is one type of routing attacks (Kannhavong et al., 2007).

1.2 Motivation

It is highly crucial for both wired and wireless networks to be secured so as to offer protected communication. The success of MANET is intensely determined by the confidence people have in its security. However, MANET characteristics such as open architecture and dynamic topology make it challenging to achieve security attributes such as confidentiality, authentication, integrity, availability, access control and non-repudiation (Wu et al., 2007). Early research on MANET mostly concentrated on developing routing mechanisms that are efficient for a dynamic and resource constraint MANET. It is therefore crucial that security aspects of MANET routing protocols be taken into consideration. This study focuses on black hole attack because it is a very dangerous attack that aims to disrupt the routing process of MANETs. The effect of black hole attack is tested on reactive routing protocols because they are more susceptible to black hole attack due to the fact that they establish routes on demand. The black hole attack targets route discovery process and can easily attack reactive protocol since they discover the routes frequently.

1.3 Problem Statement

The black hole attack against MANETs and its detection schemes have been mostly studied and analysed using AODV routing protocol in the previous research works. AODV is the most widely used protocol for MANETs because of its low control message overhead. Other reactive routing protocols such as DSR have been given less attention in the analysis of this attack. It is necessary and important to perform analysis of the black hole attack using other protocols so that a comparative analysis of its impact on performance of MANETs when using different routing protocols can be done.

1.4 Research Objectives

The objectives of this research are as follows;

1. To analyse the impact of black hole attack in MANETs.
2. To simulate AODV and DSR under black hole attack using Network Simulator 2 (NS-2).
3. To compare performance of AODV and DSR protocols under black hole attack.
4. To make recommendation of the preferred reactive routing protocol under black hole attack based on the simulation results analysis.
5. To compare performance of existing proposed black hole attack solutions.

1.5 Research Questions

1. What is the impact of black hole attack on performance of MANETs?
2. Which of the two reactive routing protocols (AODV and DSR) performs better under black hole attack?
3. Which of the existing proposed black hole attack solutions perform best?

1.6 Research Scope and Limitations

Each of the layers in the communication protocols stack of ad-hoc networks has its own weaknesses and challenges (Mishra & Sharma et al., 2010), but the study focuses only on routing layer attacks because routing is a vital factor in mobile network communications. The impact of black hole attack is studied and analysed using the two mostly used MANET reactive routing protocols AODV and DSR. In carrying out the study, it is assumed that black hole nodes do not coordinate to attack and therefore the instance of several black hole nodes working together has not been considered.

Recent deployments of ad-hoc networks indicate a significant presence of unidirectional or asymmetric links caused by heterogeneous transmission of mobile nodes. Even when nodes are transmitting at the same power, unidirectional links may be created due to random fluctuations in signal propagation and presence of noise sources near a node. Nevertheless, bidirectional links are assumed when

designing routing algorithms because the presence of unidirectional links severely affects the functionality of several routing protocols, so it is assumed that there are only bidirectional links in the network (Garg & Mahapatra, 2009).

1.7 Research Methodology

1.7.1 Approach

Since the primary goal of this study is to achieve the above mentioned objectives and find answers to the research questions, the ***quantitative approach*** towards the study is used. The quantitative approach emphasizes studies that are experimental in nature and give some results. These results are analysed and conclusions derived from their analysis (Borrego et al., 2009). The work is divided into two models, theoretical model and simulation model. Theoretical model involves studying the related literature. Simulation model involves configuration of the network using simulation software and running of the simulations. The results are then obtained from the simulations, analysed and conclusions drawn. Figure 1.1 below illustrates the research approach taken in this study.

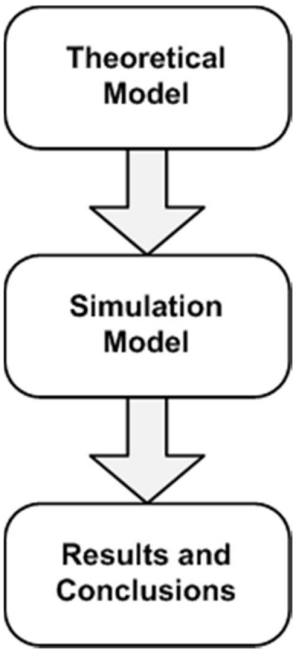


Figure 1.1: Research Approach

1.7.2 Research Stages

The study is divided into four stages:

i. Problem identification
ii. Literature study
iii. Building simulation
iv. Results analysis and conclusions

1.7.2.1 Problem Identification

The identification of a research problem is the first and most important step in the research process. The researcher first identified the major research area of her interest which is MANETs. After going through most of the literature related to MANETs, the researcher narrowed down the area by considering security issues of MANETs, and specifically focused on the black hole attacks.

1.7.2.2 Literature Study

The detailed literature study was carried out to develop a solid background of the research. The literature on the black hole attack, AODV and DSR routing protocols was studied and the previously proposed black hole attack solutions were studied. Different network simulation tools and their functionality were also studied, but more focus was put on NS-2 which has been used in this research study.

1.7.2.3 Building Simulation

Various simulation models using the two protocols (AODV and DSR) in the study were developed based on the requirements of the research problem. The knowledge acquired from the literature study played an important role in building the simulations.

1.7.2.4 Results analysis and Conclusions

Results obtained from the simulation were analysed using graphs and conclusions drawn based on the analysis.

1.8 Research Contributions

The contributions of this study are as follows:

- The significance of discovering the protocol that is more susceptible to black hole attack is that more research will be conducted on the vulnerable protocol to make it more secure.

- The analysis of the impact of black hole attack contributes to the body of knowledge on how severe the attack is.

- A recommendation of the preferred reactive routing protocol under black hole attack is done, which can assist researchers intending to realise a good network performance in an environment that is attacked by a black hole node.

- The previously proposed black hole solutions have been tested using simulations, so this study contributes to the body of knowledge by finding out which of these solutions perform better than others.

- The following peer-reviewed conference papers emanated from this research:
    i. **Lineo Mejaele** and Elisha Oketch Ochola, ñAODV vs. DSR: Simulation Based Comparison of Ad-hoc Network Reactive Protocols under Black Hole Attackò, proceedings of second International Conference on Advances in Computing, Electronics and Electrical Technology - CEET 2014, Kuala Lumpur, Malaysia, 20-21 December, 2014.

        - The same paper ñAODV vs. DSR: Simulation Based Comparison of Ad-hoc Network Reactive Protocols under Black Hole Attackò was also published in the International Journal of Advances in Computer Networks and Its Securityï IJCNS Volume 5: Issue 1 [ISSN: 2250-3757]. Publication date: 30 April 2015.

ii. **Lineo Mejaele** and Elisha Oketch Ochola, ñAnalysing the Impact of Black Hole Attack on DSR-based MANET: The Hidden Network Destructorò, proceedings of second International Conference on Information Security and Cyber Forensics ï InforSec 2015, Cape Town, South Africa, 15-17 November, 2015.

1.9 Outline of Chapters

This dissertation comprises of seven chapters. Figure 1.2 outlines the structure of the dissertation. Chapter 1 gives the introduction to the study. The descriptions of what subsequent chapters comprise are given below Figure 1.2.

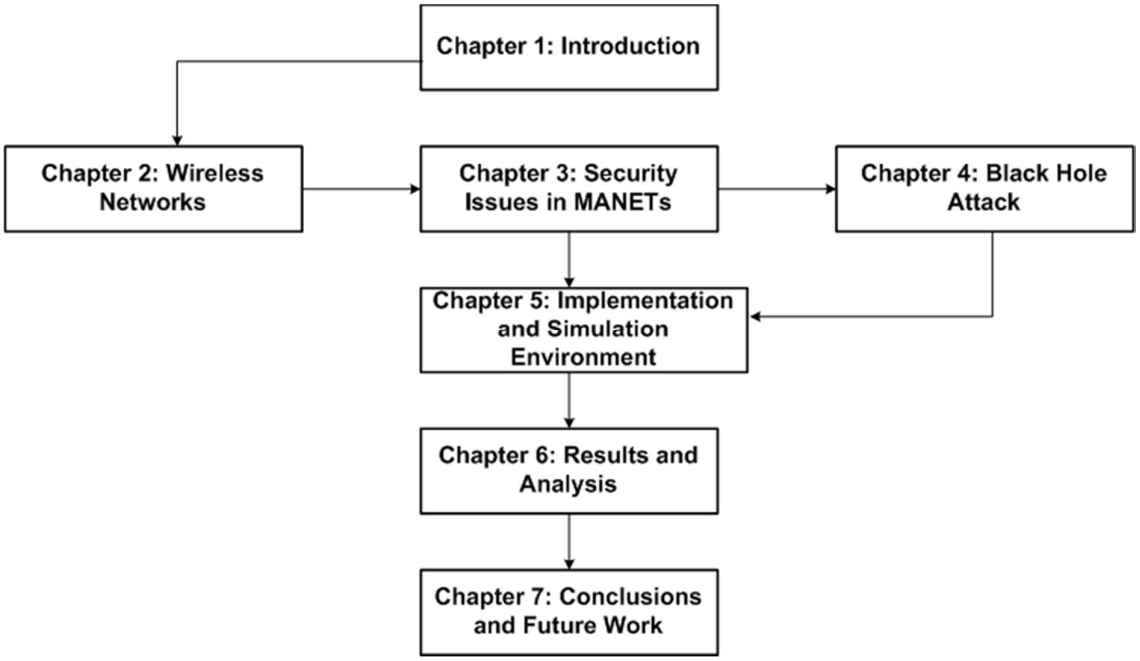


Figure 1.2: Dissertation Structure

Chapter 2 gives the background study of wireless networks, paying more attention on the literature study of MANETs, discussing the characteristics, applications, routing protocols of MANETs. It further focuses on the detailed operation of the two routing protocols, AODV and DSR which are the centre of this research work.

Chapter 3 concentrates on the security issues of MANETs. It clearly outlines the characteristics of MANETs that make them vulnerable to security attacks. It further

discusses the security attributes that must be fulfilled by a network for proper communication. Then different types of attacks are described in this chapter.

Chapter 4 presents an in-depth discussion of black hole attack. Firstly, the chapter explains the black hole attack in detail, describes different ways in which the attack can occur and different types of this attack. Secondly, the chapter describes how black hole attack occurs in a network that uses AODV routing protocol and in a network that uses DSR routing protocol. The chapter further discusses some of the mitigation techniques that have been previously proposed to combat the effects of black hole attack which have been tested using AODV. Lastly, the previous work in the literature that is similar to this study is discussed.

Chapter 5 discusses the implementation of the research study. It firstly gives an overview of the research objectives, and then describes NS-2, which is the simulation software used in this study. The chapter continues to give reasons for the choice of simulation software and gives an overview of the NS-2 simulation, then gives the simulation parameters used in the setups. Lastly the modifications made to C++ code of NS-2 to include a black hole node in the network are illustrated.

Chapter 6 discusses the simulation results and results obtained from literature, and gives analysis of the results. It first describes the output trace file of NS-2, and then the scripting language used to filter only the required fields from trace files. It then discusses evaluation performance metrics used in this study and thereafter results obtained for each metric are presented and analysed.

Chapter 7 concludes the study, reflecting on research questions presented in Section 1.5 and gives some recommendations for future work.

1.10 Summary

This chapter has presented the background of the study by describing MANETs, their routing protocols and features that expose them to many security attacks. The motivation behind carrying out this research work was then described and the statement of the problem explained. The chapter further listed the objectives and the research questions, and outlined the methodology used to meet the objectives.

Moreover, the chapter explained the scope covered by this study and how the study contributes to the body of knowledge. Lastly, the outline of subsequent chapters was presented. The next chapter gives the description of wireless networks.

2 Wireless Networks

2.1 Introduction

This chapter provides background literature on wireless networks. It describes different types of wireless networks focusing mainly on MANETs. It clearly explains characteristics and applications of MANETs, and further describes routing in MANETs, outlining different MANET routing protocols based on their classification and explaining the protocolsô route discovery and maintenance mechanisms.

2.2 Related Background

ñThe era of wireless communication began at the end of the 19th century with the first successful wireless radio transmission performed by an American scientist of Serbian origin Nikola Tesla in 1893ò (MladenoviĹ & JovanoviĹ , 2012: 1). Wireless networks are computer networks that are not connected by cables of any kind. Radio waves are the foundation of wireless systems. The advantages of wireless communication are smaller demands for infrastructure equipment, reduced average cost, shorter time for establishing the connection and increased user mobility.

2.2.1 Types of Wireless Networks

There exist two types of mobile wireless networks. The first type is the **infrastructure network** which has wired and fixed gateways. The common applications of this type of network include wireless local area networks (WLANs) and cellular networks. The second type is the **infrastructure-less** mobile network, normally referred to as an ad-hoc network. The nodes in infrastructure-less networks move freely and can be connected randomly because there are no gateways and routers monitoring the nodes. Ad-hoc network can be classified into Static Ad-hoc Network (SANET) and Mobile Ad-hoc Network (MANET). Examples of SANET are sensor networks and Mesh networks (Al-Omari & Sumari, 2010) . Figure 2.1 shows a schematic overview of wireless networks.

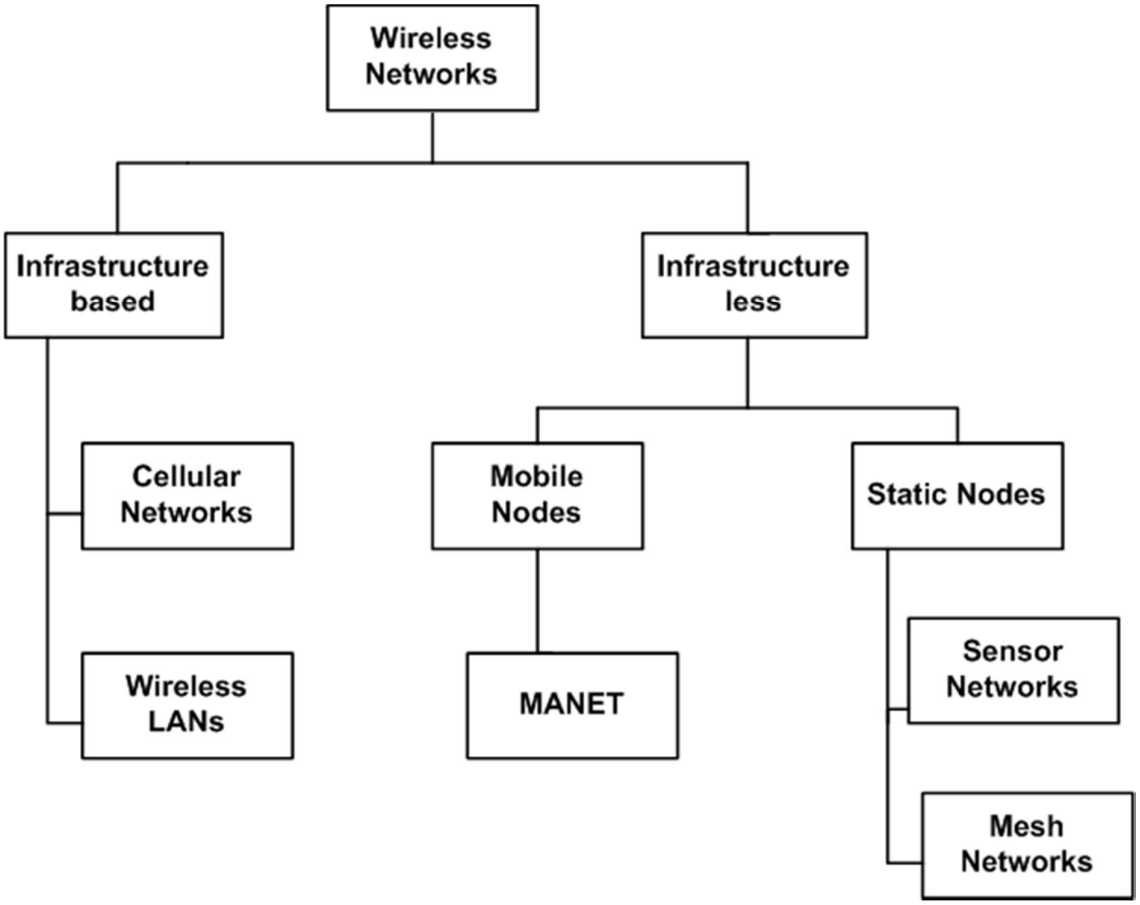


Figure 2.1 : Schematic Overview of Wireless Networks

2.2.1.1 Infrastructure Wireless Networks

This is the network design that allows the wireless stations to communicate with each other (MladenoviĹ & JovanoviĹ, 2012). The bridges for these networks are referred to as base stations and this network relies on fixed base stations. The base station regulates the allocation of radio resources. For two mobile nodes to communicate, they must both be within the transmission range of the base station. A sending node does not have to know the route to a destination node; it just notifies the base station of its intention to communicate with a particular destination node. The base station then forwards the messages from source node to destination node because it knows all the routes. If any node can move out of range of one base station into the range of another base station, a signal transmission of that node is transited to the new base station and a mobile node continues to communicate throughout the network (Al-Omari & Sumari, 2010).

2.2.2.2 Infrastructure-less Wireless Networks (Ad-hoc Networks)

Infrastructure-less wireless network is a group of two or more devices that have the capability to connect and communicate without any central monitoring, or any network infrastructure. Examples of applications of ad-hoc networks are emergency search-and-rescue operations, meetings or conventions in which persons wish to quickly share information, and data acquisition operations in hospitable terrain (Al-Omari & Sumari, 2010).

1. Static Ad-hoc Networks

   In static ad-hoc networks, the physical position of the nodes or the stations is stationary. The nodes in the network are not moving, hence these ad-hoc networks are referred to as static (Zhang et al., 2009).

2. Mobile Ad-hoc Networks

   In mobile ad-hoc network, the entire network may be mobile. The nodes are at liberty to join or leave the network freely because there is no constraint on the movement of the nodes. The topology of mobile ad-hoc network can change fast because the nodes are at liberty to move and can arbitrarily arrange themselves. Figure 2.2 shows some nodes forming ad-hoc networks, and illustrates the nodes moving randomly in different directions and different speeds (Al-Omari & Sumari, 2010).

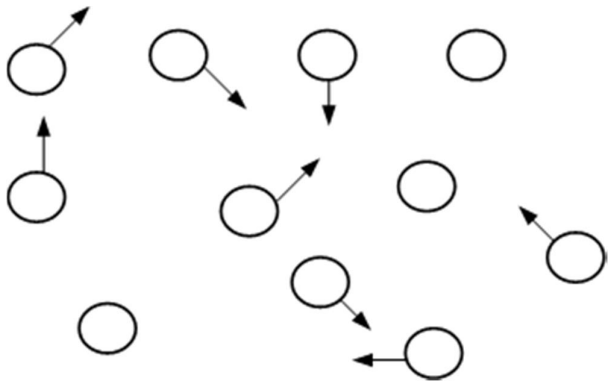


Figure 2.2: Nodes Forming Ad-hoc Network

2.3 Mobile Ad-hoc Networks

MANET is a group of mobile devices that can spontaneously interconnect and share resources via wireless communication channels, with no fixed network infrastructure or centralised management. MANETs can be assembled rapidly and at low cost because they do not require central monitoring or fixed network infrastructure (Osathanunkul & Zhang, 2011). In MANET, the nodes move arbitrarily in different directions and speeds, hence the dynamic topology (de Oliveira Schmidt & Trentin, 2008; Thachil & Shet, 2012). The proper functioning of MANETs depends on the mutual agreement and understanding between the nodes because there are no devices dedicated to monitor communication between the nodes. The nodes that are in the transmission range of each other can forward messages to each other directly; otherwise the packets have to be forwarded via intermediate nodes to the destination node (Wu et al., 2007). Every mobile node has to take the role of a router in order to forward packets for other nodes (Stojanovic et al., 2012).

Mobile nodes in MANET do not necessarily have to be of the same type. They can be PDAs, laptops, mobile phones, routers, printers, etc. as illustrated by Figure 2.3. The nodes are equipped with antennas which operate as wireless transmitters and receivers. The antennas may be omnidirectional, highly directional or a combination. The mobile nodes are resource constraint in terms of bandwidth and battery power (Wu et al., 2007; Rajabhushanam & Kathirvel, 2011).

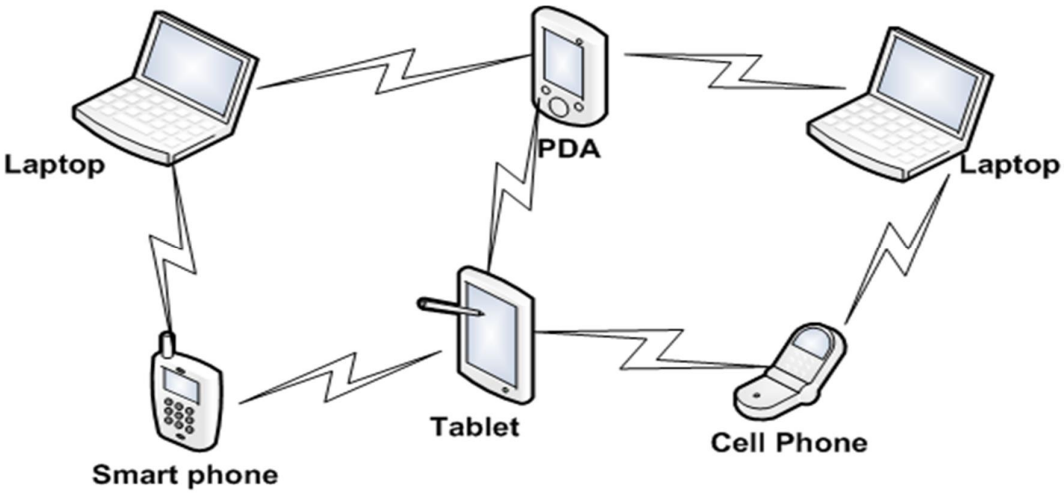


Figure 2.3: Mobile Ad-hoc Network

Figure 2.4 illustrates transmission ranges in MANET. The range of each nodeôs radio transceiver is specified by the circles. An example of three mobile nodes participating in a network is demonstrated by Figure 2.4. Since the outer most laptops are not in the transmission range of each other, the middle PDA can take the role of a router and forward the packets between the outer most nodes.

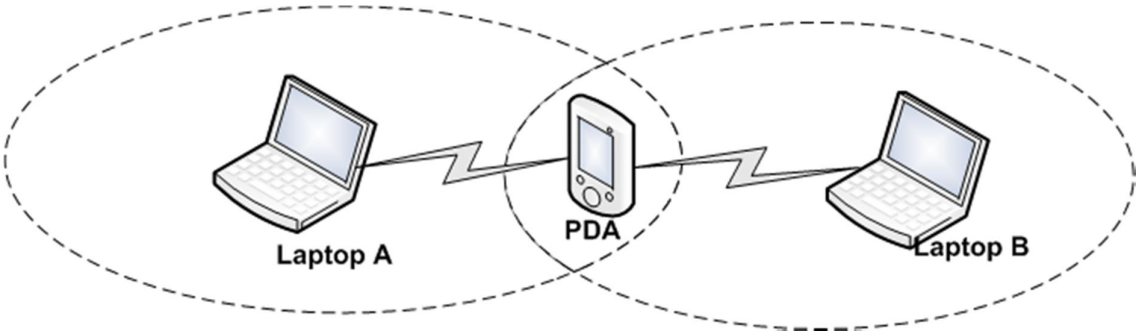


Figure 2.4: Illustration of transmission ranges

There are three types of MANETs which are Vehicular Ad-hoc Networks (VANETs), Intelligent Vehicular Ad-hoc Networks (InVANETs) and Internet Based Mobile Ad-hoc Networks (iMANET) (Al-Omari & Sumari, 2010).

2.4 Applications of MANETs

Ad-hoc networking is becoming significant in many applications due to the advancement in wireless communication and the increasing number of portable devices. MANETs can be deployed in areas where it is not possible to set up the network infrastructure or temporary network connectivity is needed. MANET can find applications in different set of networks, stretching from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources (Goyal et al., 2011). The common applications consist of military battlefield, disaster relief, temporary networks and vehicular networks as explained in Section 2.4.1, Section 2.4.2, Section 2.4.3 and Section 2.4.4 respectively.

2.4.1 Military Battlefield

Currently the military equipment has some computer wireless cards, so they can form a MANET and communicate with each other in the battlefield. MANETs help to

maintain information network between the soldiers, vehicles, and military information headquarters, therefore there will not be any geographical obstacles in a military action (Wu et al., 2007).

2.4.2 Disaster Relief

MANET can be used to setup a quick network in emergency situations where the network infrastructure has been destroyed and there is a need for an instant short term network. The causes for damage to network infrastructure could be fire, earthquakes, and floods. In the case where the damaged communication network is rapidly needed, emergency rescue operations must take place, and rescue team members utilise small hand held devices to pass information amongst themselves (Goyal et al., 2011).

2.4.3 Temporary Networks

Nowadays, mobile devices such as laptops, notebooks, and tablets are used by individuals in meetings, conferences and classrooms. A network is required in order for the participants to share information, so MANET can assist in forming a temporary network (Thakare & Joshi, 2010).

2.4.4 Vehicular networks

Most vehicles today are equipped with short range radios that enable them to communicate with other vehicles, so the vehicles can form a MANET. The vehicles in MANET would communicate accident warning to the drivers (Rajesh & Anil, 2012).

2.5 Routing in MANETs

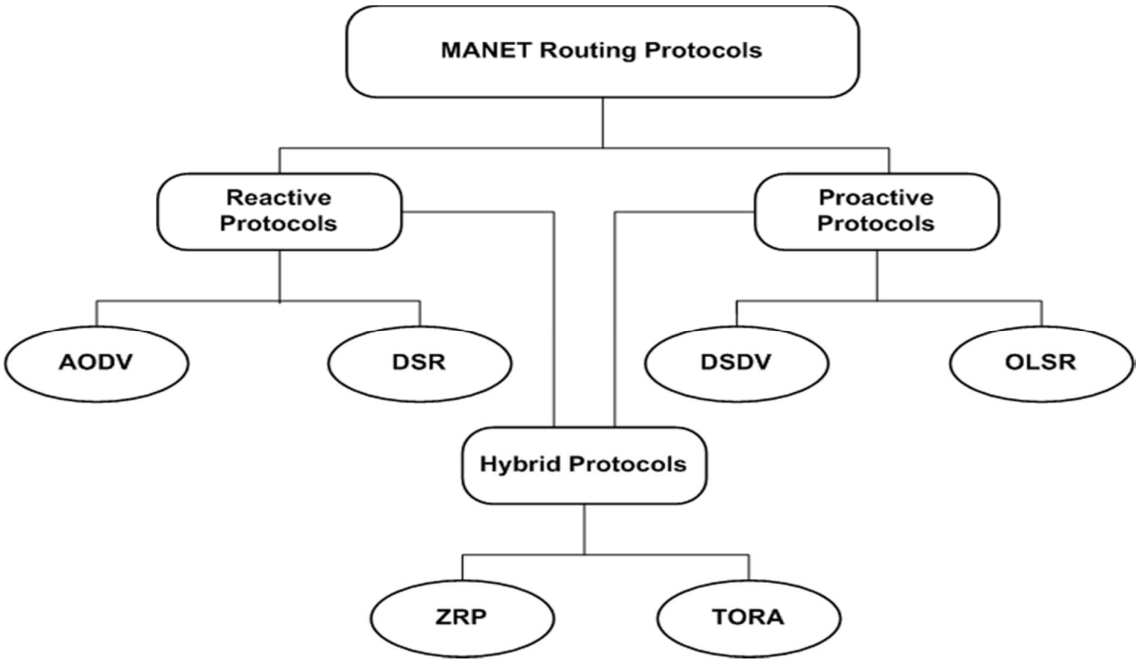
The topology of MANETs keeps changing rapidly due to free movement of nodes joining and leaving the network any time. Routing is important in order to discover the recent topology so that an updated route to a certain node can be established and a message relayed to the correct destination (Kannhavong et al., 2007; Rajabhushanam & Kathirvel, 2011).

End-to-end communication between the nodes is established through the use of traditional TCP/IP structure. However due to mobility and limited resources, each layer in the TCP/IP model needs to be redefined or altered in order to operate efficiently in MANETs. This makes it very challenging to design an efficient and reliable routing plan for MANETs (Abolhasan et al., 2004) .

The traditional routing protocols that have been structured for hard wired networks, such as distance vector and link state protocols cannot be applied in MANETs directly. This is because mobility and dynamic topology are the fundamental characteristics of MANETs (Sharma & Sharma, 2012). Therefore, in order to overcome routing challenges in MANETs and attain effective routing, a number of routing protocols are defined specifically for MANETs.

2.6 Classification of MANET Routing Protocols

MANETs routing protocols can be categorised into proactive, reactive and hybrid protocols based on how the nodes establish and maintain paths (Giruka & Singhal, 2007). The hierarchy of these protocols is shown in Figure 2.5.



.

Figure 2.5: Hierarchy of MANET Routing Protocols

2.6.1 Proactive Protocols

These are table-driven routing protocols that try to keep a record of fresh and updated network routes. Every node in the network keeps a table to store the routing information (Goyal et al., 2011). In order to maintain a consistent network view, the nodes exchange topology information. The exchanged information helps to reflect any changes in the topology. Every time a node wants to send messages, it could obtain a path to the destination through searching local route table, without delay of remote route discovery (Kannhavong et al., 2007). Maintaining an up-to-date topology in the routing tables causes a high control overhead. Examples of popular proactive routing protocols are Destination-sequenced Distance- Vector routing protocol (DSDV), and Optimized Link State Routing Protocol (OLSR) (Thakare & Joshi, 2010).

2.6.2 Reactive Protocols

Reactive protocols as explained by Johnsort (1994) are on demand routing protocols. As the name suggests, the routes to destination are established only when the nodes must send data to destination whose route is unknown. This implies that the source node initiates the searching of routing paths only when needed. When a node wants to send data to a destination node, it starts a route discovery process within the network. Comparative to proactive protocols, the control overhead in reactive protocols is reduced; however the route searching process that occurs before data packets can be forwarded may cause source node to suffer long delays. Examples of popular reactive protocols are Dynamic Source Routing (DSR) and Ad-hoc On-demand Distance Vector (AODV) (Thakare & Joshi, 2010).

2.6.3 Hybrid Protocols

Hybrid protocols are a combination of proactive and reactive protocols. Their design merges the advantages of both proactive and reactive protocols to yield better results (Singh & Sharma, 2012). The majority of hybrid routing protocols are structured using a hierarchical or layered network model.

Firstly, proactive routing is used to fully acquire all the routing information that is unknown. Then reactive routing mechanisms are used to maintain the routing

information when network topology changes. The common hybrid routing protocols are zone routing protocol (ZRP) and temporally ordered routing algorithm (TORA) (Tseng et al., 2011).

2.7 Description of Popular Ad-hoc Routing Protocols

This section describes the operation of the most popularly used protocols under the three categories explained in Section 2.6. Since the research focuses on the performance of the two reactive protocols, DSR and AODV are discussed in detail in Section 2.7.5 and Section 2.7.6 respectively. Other routing protocols are briefly described.

2.7.1 Destination-Sequenced Distance-Vector Routing Protocol (DSDV)

DSDV as explained by Perkins and Bhagwat (1994) is a table-driven protocol for MANET which was invented to solve the routing loop problem. A routing table that shows route information to other nodes in the network is kept in each node. The routing table is updated periodically to provide a fresh view of the whole network. The fundamental issue is the creation and maintenance of tables; the routing updates must be transmitted regularly to keep the tables updated, this has to happen even when traffic of packets is congested. DSDV operates only when the routing updates about changes in topology have reached all the nodes in the network.

This protocol is inefficient because as the network grows, the overhead also grows. However, when the ad-hoc network has a small number of mobile nodes with few changes in network topology, DSDV becomes more effective (Jhaveri et al., 2010).

2.7.2 Optimized Link State Routing Protocol (OLSR)

OLSR is described by Jacquet et al. (2001) as a proactive link state routing protocol for MANETs. The routing table that reflects routing information to every node in the network is kept by each node. The periodic updates that maintain topology information about the network are done by exchanging link-state messages. Thus the routes can be obtained immediately when required. Whenever there is a change in the topology of the network, the topological information gets flooded to all

available nodes. So the basic idea behind the design of this protocol is to cut the number of broadcast messages in comparison to other pure flooding mechanisms, and thereby decrease control overhead. OLSR uses multipoint relays (MPRs) to support this idea (Kuppusamy et al., 2011). During each update of the topology, each node in the network chooses a group of nearby nodes that will retransmit its packets. This group of nodes is referred to as the multipoint relays of that node. All other nodes which are not part of the group can read and process each packet but do not retransmit the packet. In the selection of the MPRs, each node broadcasts a list of its one hop neighbours periodically using hello messages. The information about own advertised neighbours is broadcast using topology control (TC) messages. This protocol is mostly suitable for huge and dense networks (Abolhasan et al., 2004).

2.7.3 Zone Routing Protocol (ZRP)

ZRP is an example of a hybrid routing protocol. It proficiently combines the features of proactive and reactive protocols. The network is divided into local neighbourhoods known as zones, and uses different protocols in different zones (Thakare & Joshi 2010). The proactive mechanisms are used to maintain routing information for the routing zone, so the control overhead is minimised. The route to destinations beyond the routing zone is obtained using reactive mechanisms; therefore the flooding drawbacks are reduced. In the operation of ZRP, the local routing information is checked regularly; therefore the waste related to pure proactive schemes is reduced (Pervaiz et al., 2010).

2.7.4 Temporally Ordered Routing Algorithm (TORA)

TORA is a routing protocol suitable for multi hop networks and it is also referred to as a link reversal protocol (Gill & Kunwar, 2014). The nodes in the network only keep information about their neighbours because TORA is a distributed algorithm. It utilises a combination of reactive and proactive routing. The route requests are started by the source node using reactive routing. Concurrently the designated destination nodes may start building traditional routing tables by using proactive operation (Kuppusamy et al., 2011).

The three basic functions performed by the protocol are; route discovery, route maintenance and route erasure. The route discovery process is started only when a node has no route to destination and needs a route. Route maintenance is important for re-establishing a route to destination node; this happens if the node has learnt that a route to destination no longer exists. Route erasure is used when there is a partition in the network; the protocol is capable of detecting the partition and erasing all routes that are not valid. The topological alterations do not call for any reaction because TORA has a unique feature of maintaining several routes to destination. The protocol reacts only when all routes to the destination are lost (Gill & Kunwar, 2014).

2.7.5 Dynamic Source Routing Protocol (DSR)

DSR is described by Johnson & Maltz (1996) as a reactive routing protocol that is founded on the idea of source routing. Source routing requires that all the details of the discovered route to the destination should always be known by the source node (Jhaveri et al., 2010). Every mobile node has a route cache that stores entries of routes that are known by the mobile node, and these entries are updated constantly whenever there is new routing information (Mbarushimana & Shahrabi, 2007). DSR routing is loop-free because each node can have multiple routes to one destination. Therefore, it is most preferred in larger networks with rapidly changing routes and high mobility rate of nodes (Jhaveri et al., 2010). DSR uses route discovery and route maintenance processes as explained in Section 2.6.5.1 and Section 2.6.5.2 respectively.

2.6.5.1 DSR Route Discovery

A node that requires forwarding data packet to some destination node starts by looking into its route cache to check if a route to that destination already exists. If it exists in the cache and has not expired, then it is used to transmit the packet to the destination node. On the contrary, if there is no such route, route discovery process is started by broadcasting the route request (RREQ) packet that encloses the destination node address, the source node address, and a distinctive identification number (Mbarushimana & Shahrabi, 2007).

When the route request is received by a node in the network, and the node is not a destination node or does not have a route to the destination, it adds its own address to the route record of the packet and broadcasts the packet again (Mbarushimana & Shahrabi, 2007). When the RREQ message is received by an intermediate node that has no route to the destination, it modifies the route record by adding its own address and rebroadcasts the packet to neighbouring nodes. The RREQ is only processed by the node if it has never seen it, and this helps to reduce the number of RREQs (Giruka & Singhal, 2007).

When the RREQ message reaches either the destination node or an intermediate node which contains a fresh route to destination in its cache, a route reply (RREP) packet is created and sent to the source node. The source node starts forwarding messages to the destination immediately after it has received RREP packet (Giruka & Singhal, 2007). The sequence numbers are used to determine whether the route is fresh or not. The route is considered to be fresh enough if the sequence number of the destination node is greater than RREQ packet sequence number (Mahmood & Khan, 2007).

2.6.6.2 DSR Route Maintenance

There are no periodic HELLO messages, so each node is liable to verify that the next hop node receives the packets forwarded to it. If a node does not receive a receipt confirmation from the next hop node, then the link is broken and the node that originated the route is informed about the broken link by forwarding a route error (RERR) message to it. A new route discovery has to be done, or another existing route can be used to send the packet (Zhou, 2003; Mbarushimana & Shahrabi, 2007).

2.7.6 Ad-hoc On-demand Distance Vector Routing Protocol (AODV)

AODV is a routing protocol that establishes a route from source to destination on demand (Dokurer et al., 2007). Amongst all MANET routing protocols, AODV is the most popular protocol and it is based on DSDV and DSR algorithms (Jhaveri et al., 2010). The notion of destination sequence number borrowed from DSDV is used to

keep record of the updated topology information between the nodes. AODV ensures a loop free routing because of the sequence numbers.

Unlike DSDV, the sequence number in AODV increases and works as a time stamp to allow a node to compare how fresh the information is. AODV is an enhancement of DSDV because instead of maintaining a complete list of routes, it generates the routes on demand and thereby decreases the number of required broadcasts (Royer & Toh, 1999). Similar to DSR, the nodes learn routes by broadcasting route request messages.

Each node does not keep a complete route from source to destination, instead route table entries are dynamically established at intermediate nodes. The combination of these techniques yields an algorithm that uses bandwidth efficiently, and is responsive to changes in topology (Perkins & Royer, 1999).

2.7.6.1 AODV Route Discovery

Route discovery process is a cycle that involves a ***broadcast network search*** and a ***unicast reply*** that consists of paths that have been discovered (Agrawal et al., 2011). All the nodes in the network keep a record in a table of information about neighbouring nodes that can forward the packets so that they reach the destination, and hello messages are broadcast periodically to keep track of neighbouring nodes. When a source node wants to send data packets to a destination node, and there is no routing information regarding the destination node in the routing table, the source node initiates a route discovery process (Jhaveri et al., 2010). In discovering the route, a source node broadcasts route request (RREQ) packet that comprises of RREQ ID, destination IP address, destination sequence number, source IP address, source sequence number and hop count (Purohit et al., 2011).

Every node that obtains the RREQ packet first checks the destination IP address to determine whether it is the destination for the packet, and if so, it sends back route reply (RREP) packet. If it is not the destination, it looks into its routing table to find if it has a fresh enough route to destination, and if not it broadcasts the RREQ packet to nearby nodes. If there is a route to destination in its routing table, a node compares a RREQ packet sequence number with the destination sequence number in the table to find if the route is updated. The route in the routing table is considered

fresh and updated if the destination sequence number in the table is higher than the sequence number attached to the RREQ packet. The intermediate node with an updated route uses the opposite route to send a unicast RREP packet to the source node, and once the source node has received a RREP packet, it begins to send data packets through this route. If the route in the table is not fresh enough, the node further sends the RREQ packet to its neighbours (Medadian et al, 2009; Jhaveri, et al., 2010).

2.7.6.2 AODV Route Maintenance

During operation, a route error (RERR) packet is sent by a node that detects a broken link. A RERR packet is relayed to every node that utilises the affected link for their communication to other nodes (Medadian, et al., 2009). Figure 2.6 illustrates how AODV route maintenance occurs.

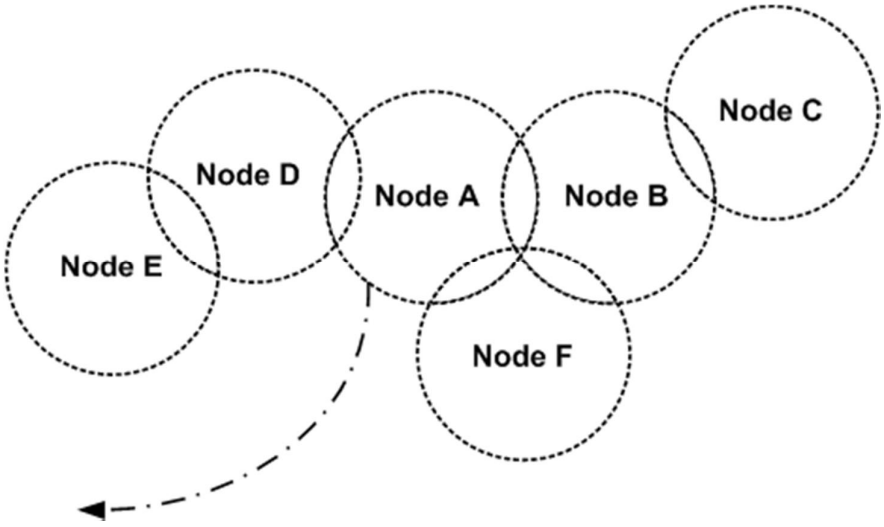


Figure 2.6: AODV Route Maintenance

An example of six mobile nodes is considered in the illustration. The transmission range for the nodes is designated by the circles. Each node can only communicate directly with nearby nodes because the communication range is constricted. If a node wants to communicate with a node that is outside the transmission range, it must start a route discovery process to establish a route.

For example, if Node D wants to transmit data packets to Node C, it establishes a route by starting a route discovery process. Once the route is established, (Node D ï

Node A- Node B - Node C), node D sends the data packet through the specified route.

As shown in Figure 2.6, if Node A leaves the network, Node F which is in the communication range of Node A and Node B will not get a HELLO message from Node A, and that is how node F discovers that Node A has moved. The route through Node A is then marked as invalid by Node F and a RERR message is transmitted to Node B to notify it that Node A is not a neighbour anymore.

2.7.7 Reactive Routing Protocols Route Discovery Illustration

Figure 2.7 and Figure 2.8 illustrate route discovery process in reactive routing protocols. In Figure 2.7, the source node 1 broadcast a RREQ message because it wants to send data packets to destination node 8. The intermediate nodes 2, 3, 4 receive RREQ message and propagate it further to their neighbours until the RREQ message reaches the actual destination node or the intermediate node that has updated route to the destination (Dokurer, Ert et al. 2007).

Upon receiving the RREQ, the destination node or an intermediate node that has a fresh enough route to the destination unicasts a RREP packet to source node as shown in Figure 2.8. Figure 2.9 summarizes route discovery process in AODV and DSR by using a flow diagram.

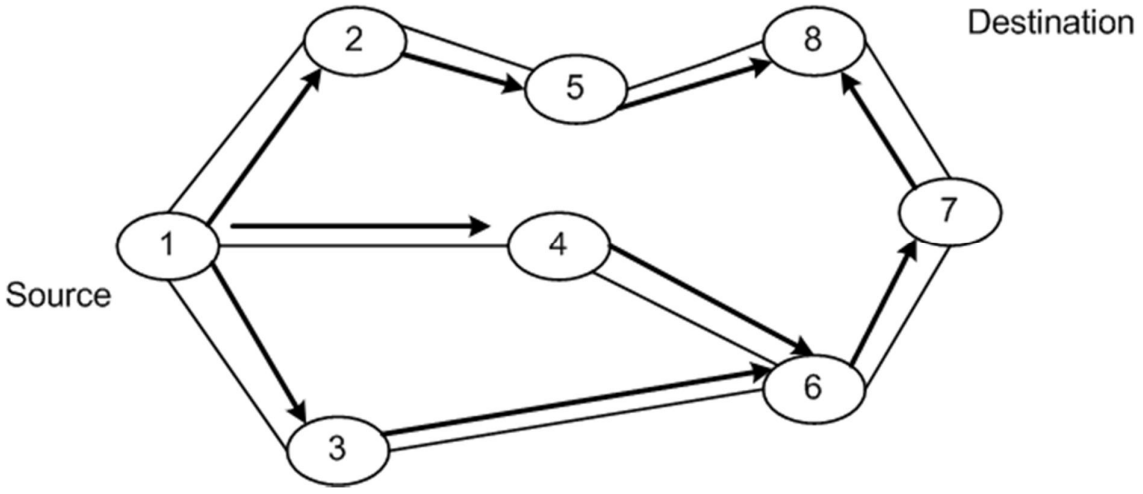


Figure 2.7: Broadcast of RREQ

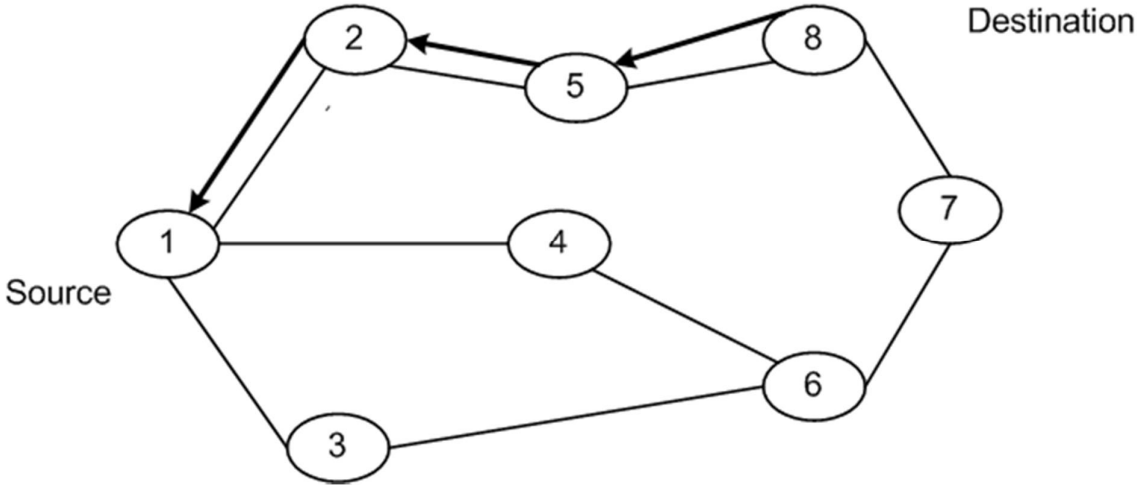


Figure 2.8: Unicast of RREP to the source

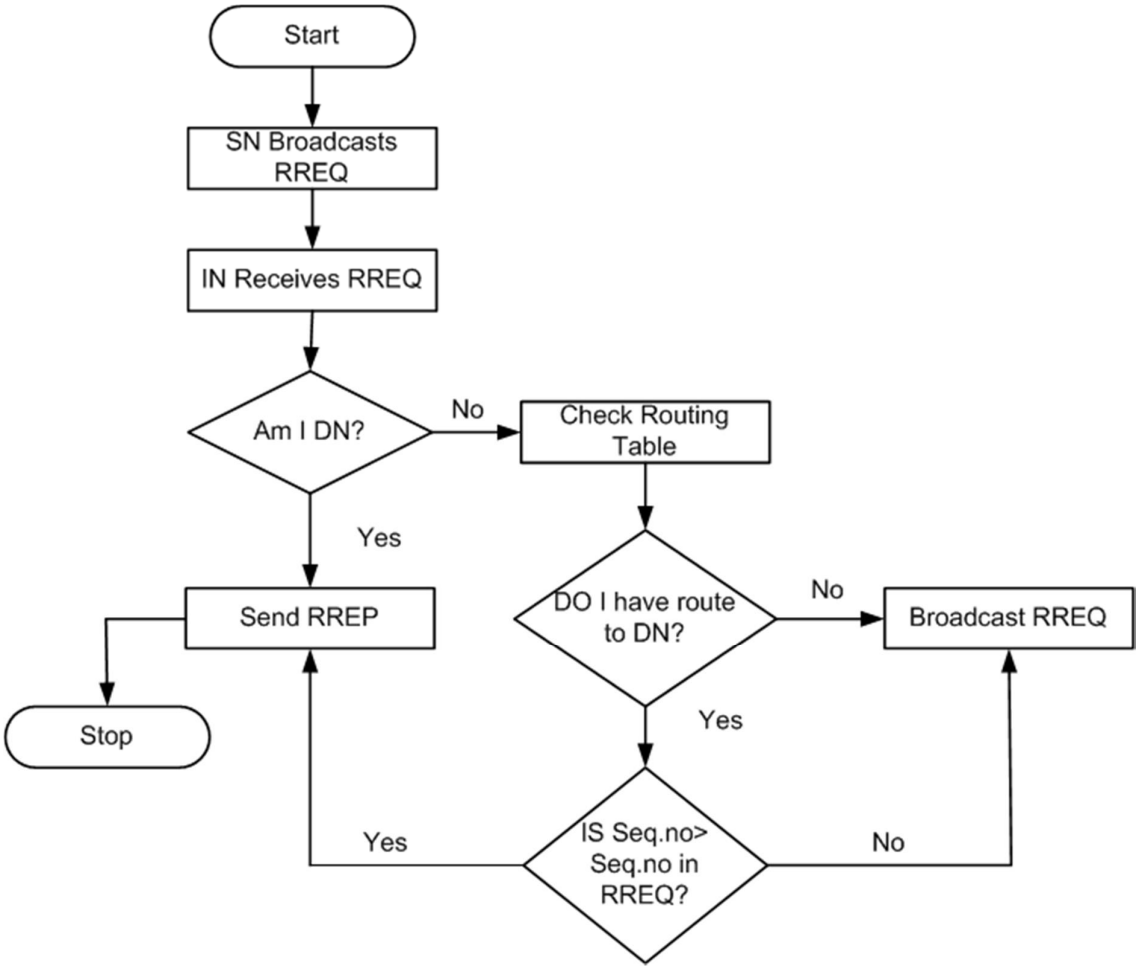


Figure 2.9: Route Discovery Flow Chart

2.8 Wireless Ad-hoc Network Technologies

The wireless technology is presently governed by the two standards, namely the Bluetooth and the IEEE 802.11 protocols. These standards are designed to manage wireless communications between devices that consume less power and are within limited transmission range (from a few up to several hundred meters). Bluetooth mainly replaces data transfer cables in communications between closely connected devices while IEEE 802.11 is focused on replacing cabled LANs formed by computers connected together (Ferro & Potorti, 2005).

2.8.1 Bluetooth

Bluetooth standard which is sometimes referred to as the IEEE 802.15.1 standard uses wireless radio communication. It is intended to provide wireless connectivity between short-range and cheap devices in order to substitute data transfer cables for computer peripherals such as keyboards, mice and printers. This range of applications is known as wireless personal area network (WPAN) (Lee et al., 2007).

When Bluetooth is activated on a device, the device functions as a slave device and waits for a master device to make an inquiry. The enquiry phase enables the master device to realise nodes in its range and their addresses. For simple paired devices that already have each others addresses, the enquiry phase is not needed. As soon as the master has learnt the address of the slave, it establishes a connection if a slave is ready for connection. The stage for starting a connection is called the paging phase. This paging phase leads to synchronization of the devices over the frequency hopping sequence. The frequency hopping sequence ensures that more than one device cannot transmit on the same frequency simultaneously (Ferro & Potorti, 2005)
.

2.8.2 IEEE 802.11

The purpose of IEEE 802.11 standard is to allow wireless communication between mobile, portable devices such as PDAs, notebooks when they require a speedy connection (Ferro & Potorti, 2005). When a device that has capability to use Wi-Fi is switched on, it starts scanning to find nearby available networks that have signals. It then chooses a network to join, either infrastructure or ad-hoc (Lee, et al., 2007).

In the case of infrastructure network where there is an access point, the device gets authenticated and connects with the access point (Ferro & Potorti, 2005).

2.9 Summary

This chapter has discussed literature on wireless networks, describing the different types of wireless networks and wireless network technologies. It mainly concentrated on MANET which is a group of mobile devices that can form a network, interconnect and share resources without the use of any fixed network infrastructure or centralised management. It further explained how MANET can find applications in areas such as military services, disaster recovery and conferences where the network infrastructure is not feasible.

Due to the high mobility and dynamic topology of MANETs, routing becomes very challenging. This chapter described the routing protocols for MANETs. It first described their classification based on how nodes establish and maintain paths, and then discussed each individual protocol in detail. Lastly the technologies behind wireless networking were discussed. The next chapter discusses the security issues in MANETs.

3 Security Issues in MANETs

3.1 Introduction

MANETs are exposed to many security attacks due to their salient characteristics such as dynamic topology, resource constraint, limited physical security and lack of infrastructure. Since MANETs use wireless links to transmit data packets, and the wireless links are vulnerable to attacks, the security problem is more severe. It is quite challenging to maintain security in MANETs than in wired networks because MANETs have far more vulnerabilities (Rajesh & Anil, 2012). This chapter discusses the various vulnerabilities that exist in MANETs, explains security goals that must be achieved for proper communication and lastly briefly explains the attacks against MANETs classified according to layer of occurrence in the protocol stack.

3.2 Vulnerabilities of MANETs

3.2.1 Lack of Secure Boundaries

The nodes in MANET are at liberty to move inside the network, join and leave the network any time. This makes it challenging to establish a security wall as compared to traditional wired networks that have a clear line of defence. In order to attack wired networks the adversaries must physically enter into the network medium, pass through firewalls and gateways before they have access to practice malicious behaviour to the target nodes in the network. However, in MANET the adversary can communicate with nodes within its transmission range, and become part of the network without any physical access to the network. The absence of secure boundaries causes MANET to be attacked at any time by any malicious node that is within the transmission range of any node in the network (Zaiba, 2011).

3.2.2 Threads from Compromised Nodes in the Network

Each mobile node operates independently, which means it is free to join or leave the network at any time. This makes it difficult for the nodes to set rules and strategies that can prevent malicious behaviour of other nodes in the mobile network. Also due to freedom of movement of the nodes in ad-hoc network, a compromised node can target different nodes in the network. Hence it becomes quite challenging to identify malicious actions of a compromised node in the network, more especially in a large network. Therefore, internal attacks from compromised nodes are more dangerous than external attacks because they are not easily identified due to the fact that a compromised node operated normally before it could be compromised (Zaiba, 2011).

3.2.3 Lack of Centralised Management Facility

There is no central equipment such as a server for monitoring the nodes in the network and this increases the vulnerability problems of MANETs. Firstly, it becomes very difficult to detect the attacks when there is no central control because the traffic in an ad-hoc network is very dynamic (Goyal et al., 2011). Secondly, lack of centralised management delays trust management for the nodes in ad-hoc network. It is not practical to perform a prior classification because no security association can be assumed for all network nodes. As a result, the usual practice of establishing a line of defence which distinguishes nodes as trusted and non-trusted cannot be achieved. Thirdly, lack of centralised authority can sometimes lead to decentralised decision-making. In MANETs, important algorithms rely on the cooperative participation of all nodes, so the adversary can make use of this vulnerability and perform attacks that can break cooperative algorithms (Singh et al., 2014).

3.2.4 Restricted Power Supply

Mobile devices in MANET get energy from batteries or other exhaustible means, so their energy is limited. This energy restriction can cause denial of service by the attacker; since the attacker is aware of the battery restriction, it can endlessly forward packets to the target node or make the target node to be involved in some time consuming activities. This causes battery power to be exhausted and the target node will be out of service. Again, the limited power supply may cause a node in

MANET to behave selfishly by not participating cooperatively in the network activities as a way to safe its limited battery. This becomes a problem particularly when it is essential for the node to cooperate with other nodes (Li & Joshi, 2008).

3.2.5 Scalability

Due to mobility of nodes, scalability is a challenge in MANET. Unlike traditional wired networks with a scale that is predefined during design, the scale of MANET keeps changing all the time. It is quite challenging to predict the number of nodes that will be there in future and as a result, protocols and services applied to MANET such as routing should be compatible to the changing scale of MANET (Zaiba, 2011).

3.3 Security Goals

Security is the mixture of systems, processes and procedures that are used to make sure that access and usage control, availability, authenticity, confidentiality, integrity, and non-repudiation are fulfilled for proper communication (Mladenović & Jovanović, 2012).

3.3.1 Access and Usage Control

Access control is a way of avoiding unauthorised access and usage of network resources and systems (Mladenović & Jovanović, 2012). Access control ensures that access to information is controlled by ad-hoc networks. Usage control makes sure that information resource is used correctly by the authorised nodes that have corresponding rights. This mechanism provides the ability to control information after it is transmitted (Yan, 2002).

3.3.2 Availability

Availability ensures that all the nodes in the network offer the designed services irrespective of the security state. If there is a route to a mobile node, then it should be accessible to all nodes that need to use it. The common attack that affects availability is Denial of Service attack (DoS). In DoS attack, a selfish node may put a larger number of junk packets into the network and thereby cause other network services to be unavailable. These junk packets exhaust a huge portion of resources

in the network and cause a performance degradation of wireless channels and the network as a whole (Li & Joshi, 2008). The DoS attack can cause physical jamming, disrupt routing protocol, disconnect the network and bring down high level services such as key management service. Routing table overflow attack and sleep deprivation attack are two examples of DoS attacks. In routing table overflow attack, routes to non-existent nodes are generated by the attacker. The goal of sleep deprivation attack is to exhaust the batteries of a victim node (Jawandhiya et al, 2010).

3.3.3 Authenticity

Authenticity guarantees that nodes taking part in a communication are genuine and not impersonators. It requires that the peer nodes communicating must have identities of each other. When there is no authentication required, an adversary could pretend to be another node, unlawfully access network resources and sensitive information and disturb the operation of other nodes (Zhou, 2003). In infrastructure wireless networks, a central monitoring device such as base station or access point can manage the authentication of the nodes, but there is no central administration in MANET so the authentication requirement is mostly met through routing protocols and inbuilt access control mechanisms (MladenoviĹ & JovanoviĹ, 2012).

3.3.4 Confidentiality

Confidentiality guarantees that private information is not accessible to unauthorised entities. Confidentiality must be a priority when information that is being transmitted in the network is sensitive. If such sensitive information can leak to enemies, they can use it against the network, and cause overwhelming consequences (Zaiba, 2011). It is challenging to preserve confidentiality in MANETs because MANETs use open medium, and all nodes can access information that is within their transmission range. Confidentiality is fulfilled mainly by using encryption methods, or alternatively using directional antennas to limit the emission of data (MladenoviĹ & JovanoviĹ, 2012).

3.3.5 Integrity

Integrity represents the ability to prevent an unauthorised change or destruction of messages being transmitted within MANET, as well as prevent subsequent messages from the attacker after the unauthorised change. Interception and change of data in a wireless medium is very frequent. Integrity guarantees that message received at the destination is exactly identical to the same message when it was sent at the source. There are two ways that can mainly compromise the integrity of messages.

i. An adversary can intentionally destruct the message by editing, replaying or deleting with a malicious goal.
ii. Some transmission errors in communication or hardware error can unintentionally cause the message to be lost or its contents to be altered (Li & Joshi, 2008).

3.3.6 Non-repudiation

Non-repudiation makes sure that the source of a message has no way of denying that it has sent the message. This helps to determine whether a node that behaves abnormally has been compromised or not. Any node that receives a message with errors from a misbehaving node can use that incorrect message as evidence to inform other nodes about the compromised node, and the node sending improper message will not deny having sent the message (Li & Joshi, 2008).

3.4 Classification of attacks

Attacks against MANET can be categorised into ***passive attacks*** and ***active attacks*** based on behaviour of the attack (Vani & Rao, 2011). They can also be categorised as ***internal*** and ***external*** based on the location of attacks (Saini & Kumar, 2010) . Some attacks are classified according to the ***layer of occurrence*** in the protocol stack (Pavani &Avula, 2012). The attacks can also be classified into ***modification attack***, ***impersonation attack*** and ***fabrication attack*** based on the technique used (Mladenoviĺ & Jovanoviĺ , 2012). Figure 3.1 below shows such categorization.

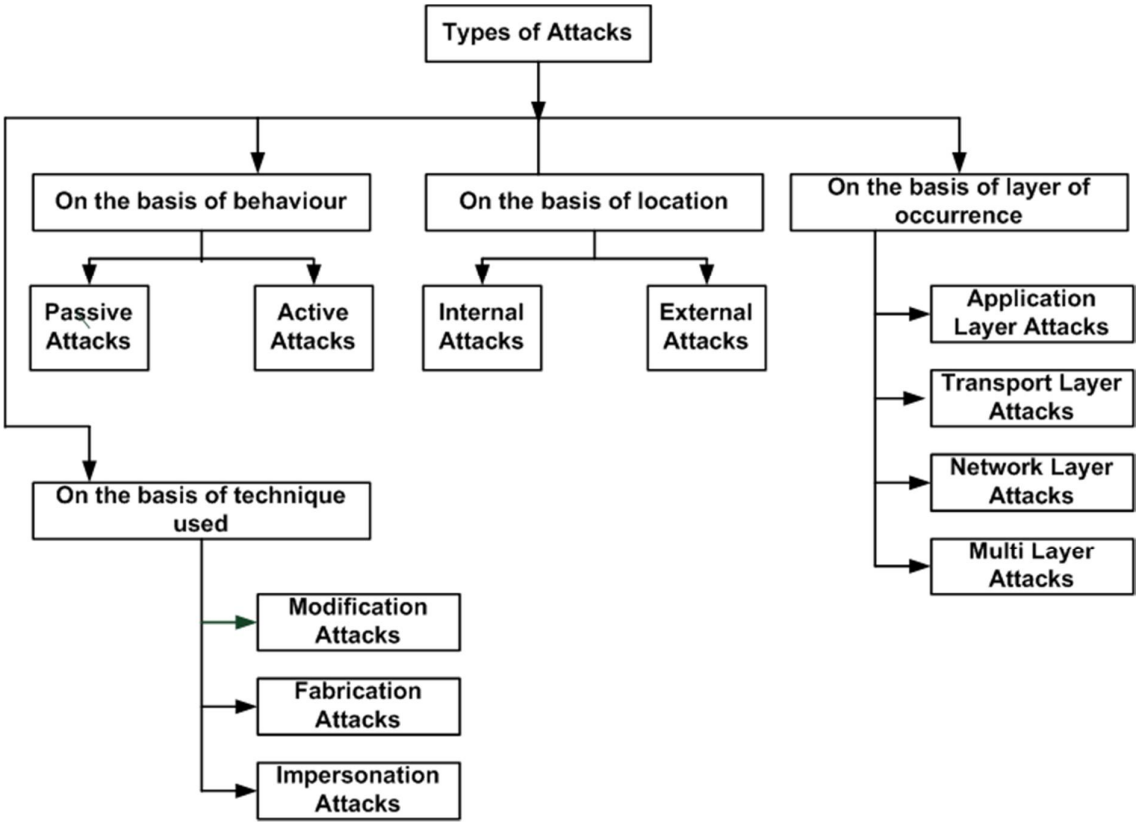


Figure 3.1: Classification of Attacks

3.4.1 Passive attacks

The normal operation of the network is not disturbed by a passive attack. A passive attacker eavesdrops to steal valuable information, or discards the received message silently (Wu et al., 2007). If an attacker can interpret the gathered data, then confidentiality will be compromised. Since the network continues to operate normally despite the attack, it is very difficult to detect this type of attack. The transmitted messages can be encrypted to make it difficult for eavesdroppers to interpret overhead data. ***Snooping*** is an example of passive attack (Rai et al., 2010).

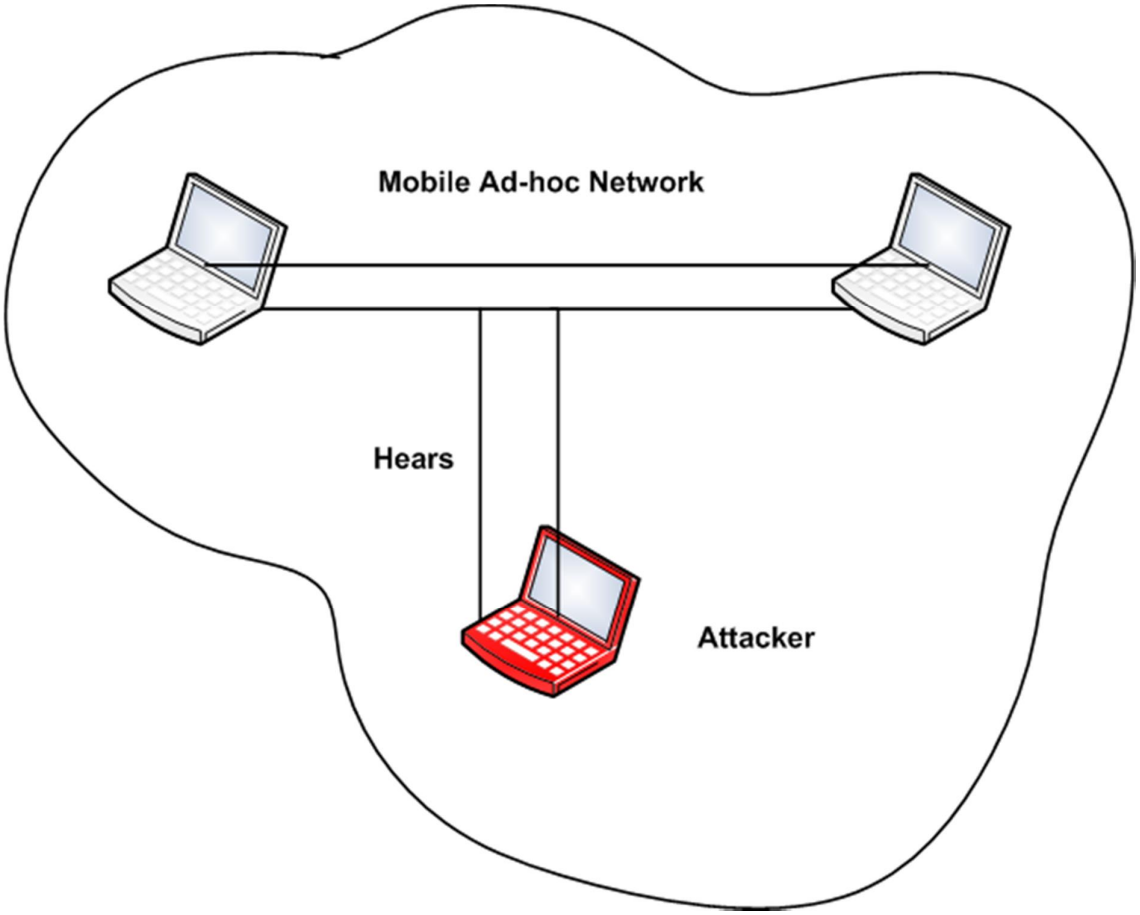


Figure 3.2: Passive Attack

3.4.1.1 Snooping

Snooping is accessing someone's data without approval. The simple form of snooping includes watching what is displayed on someone's computer screen and viewing what is being typed or reading someone's email. Software programs are used to perform complicated snooping that involves remotely monitoring all activities on a network device computer (Rai et al., 2010).

3.4.2 Active attacks

Active attacks disrupt the normal operation of the network. This is achieved by destroying or modifying data transmitted in the network (Rai et al., 2010).The attack can generate fabricated messages or alter the contents of messages (Wu et al., 2007). Active attacks can be internal or external. The examples of active attacks are modification, jamming, impersonation, fabrication, black hole attack, wormhole attack, resource consumption, and routing attacks (Kumar & Rishi, 2010).

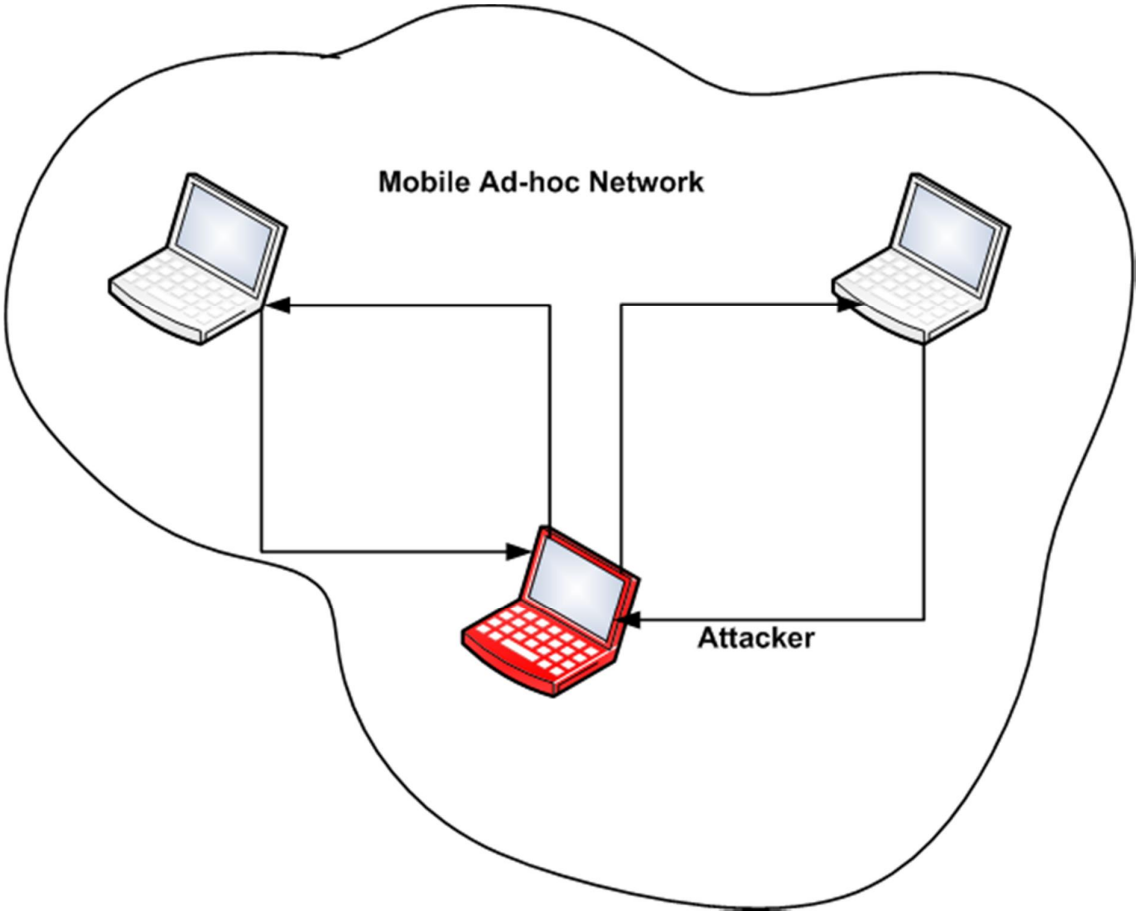


Figure 3.3: Active Attack

3.4.3 External attacks

An attack that is caused by nodes outside the network is an external attack. The encryption mechanisms and firewalls can be used to prevent external attacks (Jhaveri et al., 2010). External attacks can be orchestrated in different ways like impersonation and Denial of Service (Alani, 2014).

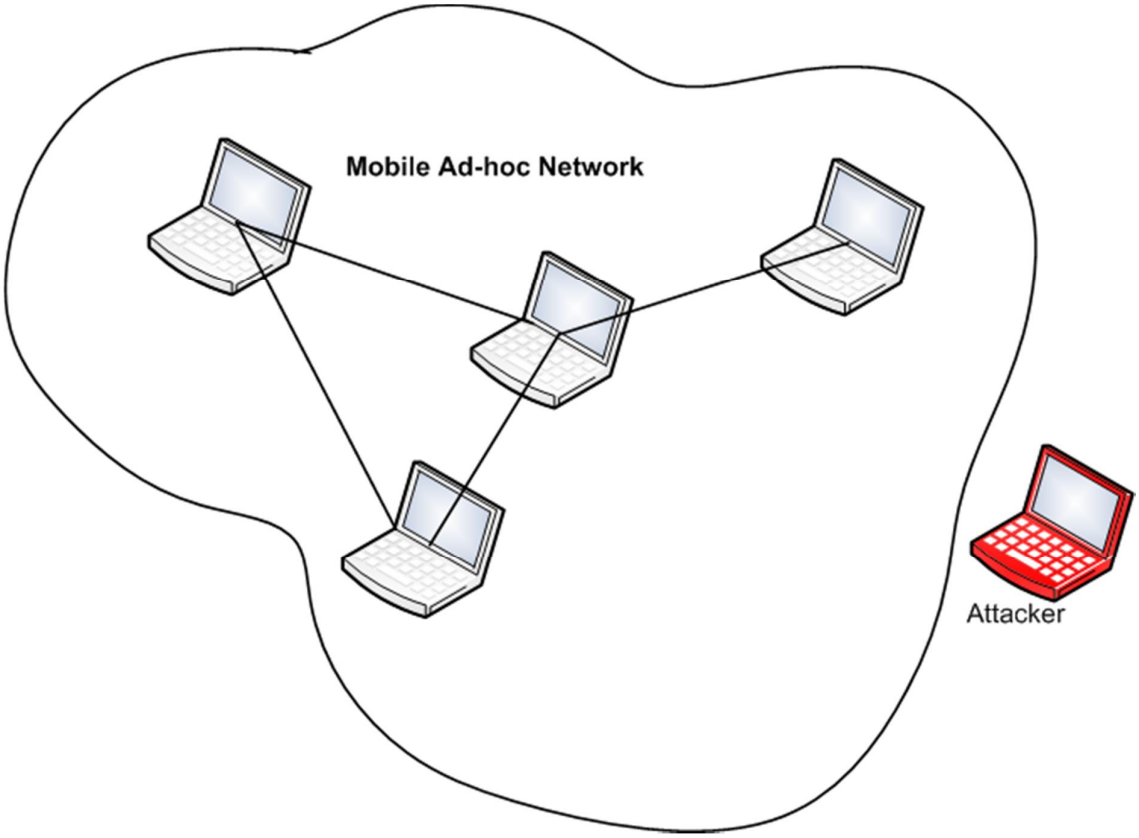


Figure 3.4: External Attack

3.4.4 Internal attacks

The hijacked or compromised nodes that are within a network launch internal attacks. Since the attackers are authorised members of the network, internal attacks are not easily detected and as such they are very dangerous (Giruka & Singhal, 2007). Mostly, the active attacks are launched from inside the network (internal) and do the most damage (El-Mousa & Suyyagh, 2010). The examples of internal attacks are routing attacks, wormhole attack and eavesdropping (Alani, 2014).

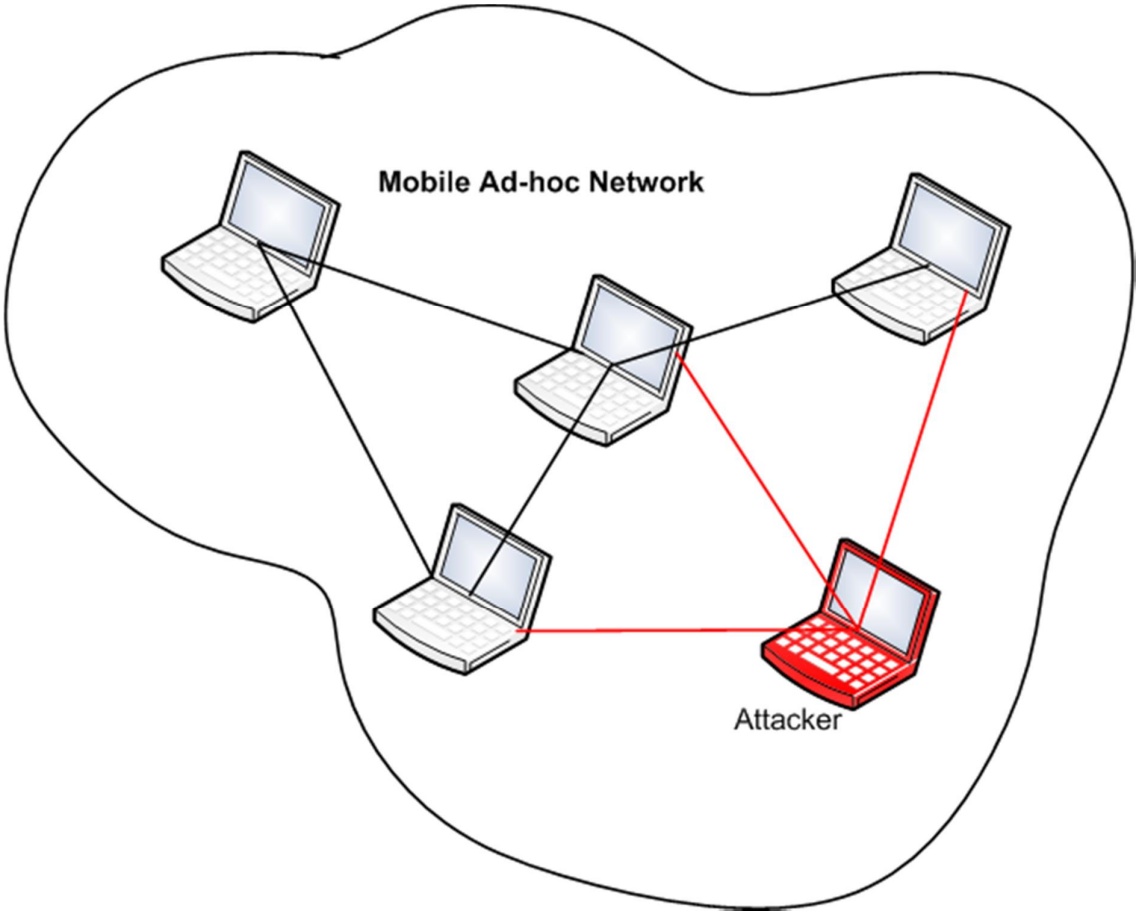


Figure 3.5: Internal Attack

3.4.5 Security attacks on protocol stack

Each layer in MANET communication has its own vulnerabilities, therefore attacks can also be classified according to the layer of occurrence as shown in Table 1 (Pavani & Avula, 2012);

Table 1: Security Attacks on Protocol Stack

Layer	Attack Examples
Network Layer	*Byzantine, Black hole, Wormhole, Resource Consumption, Gray hole, Routing attack*
Transport Layer	*Session hijacking, SYN Flooding*
Application Layer	*Repudiation,*
Multi- Layer	*Denial of Service (DoS), Impersonation*

3.4.5.1 Network layer attacks

Standard routing protocols in MANETs such as DSR and AODV were designed without considering any security constraints in MANETs. Routing happens at the network layer and several types of attacks on network layer are described in Section 3.4.5.1.

3.4.5.1.1 Byzantine attack

Byzantine attack occurs when a group of compromised intermediate nodes collaborate and launch attacks such as generating routing loops, transmitting packets through non-optimal paths, or selectively dropping packets. These attacks can cause routing services to be disrupted or degraded (Wu et al., 2007). These kinds of attacks are not easily detected because the network appears to be operating normally in the eyes of the user. Byzantine attacks are classified into black hole attack, wormhole attack, and flood rushing attack based on the number of nodes attacking the network and the method used to attack the network (Sivakami & Nawaz, 2015). Black hole attack and wormhole attack are described in Section 3.4.5.1.2 and Section 3.4.5.1.3 respectively. The flood rushing attack is described in Section 3.4.5.1.6.

3.4.5.1.2 Black hole attack

The adversary attacks the network by claiming to have the shortest route to a target node whose packets it wants to interrupt. It then attracts all packets destined to a

target node to itself, and then drops them (Pavani & Avula, 2012). Since this attack is the main focus of this research, its detailed description is given in Chapter 4.

3.4.5.1.3 Wormhole attack

Pair of malicious nodes works together to channel data packets received in one part of the network into a low latency tunnel and replays them in a different part. This is one of the severe attacks because it can disrupt all communications that ensure authenticity and confidentiality. Tunnelling routing control messages can disturb routing services. This tunnel between two scheming attackers is called a wormhole (Patel & Sharma, 2013).

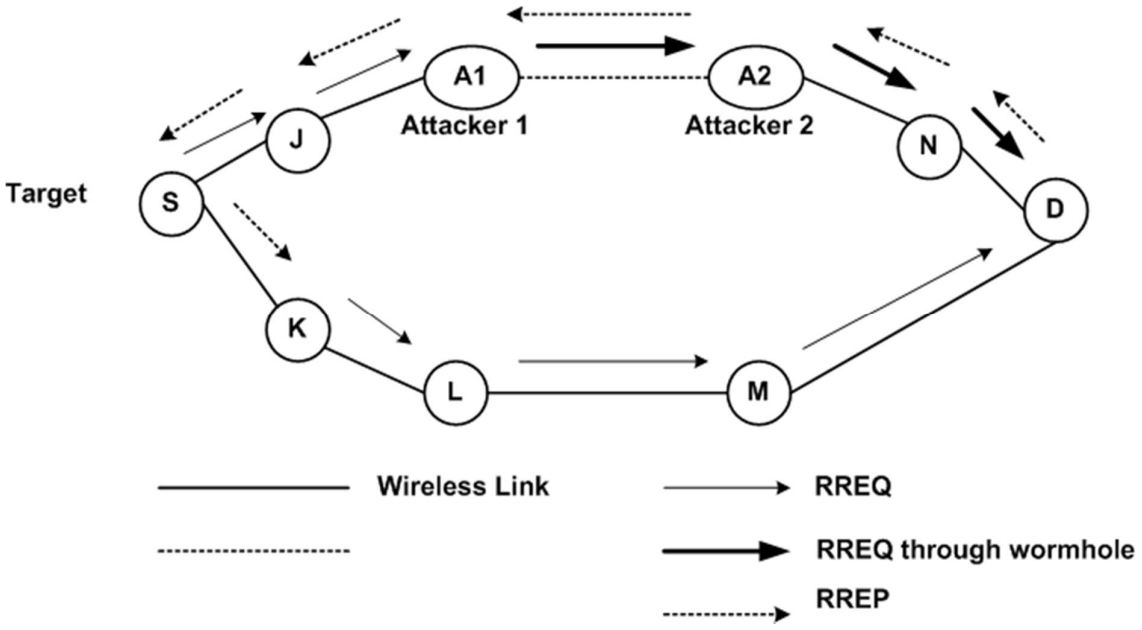


Figure 3.6: Example of Wormhole Attack (Kannhavong et al., 2007)

Figure 3.6 illustrates how a wormhole attack can occur against a reactive routing protocol. Suppose node A1 and node A2 in Figure 3.6 are two attackers that are scheming together to attack target node S. Node S wants to send data packets to destination node D, so it initiates a route discovery process by broadcasting the RREQ message. This RREQ is received by S's neighbours J and K and they forward the RREQ as usual. However, when node A1 receives the RREQ from node J, it records and channels the RREQ to its partner A2. Node A2 then broadcasts the RREQ again to its neighbour N. This RREQ reaches the destination node D first

because the tunnel created by the attacking nodes is of high speed. The destination node, D will unicast a RREP to source node S through the route D-N-J-S. The same RREQ that arrives later will be ignored by node D. This means, S will choose route S-J-N-D to send data to D, and this route passes through the wormhole tunnel created by node A1 and A2.

3.4.5.1.4 Resource consumption attack

The attacker targets to consume the resources of other devices in the network. The resources include bandwidth, battery power and computational power which are constraint in MANETs. The attacker could overload the network by sending unnecessary route requests or excessively sending stale packets to other nodes (Rai et al., 2010). This attack is also known as *sleep deprivation attack*. In AODV protocol, the attacker exploits route discovery process. It does not set the timer while waiting for the route reply. Instead it exhausts the network by continuously sending RREQ packets as shown in Figure 3.7. The malicious packets will congest MANET links and this jamming causes a disruption in gaining access to services of available servers in the network. For example, if N1 in Figure 3.7 denotes a server, then its services could be made inaccessible by attacker N3 (Abdelhaq et al., 2011).

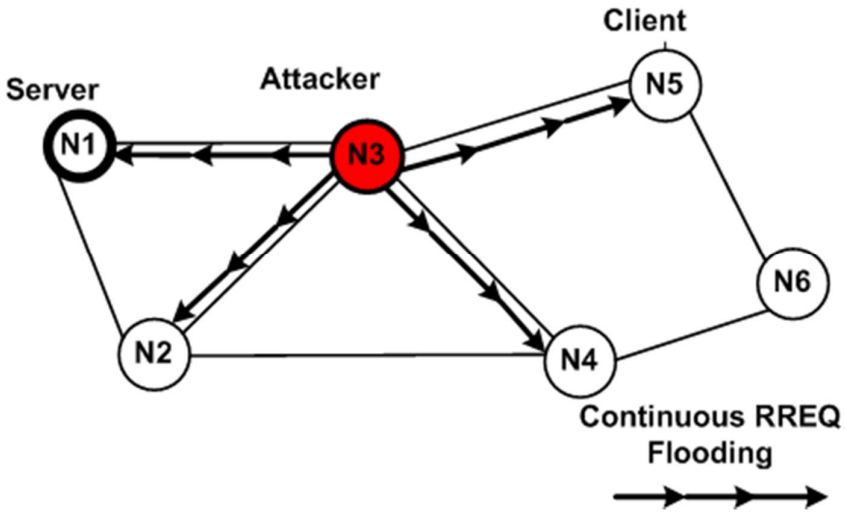


Figure 3.7: Resource Consumption Attack (Alani, 2014)

3.4.5.1.5 Gray hole attack

Gray hole is a special type of a black hole attack. A malicious node in this attack drops the packets selectively (Kanthe et al., 2012). During route discovery process, a malicious node pretends to be trustworthy, but thereafter begins to silently drop packets. There are three types of gray hole attacks. Firstly, a gray hole may choose to discard packets coming from or intended for specific nodes, but forward all packets to certain nodes. Secondly, a gray hole may act maliciously for a certain period, but later on act just like other normal nodes. The third type is a combination of the first two types. A gray hole node may discard packets from specific nodes for certain time only, and later on act normally. It is quite challenging to detect these types of attack due to this uncertainty (Jhaveri et al., 2010). Figure 3.7 demonstrates the operation of gray hole attack.

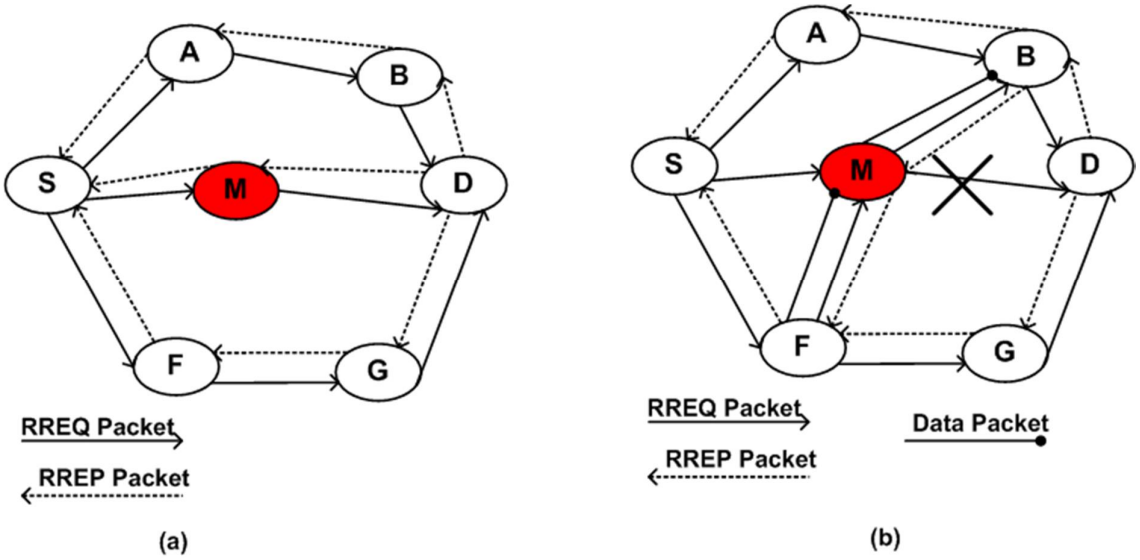


Figure 3.8: Gray Hole Attack

In Figure 3.7 (a), initially node M behaves as an ordinary node and forwards all packets from source node S to destination node D. After some time as shown in Figure 3.7 (b), node M behaves maliciously and starts dropping packets sent by source node S to destination node D.

3.4.5.1.6 Routing attacks

There are many attacks which can be launched against the routing protocols in order to mess up the normal functioning of the network. Such attacks have been briefly described below.

1. Routing Table Overflow: The aim of the attacker is to generate adequate routes so as to prevent new routes from being created. The attacker achieves this by creating routes to nodes that do not exist. This creation of routes causes routing tables to overflow, which would stop creation of entries that correspond to new routes to existing nodes. For proactive routing algorithms, routing information is discovered even before it is needed, while in the case of reactive algorithms a route is found only when it is needed.

2. Routing Table Poisoning: If there is a compromised node in the network, it will either alter routing updates that have been sent to other authorised nodes or generate and send false routing updates. Routing table poisoning may hinder routing process in the network, cause congestion in some parts of the network or make some portion of the network to be unreachable.

3. Packet Replication: The attacking node reproduces out-dated packets in the network. This replication contributes to the consumption of resources such as bandwidth and power which are needed by other nodes, and also confuses the routing process in the network.

4. Route Cache Poisoning: For on-demand routing protocols, the nodes keep a record of recent routes that are known in a route cache. Similar to routing table poisoning, a compromised node in the network can alter the entries in the route cache to cause confusion.

5. Rushing Attack: An attacker takes advantage of the route discovery process. When a source node broadcasts a RREQ, an attacker that receives this request quickly floods it throughout the network before other nodes. By the time other nodes that received the same request start to forward the request, it is assumed to be a duplicate of the request previously sent by the attacker, and hence the nodes that receive the request discard it. This means the attacker would be an intermediate node in all the routes that are discovered by the source node, hence all messages

from the source node would not be safe as they pass through the attacker. Rushing attacks are very difficult to be detected in ad-hoc wireless networks (Rai et al., 2010; Wu, et al., 2007).

3.4.5.2 Transport layer attacks

Transport layer is responsible for end to end communication services between applications in the network. Transmission Control Protocol (TCP) is the popular transport protocol, which is used for connection oriented transmissions. User Datagram Protocol (UDP) is mostly used in forwarding simple messages between applications in the network. Attacks at this layer target the loopholes in the operation of these protocols as described below.

3.4.5.2.1 Session hijacking

The authentication of two communicating parties is done only at the beginning of the session so session hijacking attack takes advantage of that. In TCP session hijacking, the attacker masquerades as a victim node by using its IP address to find the sequence number expected by the target node. The attacker then pretends to be the victim node, perform Denial of Service (DoS) attack on the victim and continues to have illegal sessions with the target node. Session hijacking over UDP is similar to TCP session hijacking but much easier to perform because the attacker does not have to determine the sequence numbers expected by target node because UDP is connectionless (Wu et al., 2007).

3.4.5.2.2 Synchronization (SYN) Flooding attack

The communication between two nodes using TCP is connection oriented, so a three-way handshake is used to create a connection. The three-way handshake involves three messages that are exchanged by nodes that want to start a communication. The messages help the nodes to alert each other when they are ready to start communicating, and to decide on initial sequence numbers for the conversation. Figure 3.6 below illustrates a three-way handshake.

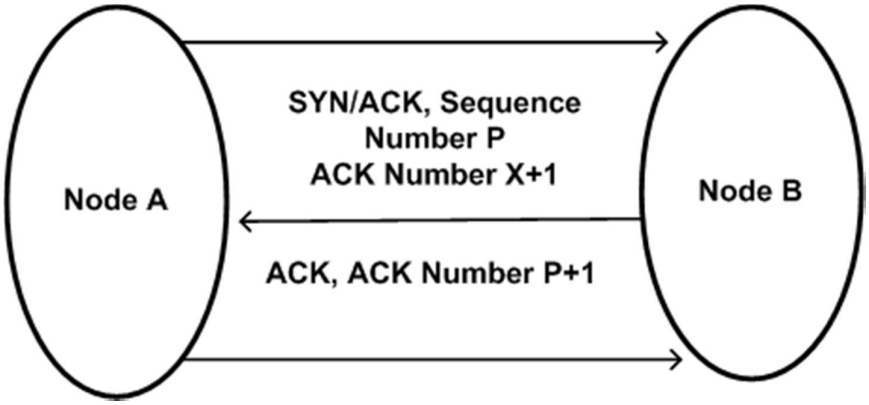


Figure 3.9: TCP Three-way Handshake

In this type of attack, a malicious node initiates a TCP connection with a victim node, but does not complete the handshake to fully open a connection. A malicious node repeatedly sends SYN packets to a target node using a fake address. A target node responds to each SYN packet by sending SYN acknowledgement (SYN-ACK) packet to a malicious node and waits to receive ACK packet that confirms that a malicious node has received SYN-ACK packet. A malicious node never sends back ACK packet, instead it continues to send SYN packets to the victim node.

All these half-opened connections are stored in the fixed table of a target node, and they could overflow the buffer of the node, denying other legitimate nodes a chance to establish a genuine TCP connection with a target node. Usually these stored half-opened connections are given a certain time frame before they can expire and be discarded, so eventually a victim node will recover when pending connections expire. Nevertheless, a malicious node can continue sending SYN packets to a victim node at a rate faster than the rate at which pending connections expire (Rai et al., 2010).

3.4.5.3 Application layer attacks

The application layer makes sure that communication between application programs in the network is effective by making services needed by the application programs available. The application layer attacks as described below target user applications.

3.4.5.3.1 Repudiation

Repudiation occurs when a node in the network takes part in a communication but later on claims that it was not involved in such communication (Wu et al., 2007). For example, a selfish person can carry out a repudiation attack in a commercial system by making an online transaction or credit card purchase and later on claim not have been involved in those operations (Rai et al., 2010).

3.4.5.4 Multi-layer attacks

There are some attacks that are not firmly related to any specific layer in the network protocol stack, and they are referred to as multi-layer attacks. The popular multi-layer attacks are Denial of Service and impersonation.

3.4.5.4.1 Denial of Service (DoS) attack

Denial of service is an attack whose aim is to deny access to some system resources and thereby deteriorate the performance of the network in delivering the expected functions. There are different ways that can be used to carry out a DoS attack, but the classical way is to use flooding mechanism in order to overflow the network resources so that the network crashes. For instance, during route discovery process, a malicious node may overflow the network by continuously sending unnecessary route requests to deny other nodes the opportunity to make use of the available network resources (Li & Joshi, 2008). The attack scenarios targets are storage, processing resources, bandwidth, battery power of the service provider (Kanthe et al., 2012). Some types of the DoS attacks are explained below.

3.4.5.4.1.1 Distributed DoS attack

In this attack, many attackers spread over the whole network, cooperate and cause available network resources to be inaccessible to genuine users. This attack is therefore the most intense type of DoS attack (Rai et al., 2010).

3.4.5.4.1.2 Jamming attack

The attacker monitors the wireless network to obtain the frequency rate at which the receiver communicates. The attacker then uses the same frequency as the receiver to send data in order to disrupt the operation of the receiver (Mishra et al., 2010).

3.4.5.4.2 Impersonation

A malicious node joins the network, pretends to be a trusted node of the network and begins to maliciously send misleading routing information. Since the attacking node has disguised itself to be legitimate, it gets permission to access the network management system. It can then alter the system configurations to benefit itself with special rights (Patel & Sharma, 2013). *Sybil attack* is a well-known impersonation attack in which a malicious node behaves as if it were a large number of nodes by impersonating other nodes or simply claiming false identities (Mishra et al., 2010).

3.4.6 Modification Attack

The attacker illegally alters the contents of the routing messages and the routing process gets messed up. The attack can be performed by altering the route sequence numbers and by changing the hop count in order to prompt attacks such as black hole attack (Pervaiz, et al., 2010). These attacks include deletion, insertion, or alteration of information in an unauthorised manner usually represented to the client as legitimate (MladenoviĹ & JovanoviĹ , 2012).

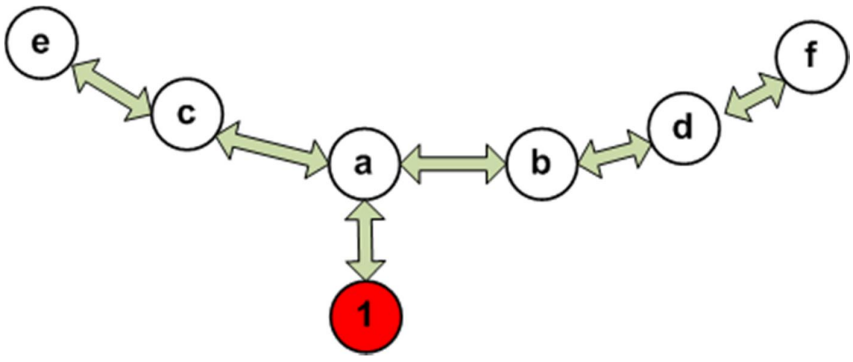


Figure 3.10: Modification attack (Mladenović & Jovanović, 2012)

Figure 3.7 above shows a malicious node (1) that may spread messages to other nodes in the network with false claims on the length of a route. It redirects traffic in the part of the network on the route between (a) and (f) nodes by propagating

messages with false values claiming that the route between (a) and (f) going through it, (1), is shorter than claimed by node (b). In this manner the traffic is rerouted through the attacking node (1) that enables taking over the session, listening to traffic, creating communication delay and provoke energy expenditure in the network.

3.4.7 Fabrication Attack

A malicious node interrupts the operation of the network or consumes resources available to other nodes by creating fake route error messages and routing updates (Pervaiz et al., 2010). Some of the best known fabrication attacks are black hole, gray hole and wormhole attacks (Mladenoviĺ & Jovanoviĺ , 2012).

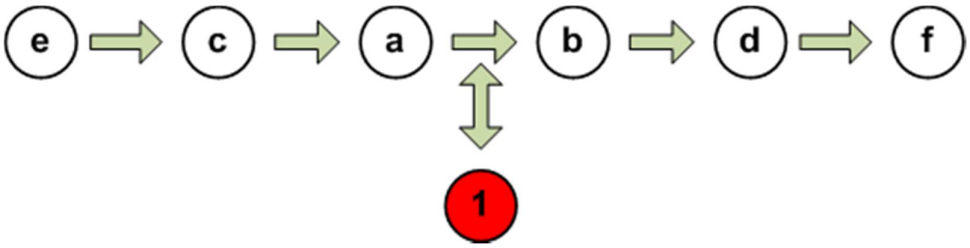


Figure 3.11: Fabrication attack (Mladenović & Jovanović, 2012)

Figure 3.8 above shows a situation where node (e) has a route to (f) through nodes (c), (a), (b) and (d). The malicious node (1) can undertake an attack (DoS) on node (f) by constantly sending route error messages to (a), thus discrediting node (b) with information that connection between (b) and (f) has been interrupted. Node (a) receives false route error messages, accepts they came from node (b) and as a consequence deletes its own routes table entry for node (f) and forwards route error message to (c) that also updates its route tables. Node (1) can constantly listen to the connection and each time, upon recognising the request of node (a) to establish a connection with node (f), can broadcast spoofed route error message and this prevents communication between these two nodes in the network.

3.5 Summary

Security is a very crucial issue in all kinds of communications. This chapter looked at the security aspects of MANETs. It firstly explained the characteristics of MANETs

that cause them to be more susceptible to attacks than the traditional wired networks. Moreover, the chapter explained the attributes that must be fulfilled by the network in order to conclude that it is secure.

Attacks against MANETs can be classified as active or passive, internal or external, fabrication, modification or impersonation and can also be classified according to the layer of occurrence. The different classifications are explained in this chapter and each of the attacks is discussed. The next chapter focuses on explaining black hole attack which is the type of attack addressed in this study.

4 Black Hole Attack

4.1 Introduction

Chapter 3 gave a brief discussion of each of the security issues in MANETs, and black hole attack being one of the issues, was also briefly discussed. This chapter gives a detailed explanation of black hole, clearly explaining the types of black hole attacks in both AODV and DSR networks. The chapter then looks at some of the solutions previously suggested to reduce the impact of black hole attack, and lastly discusses previous research work related to this study.

4.2 Overview of Black Hole Attack

Black hole attack is one of the harmful attacks caused by a malicious node that misbehaves in a network. This malicious node is referred to as a black hole (Vani & Rao, 2011). A malicious node exploits the process of discovering routes in reactive routing protocols. When a source node broadcasts a route request, a malicious node misleads other nodes by claiming to have the shortest and freshest route to destination. It achieves this by sending false route replies, attracting data packets to be routed through it and just discarding them instead of forwarding. This is similar to how a black hole in the universe behaves (Raj & Swadas, 2009).

The messages in ad-hoc network are divided into routing messages and data messages (Zapata & Asokan, 2002). One type of black hole attack targets the actual data traffic by deliberately discarding, delaying or changing the contents of data traffic. To alleviate this type of attack, a promiscuous mode[1] of each node is set so that each node can watch the neighbouring node to see if it transmits data traffic as expected (Sun et al., 2003).

Another type of black hole attack occurs when a malicious node attacks routing control messages; once a malicious node receives a RREQ from nearby nodes, it sends a forged RREP message claiming to have a fresh and short route to the destination. The data packets that are sent to the destination will therefore pass through a malicious node which will absorb them (Sharma & Sharma, 2012) .

[1] Mode in which a node on the network accepts all packets, regardless of their destination address

It becomes challenging to detect black holes if they use sequence numbers that are in the same range with sequence numbers that are being utilised currently in the network (Sharma & Sharma, 2012). For TCP communication which is connection-oriented, a source node eventually discovers a malicious behaviour because there will not be any acknowledgements received from the destination, so the source node will use a different route. For UDP communication which is connection-less, it is very difficult to detect a black hole because there will not be any acknowledgements messages expected (Thachil & Shet, 2012).

The presence of a malicious node interrupts communication between mobile nodes, because it absorbs all traffic from the source node. When the black hole is in possession of the data packets, it can perform a DoS attack by dropping the packets or intercepting the packets. Confidentiality of the message is also not preserved when there is a black hole attack (Vani & Rao, 2011) . According to Sharma and Sharma (2012), a network overhead is increased in the presence of a black hole attack, the energy of the nodes in the network gets exhausted thereby reducing the networkôs lifetime and ultimately the network is destroyed. Black hole attack is very harmful because the data being discarded by malicious node may include critical data of the network.

4.3 Types of Black Hole Attack

In MANET, black hole attacks can be classified into single black hole attack and co-operative black hole attack (Tseng et al., 2011).

Single black hole attack: There is only one malicious node attack on the route.

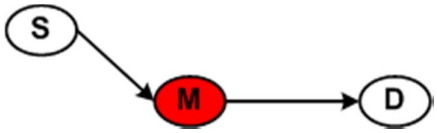


Figure 4.1: Single Black Hole Attack

Figure 4.1 shows a route from source node, S to destination node, D and there is only one malicious node, M.

Co-operative black hole attack: Malicious nodes act in a group. Figure 4.2 shows two malicious nodes, M1 and M2 working co-operatively to attack the network.

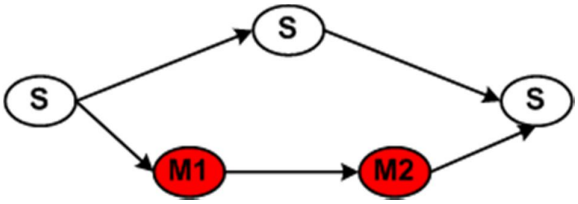


Figure 4.2: Co-operative Black Hole Attack

The black hole attack can also be classified into two categories based on the cause of the attack as follows (Sharma & Gupta, 2009):

i. Black hole attack caused by RREP
ii. Black hole attack caused by RREQ

Black hole attack caused by RREP

For black hole attack caused by RREP, when a source node initiates the route discovery process by broadcasting a route request, a malicious node misleads other nodes by pretending to have an updated route to destination that is shortest and freshest (Vani & Rao, 2011). The black hole sends a forged RREP message pretending to have a fresh and short path to the destination. This means the black hole always returns a positive RREP even when it has no valid route to the destination. The data packets that are transmitted to the destination will therefore pass through a malicious node which will silently absorb or discard them (Sharma & Sharma, 2012). Figure 4.3 illustrates black hole attack caused by RREP.

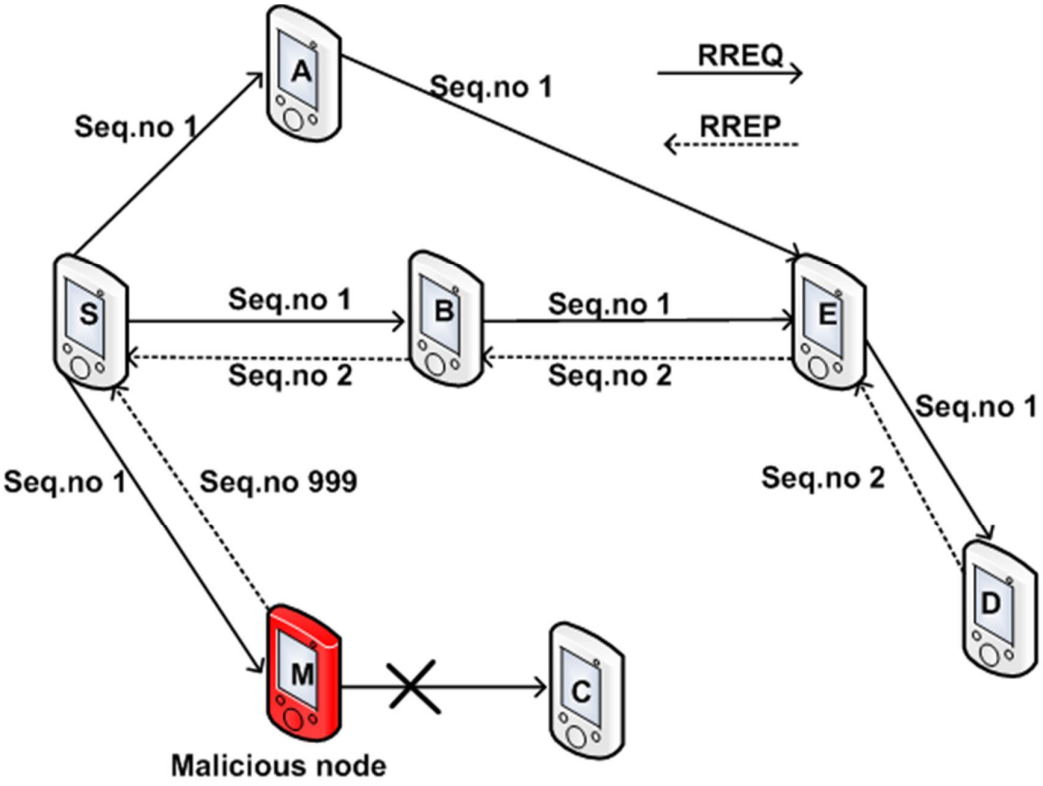


Figure 4.3: RREP Black Hole Attack

ÅSource node, S needs to transmit messages to destination node, D and it has no fresh enough path to D, so it broadcasts RREQ to discover the route.

ÅUpon receiving a RREQ packet, a malicious node, M immediately responds with the highest sequence number RREP, claiming to have a fresh route to D. Malicious node, M is advantaged because it replies without searching for the route in its routing table.

ÅSince a RREP sent by M has the highest sequence number, S will take a route from M and send data packets to M for forwarding. M will absorb all the packets and discard them.

Black hole attack caused by RREQ

For black hole attack caused by RREQ, a black hole sends a forged RREQ message to attack a target node in the network. This black hole pretends to be rebroadcasting the RREQ packet that originated from a target node in the network. It then adds itself as the next hop in the route record, so the entire messages destined to the target

node will pass through it and it will discard the messages (Sharma & Gupta, 2009). Figure 4.4 illustrates black hole attack caused by RREQ.

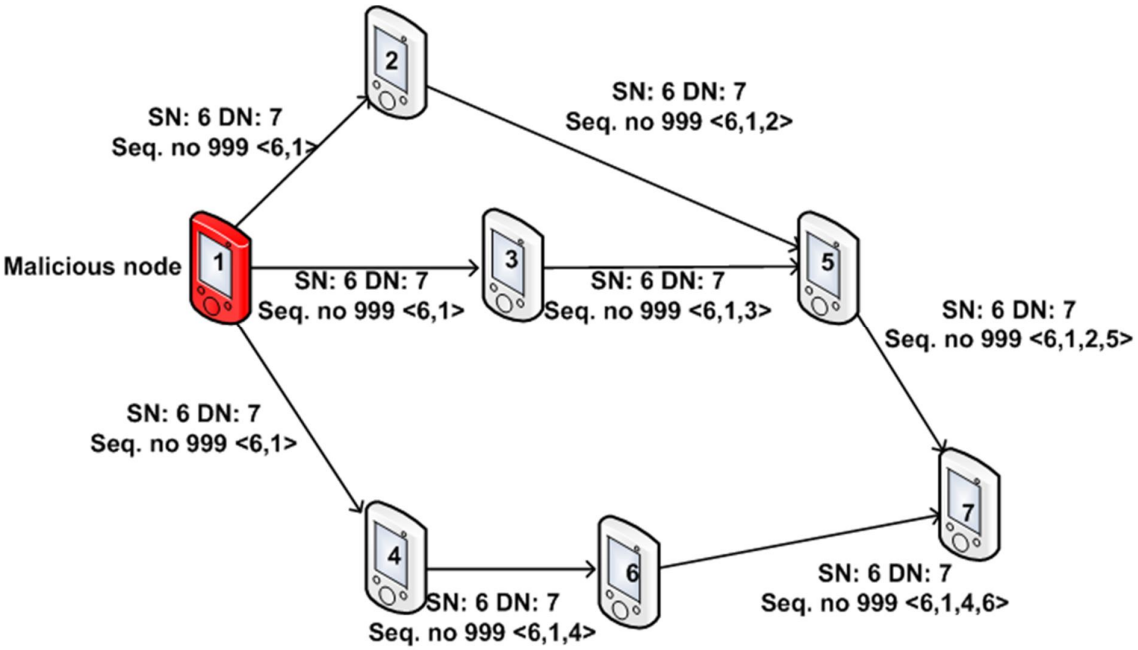


Figure 4.4: RREQ Black Hole Attack

ÅA malicious node 1 forges a RREQ packet for a path to destination node 7. The RREQ packet appears to have been created by 6 and forwarded by node 1 which adds itself as next hop in the route record.

ÅThe intermediate nodes 2, 3 and 4 receive the fake RREQ packet and updates their route caches with false routing information because the RREQ packet is given a high sequence number to mislead them.

ÅAll data packets intended for node 6 will be forwarded to node 1 with the trust that node 1 will pass them to node 6. Instead of forwarding the data packets, node 1 launches a black hole attack by discarding or absorbing the packets.

ÅThe similar malicious operation done to node 6 is performed on node 2, 3, 4, and 5. If this malicious behaviour is repeated time after time, all other nodes will be misled into believing that the route that passes through node 1 is the best to all other nodes.

4.6 Mitigation Techniques for Black hole attack

This section describes some of the techniques that were suggested by researchers to mitigate the black hole attack. The solutions have been tested using the base protocol AODV; however these solutions can be applicable to other reactive routing protocols such as DSR (Weerasinghe & Fu, 2007).

4.6.1 Detection, Prevention and Reactive AODV (DPRAODV)

Raj (2009) proposed DPRAODV. In this scheme, AODV protocol is modified to have a new control packet called **ALARM** and a **threshold value.** A threshold value is the average of the difference of destination sequence number in the routing table and sequence number in the RREP packet.

In the usual operation of AODV, the value of sequence number is checked in the routing table by the node that receives a RREP packet. The sequence number of RREP packet has to be higher than the sequence number value in the routing table in order for RREP to be accepted. In DPRAODV, there is an extra threshold value that is compared to RREP sequence number, and if RREP sequence number is greater than the threshold value, then the sender is considered malicious and added to the black list. The neighbouring nodes are notified using an ALARM packet so that the RREP packet from the malicious node is not processed and gets blocked. Automatically, the threshold value gets updated using the data collected in the time interval. This updating of the threshold value helps to detect and stop black hole attacks.

The ALARM packet contains the black list that has a malicious node, so that the neighbouring nodes reject any RREP packet from a malicious node. Any node that receives a RREP packet checks the black list and if the reply comes from a node that has been blacklisted, it is ignored and further replies from that node will be discarded. Thus the ALARM packet isolates a malicious node from the network.

4.6.2 Intrusion Detection System AODV (IDSAODV)

Suryawanshi and Tamhankar (2012) proposed IDSAODV in order to decrease the impact of black hole. This is achieved by altering the way normal AODV updates the

routing process. The routing update process is modified by adding a procedure to disregard the route that is established first.

The tactic applied in this method is that the network that is attacked has many RREP packets from various paths, so is assumed that the first RREP packet is generated by a malicious node. The assumption is based on the fact that a black hole node does not look up into its routing table before sending a RREP packet. Therefore, to avoid updating routing table with wrong route entry, the first RREP is ignored.

This method improves packet delivery but it has limitations that; the first RREP can be received from an intermediate node that has an updated route to the destination node, or if RREP message from a malicious node can arrive second at the source node, the method is not able to detect the attack.

4.6.3 Enhanced AODV (EAODV)

Ahmad et al. (2011) proposed EAODV. Similar to IDSAODV, EAODV allows numerous RREPs from various paths to lighten the effect of black hole attack. This method makes an assumption that eventually the actual destination node will send a RREP message, so the source node overlooks all previous RREP entries, including the ones from malicious node and takes the latest RREP packet.

The source node keeps on updating its routing table with RREPs being received until a RREP from the actual destination is received. Then all RREPs get analysed and suspicious nodes are detected and isolated from the network. The limitation to this method is that it adds two processes that increase delay and exhaust energy of the nodes.

4.6.4 Secure AODV (SAODV)

Lu et al. (2009) proposed a secure routing protocol SAODV that addresses black hole attack in AODV. The difference between AODV and SAODV is that in SAODV, there are random numbers that are used to verify the destination node. An extra *verification packet* is introduced in the route discovery process. After receiving a RREP packet, the source node stores it in the routing table and immediately sends a verification packet using reverse route of received RREP. The verification packet contains a *random number* generated by source node.

When two or more verification packets from the source node are received at the destination node, coming from different routes, the destination node stores them in its routing table and checks whether the contents contain the same random numbers. If the *verification packets* contain same random numbers along different paths, the destination node sends *verification confirm packet* to the source node which contains random number generated by destination node.

If *verification* confirm *packet* contains different random numbers, the source node will wait until at least two or more verification confirm packets contain same random numbers. When the source node receives two or *more verification confirm packet* with same random numbers, it will use the shortest route to send data to the destination node. The security mechanism in this protocol is that malicious node cannot pretend to be destination node and send correct *verification confirm packet* to the source node.

4.6.5 Solution using Packet Sequence Number

In the regular operation of AODV, the source node compares the value of RREP sequence number with sequence number in its routing table. The RREP packet is accepted only if its sequence number has a value higher than the sequence number in sourceŝ routing table.

According to Vani and Rao (2011), RREP sequence number is also compared to the threshold value to solve black hole problem. This threshold value gets updated after every time interval. Any node that sends a RREP packet with a sequence number greater than the threshold value is alleged to be malicious and is blacklisted. Sharma and Sharma (2012) propose that two additional small tables need to be added to every node. The sequence number for the *last packet sent* by a node is to be recorded in one table and another table should record the sequence number for *last packet received* from every node. Every time a packet is received or sent by a node, the tables are updated.

During route discovery process, the source node broadcasts a RREQ packet to nearby nodes. The destination node or the intermediate node that has a fresh route to the destination will reply to the sender with RREP packet that contains the last packet sequence number received from the source node. The source node will

therefore verify that the sequence number of RREP received matches the record it has in the table, and if it does not, the RREP packet is suspected to be from a malicious node. Since the sequence number is already part of communication in the base protocol, this solution does not increase overhead to the transmission channel. It makes it easy to recognise a suspicious reply.

4.6.6 Solution utilizing network redundancy

This is an improvement of the normal AODV. The solution proposes that the source node does not immediately start sending data packets after receiving a route reply. It waits to receive other route replies from nearby nodes to confirm that they contain the same next hop information. This solution uses an assumption that there are redundant routes that can be used to reach the destination node. When a RREP packet arrives at the source node, the full path is extracted and the source node waits for another RREP packet. The routes from other RREP packets are compared with the route extracted from the first RREP, and they must have shared hops. If there are no shared hops in the routes, the source node takes the routes to be untrustworthy and waits for more RREP packets until there are shared hops or until the expiration of the routing timer. Even though this solution assures a safe route, it increases the time delay and messages will never be forwarded to the destination node if there are no shared hops in the paths (Sharma & Sharma, 2012).

4.7 Related Works

This section surveys some of the related work that has been published in the literature.

Mohebi et al. (2013) analysed the performance of AODV and DSR routing protocols when attacked by black hole. In their work, they simulated AODV and DSR when there is no attack and when attacked by co-operative black hole using OPNET simulation tool. Network throughput, end-to-end delay and network load have been used as metrics to analyse the performance of the network. The scenarios that they used aimed to reveal how the protocols perform when the number of mobile nodes and the number of black hole nodes are varied. The results they obtained show that under normal operation, MANET performs better than MANET that is attacked by co-

operative black hole. Also, the results show that DSR is not the best protocol to use in a huge network that has many mobile nodes because its performance deteriorates in such environment.

Dadhania and Patel (2013) evaluated the performance of AODV and DSR in the presence of black hole attack and without black hole attack. Experiments have been conducted using NS-2 simulator. Performance metrics considered for evaluation are throughput, packet delivery ratio and end-to-end delay. Based on their research and analysis, they have drawn a conclusion that AODV is more vulnerable to black hole attack.

Gill and Kunwar (2014) focused on comparative analysis of AODV and TORA routing protocols when the network is under black hole attack. NS-2 simulator is used to make simulations. The analysis is done using end-to-end delay, throughput, network load, packets received, packets dropped, and routing overload as performance metrics. The simulation results show that in the presence of black hole attack, TORA performs much better than AODV.

Singh and Singh, (2013) analysed the three routing protocols, AODV, OLSR and ZRP in the presence of black hole attack. The simulations were undertaken using NS-2 and the analysis was done using performance parameters such as average end-to-end delay, throughput and packet delivery ratio. The conclusion drawn from their study is that when the network is attacked by black hole, OLSR and ZRP perform better than AODV.

Bala et al. (2009) simulated the black hole attack on AODV using NS-2. The simulation results show packet loss, throughput and end-to-end delay with black hole and without black hole. The analysis show that packet loss increases in a network with black hole node. Throughput and end-to-end delay decrease in the network with black hole attack.

4.8 Summary

This chapter has discussed the black hole attack in detail. Firstly, it gave a general overview of the attack, discussing the different types of this attack and explaining how it affects the operation of the network. The black hole in the network can deprive

traffic from the source node and disrupt communication. The chapter continued to give illustrations of how the black hole attack caused by RREP and black hole attack caused by RREQ can occur in AODV and DSR networks. Since the black hole node in the network always responds positively with a RREP message even though it does not have a valid route to destination, there are several methods that have been previously proposed to eliminate this behaviour, and the chapter lastly discussed previous work related to this study and some of the mitigation techniques that were tested using AODV protocol. Implementation and simulation environment are presented in the next chapter.

5 Implementation and Simulation Environment

5.1 Introduction

This study evaluated the black hole attack impact on performance of MANET using AODV and DSR protocols. It further compared the performance of AODV and DSR under black hole attack. The solutions that have been previously proposed to combat effects of black hole attack, which were tested using the base protocol AODV, were studied and the study tries to determine the solution that performs better than others. This is achieved by using network simulator version 2 (NS-2) to simulate MANET scenarios that include black hole node (Fall & Varadhan, 2005).

It can be very expensive to carry out a networking research by setting up an actual network with several computers and routers. Network simulators save a lot of money and time in accomplishing network research goals that is why a simulator-based approach has been chosen for this study. The disadvantage of simulation is that some factors have to be estimated because it is not possible to accurately duplicate the whole world inside a computer model. Thus simulation over simplifies real network scenarios. There exists a variety of network simulation tools that are used in research, but NS-2 has been selected for this study because the protocols under study (AODV and DSR) have already been implemented in NS-2. Also NS-2 is distributed freely and is an open source environment which allows the creation of new protocols, and modification of existing ones, so it is possible to introduce a black hole attack in NS-2 by modifying its source code. Moreover, NS-2 is well documented and user online support is provided (Pan & Jain, 2008).

This chapter explains NS-2 and the implementation of the research study on NS-2 simulation tool stipulating in detail the parameters used in the simulation and outlining the changes made to the NS-2 source code to introduce black hole attack.

5.2 Network Simulator - 2 (NS-2)

NS-2 is an object-oriented discrete event driven network simulator which was originally developed at University of California-Berkely. This means that NS-2 starts packet sending at time specified and stops at time specified. It implements a variety of protocols such as TCP and UDP, traffic source behaviour such as FTP, Telnet and CBR, queue management mechanisms such as Drop tail and routing algorithms (Chung & Claypool, 2002).

NS-2 can be used to simulate both local area networks and wide area networks. Since it is designed specifically for research in communications networks, new protocols, mobility models, amendments to existing protocols are regularly contributed by various research communities and it is due to its modularity and extensibility that it has gained popularity in research studies (Issariyakul & Hossain, 2012).

NS-2 uses two programming languages; C++ and OTcl (Tcl script language with object-oriented extensions). C++ is used for the backend that runs the actual simulation, whereas OTcl is used as a front-end (user interface). The reason for two languages is because of the structures of these languages; C++ can be used proficiently to design and implement a network, but it does not have a visual and graphical representation. On the other hand, OTcl is graphical and descriptive and can therefore be easily used to revise and alter different parameters.

Since OTcl is an interpreted language, changes to its code do not require compilation. On the other hand, C++ needs compilation after changes to the source code for linking and producing an executable file. Therefore, OTcl is much quicker to change but takes longer to run as interpretations have to be performed during run time. However, C++ runs very quickly during runtime but takes longer to change since compilation is required. Thus, with advantages of both languages, NS-2 reaps the benefits offered by C++ and OTcl.

For efficiency, the route for control data and the route for the actual traffic data are implemented separately in NS-2. C++ is used to write and compile the event scheduler and the basic network objects. The OTcl script is used to start the event

scheduler which guides the source node as to when to begin and end traffic data transmission, and to setup network topology (Chung & Claypool, 2002).

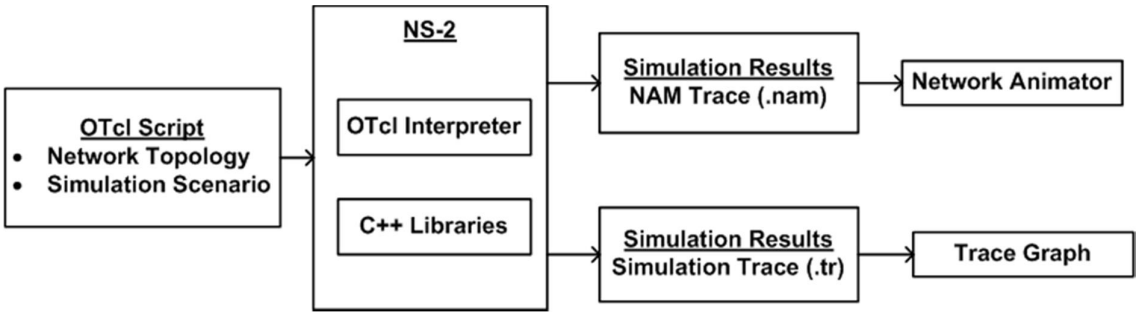


Figure 5.1: NS-2 Schema (Chung & Claypool, 2002)

As shown in Figure 5.1, the user writes an OTcl script and NS-2 interprets the script. From the interpretation, two analysis reports are created at the same time. The reports are created in the form of files by NS-2. One of the reports is a NAM (Network Animator) file that displays the graphical representation of the simulation. The other report is a trace file that shows all the actions of the objects in the simulation.

Trace file is a log of all events that occur during simulation. From trace file, further analysis can be performed with the help of tools such as PERL and AWK to extract events that are relevant to the result being investigated (e.g., end-to-end delay). NAM tool is essential as it provides a graphical representation of the events in the trace file to better conceptualize the series of events that occur during simulations. However, NAM does not support graphical representations for wireless simulations.

5.3 Implementation on NS-2

This section explains how simulation of black hole attack was achieved.

5.3.1 Simulation overview

The two routing protocols AODV and DSR were simulated under normal operation and in the presence of black hole using NS-2.35. The simulator scenarios aim to show the performance of AODV and DSR when there is no attack and in the presence of black hole attack, using different number of mobile nodes, different

speeds and different traffic load. Therefore two simulations were used for each protocol, in the first scenario, a black hole node was not included and in the second scenario, a black hole node was added.

A typical simulation with NS-2 basically consists of creating the input files as shown in Figure 5.2 below:

i. Scenario file that describes position and movement pattern of the nodes
ii. Communication file that describes connection and traffic in the network

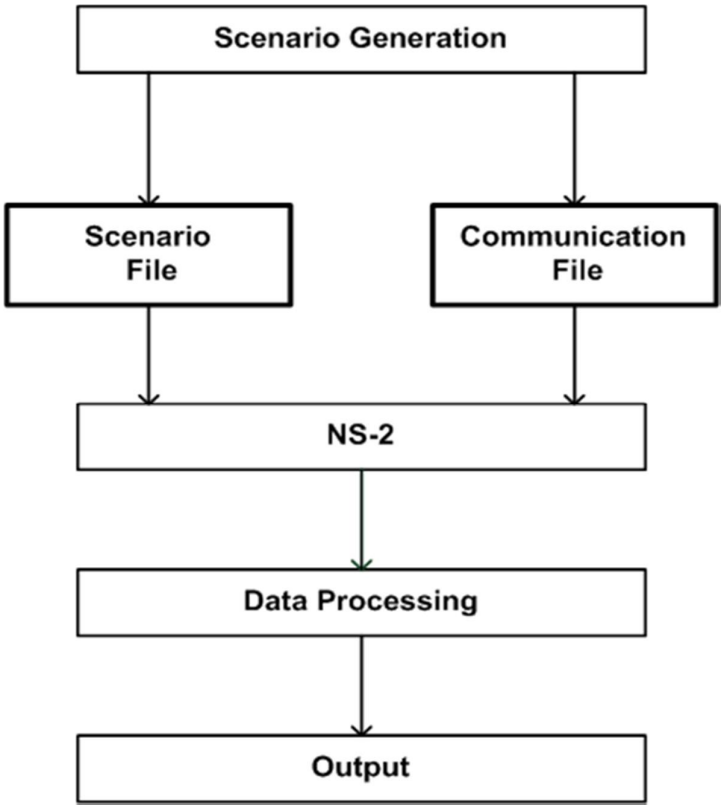


Figure 5.2: NS-2 Simulation Processes

The scenario file gives precise information about the movement of each node, the packets created by each node, and the time at which each change in movement or packet creation is to happen. Each run of simulation produces a detailed trace file that shows events happening during simulation such as number of packets delivered successfully, routes taken by packets, and extra information about internal operation of scripts executed. This data is further analysed with AWK file and Microsoft Excel to produce the graphs.

5.3.2 Simulation Parameters

The random way point model is used to create the mobility scenarios. Random way point model which utilises *'setdest'* utility. *'setdest'* is a third party application of NS found in the directory; *…/ns-2.35/indep-utils/cmu-scen-gen/setdest*. It randomly creates positions of the nodes in the network using the stated speed and pause time. Random way point mobility stipulates that after some time interval a node moves with a random speed towards a destination node that it selects randomly. The node pauses for a certain time at the destination, and randomly selects another destination. The node repeats this process till the end of simulation. The connection patterns are generated by *'cbrgen'* utility, the third party application of NS which is found in the directory; *…/ns-2.35/indep-utils/cmu-scen-gen/cbrgen.tcl*. The utility generates connections randomly chosen from nodes in the network.

In this study, the simulations are done on a square area of 670m X 670m. The total number of nodes ranges from 20 to 100 and the nodes move at the maximum speed ranging from 20m/s to 80m/s. The packets are transmitted at the rate of 4 packets/ sec. Each simulation instance lasts for 500 seconds. The model utilised as a wireless transmission channel at the physical layer is two ray ground propagation. The algorithm that is utilised at the data link layer is IEEE 802.11. AODV and DSR are used as a network layer routing protocols.

The transport layer protocol that is employed is User Datagram Protocol (UDP) and the generated data packets are constant bit rate (CBR). The size of the packets is 512 bytes. UDP protocol is used because it is connectionless so the source node does not notice when there is no connection between itself and the destination node. It continues to send the packets even when there is a malicious node discarding them. If Transmission Control Protocol (TCP) was used, the source node would stop sending the packets if it does not get acknowledgement packet from the destination node. Therefore, since UDP connection is not lost during simulation it is easy to accurately count the number of packets sent and received. If TCP protocol had been used, sent and received packets could not be counted because the source node closes the connection if it does not receive an acknowledgement packet from the destination after some time.

Figure 5.3 below shows a snapshot of the wireless node configuration parameters used.

```
set val(chan)           Channel/WirelessChannel     ;# channel Type
set val(prop)           Propagation/TwoRayGround    ;# radio-propagation model
set val(netif)          Phy/WirelessPhy             ;# network interface type
set val(mac)            Mac/802_11                  ;# MAC type
set val(ifq)            Queue/DropTail/PriQueue     ;# interface queue type
set val(ll)             LL                          ;# link layer type
set val(ant)            Antenna/OmniAntenna         ;# antenna model
set val(ifqlen)             50                      ;# max packet in ifq
set val(adhocRouting)   AODV, DSR                   ;# routing protocol
```

Figure 5.3: Wireless Node Configurations

For consistency, the same mobility model and connection pattern is used throughout the simulations.

5.3.3 Simulation of black hole attack

A malicious node is introduced to both AODV and DSR to implement a black hole by modifying NS-2 C++ source code as shown below. A malicious node attracts the packets and discards them.

5.3.3.1 AODV Modifications

i. *Declared malicious node variable in aodv.h file.*
   bool malicious;
ii. *Initialized the variable to false in aodv.cc constructor function to show that initially all nodes are not malicious.*
   malicious= false;
iii. In AODV.cc the following code was added to command function to detect which node is malicious.

```
if(strcmp(argv[1], "hacker") == 0) {
malicious = true;
return TCL_OK;
}
```

iv. In AODV.cc route handling function, the following code was added to maliciously drop packets.

```
// if I am malicious node
if (malicious == true) {
if (cmh->ptype() == PT_CBR) {
drop(packet, DROP_RTR_ROUTE_LOOP);
return;//Required if you get pkt flow not specified error.
```

```
// DROP_RTR_ROUTE_LOOP is added for no reason.
}
}
```

5.3.3.2 DSR Modifications

i. Declared malicious node variable in DSRagent.h file.
bool malicious;

ii. Initialized the variable to false in DSRagent.cc constructor function to show that initially all nodes are not malicious.
malicious= false;

iii. In DSRagent.cc the following code was added to command function to detect which node is malicious.

```
if(strcmp(argv[1], "hacker") == 0) {
malicious = true;
return TCL_OK;
}
```

iv. In DSRagent.cc handleFlowForwading function, the following code was added to maliciously drop packets.

```
// if I am malicious node
if (malicious == true) {
if (cmh->ptype() == PT_CBR) {
drop(packet, DROP_RTR_ROUTE_LOOP);
return;//Required if you get pkt flow not specified error.
// DROP_RTR_ROUTE_LOOP is added for no reason.
}
}
```

5.3.3.3 Recompiling NS-2

After modifying the existing NS2 algorithm to incorporate the black hole behaviour, NS-2 has to be recompiled by using the ñ**Make**ò command. There are three make files in the directory NS-2.35/ns-2.35; Makefile.vc, Makefile.in and Makefile, but modifications are made at the Makefile.in. The following commands have to be executed;

- ***make clean***
- ***make depend***
- ***make***

5.4 Evaluation of Simulation

Figure 5.4 and Figure 5.5 show snapshot captured by NAM during simulation. As it has already been explained in Section 5.2, NAM provides a graphical representation of the simulation. For clarity, the snapshot illustrates only a sample of seven mobile nodes in a network. The source node is denoted by an orange node 0, the destination node is denoted by a purple node 3, and the malicious node is represented by a red node 5. Figure 5.4 demonstrates a simulation in an environment with no attack, and the destination node receives data packets sent by the source. Figure 5.5 demonstrates a network environment with a black hole node absorbing data packets from the source node instead of forwarding them to the destination node.

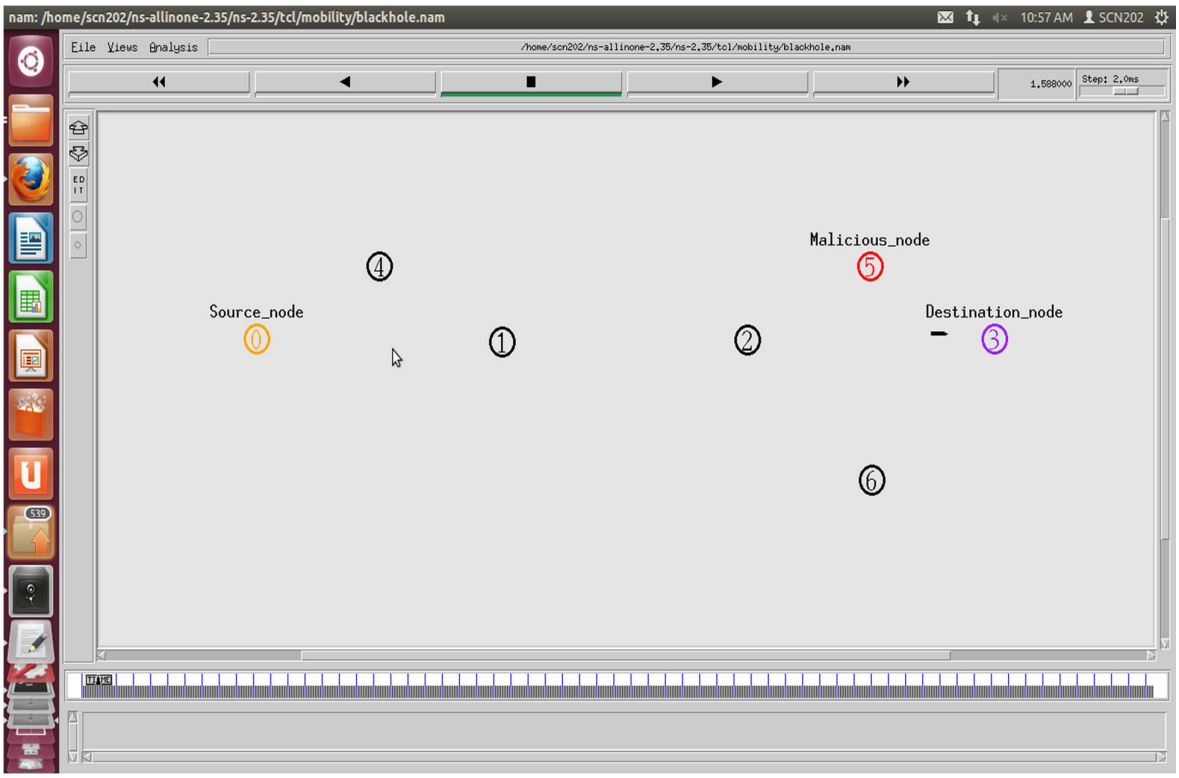


Figure 5.4: Connection between node 0 and node 3 correctly established

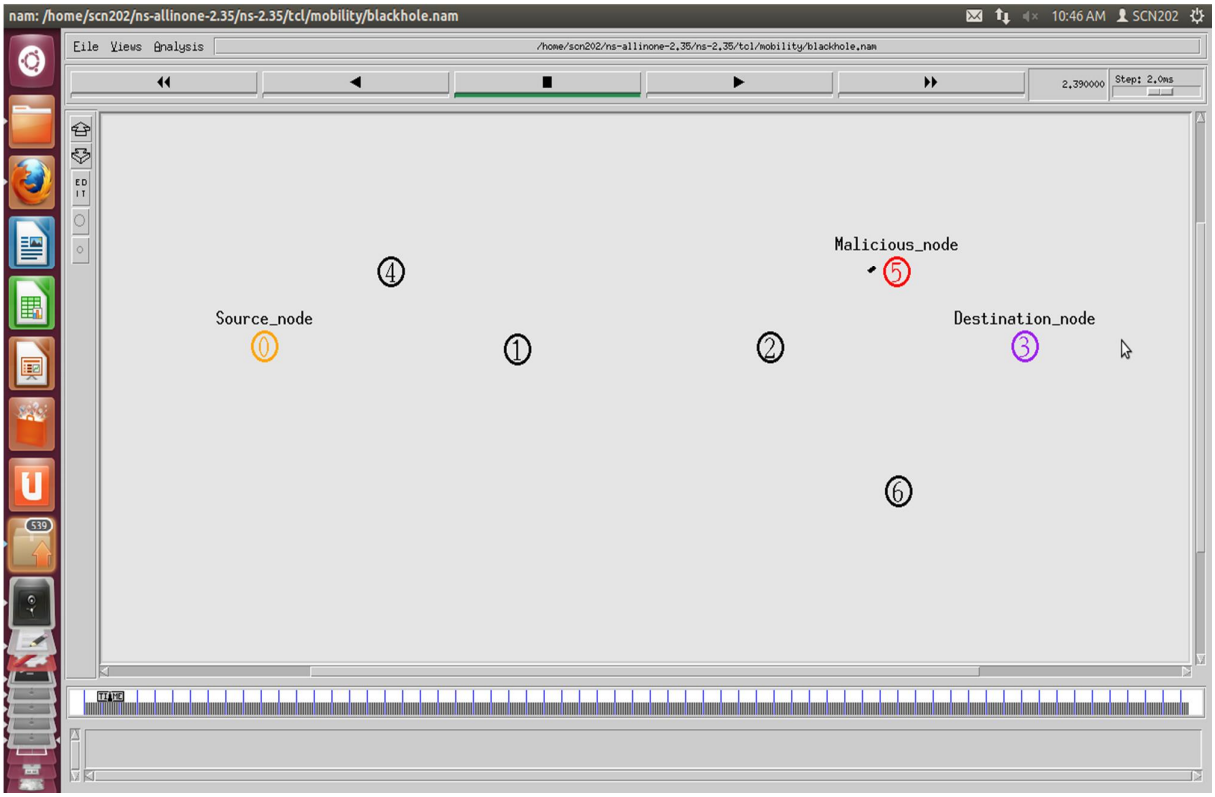


Figure 5.5: Node 5 (black hole) absorbs the packets

5.5 Summary

This chapter has discussed the implementation and simulation environment of the study. It first explained NS-2 simulation framework and highlighted its capabilities and why it is the mostly used tool for research. It further discussed the simulation parameters that were used on NS-2 to achieve the objectives of the research, also highlighting on the modifications that were done on the NS-2 AODV and DSR source code to introduce the black hole attack.

The next chapter presents the performance results and analysis of the results obtained from NS-2 simulations.

6 Simulation Results and Analysis

6.1 Introduction

The previous chapter has covered the implementation of the study on NS-2 and the simulation environment. This chapter presents evaluation of the results obtained from simulations. It begins by describing how results are obtained from NS-2 trace files; it then describes the performance metrics used to evaluate the routing protocols. The results are then presented and analysed based on the performance metrics. The chapter further gives a comparison of black hole attack solutions from literature study.

6.2 Examining the Trace Files

The simulation results are extracted from a trace file. A trace file is a report generated by NS that lists all the events that occur during simulations. It records the time when packet was sent, the sending node, the receiving node, the kind of packet sent, whether the packet was dropped and the reason for dropping. For simulations in this study, ñwireless traceò file format is used because MANETs are wireless networks. The sample of the new trace file is reflected in Appendix II.

The fields in the trace file are not all required to get results from the trace files, so filtering must be done to interpret trace files results. This can be tedious if it is done manually. Hence AWK scripting language has been used to process trace files. AWK is actually a programming language designed to process text files.

6.3 Performance Metrics

Various metrics can be used to analyse the performance of the routing protocols in a normal network environment and in a malicious environment. The performance of AODV and DSR in this study is measured based on throughput, packet delivery ratio and end-to-end delay.

6.3.1 Throughput

Throughput is the degree at which messages are transmitted successfully over a communication channel. It can also be described as the ratio of amount of data received from the sender to the total time consumed in transmitting the whole message to the destination. Normally throughput is measured using bits per second.

$$Throughput = \frac{\sum_{1}^{n} CBR_{recv}}{Simulation\ time} \quad \text{é é é é é é é é é é é é é é é é é é é é} \quad \textbf{(1)}$$

where CBR_{recv} represents number of constant bit rate packets received by destination node.

The main factors that affect throughput are bandwidth, limited energy, change in topology and untrusted communication.

6.3.2 Packet Delivery Ratio (PDR)

This is the ratio of the total number of data packets received at the destination to the total number of data packets sent at the source.

$$PDR\ \% = \frac{\sum_{1}^{n} \mathrm{CBR}_{\ recv}}{\sum_{1}^{n} CBR_{sent}} \times 100 \quad \text{é ...} \quad \textbf{(2)}$$

where;
PDR % represents percentage of packet delivery ratio.
CBR_{recv} represents number of constant bit rate packets received by destination node.
CBR_{sent} represents number of constant bit rate packets sent by source node.

6.3.3 End-to-end Delay

This is the average time taken from creating a packet at the source node until it is received at the destination node, and is expressed in seconds. The general network delay caused by buffer queues, routing activities, transmission times, etc. is included when calculating end-to-end delay. Different applications need different delay level, for instance voice and video transmissions require lesser delay and show little tolerance to delay level.

$$\text{Avg End\_to\_end Delay} = \frac{(CBR_{recvTime} - CBR_{sentTime})}{\sum_{1}^{n} CBR_{recvTime}} \quad \text{.é é .} \quad \textbf{(3)}$$

where;

Avg End_to_end Delay represents the average time delay taken for message to be transmitted from source to destination.

$CBR_{recvTime}$ represents time at which constant bit rate packet reaches the destination.

$CBR_{sentTime}$ represents time at which constant bit rate packet is sent by source node.

6.4 Simulation Results

The consequences of black hole attacks are shown by using graphs. The graphs are obtained from the output results of AWK scripts. The performance metrics explained in Section 6.2 are used to analyse the performance of AODV and DSR by changing the following parameters in the simulation:

i. Network Size: Variation in the number of mobile nodes.
ii. Mobility: Variation in the maximum speed.
iii. Network Traffic Load: Variation of the load offered to the network.

The graphs present a comparative analysis of the performance metrics of both AODV and DSR for different number of nodes, different mobility, and different traffic loads.

6.4.1 Effect of Network Size

The total number of mobile nodes participating in the network at each simulation instance was varied from 20 to 100. The speed at which the nodes move was maintained consistently at 20 m/s and a maximum of 10 connections was kept. Since the aim is to find the outcome caused by a change in network size, the only variable altered was the number of mobile nodes. The network size variations were done in both AODV based network and DSR based network. A black hole node was introduced in each network type. The graphs in this section plot throughput, packet delivery ratio, and end-to-end delay against the number of mobile nodes in the network.

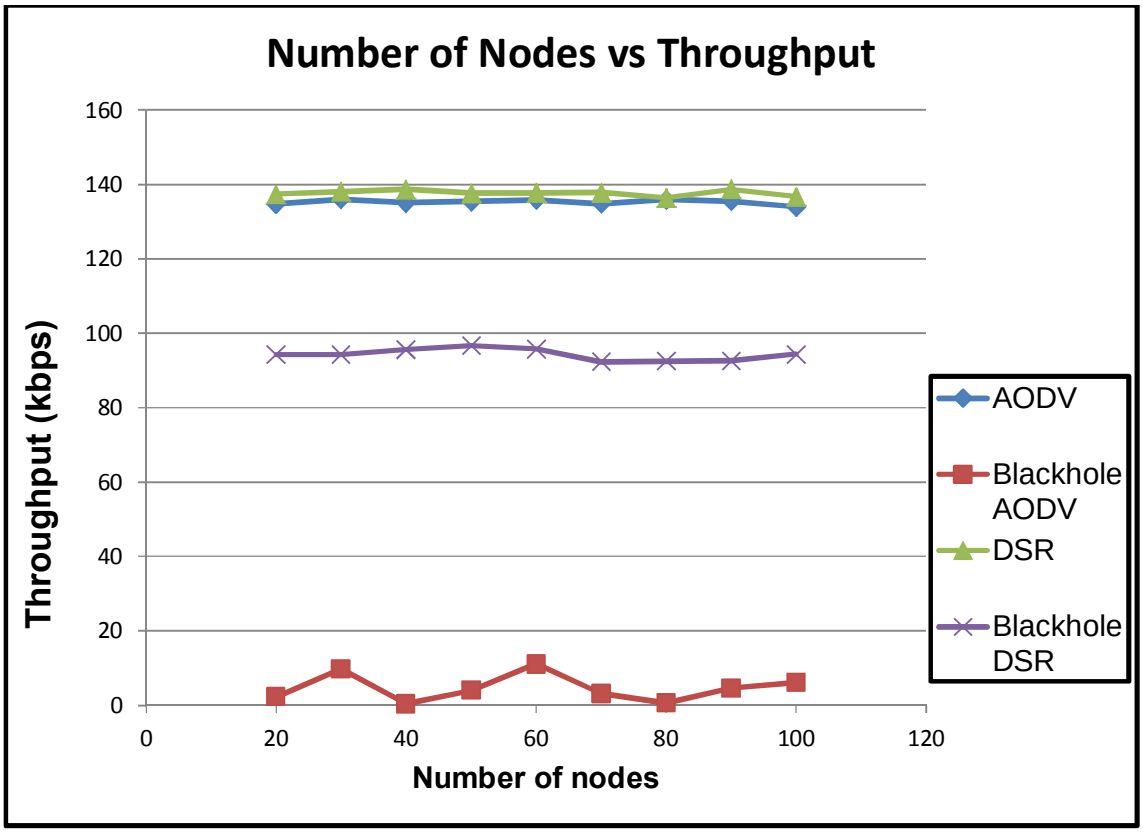


Figure 6.1: Throughput AODV vs. DSR

The simulation results of Figure 6.1 show that the rising number of mobile nodes does not cause a significant change in throughput. DSR's throughput is a little higher than AODV's throughput because DSR at all times searches for the most freshest and available route. Again, it is observed from the results that throughput for both

protocols decreases when the network is attacked by the black hole because some of the packets are absorbed by a malicious node so the total number of packets received at the destination is reduced. DSR under black hole attack performs better than AODV under black hole attack because of the source routing nature of DSR. It does not have to entirely depend on the routing table of intermediate nodes during the route discovery process.

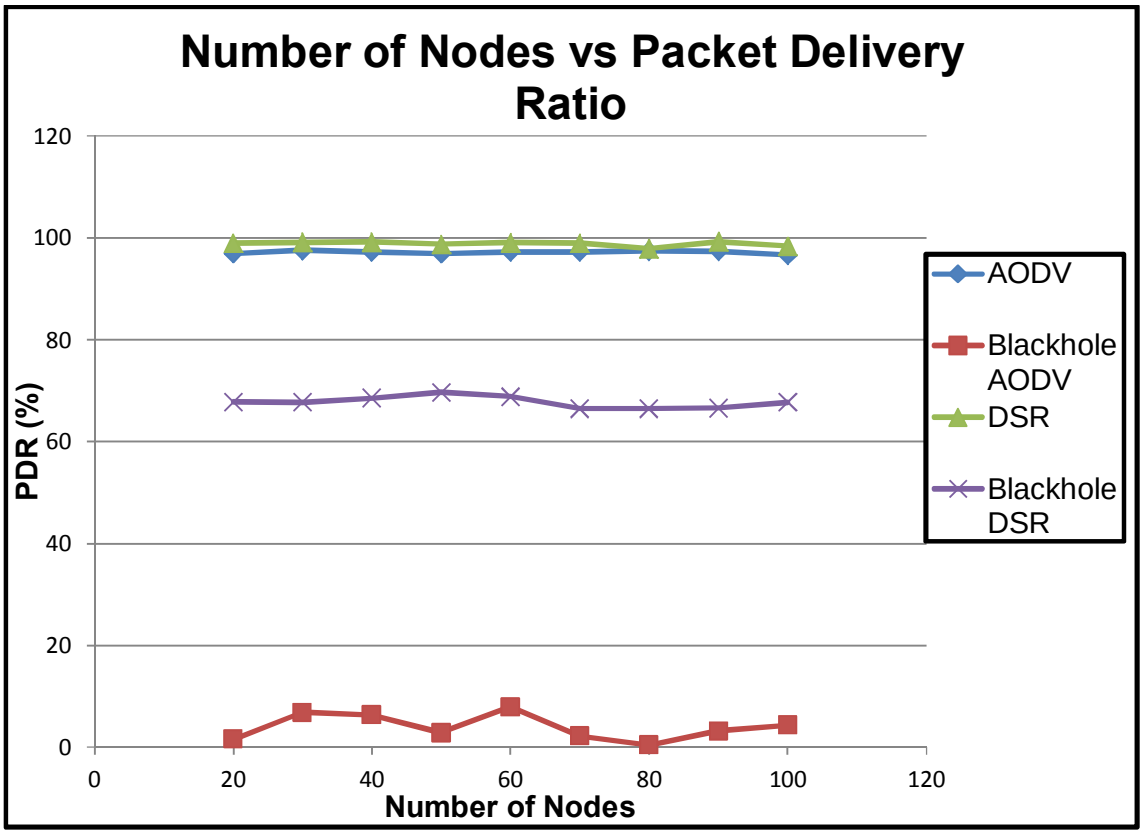


Figure 6.2: Packet Delivery Ratio AODV vs. DSR

The results of Figure 6.2 show that increasing the number of mobile nodes in the network does not bring significant change to packet delivery ratio for both AODV and DSR. The ratio remains approximately 100%. Also from the results, it is observed that packet delivery ratio for DSR is slightly higher than that of AODV.

This is because DSR works more efficiently when the size of the network is small, so the maximum number of nodes in all network scenarios in the study is 100. In the presence of black hole attack, packet delivery ratio is reduced. This is due to the fact that some packets are discarded by malicious node during the attack. DSR performs

better than AODV when the black hole attack is launched against the network. Packet delivery ratio of AODV reduces to a very low level in the presence of black hole attack.

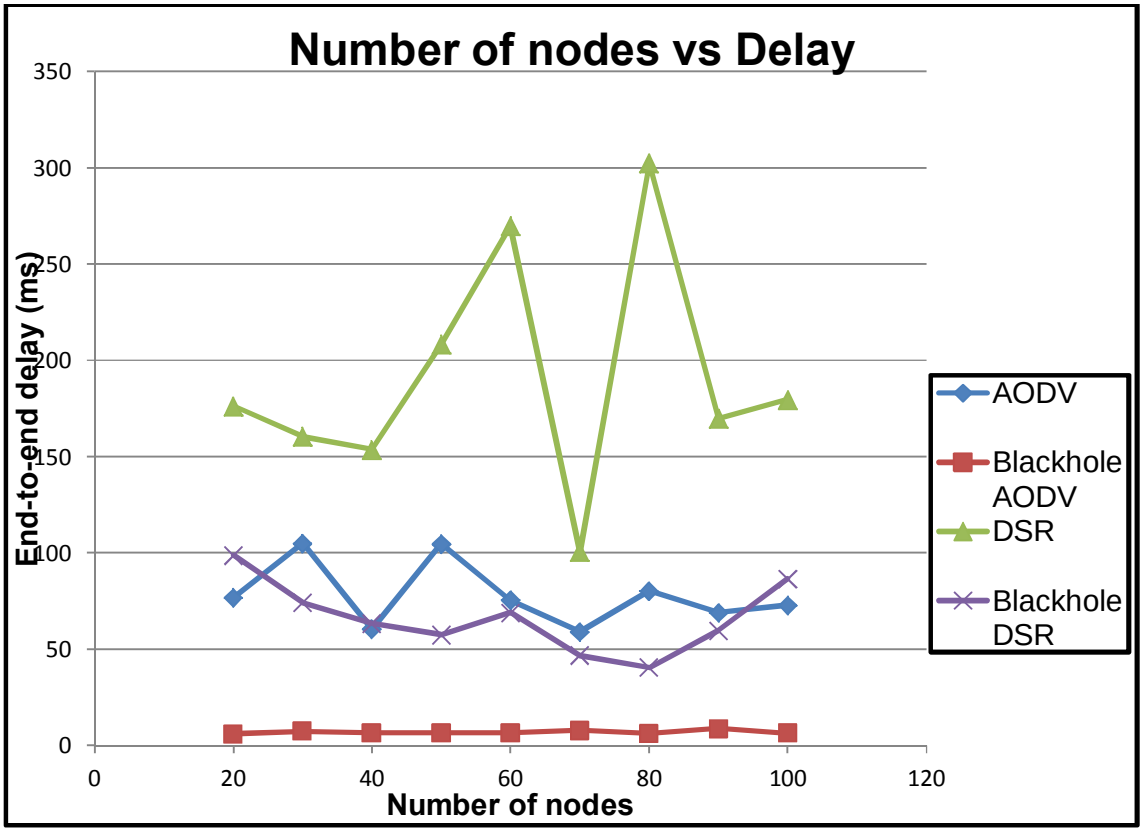


Figure 6.3: End-to-end Delay AODV vs. DSR

From Figure 6.3, it is observed that increasing the number of nodes in the network increases end-to-end delay. This is caused by the increasing number of neighbouring nodes. The simulation results also reveal that DSRôs delay is greater than AODVôs delay. This is because DSR is a source routing protocol, so the source node carries a large overhead because it keeps a complete record of route from source to destination, including the intermediate nodes, hence the high delay. Unlike DSR, AODV does not keep a complete route record. End-to-end delay decreases when there is a black hole attack because the malicious node does not have to search for the route in the routing table.

6.4.2 Effect of Mobility

The maximum speed was changed from 20 m/s to 80 m/s, keeping the total number of nodes constant at 20 nodes and maximum of 10 connections. The changes were done in both AODV and DSR. The black hole attack was launched in both AODV based network and DSR based network. The graphs in this section plot throughput, packet delivery ratio, and end-to-end delay against the increase in the mobility of the network.

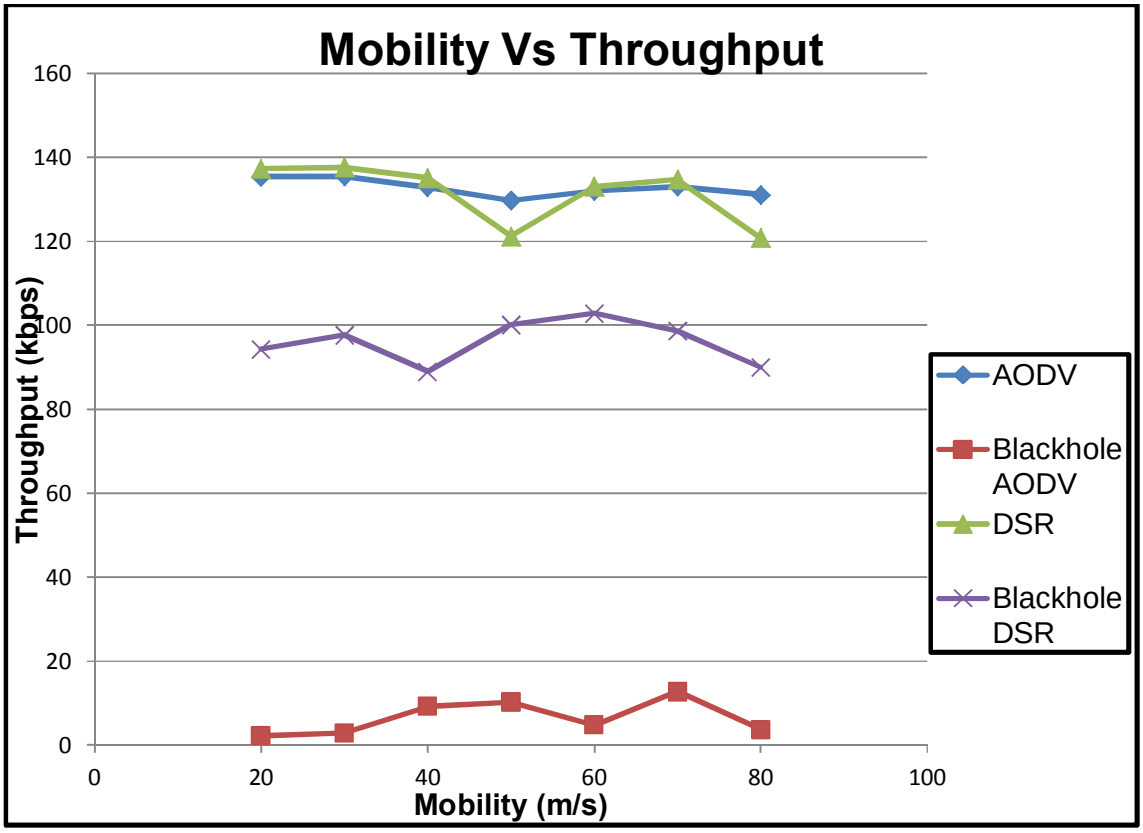


Figure 6.4: Throughput AODV vs. DSR

The simulation results of Figure 6.4 show that increasing the speed (mobility) of nodes in the network does not bring significant change in throughput. For both protocols, throughput decreases slightly. This is caused by the rapid change of positions of the nodes, which may cause the path to the destination to change while some packets have been transmitted from the source node using the old route. Therefore the transmitted packets get lost on the way. Throughput of the network under black hole attack decreases because of the packets discarded by the

malicious node. AODVôs throughput drops drastically compared to DSRôs throughput.

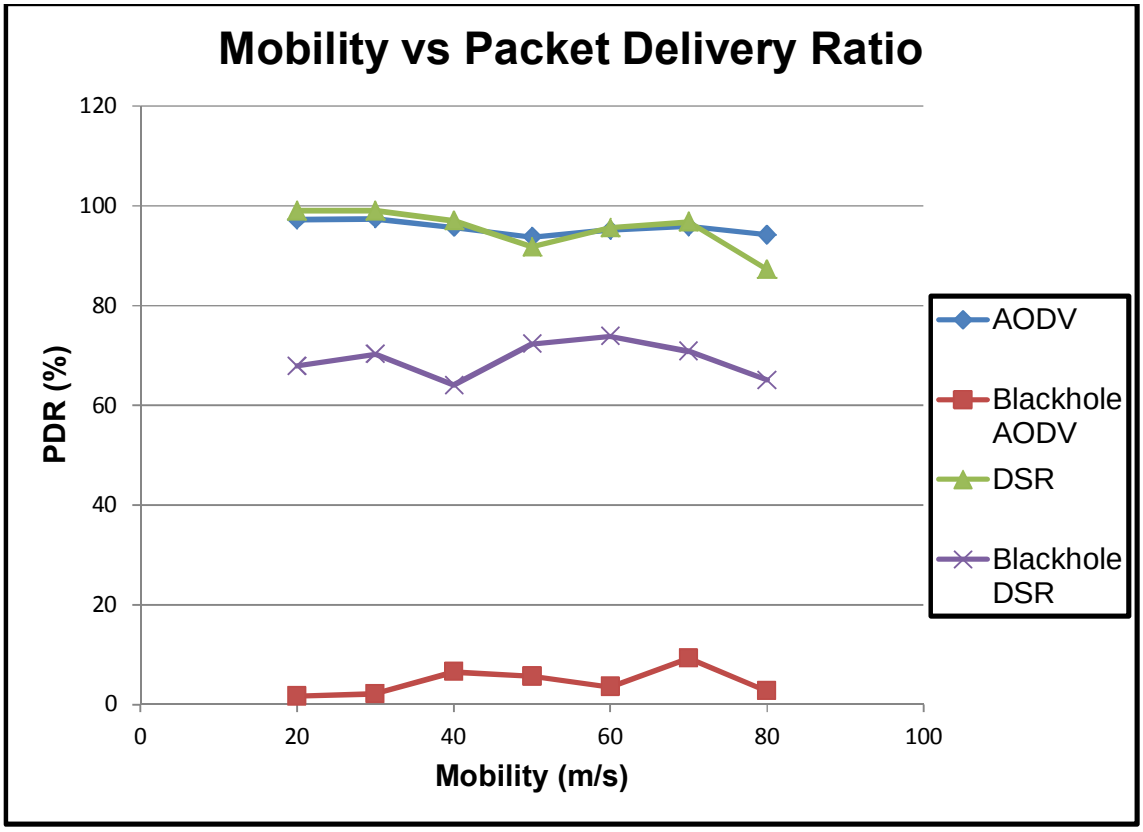


Figure 6.5: Packet Delivery Ratio AODV vs. DSR

When the mobility of the nodes is increased packet delivery ratio decreases slightly. This is because some of the packets may get lost along the way to the destination when the path from the source node to the destination node changes due to rapid change of intermediate nodesôpositions. The packet delivery ratio of AODV is very low compared to that of DSR when the black hole attack has been launched against the network.

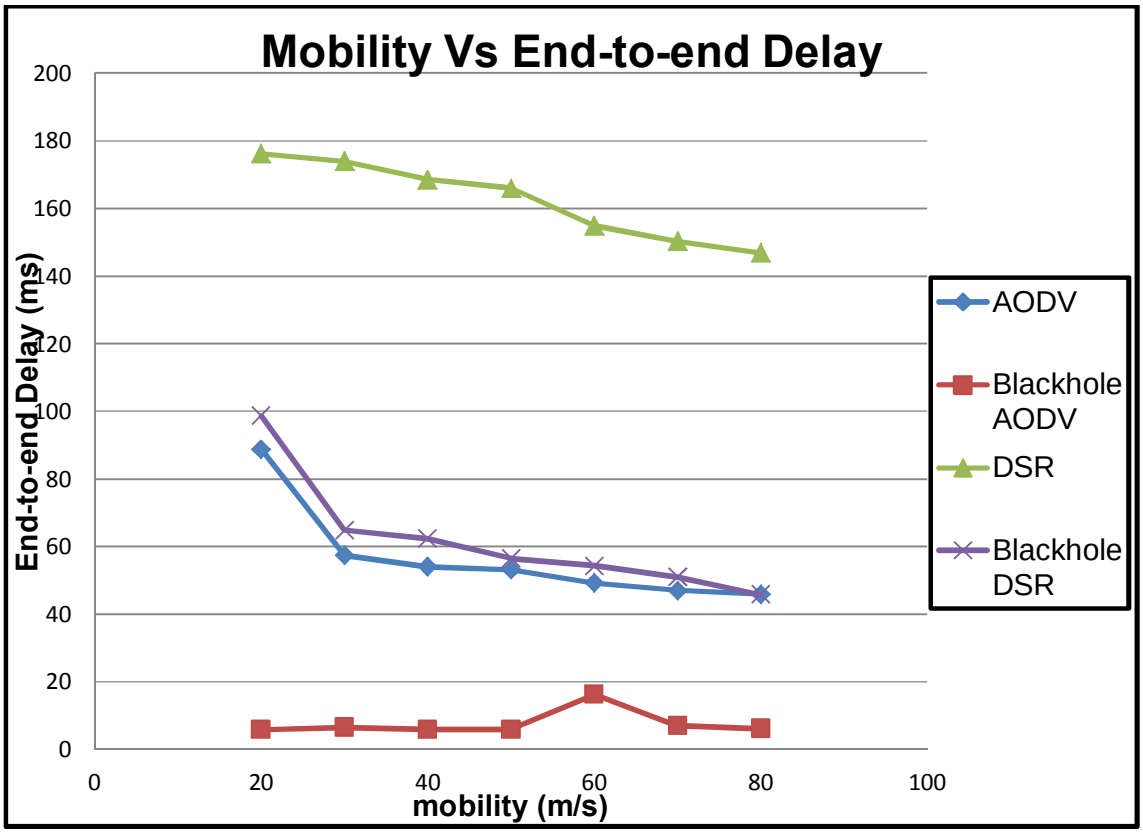


Figure 6.6: End-to-end Delay AODV vs. DSR

Figure 6.6 shows that end-to-end delay decreases with increase in speed because the nodes move more frequently, and the routing updates are exchanged more frequently. When there is a black hole attack, end-to-end delay gets even lower because the malicious node pretends to have a valid route to the destination without checking in the routing table, so the route discovery process takes a shorter time.

6.4.3 Effect of Network Traffic Load

The traffic connections between the nodes were varied from 2 to 6, keeping the total number of nodes constant at 20 nodes and maximum speed constant at 20 m/s. The simulations were done on AODV based network and DSR based network, and the black hole attack was launched to each network. The graphs in this section plot throughput, packet delivery ratio, and end-to-end delay against the increase in traffic load of the network.

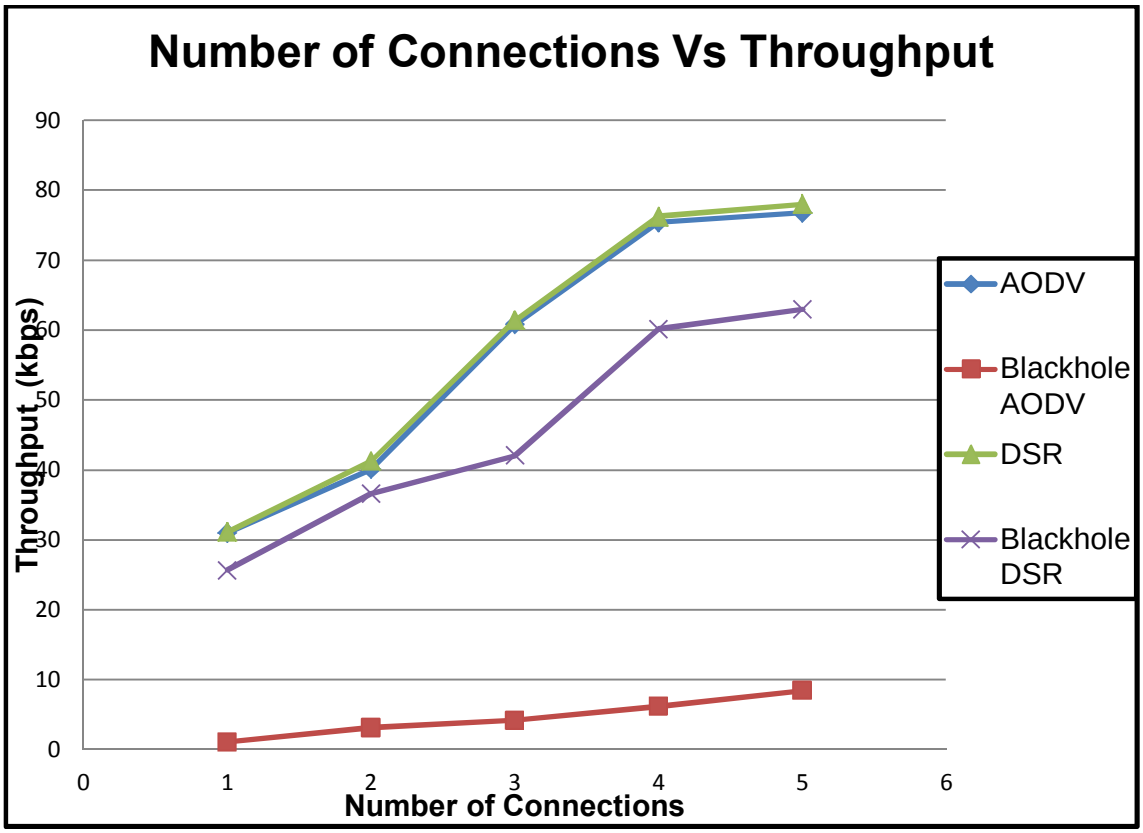


Figure 6.7: Throughput AODV vs. DSR

As traffic load increases, throughput for both protocols is increased because they are on demand protocols and establish routes only when needed, therefore increasing the load does not affect the good performance of the protocols. The performance degrades when the black hole attack is launched; this is because of the reduction in the number of packets that are received at the destination. The performance of AODV decreases more than that of DSR when there is an attack.

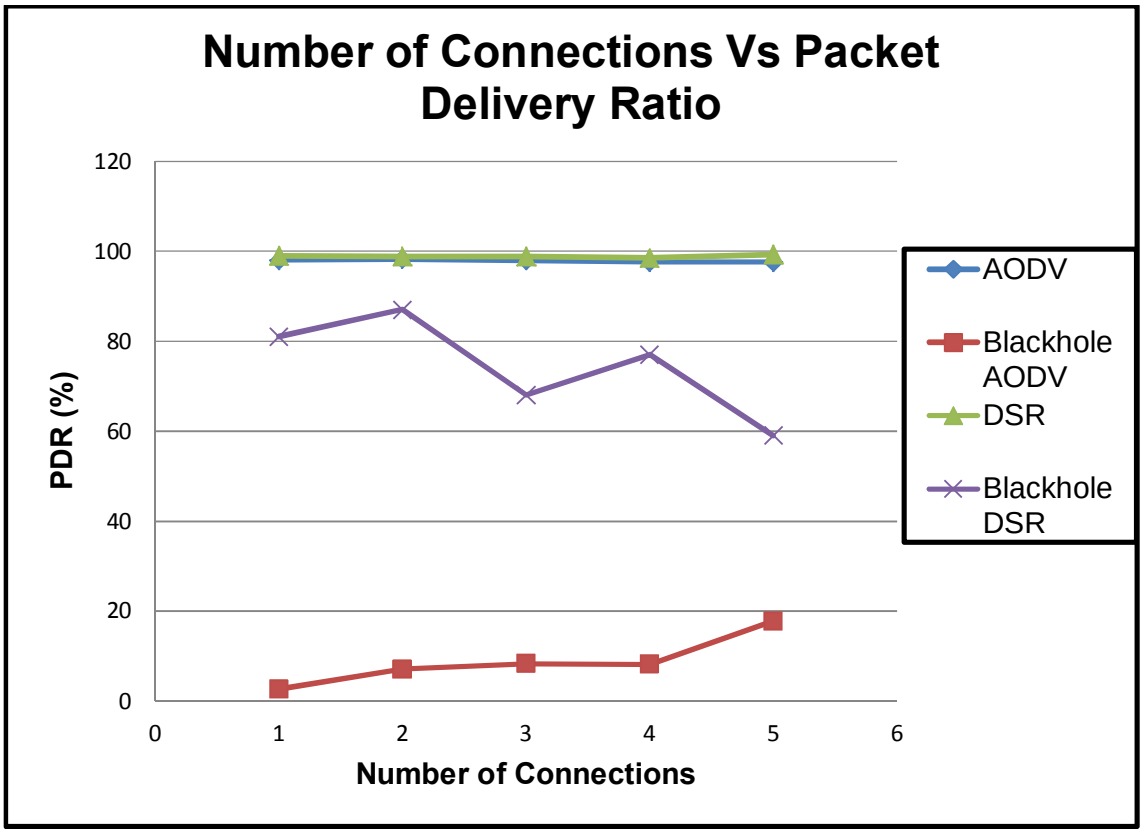


Figure 6.8: Packet Delivery Ratio AODV vs. DSR

Packet delivery ratio decreases slightly when the number of connections is increased. This is because as traffic increases, packets lost will also increase because the bandwidth requirements of the network are increased. When there is a black hole attack, the number of packets lost increases for both protocols; hence packet delivery ratio also decreases. The decrease is more drastic in AODV than in DSR.

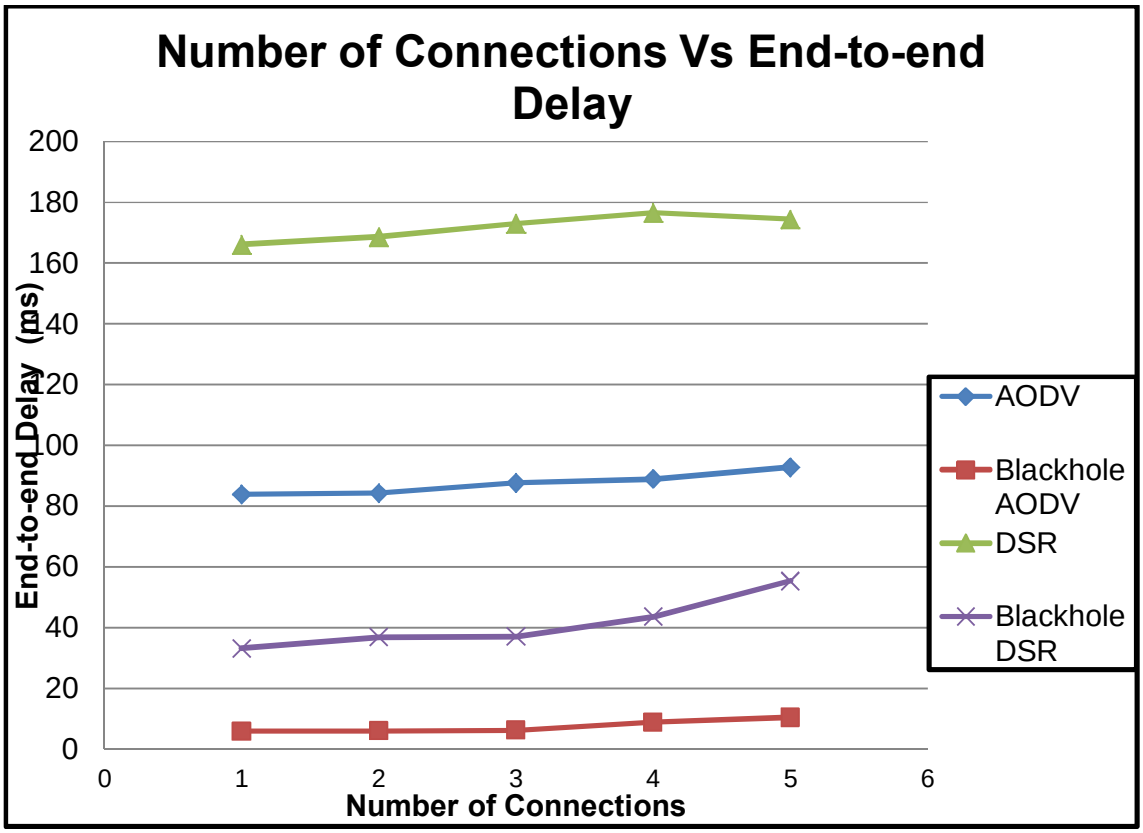


Figure 6.9: End-to-end Delay AODV vs. DSR

End-to-end delay is increased for both protocols as traffic load increases because the network gets overloaded and requires more bandwidth, so transmission rate is reduced. In the presence of a malicious node, end-to-end delay is reduced because the malicious node shortens the route discovery process time by responding with a positive RREP without looking for the route in the routing table.

6.5 Comparison of Black Hole Attack Mitigation Techniques

The following table compares the four mitigation techniques against black hole attack that have been discussed in Section 4.6, so that a conclusion can be drawn as to which technique best removes black hole attack in the network. Results in the table have been extracted from published papers proposing the discussed black hole attack solutions.

Table 2: Black hole attack solutions

Technique	Results	Impact on network
DPRAODV	PDR is improved by 80 to 85% than AODV under attack	▪ Increase in routing overhead ▪ Minimum increase in end-to-end delay
IDSAODV	PDR is improved by 73.26 % than AODV under attack	▪ No additional overhead ▪ No modification in packet format
EAODV	PDR is improved by 70 % than AODV under attack	▪ Offers no overhead
SAODV	PDR is improved by approximately 100% than AODV under attack (Effectively prevent black hole attack)	▪ Maintains high routing efficiency ▪ Brings burden of having to store RREP and verification confirm packet in each route discovery phase

Table 2 compares the four black hole attack solutions that have been previously proposed and tested in the literature. The comparison shows their efficiency in removing the black hole attack and the impact they bring to the network.

As far as efficiency to remove black hole attack is concerned, the solutions can be arranged as follows, in terms of preference from best to worst performance.

1. SAODV
2. DPRAODV
3. IDSAODV
4. EAODV

SAODV is considered the best because it is believed to effectively (å100%) prevent black hole attack.

When considering the solution that does not bring any negative impact to the network, the solutions can be arranged as follows, in preference order.

1. IDSAODV
2. EAODV
3. SAODV
4. DPRAODV

IDSAODV is considered the best because it brings no additional overhead. EAODV also does not bring any overhead, but its efficiency to remove black hole attack is lower than that of IDSAODV.

6.7 Summary

This chapter has provided results from simulations using NS-2 and results from literature study. The results have been presented by the use of graphs, comparing the performance of AODV and DSR both under normal operation and when the network is attacked by black hole. It further presented the analysis of the results and the analysis has been done based on throughput, packet delivery ratio and end-to-end delay as performance metrics. The comparison of the black hole mitigation techniques was also analysed.

From the results using the mentioned metrics, it has been observed that black hole attack deteriorates the performance of MANETs and it is also observed that AODV is more vulnerable to black hole attack than DSR. The next chapter gives the concluding remarks of the study and recommendations for future study.

7 Conclusion and Future Work

7.1 Concluding Remarks

MANETs are useful in situations where it is not possible to setup a network structure, but they are prone to many security attacks due to features like freedom of nodes to move and lack of infrastructure. It is therefore very crucial to provide security for these kinds of networks, and it is more challenging to secure the routing process. Black hole attack is an attack that aims to disrupt the routing process in MANETs. This study evaluated the effect of black hole attack on the overall performance of MANETS. In evaluating the effect of black hole attack on MANETs, the two popular reactive routing protocols, AODV and DSR were compared. The aim of comparing the protocols was to discover which protocol performs better when the network is attacked by black hole. The study also compared some of the mitigation techniques that have been proposed to eliminate black hole attack so that the best black hole solution can be discovered.

To attain the objectives of the study, NS-2 simulator was used to set up AODV and DSR networks. Firstly both protocols were simulated in a network that is not attacked, and then the protocols were simulated in a network where black hole attack has been launched. The performance metrics that were used to perform the evaluation are throughput, packet delivery ratio and end-to-end delay. To compare black hole attack solutions, the background literature of four mitigation techniques, DPRAODV, IDSAODV, EAODV, and SAODV was studied.

The observation derived from simulations is that when the network is attacked by a black hole, its performance degrades. This is revealed by the reduction in throughput, packet delivery ratio and end-to-end delay in the network that is under attack. The decrease in end-to-end delay might be considered to be an advantage, but it is only caused by the fact that during black hole attack, a malicious node does not search its routing table when it receives a RREQ, instead it pretends to have a fresh enough route to the destination and sends RREP.

A sample of mobile network with 50 nodes is considered to analyse the rate at which the performance metrics are affected by the black hole attack. In an AODV network, all the three performance metrics; throughput, packet delivery ratio and end-to-end delay are reduced by approximately 97% when the network is under black hole attack. In a DSR network, both throughput and packet delivery ratio are reduced by approximately 30% and end-to-end delay is reduced by 44%. This analysis is illustrated by Table 3 below.

Table 3: Impact of Black hole on network with 50 nodes

Performance Metrics	AODV (% Decrease)	DSR (% Decrease)
Throughput	97.0%	29%
Packet Delivery Ratio	97.1%	29.6%
End-to-end Delay	96.6%	44.0%

The above statistics leads to a conclusion that the effect of black hole attack in an AODV network is more pronounced than in a DSR network. Therefore, DSR is most suitable than AODV for networks that experience regular black hole attacks.

After studying and comparing the mitigation techniques, it can be concluded that SAODV removes black hole attack more effectively than other techniques though it brings the burden of extra storage to the network. This implies that when considering effectiveness of preventing black hole SAODV is the best solution. When considering the solution that does not disrupt the normal operation of the network, it can be concluded that IDSAODV is the best solution as it does not bring any additional overhead to the network. Even though many solutions have been proposed to combat the effects of black hole attack, it has been realised that all solutions have some drawbacks, and are not totally efficient.

7.2 Recommendations for Future Work

This study has analysed the black hole attack effect on AODV based MANET and DSR based MANET, there is need to analyse the impact of this attack using other MANET routing protocols in future, so that the best routing protocol for minimising impact of black hole attack may be determined.

Also, there are several attacks that can be launched against MANETs, but this study has only focused on black hole attack. It is important to conduct a research on other types of attacks such as; wormhole, gray hole, and byzantine and their impact be compared to black hole attacks impact. This will assist in classifying the attacks based on their level of impact on the performance of MANETs.

Random way point mobility model was used to generate scenarios in this study, but there are several other mobility models which can be used in future to study behaviour of routing protocols when different models are used. The performance metrics that have been used in this study are throughput, packet delivery ratio an end- to-end delay, other performance metrics can be used in future to determine how they are affected by the black hole attack.

Again only four black hole attack mitigation techniques were studied and compared in this study. There are several other techniques that have been proposed and tested which can also be included in the comparison so that the best of all the techniques can be derived. Furthermore, the security algorithm against black hole attack can be proposed and implemented as an improvement to the already existing algorithms.

7.3 Summary

This chapter briefly gave the background literature of the study. The aim of the study was then described by giving the objectives. The chapter further described how the study was carried out to meet the objectives. The observations derived from the results were presented and the chapter stipulated the conclusions based on the results. Lastly, the recommendations for future research were outlined.

8 References

ABDELHAQ, M., HASSAN, R., ISMAIL, M., ALSAQOUR, R. and ISRAF, D., 2011. Detecting sleep deprivation attack over manet using a danger theory-based algorithm. *International Journal of New Computer Architectures and their Applications (IJNCAA),* **1**(3), pp. 534-541.

ABOLHASAN, M., WYSOCKI, T. and DUTKIEWICZ, E., 2004. A review of routing protocols for mobile ad hoc networks. *Ad hoc networks,* **2**(1), pp. 1-22.

AGRAWAL, R., TRIPATHI, R. and TIWARI, S., 2011. Performance Evaluation and Comparison of AODV and DSR Under Adversarial Environment, *Computational Intelligence and Communication Networks (CICN), 2011 International Conference on* 2011, IEEE, pp. 596-600.

AHMAD, Z., JALIL, K.A. and MANAN, J., 2011. Black hole effect mitigation method in AODV routing protocol, *Information Assurance and Security (IAS), 2011 7th International Conference on* 2011, IEEE, pp. 151-155.

ALANI, M.M., 2014. MANET security: A survey, *Control System, Computing and Engineering (ICCSCE), 2014 IEEE International Conference on* 2014, IEEE, pp. 559-564.

AL-OMARI, S.A.K. and SUMARI, P., 2010. An overview of mobile ad hoc networks for the existing protocols and applications. *J GRAPH-HOC* **2**(1), pp. 87-110.

BALA, A., BANSAL, M. and SINGH, J., 2009. Performance analysis of MANET under blackhole attack, *Networks and Communications, 2009. NETCOM'09. First International Conference on* 2009, IEEE, pp. 141-145.

BORREGO, M., DOUGLAS, E.P. and AMELINK, C.T., 2009. Quantitative, qualitative, and mixed research methods in engineering education. *Journal of Engineering Education,* **98**(1), pp. 53-66.

CHUNG, J. and CLAYPOOL, M., 2002. NS by Example. [Online] http://web.uettaxila.edu.pk/CMS/SeISOPNbsSp09/tutorial%5CNSbyExamples.pdf. Accessed on 27 July 2015.

DADHANIA, P. and PATEL, S., 2013. Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks. *IJERA,* **3**(1), pp. 1487-1491.

DE OLIVEIRA SCHMIDT, R. and TRENTIN, M.A.S., 2008. Manets routing protocols evaluation in a scenario with high mobility manet routing protocols performance and behavior, *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE* 2008, IEEE, pp. 883-886.

DOKURER, S., ERT, Y. and ACAR, C.E., 2007. Performance analysis of ad-hoc networks under black hole attacks, *SoutheastCon, 2007. Proceedings. IEEE* 2007, IEEE, pp. 148-153.

EL-MOUSA, A. and SUYYAGH, A., 2010. Ad Hoc networks security challenges, *Systems Signals and Devices (SSD), 2010 7th International Multi-Conference on* 2010, IEEE, pp. 1-6.

FALL, K. and VARADHAN, K., 2005. The ns Manual (formerly ns Notes and Documentation). *The VINT project,* [Online] http://web.cs.sunyit.edu/~ nelsond/WebPage/HPC/docs/ns_tutorial-doc.pdf . Accessed on 27 July 2015.

FERRO, E. and POTORTI, F., 2005. Bluetooth and Wi-Fi wireless protocols: a survey and a comparison. *Wireless Communications, IEEE,* **12**(1), pp. 12-26.

GARG, N. and MAHAPATRA, R., 2009. MANET Security issues. *International Journal of Computer Science and Network Security,* **9**(8), pp. 241.

GILL, M.A.K. and KUNWAR, Y., 2014. Performance Analysis and Comparison of MANET Routing Protocols under Black Hole Attack. *International Journal of Emerging Trends in Science and Technology,* **1**(07), pp. 1029-1035.

GIRUKA, V.C. and SINGHAL, M., 2007. Secure Routing in Wireless Ad-Hoc Networks. *Wireless Network Security,* pp. 137-158.

GOYAL, P., PARMAR, V. and RISHI, R., 2011. Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management,* **11**, pp. 32-37.

ISSARIYAKUL, T. and HOSSAIN, E., 2012. *An introduction to network simulator NS2.* 2nd Ed. London: Springer.

JACQUET, P., MUHLETHALER, P., CLAUSEN, T., LAOUITI, A., QAYYUM, A. and VIENNOT, L., 2001. Optimized link state routing protocol for ad hoc networks, *Multi Topic Conference, 2001. IEEE INMIC 2001. Technology for the 21st Century. Proceedings. IEEE International* 2001, IEEE, pp. 62-68.

JAWANDHIYA, P.M., GHONGE, M.M., ALI, M. and DESHPANDE, J., 2010. A survey of mobile ad hoc network attacks. *International Journal of Engineering Science and Technology,* **2**(9), pp. 4063-4071.

JHAVERI, R.H., PATEL, A.D., PARMAR, J.D. and SHAH, B.I., 2010. MANET Routing Protocols and Wormhole Attack against AODV. *IJCSNS International Journal of Computer Science and Network Security,* **10**(4), pp. 12-18.

JOHNSON, D.B. and MALTZ, D.A., 1996. Dynamic source routing in ad hoc wireless networks. *Mobile computing, Springer* , pp. 153-181.

JOHNSORT, D., 1994. Routing in ad hoc networks of mobile hosts, *Mobile Computing Systems and Applications, 1994. WMCSA 1994. First Workshop on* 1994, IEEE, pp. 158-163.

KANNHAVONG, B., NAKAYAMA, H., NEMOTO, Y., KATO, N. and JAMALIPOUR, A., 2007. A survey of routing attacks in mobile ad hoc networks. *Wireless Communications, IEEE,* **14**(5), pp. 85-91.

KANTHE, A.M., SIMUNIC, D. and PRASAD, R., 2012. Effects of malicious attacks in mobile ad-hoc networks. *Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on* 2012, IEEE, pp. 1-5.

KUMAR, M. and RISHI, R., 2010. Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review. *International Journal of Computer Applications IJCA,* **12**(2), pp. 24-28.

KUPPUSAMY, P., THIRUNAVUKKARASU, K. and KALAAVATHI, B., 2011. A study and comparison of OLSR, AODV and TORA routing protocols in ad hoc networks, *Electronics Computer Technology (ICECT), 2011 3rd International Conference on* 2011, IEEE, pp. 143-147.

LEE, J., SU, Y. and SHEN, C., 2007. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi, *Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE* 2007, IEEE, pp. 46-51.

LI, W. and JOSHI, A., 2008. Security issues in mobile ad hoc networks - a survey. [Online] http://www.researchgate.net/profile/Wenjia_Li3/publication/266280897_Security_Issues_in_Mobile_Ad_Hoc_Networks_A_Survey/links/54db80ef0cf2ba88a69029e9.pdf. Accessed on 27 July 2015

LU, S., LI, L., LAM, K. and JIA, L., 2009. SAODV: a MANET routing protocol that can withstand black hole attack, *Computational Intelligence and Security, 2009. CIS'09. International Conference on* 2009, IEEE, pp. 421-425.

MBARUSHIMANA, C. and SHAHRABI, A., 2007. Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks, *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on* 2007, IEEE, pp. 679-684.

MEDADIAN, M., MEBADI, A. and SHAHRI, E., 2009. Combat with Black Hole attack in AODV routing protocol, *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on* 2009, IEEE, pp. 530-535.

MISHRA, R., SHARMA, S. and AGRAWAL, R., 2010. Vulnerabilities and security for ad-hoc networks, *Networking and Information Technology (ICNIT), 2010 International Conference on* 2010, IEEE, pp. 192-196.

MLADENOVIĹ, D. and JOVANOVIĹ, D., 2012. Mobile ad hoc networks security, 2012 OTEH *5th International Conference on Defensive Technologies Belgrade,* pp.1-7.

MOHEBI, A., KAMAL, E. and SCOTT, S., 2013. Simulation and Analysis of AODV and DSR Routing Protocol under Black Hole Attack. *International Journal of Modern Education and Computer Science (IJMECS),* **5**(10), pp. 19.

OSATHANUNKUL, K. and ZHANG, N., 2011. A countermeasure to black hole attacks in mobile ad hoc networks, *Networking, Sensing and Control (ICNSC), 2011 IEEE International Conference on* 2011, IEEE, pp. 508-513.

PAN, J. and JAIN, R., 2008. A survey of network simulation tools: Current status and future developments. [Online] http://www1.cse.wustl.edu/~jain/cse567-08/ftp/simtools.pdf, Accessed on 27July 2015.

PATEL, M. and SHARMA, S., 2013. Detection of malicious attack in MANET: a behavioural approach, *Advance Computing Conference (IACC), 2013 IEEE 3rd International* 2013, IEEE, pp. 388-393.

PAVANI, K. and AVULA, D., 2012. Performance evaluation of mobile ad hoc network under black hole attack, *Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012), International Conference on* 2012, IET, pp. 1-6.

PERKINS, C.E. and BHAGWAT, P., 1994. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. *ACM SIGCOMM Computer Communication Review,* **24**(4), pp. 234-244.

PERKINS, C.E. and ROYER, E.M., 1999. Ad-hoc on-demand distance vector routing, *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on* 1999, IEEE, pp. 90-100.

PERVAIZ, M.O., CARDEI, M. and WU, J., 2010. Routing security in ad hoc wireless networks. *Network Security,* Springer, pp. 117-142.

PUROHIT, N., SINHA, R. and MAURYA, K., 2011. Simulation study of Black hole and Jellyfish attack on MANET using NS3, *Engineering (NUiCONE), 2011 Nirma University International Conference on* 2011, IEEE, pp. 1-5.

RAI, A.K., TEWARI, R.R. and UPADHYAY, S.K., 2010. Different types of attacks on integrated MANET-Internet communication. *International Journal of Computer Science and Security,* **4**(3), pp. 265-274.

RAJ P.N. and SWADAS, P.B., 2009. DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET. IJCSI **2**, pp. 54-59.

RAJABHUSHANAM, C. and KATHIRVEL, A., 2011. Survey of wireless MANET application in battlefield operations. (*IJACSA) International Journal of Advanced Computer Science and Applications,* **2**(1), pp. 50-58.

RAJESH, Y and ANIL K.S., 2012. Secure AODV protocol to mitigate black hole attack in mobile ad hoc networks. *ICCNT, 2012, IEEE*, pp 1-4.

ROYER, E.M. and TOH, C.K., 1999. A review of current routing protocols for ad hoc mobile wireless networks. *Personal Communications, IEEE,* **6**(2), pp. 46-55.

SAINI, A. and KUMAR, H., 2010. Comparison between Various Black Hole Detection Techniques in MANET, *National Conference on Computational Instrumentation* 2010, pp. 157-161.

SHARMA, N. and SHARMA, A., 2012. The Black-hole node attack in MANET, *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on* 2012, IEEE, pp. 546-550.

SINGH, H. and SINGH, M., 2013. Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs. *International Journal of Advanced Trends in Computer Science and Engineering,* **2**(3), pp. 43-46.

SINGH, P.K. and SHARMA, G., 2012. An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET. *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* 2012, IEEE, pp. 902-906.

SINGH, U.K., KAILASHPHULERIA, S.S. and GOSWAMI, D., 2014. An analysis of Security Attacks Found in Mobile Ad-hoc Network. *International Journal of Scientific & Engineering Research,* **5**(5),pp. 1586-1592.

SIVAKAMI, R. and NAWAZ, G.K., 2015. Defending Against Security Breaches of Byzantine Attacks in Manets. ARPN Journal of Engineering and Applied Sciences, **10** (8), pp. 3667-3672.

STOJANOVIC, M., ACIMOVIC-RASPOPOVIC, V. and TIMCENKO, V., 2012. The Impact of Mobility Patterns on MANET Vulnerability to DDoSAttacks. Electronics and Electrical Engineering, **3**(119), pp. 1392 ï 1215.

SUN, B., GUAN, Y., CHEN, J. and POOCH, U.W., 2003. Detecting black-hole attack in mobile ad hoc networks, *Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492)* 2003, IET, pp. 490-495.

SURYAWANSHI, R. and TAMHANKAR, S., 2012. Performance Analysis and Minimization of Blackhole Attack in MANET. *IJERA,* **2**(4), pp. 1430-1437.

THACHIL, F. and SHET, K., 2012. A trust based approach for AODV protocol to mitigate black hole attack in MANET, *Computing Sciences (ICCS), 2012 International Conference on* 2012, IEEE, pp. 281-285.

THAKARE, A.N. and JOSHI, M., 2010. Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks. *IJCA Special issue on "Mobile Adhoc Networks", MANETs,* pp. 211-218.

TSENG, F., CHOU, L. and CHAO, H., 2011. A survey of black hole attacks in wireless mobile ad hoc networks. *Human-centric Computing and Information Sciences,* **1**(1), pp. 1-16.

VANI, A. and RAO, D.S., 2011. Removal of black hole attack in ad hoc wireless networks to provide confidentiality security service. *International Journal of Engineering Science,* **3**(6), pp. 2377-2384.

WEERASINGHE, H. and FU, H., 2007. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation, *Future generation communication and networking (fgcn 2007)* 2007, IEEE, pp. 362-367.

WU, B., CHEN, J., WU, J. and CARDEI, M., 2007. A survey of attacks and countermeasures in mobile ad hoc networks. *Wireless Network Security.* Springer*,* pp. 103-135.

YAN, Z., 2002.Security in ad hoc networks. [Online] http://skirubame.ucoz.com/ld/0/48_Security_in_Adh.pdf. Accessed on 27 July 2015

ZAIBA, I., 2011. Security issues, challenges and solution in MANET. IJCST, **2**(4), pp. 108-109-112.

ZAPATA, M.G. and ASOKAN, N., 2002. Securing ad hoc routing protocols, *Proceedings of the 1st ACM workshop on Wireless security* 2002, ACM, pp. 1-10.

ZHANG, X., SEKIYA, Y. and WAKAHARA, Y., 2009. Proposal of a method to detect black hole attack in MANET, *Autonomous Decentralized Systems, 2009. ISADS'09. International Symposium on* 2009, IEEE, pp. 1-6.

ZHOU, H., 2003. A survey on routing protocols in MANETs. *Department of Computer Science and Engineering, Michigan State University, East Lansing, MI,* pp. 48824-41027.

ZHOU, J., CHEN, J. and HU, H., 2007. SRSN: Secure routing based on sequence number for MANETs, *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on* 2007, IEEE, pp. 1569-1572.

9 Appendices

Appendix I: TCL Simulation Script

Below is a TCL script for simulating wireless network with 20 mobile nodes.

```
# MANETAODV.tcl
#===================================================================
# Define options
#===================================================================
set val(chan)           Channel/WirelessChannel
set val(prop)           Propagation/TwoRayGround
set val(netif)          Phy/WirelessPhy
set val(mac)            Mac/802_11
set val(ifq)            Queue/DropTail/PriQueue
set val(ll)             LL
set val(ant)            Antenna/OmniAntenna
set val(x)                  670   ;# X dimension of the topography
set val(y)                  670   ;# Y dimension of the topography
set val(ifqlen)             50    ;# max packet in ifq
set val(seed)               0.0
set val(adhocRouting)       AODV
set val(nn)                 20    ;# how many nodes are simulated
set val(cp)                 "../mobility/scene/Connections"
set val(sc)                 "../mobility/scene/scen-20-test"
set val(stop)               500.0   ;# simulation time

#===================================================================
# Main Program
#===================================================================
# Initialize Global Variables
# create simulator instance
set ns_          [new Simulator]
$ns_ use-scheduler Heap

# setup topography object
set topo   [new Topography]

# create trace object for ns and nam
set tracefd     [open wireless1-out.tr w]
set namtrace    [open wireless1-out.nam w]
$ns_ trace-all $tracefd
$ns_ namtrace-all-wireless $namtrace $val(x) $val(y)

# define topology
$topo load_flatgrid $val(x) $val(y)

# Create God
set god_ [create-god $val(nn)]

# define how node should be created
#global node setting

$ns_ node-config -adhocRouting $val(adhocRouting) \
```

```
                -llType $val(ll) \
                -macType $val(mac) \
                -ifqType $val(ifq) \
                -ifqLen $val(ifqlen) \
                -antType $val(ant) \
                -propType $val(prop) \
                -phyType $val(netif) \
                -channelType $val(chan) \
            -topoInstance $topo \
            -agentTrace ON \
                -routerTrace OFF \
                -macTrace OFF

# Configure physical layer
#create nodes receiving range 250m, carrier sensing range
#500m
#Phy/WirelessPhy set CPThresh_ 10.0
#Phy/WirelessPhy set CSThresh_ 9.21756e-11 ;#550m
#Phy/WirelessPhy set RXThresh_ 4.4613e-10 ;#250m

# Create the specified number of nodes [$val(nn)] and "attach" them
to the channel.

for {set i 0} {$i < $val(nn) } {incr i} {
     set node_($i) [$ns_ node]
     $node_($i) random-motion 0       ;# disable random motion
}

# Define node movement model
puts "Loading connection pattern..."
source $val(cp)

# Define traffic model
puts "Loading scenario file..."
source $val(sc)

# Define node initial position in nam
for {set i 0} {$i < $val(nn)} {incr i} {

# 20 defines the node size in nam
# the function must be called after mobility model is defined
        $ns_ initial_node_pos $node_($i) 20
}

#Adding a malicious node
$ns_ at 0.0 "[$node_(5) set ragent_] hacker"
#$ns_ at 0.0 "[$node_(23) set ragent_] hacker"

# Tell nodes when the simulation ends
proc finish {} {
    global ns_ tracefile namfile
    $ns flush-trace
    close $tracefile
    close $namfile
    exec nam blackhole.nam &
```

```
    exit 0
}
for {set i 0} {$i < $val(nn) } {incr i} {
    $ns_ at $val(stop).0 "$node_($i) reset";
}
$ns_ at $val(stop) "$ns_ nam-end-wireless $val(stop)"
$ns_ at  $val(stop).0002 "puts \"NS EXITING...\" ; $ns_ halt"

puts $tracefd "M 0.0 nn $val(nn) x $val(x) y $val(y) rp
$val(adhocRouting)"
puts $tracefd "M 0.0 sc $val(sc) cp $val(cp) seed $val(seed)"
puts $tracefd "M 0.0 prop $val(prop) ant $val(ant)"

puts "Starting Simulation..."
#$defaultRNG seed  0
$ns_ run
```

Appendix II: Sample of New Trace File

```
r 1.019151540 _3_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] -------
[6:255 -1:255 27 0] [0x2 4 1 [3 0] [0 4]] (REQUEST)
r 1.019151540 _2_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] -------
[6:255 -1:255 27 0] [0x2 4 1 [3 0] [0 4]] (REQUEST)
r 1.019151571 _5_ RTR  --- 0 AODV 48 [0 ffffffff 6 800] -------
[6:255 -1:255 27 0] [0x2 4 1 [3 0] [0 4]] (REQUEST)
r 1.023470126 _1_ RTR  --- 0 AODV 44 [13a 1 2 800] ------- [5:255
0:255 29 1] [0x4 2 [3 4] 10.000000] (REPLY)
f 1.023470126 _1_ RTR  --- 0 AODV 44 [13a 1 2 800] ------- [5:255
0:255 28 0] [0x4 3 [3 4] 10.000000] (REPLY)
r 1.029001792 _0_ RTR  --- 0 AODV 44 [13a 0 1 800] ------- [5:255
0:255 28 0] [0x4 3 [3 4] 10.000000] (REPLY)
s 1.029001792 _0_ RTR  --- 0 cbr 1020 [0 0 0 0] ------- [0:0 3:0 30
1] [0] 0 0
r 1.038747793 _1_ RTR  --- 0 cbr 1020 [13a 1 0 800] ------- [0:0 3:0
30 1] [0] 1 0
f 1.038747793 _1_ RTR  --- 0 cbr 1020 [13a 1 0 800] ------- [0:0 3:0
29 2] [0] 1 0
r 1.048633793 _2_ RTR  --- 0 cbr 1020 [13a 2 1 800] ------- [0:0 3:0
29 2] [0] 2 0
f 1.048633793 _2_ RTR  --- 0 cbr 1020 [13a 2 1 800] ------- [0:0 3:0
28 5] [0] 2 0
r 1.058398920 _5_ RTR  --- 0 cbr 1020 [13a 5 2 800] ------- [0:0 3:0
28 5] [0] 3 0
D 1.058398920 _5_ RTR LOOP 0 cbr 1020 [13a 5 2 800] ------- [0:0 3:0
27 5] [0] 3 0
s 1.080000000 _0_ AGT  --- 1 cbr 1000 [0 0 0 0] ------- [0:0 3:0 32
0] [1] 0 0
r 1.080000000 _0_ RTR  --- 1  cbr 1000 [0 0 0 0] ------- [0:0 3:0 32
0] [1] 0 0
s 1.080000000 _0_ RTR  --- 1 cbr 1020 [0 0 0 0] ------- [0:0 3:0 30
1] [1] 0 0
r 1.089602000 _1_ RTR  --- 1 cbr 1020 [13a 1 0 800] ------- [0:0 3:0
30 1] [1] 1 0
```

Appendix III: Accompanying CD-ROM

- **Dissertation Soft Copy**
  - The soft copy of the dissertation is located in the dissertation folder.
- **Software**
  - The source code that is used for implementation is located in the software folder and the NS-2 files that have been modified to implement the black hole attack are found in the following directories.

    ~software/nsallinone-2.35/ns2.35/Aodv/Aodv.cc
    ~ software/nsallinone-2.35/ns2.35/Aodv/Aodv.h
    ~ software/nsallinone-2.35/ns2.35/dsr/dsr.cc
    ~ software/nsallinone-2.35/ns2.35/dsr/dsr.h
- **Simulation Scripts**
  - The TCL scripts and AWK scripts that have been used in simulations are stored in the simulations scripts folder. In ns-2.35 software, these scripts have been located in the directory below.

    ~software/nsallinone-2.35/ns2.35/tcl/mobility/
- **Simulation Manual**
  - The manual that explains how the simulation scripts are run to get the results is located in the manual folder.
- **Results**
  - All Microsoft Excel files displaying the results that are used in the results and analysis of the dissertation are stored in the results folder.